2025

confiance-numerique.fr

Observatory of Digital Trust Sector

ACN

ACN

Alliance pour la confiance numérique

Observatory of Digital TrustSector

2025

finished printing in May 2025

SUMMARY

ACN
Alliance pour la confiance numérique

A WORD FROM ACN ALLIANCE FOR DIGITAL TRUST

Daniel Le Coguic
ACN Chairman

On the occasion of the publication of this 11th edition of the ACN Observatory, it is essential that we take a moment to reflect together on the future of our digital trust industry. This reference document, with all its data, is an essential strategic compass for understanding the role of our industry in today's world.

The current economic and geopolitical context presents us with considerable challenges, but it also offers us unique opportunities to defend our values and strengthen our sovereignty. The world is going through a period of heightened tension. Armed conflicts, including on European soil, trade wars and the use of tariffs as diplomatic tools, the balkanisation of cyberspace and the exponential growth of the digital footprint in society are all signs of a rapidly changing world. These geopolitical upheavals and digital changes have a direct impact on our economy and our ability to project ourselves into the future. However, these challenges should not discourage us. On the contrary, they should encourage us to redouble our efforts to transform this situation into a lever of opportunity for our industry and for our country.

Digital trust is an essential pillar of modern society. It has become a highly political issue, central to the strategic thinking of our businesses, our institutions and our citizens. The need to reduce our dependence, to strengthen our digital sovereignty and our strategic autonomy is more obvious than ever. The companies in our industry, whether they specialise in digital identity, cybersecurity, blockchain, trusted infrastructures or trusted AI, have a crucial role to play in meeting these challenges.

In each of these areas, we are experiencing major changes. Digital identity, which is the cornerstone of trust in the digital world, will soon see a major acceleration under the impetus of the implementation of the European Union's digital identity portfolio project.

In terms of cybersecurity, the French 'Resilience' bill, which transposes the European REC, NIS2 and DORA texts in particular, will also be central to strengthening our collective security and resilience, which is essential in view of the explosion in threats

“ Digital trust is an essential element of modern society. ”

that we are seeing on a daily basis. The industry is working hand in hand with the public authorities, as well as with members of parliament and local authorities, to ensure that this founding piece of legislation not only achieves its objectives, but also enables us to capitalise strongly on excellent French and European solutions. Indeed, while the primary objective of the bill is the general resilience of the nation, it is imperative that this goes hand in hand with strengthening our industry and our strategic autonomy by putting in place a truly ambitious industrial policy, enabling us to reduce our dependence on digital tools from outside Europe and take back control of our digital future.

Finally, artificial intelligence is playing an increasingly central role in the challenges of digital confidence. The French government made no mistake about this and organised the AI Summit in February, placing France at the heart of global debates in this field. The increased understanding of the need for digital sovereignty and the spotlight on this issue are encouraging us to work together to create common legal, technical and ethical guidelines. A code of conduct for the industry is currently being drawn up and will shortly be made public. The development of our Observatory, which in this 2025 edition now fully includes trusted AI in its segmentation, reflects this need for better observation, measurement and understanding of developments in this field.

The effectiveness of our actions depends on good coordination and the elimination of redundancies. The merger between ACN and Alliance Blockchain France, which took place at the beginning of the year, is a concrete example of this, and has enabled us to create a more coherent scope of action, activate numerous synergies and make our actions more audible and understandable.

It is essential that we continue to streamline our actions and make them easier to understand within the digital trust ecosystem. While respecting the DNA of each structure, it is up to us to create a unified institutional representation. This type of rapprochement is a strong signal of the maturity of our ecosystem. This move is coupled with the establishment of exchange gateways with our European partners: following on from the partnership set up by ACN with its German counterparts last year, several other similar initiatives are currently being finalized with other EU partners.

In 2025, we need to regain control over the course of events, geostrategically and socially.

The challenges are many, but optimism is the order of the day. This year will undoubtedly be a pivotal one for digital confidence. More than ever, we need to build our future together, and turn uncertainties into opportunities for France and Europe. The French digital trust industry must be the spearhead of our technological sovereignty and strategic independence.

“ Necessity of reducing our dependencies, strengthening our digital sovereignty and our strategic autonomy is more evident than ever. ”

A WORD FROM THE MINISTER

Clara CHAPPAZ

Minister for Artificial Intelligence and the Digital Economy

At a time when global power relations are being reshaped by heightened geopolitical tensions, artificial intelligence is emerging as a major disruptive technology. While it offers unrivalled potential for transformation, it is also a source of considerable challenges. The government has fully grasped the importance of this technological revolution in strengthening our digital sovereignty, improving public action and better protecting our fellow citizens.

AI is much more than technical progress: it is redefining our uses, our professions and our skills. AI is much more than technical progress: it is redefining our uses, our professions and our skills. And it's doing so at an unprecedented speed. The irruption of generative AI into our daily lives illustrates this acceleration: in the space of a few months, it has turned our reference points upside down. It is therefore essential for the State to play its part in guiding, framing and channelling this revolution, so that it is aligned with our fundamental values.

This is the whole point of creating a full-fledged ministry dedicated to Digital and AI: to affirm that the State must be present where our future is being played out.

Since 2018, France has built a clear national artificial intelligence strategy, structured around four pillars: excellence in research, support for innovation, adoption in the real economy and the promotion of ethical and reliable AI. This strategy has been backed by over 3 billion euros of investment and is now bearing fruit: France has become the European leader in AI, with almost 2 billion euros raised by 2024 and over a thousand start-ups active in the field. Players such as Mistral, LightOn and Preligens are now promoting our expertise on a global scale.

The Summit for Action on AI, which we organized last February, helped to set this ambition in motion internationally. With the creation of the Coalition for Sustainable AI and the Foundation for an AI of general interest, we have launched a new phase in our national strategy, focusing on three key priorities:

- Accelerate the spread of AI.
- Strengthen our technological sovereignty.
- And prevent excesses linked to these technologies.

“ France has become the European leader in AI, with nearly 2 billion euros raised by 2024 and over a thousand start-ups active in the field ”

These are the priorities that shape my day-to-day work.

The first of these - the spread of AI - requires a collective increase in skills. AI must not remain the domain of experts alone. It must become a lever for innovation, productivity and simplification for all organizations. In the public sector, we are investing heavily alongside DINUM to develop concrete solutions such as the Albert program and the Alliance incubator, which are building the digital public services of tomorrow.

Our digital sovereignty is the other major challenge. Today, too much of our digital infrastructure depends on foreign players. This dependence exposes us to major risks. Sovereignty does not mean withdrawal: it means choice. We must be able to decide on our tools, our standards and our values. This means controlling our computing capacity, supporting our industry and providing massive training in digital skills.

Finally, this sovereignty would be incomplete without a genuine digital protection policy.
While AI is a formidable lever for innovation, it can also be a factor in abuses such as disinformation, digital violence and addiction. These risks, which primarily affect the very young, require us to act. The SREN law already provides solutions to better supervise platforms and protect minors. As for the Digital Resilience bill, it will reinforce cybersecurity requirements in all public services.

You know better than anyone: digital trust is not an option; it’s a prerequisite for success. It relies on a solid, committed and structured ecosystem. That’s what your industry represents, and I’d like to salute it here for its essential role in securing and ensuring the ethics of our digital transition.

More than ever, digital technology is a lever of sovereignty, and artificial intelligence is a social issue. Together, we must ensure that it is also a vector for shared progress. The State will be at your side to meet this challenge.

“ Today, too much of our digital infrastructure depends on foreign players, and this dependence exposes us to major risks. ”

- Main segments in digital trust in 2024
- Key figures 2024
- France growth comparison 2017- 2024
- Analysis by company size 2024
- Top players 2024

KEY FIGURES

Digital Trust is crucial in our economy and in our society in the midst of digital transformation. It includes **digital security** (digital identity, trusted electronic systems and subsystems), **cybersecurity** (products/software and services) as well as **Trustworthy AI**.

The *Alliance pour la Confiance Numérique* (ACN) was set up to bring together and support the players in this sector in France and to ensure its institutional representation.

The ACN has set up the **Observatory of Digital Trust** to gather and study data on the main characteristics and trends of this sector. It is within this framework that this study was carried out in 2025, covering the field of cybersecurity, digital security and Trustworthy AI.

Digital Trust in France in 2024 corresponds to:

- **€21.3 billion in revenue** i.e. 6.2% growth between 2023 and 2024,
- **€10 billion of added value,**
- **107,000 people employed** in the setcor,
- **53% of revenue** from **cyber security, 40%** from **digital security,** and 7% from **Trustworthy AI.**

French Digital Trust companies in the world in 2024 represent:

- **€33.5 billion in revenue** generated worldwide by the French Digital Trust industry (revenue in France, revenue exported from France and revenue generated abroad by companies owned by French shareholders).

- **World leaders** in digital security (Thales, Airbus D&S, Atos Eviden, ST Microelectronics), identity and access management (Thales, Idemia, IN Groupe, Docaposte), cybersecurity services (Thales, Atos Eviden, Orange Cyberdefense, Sopra Steria, Capgemini), and secure payments (Worldline).

- **€17 billion in international revenue,** i.e. 51% of total revenue (revenue exported from France and revenue generated abroad by companies owned by French capital).

- **€6.1 billion of revenue exported from France,** an average export rate of 29%.

Digital Trust is a thriving industry:

- **7% average annual growth** in France over the 2018-2024 period, compared to 0.8% for the French GDP* (*GDP growth measured by INSEE in chained volume).
- Digital Trust is the **French industrial sector that has experienced the strongest growth** over the past 10 years
- Digital Trust has shown itself to be particularly resilient in the face of the COVID crisis in 2020, with **3.6% growth in 2020** compared to -7.8% for the French GDP.
- Digital Trust is the **most productive sector,** i.e. with the highest ratio of added value to revenue.

€21.3 billion
in revenue in France

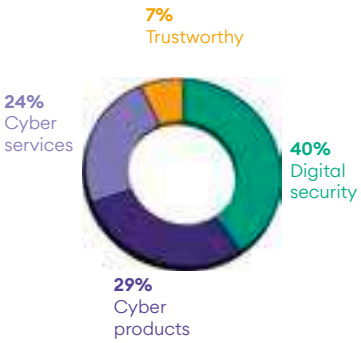
€33.5 billion
in revenue internationnaly

107,000 people employed

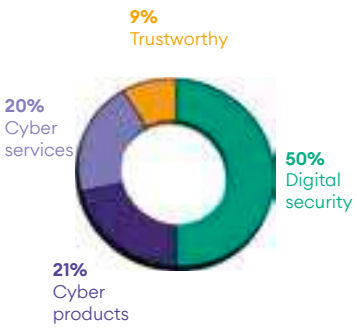
6,2% growth in France in 2024

Main segments in digital trust in 2024

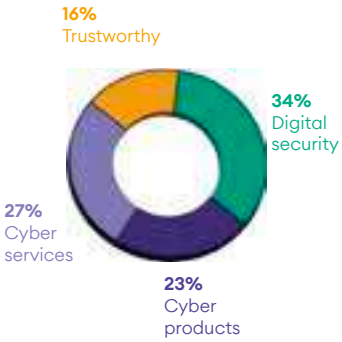
• Revenue



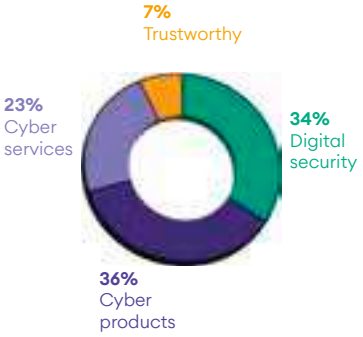
• Numbers of companies



• Workforce



• Added Value



2,499 companies
in the sector in France

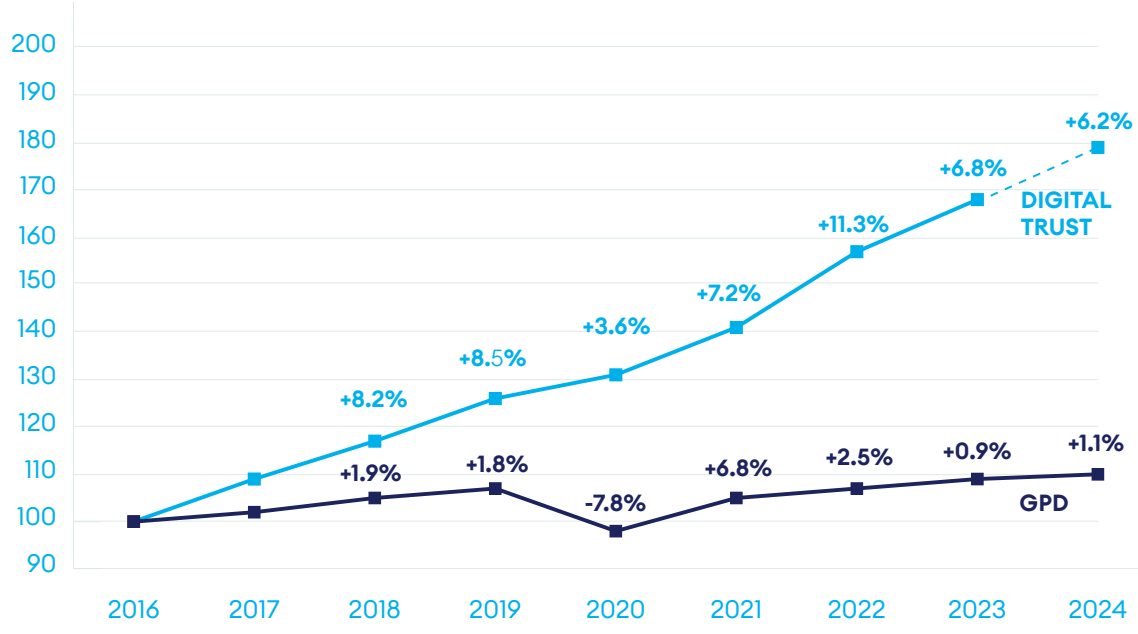
Digital Trust is an ecosystem of companies of all sizes :

- **75 are large enterprises,**
- **72 ISEs** (Intermediate-sized enterprises),
- **749 SMEs** (Small and Medium-sized Enterprises),
- **1,603 Micro-enterprises.**

Key figures 2024

Global revenue	**€33.5 B**
Revenue abroad	**€12.1 B**
Revenue France	**€21.3 B**
	expert revenue incl. **€6.1 B**
Added Value France	**€10 B**

France growth comparison 2017- 2024

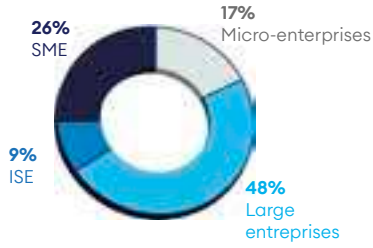


Index with base 2016

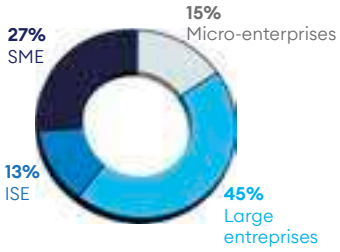
GDP growth measured by the INSEE, and IMF for 2024

This growth does not take into account growth in Trustworthy AI

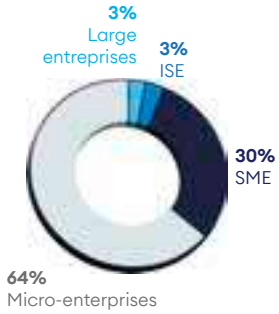
Analysis by company size 2024



Revenue

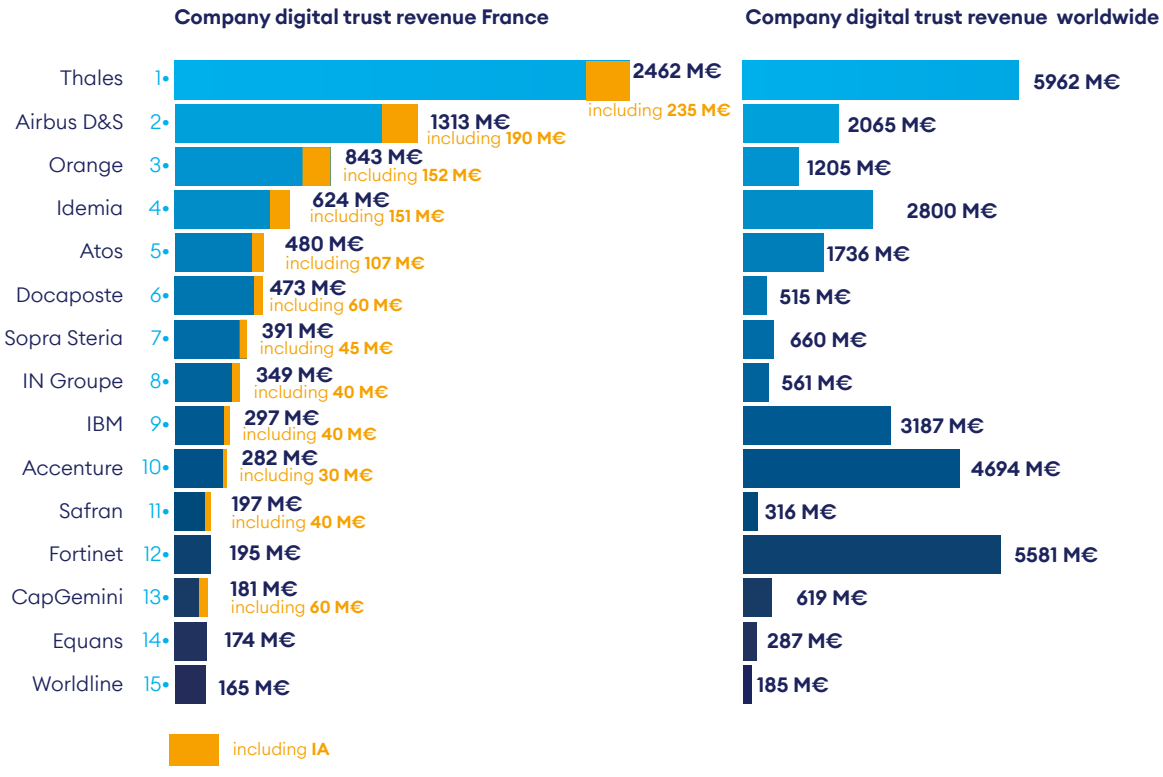


Workforce



Number of companies

Top 15 players France 2024



Note: The 2025 edition of the Observatory introduces an expanded scope of analysis with the inclusion of the Trustworthy AI segment. This structural change has led to an adjustment in the reported revenue figures for the companies concerned, affecting their ranking in the Top 15. Several groups have benefited from the integration of their Trustworthy AI activities, including Thales, Airbus, Orange, Atos, and Idemia. Additionally, certain data has been updated following the release of new financial statements from French offices, particularly for companies whose figures had not been available in previous editions, such as Orange Cyberdéfense. Finally, some Trustworthy AI activities have been reallocated from other existing segments. For all these reasons, the 2025 results are not directly comparable to those of previous editions.

The Digital Trust sector in France enjoys European and global leaders:

• **Thales** has created a world leader in digital security with the acquisition of Gemalto in 2019, and Imperva and Tesserent in 2024.

• **Thales, Idemia, Docaposte et IN Groupe** are world leaders in digital identity, identification and authentication.

• **Airbus Defence & Space** is an European leader in digital security and a global leader in wide area observation and secure communications.

• **Atos (Eviden), Orange, Sopra Steria et Capgemini** are the 4 French leaders among digital services companies, and are also the French leaders in cybersecurity (with Thales and Airbus Defence & Space).

• **Docaposte** is a French leader in many segments of digital security and cyber products. Docaposte is the initiator of a sovereign cloud offer «Numspot», announced in the fall of 2022. In collaboration with Dassault Systèmes, Bouygues Télécom and CDC, this sovereign cloud offer will enable the operation of trusted services that are SecNumCloud certified.

• The American company **Accenture** maintains its position in the top 10 thanks to its growth and previous takeovers (Arismore, etc.).

• **Thales** includes Gemalto, Imperva, Tesserent and Ercom.

• **Ates** includes Idnomic, Ipsotek, Motiv ICT Security, Sec consult, In fidem, Paladion...

• **Orange Cyberdéfense** includes Securelink, Securedata, Lexsi...

• **Sopra Steria** includes CS Group, Tobania, Ordina, Sodifrance, Bluecarat, Kentor, Eva Group...

• **Capgemini** includes Altran et Leidos Cyber.

• **Docaposte** includes AR24, CDC Arkhineo, Open Value...

• **Accenture** includes Arismore, Link by net, Openminded...

• **Chapsvision / Flandrin** technologies includes Deveryware, Bertin IT, Vecsys, Elektron et Geotrend.

• **Idemia** includes Otono networks.

• **IN Groupe** includes Surys et Nexus.

• **Econocom** includes Exaprobe.

• **Worldline** includes Ingenico.

• **GFI Informatique** includes SIS.

• **Cisco** includes Sentryo.

• **Sogetrel** includes Eryma.

Top 1-10 players in France

Top 11-20 players in France

Digital Trust Revenue generated in France ranged between €125 M and €200 M

Top 21-50 players in France

Digital Trust Revenue generated in France ranged between €60 M and €120 M

Note: Flags indicates the nationality of capital of the players in France.

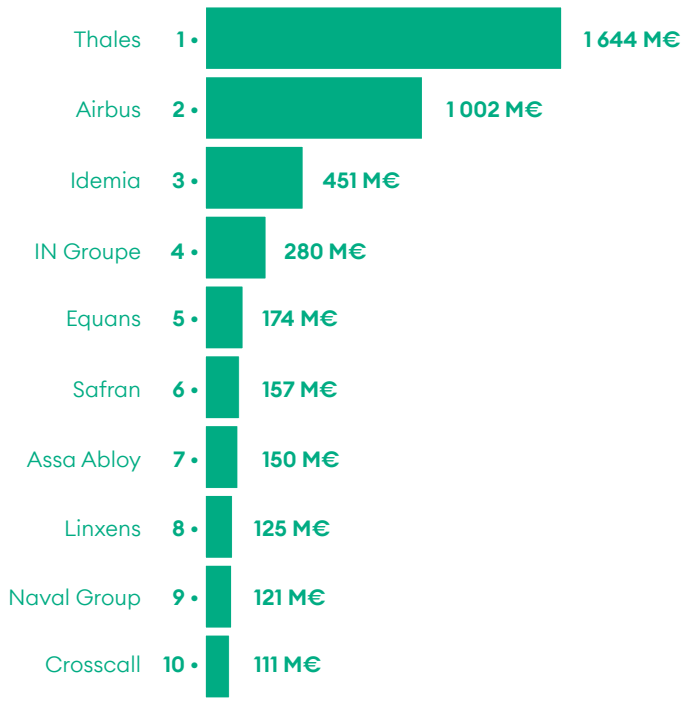
Among the players ranked between 10th and 20th and with a revenue of more than €125 M from France in 2024, there are French players such as Cap Gemini, Nomios and I-tracing (cyber services), Worldline (payment security), Safran (including specific AI) and Equans (digital security) as well as foreign players such as: Assa Abloy (Access control and authentification), Linxens (smart cards), Fortinet (cyber products), and Econocom (cyber services).

The companies around the 50th position have digital trust sales in France amounting for €60 M approximately: Somfy, Securitas (Stanley Security), Serma Safety & security, Schneider, Honeywell, Palantir, Devoteam, SAP, Oracle, Bechtle, Inetum, Claranet, Computacenter, Scalian...

Finally, although French players largely dominate the top 10 of the sector, there is a stronger presence of foreign companies established in France, US players in particular, among the top 10-50.

FOCUS

Digital Security Segment



• Growth 2023-2024
+4%

• Revenue
8,493 M€

• Workforce
36,212

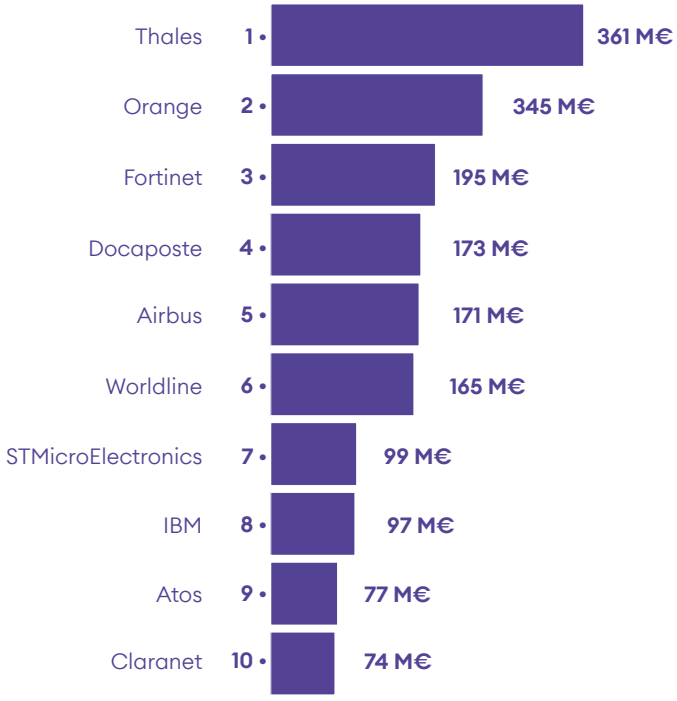
• Number of companies
1,770

• Added value
3,410 M€

	Revenue M€	Workforce	Number of companies	Added alue M€
Access control	1 804	7 084	331	672
Identification & Authentification of people	2 457	10 123	509	966
Wide area observation and detection	564	2 346	191	301
Tracking and tracing	621	2 631	221	233
Secure communications	1 809	7 557	318	682
Command, control and support for decision making	772	3 449	274	357
Intelligence and information gathering	466	3 020	234	199

FOCUS

Cybersecurity Product Segment



• Growth 2023-2024
+9,2%

• Revenue
6,188 M€

• Workforce
24,641

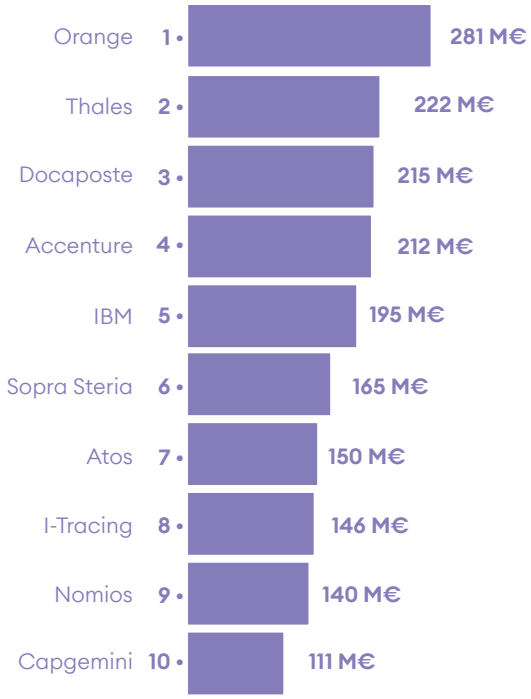
• Number of companies
739

• Added Value
3,627 M€

	Revenue M€	Workforce	Number of companies	Added Value M€
Cyber governance	1 021	5 203	225	585
Identity and access management	932	3 094	214	594
Data security	1 897	7 063	352	1 144
Application security	397	1 474	172	274
Secure digital infrastructures	1 540	6 265	358	874
Product and equipment security	401	1 542	162	157

FOCUS

Cybersecurity Services Segment



• Growth 2023-2024
+6,6%

• Revenue
5,036 M€

• Workforce
29,271

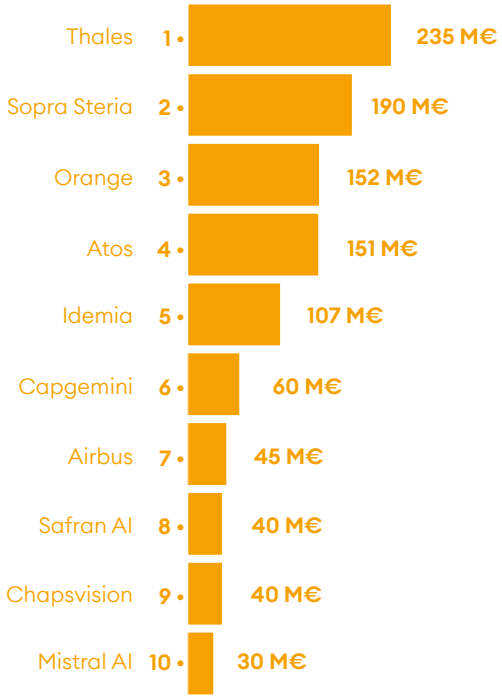
• Number of companies
717

Added Value
2,332 M€

	Reevnue M€	Workforce	Number of companies	Added value M€
Audit, planning and consulting in cybersecurity	2 189	13 147	670	898
Cyber implementation	1 614	9 938	468	699
Outsourcing - operating	1 119	5 121	362	666
Cybersecurity training	115	106	205	69

FOCUS

Trusted AI Segment



• Growth 2023-2024
+9,3%

• Revenue
1,586 M€

• Workforce
17,206

• Number of companies
315

• Added Value
730 M€

	Revenue M€	Workforce	Number of companies	Added Value M€
Generative AI	284	3 080	125	131
Specific AI	1 302	14 126	257	599

1. DIGITAL TRUST

CYBERSECURITY, DIGITAL SECURITY AND TRUSTWORTHY AI: A COMPLEMENTARY TECHNOLOGICAL TRIPTYCH

Digital Trust is the foundation of digital progress. Over the years, it has become a societal and industrial concern as critical as the development of digital technologies themselves. It reflects the confidence individuals and organisations can place in digital systems–now central to all aspects of life - to enhance their physical, financial, and reputational security while protecting their privacy and data, including personal information.

The Observatory of Digital Trust covers three key industries:

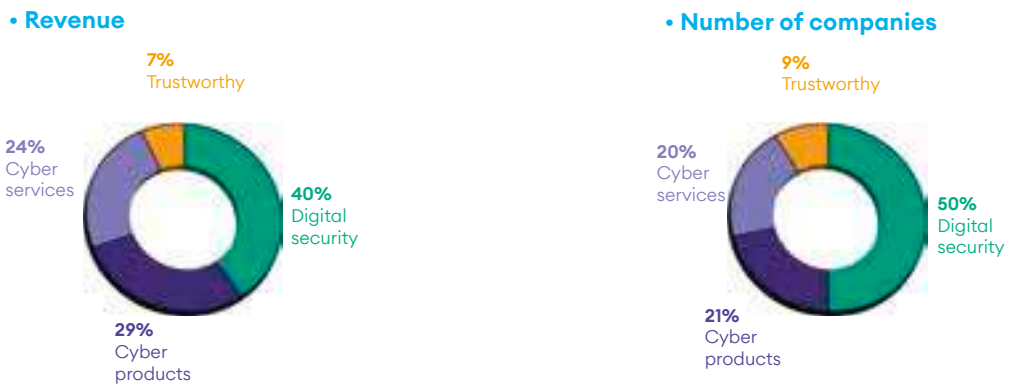
• **Cybersecurity**, which refers to the «internal» security of digital systems. It includes two categories of activities, often combined in practice: services (consulting, design, implementation, operation, training) and software & solutions. These serve professional markets (government, public sector, critical infrastructure, companies, SMEs) as well as the general public (computers, smartphones, connected homes, vehicles, and Iot devices).

• **Digital Security**, which encompasses electronic products and solutions that implement secure digital systems to establish trust in the external world. These technologies are deployed to build confidence in the citizen environment–particularly through identity and access management, biometrics, secure transactions, connected objects and vehicles, industrial processes, logistics, transportation, networks, and smart cities.

Digital security products include hardware (smart cards, identity documents, readers) and equipment (access control, biometrics, detection, geolocation, etc.).

• **Trustworthy AI**, which refers to artificial intelligence designed and deployed according to stringent legal, technical, and ethical standards. It is based on principles such as transparency, explainability, robustness, safety, human oversight, and respect for privacy. It also includes a sovereignty dimension, focusing on solutions developed by French providers. Trustworthy AI includes both generative models (LLMs, SLMs, GAI, etc.) used to generate content or assist users (chatbots, recommendation engines, summarisation tools), and domain-specific models tailored to targeted use cases (information extraction, image or voice processing, fraud detection, predictive maintenance, cybersecurity, etc.) depending on industry needs and data types.

Turnover and number of businesses in 2024

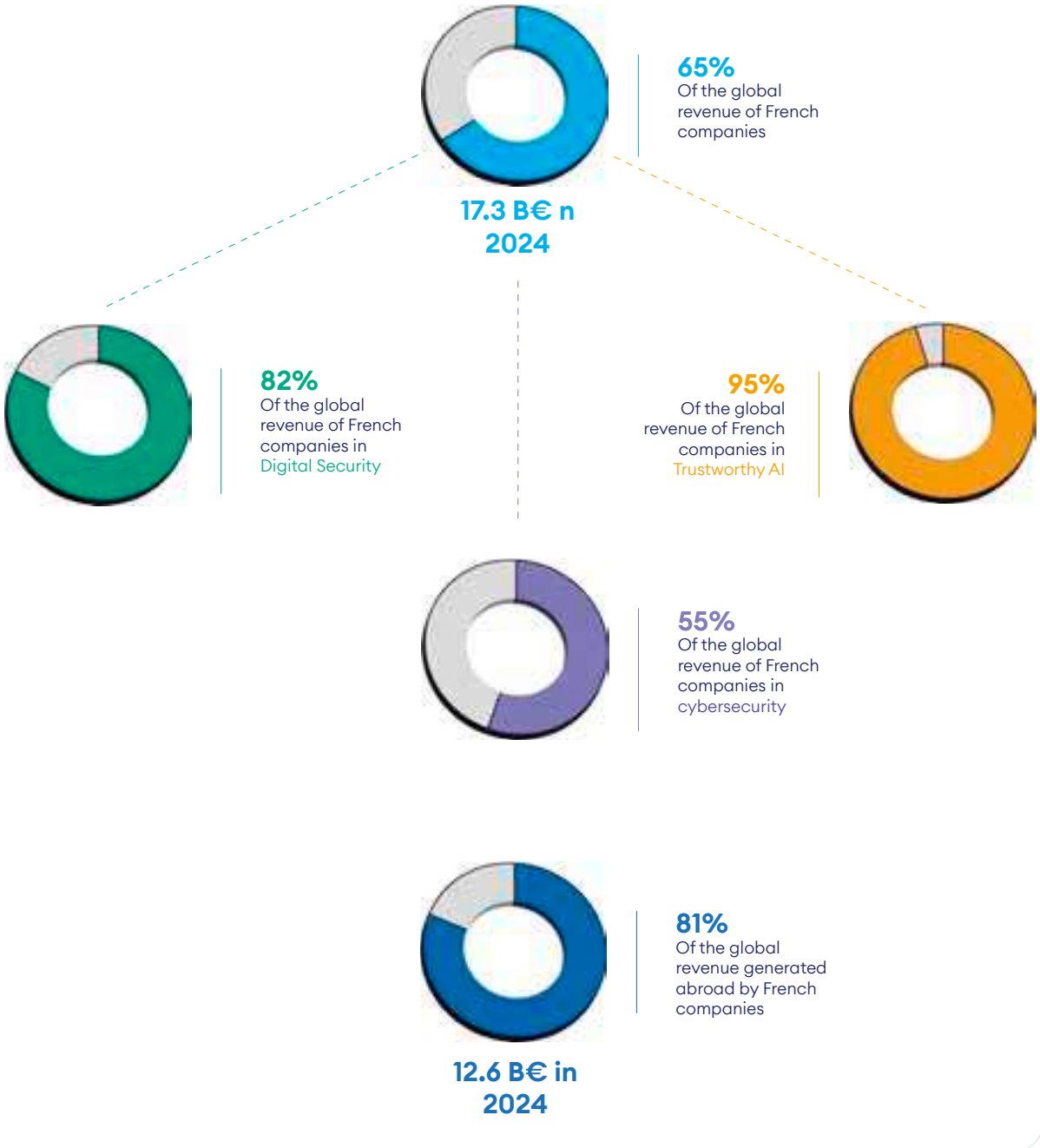


ACN is at the core of the industry

Among the ACN members there are:

• 15 large enterprises or ISE, including the 9 French leaders in Digital Trust.
• But also 92 SMEs, Micro-enterprises and innovative startups as direct members and more than 200 SMEs in the sector via the ecosystems of its partner members (Bretagne Développement Innovation, Pôle SCS, SPAC, etc).

ACN members account for

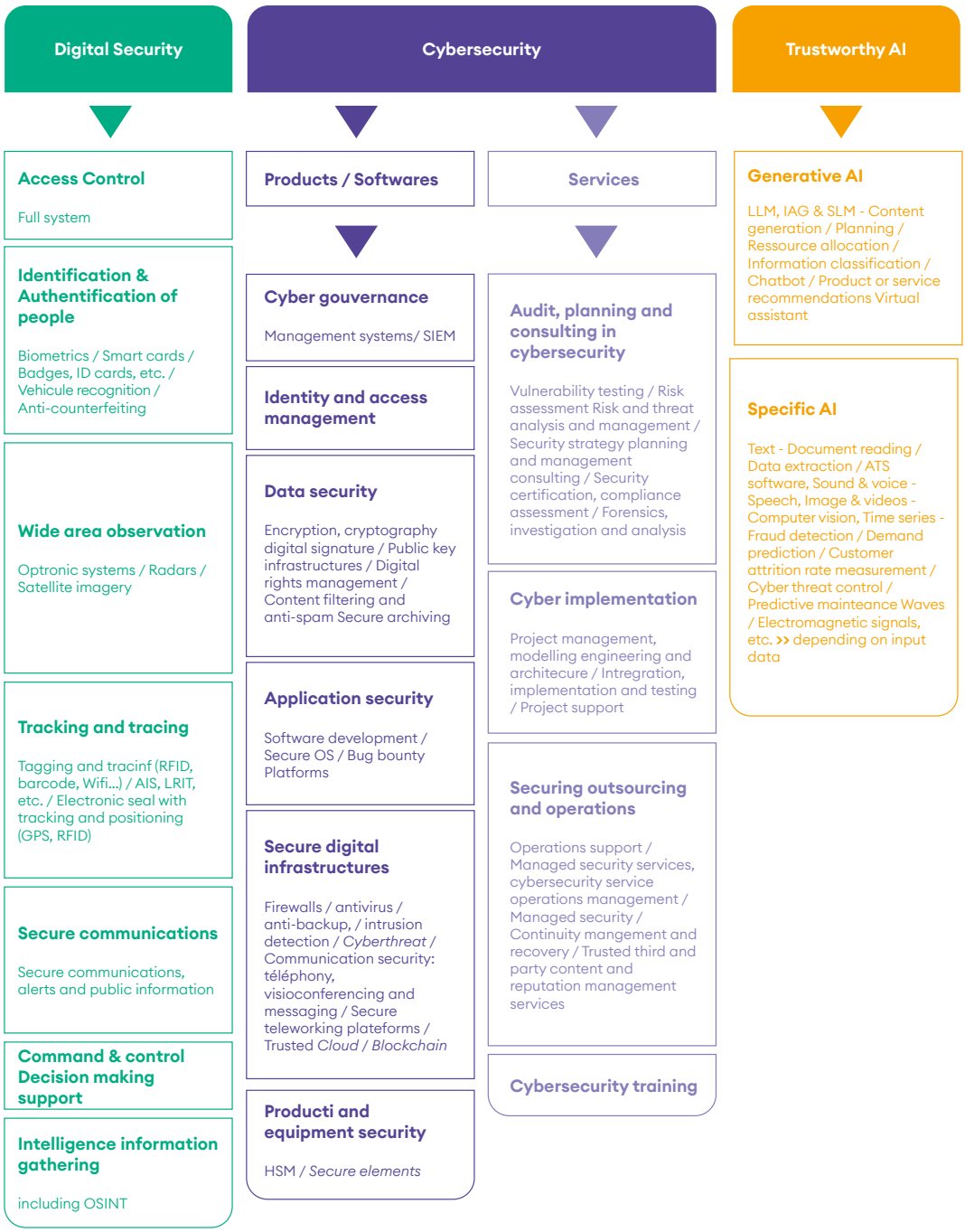


1.2 THE SCOPE OF DIGITAL TRUST - SEGMENTATION

The diagram below shows the different segments of the Digital Trust, divided into three areas:

- **Digital security**, which corresponds to trusted electronic systems or subsystems;
- **Cybersecurity products**, which corresponds to the development of cybersecurity software;
- **Cybersecurity services**, which corresponds to auditing, consulting, and implementation of cyber products, secure outsourcing or cyber training.
- **Trustworthy AI**, corresponding to generative AI or specific AI developed in France according to trust criteria.

Scope of digital Trust



1.3 METHODOLOGY

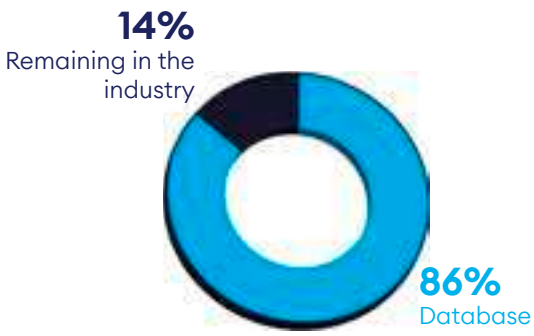
This Observatory aims at both defining the perimeter of the industry and assessing its economic weight and characteristics.

DECISION Études & Conseil has been conducting this Observatory since 2017.
The data presented in this report are taken from a DECISION's database listing 683 companies out of the 2,499 that make up the Digital Trust sector. This database takes into account:

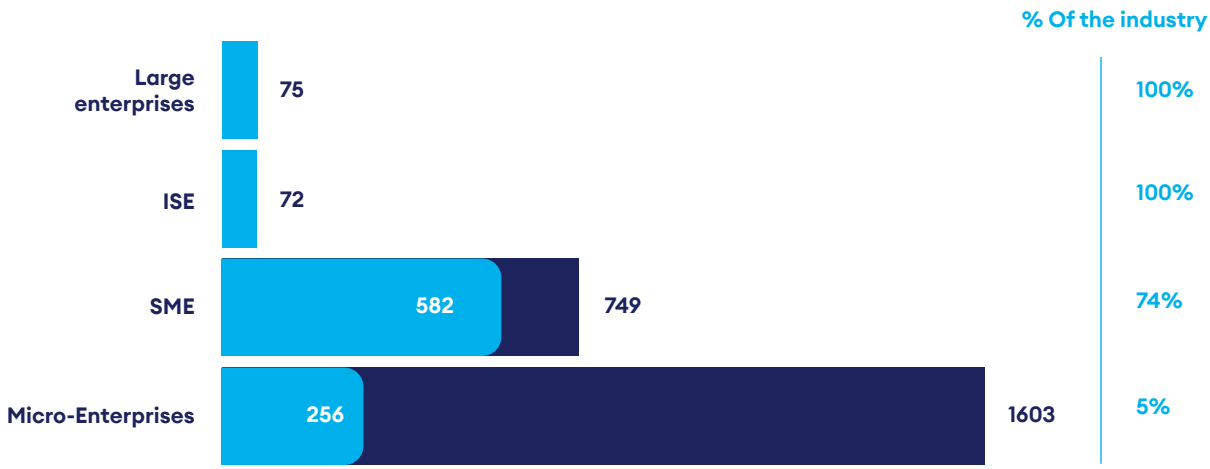
- All large enterprises in the sector (75/75);
- All the intermediate-sized enterprises (ISEs) in the sector (72/72);
- The majority of small and medium-sized enterprises (SMEs) in the sector (582/749);
- The most remarkable and innovative micro-enterprises and startups (256/1603).

Thus, although only 39% of the companies in the sector are included in the database, it is representative of 86% of the total revenue of the French Digital Trust industry.

Revenue



Number of companies



Data gathering for the database

For each company in the database, the following data are collected annually for France:

• **Administrative data:** SIREN, SIRET, address, NAF code, name of the main shareholder of the group, date of creation, name and function of the manager, contact details, etc...

• **Economic data for the period 2015-2024:** Revenue, number of employees, export revenue, added value, net profit.

Player analysis and segmentation

DECISION then carries out a specific analysis of each company in order to estimate the share of the activity dedicated to digital trust and the distribution of the revenue according to the 19 ACN segments (the ACN segmentation is now fully integrated in the wider segmentation of the Comité Stratégique de la Filière des Industries de Sécurité). This analysis of companies is carried out thanks to DECISION's expertise in the security sector acquired over the last 15 years, and in particular thanks to direct interviews with the key players in the sector. Finally, an online form is sent every year to the members of the sector and allows to refine the analyses.
From the information in the database, a method of extrapolation has been implemented in order to construct figures for the entire industry in France.

Growth calculation

Growth in France is estimated each year for each of the segments by taking into account three components:

• **Database:** A sub-sample analysis is carried out in order to measure the total growth in France of representative players in each segment, i.e. companies generating more than 10% of their revenue from their activities in the segment concerned.

• **Company documents:** Analysis of annual reports, financial documents and communications from companies in the sector.

• **Online questionnaire:** The online questionnaire filled in each year by the industry members provides data on the growth of the past year. For the 2025 edition, the members who answered the questionnaire represent 5% of the sector's revenue in France. Finally, a specific analysis of the evolution of the global activity (global and security) of the main Digital Trust players is carried out each year to estimate the revenue achieved by the sector abroad and its evolution.

Comparisons with previous Observatories

Each year, in addition to estimating growth, DECISION refines the segmentation of the various players in the sector, in particular thanks to information from the online questionnaire.

Consequently, **the figures in absolute value of each edition of the Observatory are not directly comparable**. The figures of this Observatory are presented for the year 2024 and according to the new segmentation of the actors. The updated 2023 figures are presented later in the following sections of this report.

2. AN IMPORTANT AND DYNAMIC INDUSTRY

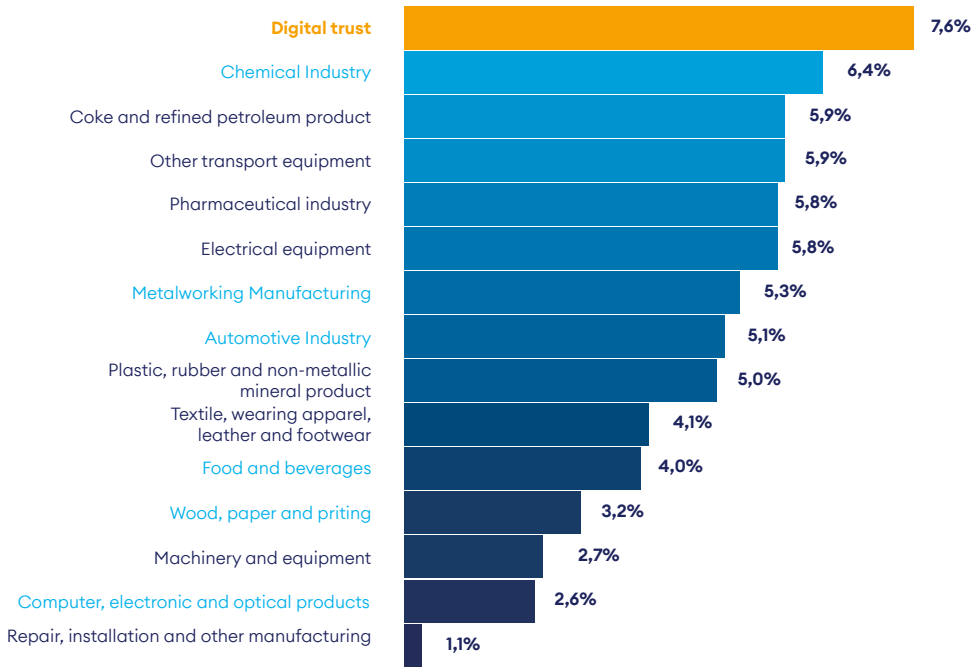
2.1 DIGITAL TRUST IS ONE OF THE FASTEST GROWING INDUSTRIES IN FRANCE OVER THE 2016-2023 PERIOD

Over the period 2016–2023, Digital Trust stands as the fastest-growing industrial sector in France, with an average annual growth rate of 7.6 %. Although measured using a method that is not directly comparable, the only other French industrial sectors recording growth above 5 % over the same period are the chemical industry, coke and refined petroleum products, the pharmaceutical industry, electrical equipment, non-automotive transport equipment, the metallurgy and metal products industry, and the automotive industry. Other sectors posted average annual growth rates between 0 % and 5 % over this period.

Digital Trust is also one of only four sectors (out of fifteen) that did not experience a recession in 2020. With growth of 3.6 % that year, it was the sector that best withstood the COVID crisis and its aftermath.

This resilience reflects the long-term and structural demand for Digital Trust goods and services. As a result, by 2030, Digital Trust could become the 11th largest industrial sector out of fifteen in terms of added value, overtaking both the electrical equipment sector and the repair, installation, and other manufactured goods sector.

Average annual growth of french industries over the 2016-2023 period



KEY

---- Industries that have both a dedicated Eurostat segment and strategic committee in the Conseil National de l'Industrie (CNI)

---- Industries that have a Eurostat segment and wich corresponds to some extent to industries with a strategic committee in the CNI (to be treated case by case)

* **Source :** DECISION, Observatory of Digital Trust

Source : DECISION, based on Eurostat data from 2016 to 2023

2.2 DIGITAL TRUST IS THE INDUSTRIAL SECTOR WHOSE ACTIVITY CREATES THE MOST WEALTH IN FRANCE

Digital Trust is the most productive sector with an added value rate of 47% (Added Value / Revenue). In other words, Digital Trust is the second industrial sector with the highest degree of wealth creation, i.e. transformation of products during the activity. Thus, the increase in revenue in this sector results on average in a higher rate of transforming activity on French soil compared to other French industrial sectors.

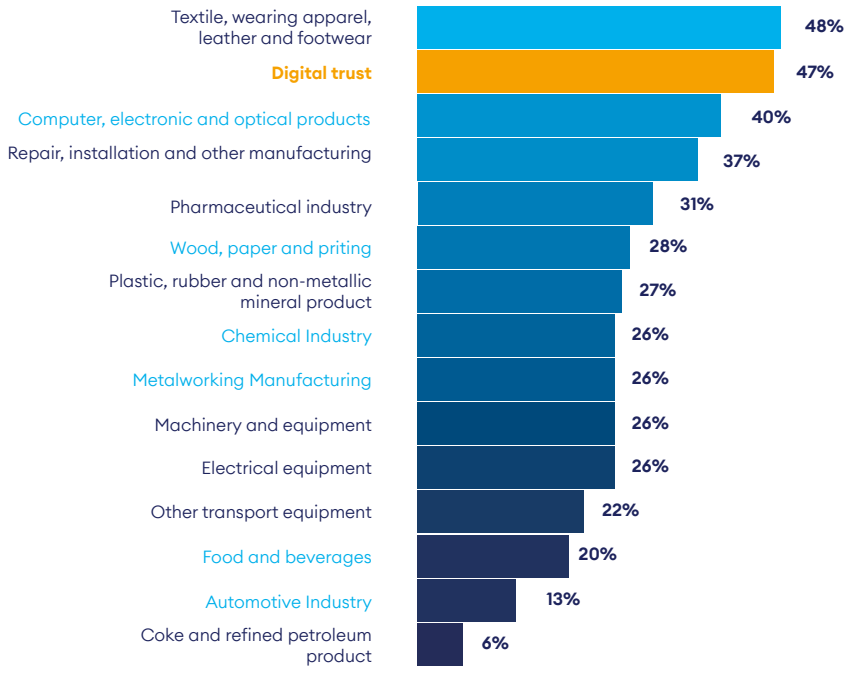
This phenomenon is mainly explained by three factors:

1. **The percentage of activity dedicated to services is relatively high in the French Digital Trust sector** (24% in 2024), through cybersecurity services (consulting, auditing, training, etc.). By definition, service activities have a very high added value rate because they use very little intermediate consumption and correspond almost exclusively to the transformation of products during the activity. However, this phenomenon alone does not justify the French security industry being the leader in terms of value added rate, as most of the French industrial sectors also include a significant part of services.

2. Electronic products dedicated to Digital Trust (digital security) correspond to 40% of the total revenue of the Digital Trust sector. However, while for the French electronics industry as a whole, a large part of the production stages upstream of the value chain is carried out in Asia, **this phenomenon hardly applies to the Digital Trust segment, which maintains all the production stages in France as much as possible because of its proximity to the sovereign sectors.** Other French sectors focus more strongly on integration activities upstream of the value chain and on pure engineering activities (design, development, etc.). As a large part of the value chain of the digital security industry is carried out from France, the rate of value added increases.

3. Finally, cybersecurity products account for 29% of the total revenue of the security industry and involve **a very large proportion of highly qualified jobs** (software development, etc.), associated with a very high rate of added value (at levels close to those of cybersecurity services).

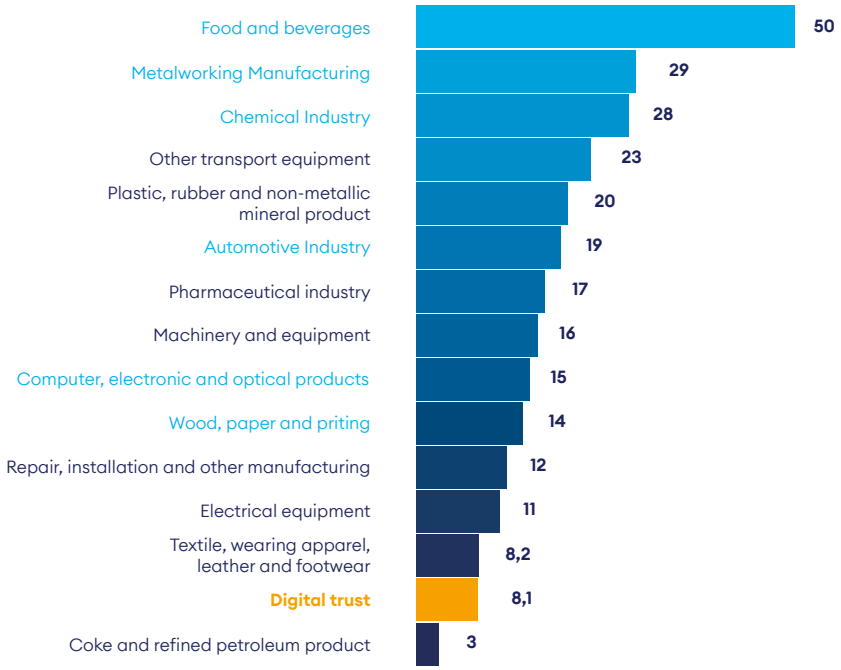
Value-added to turnover ratio (VA/Turnover) of French industries in 2022



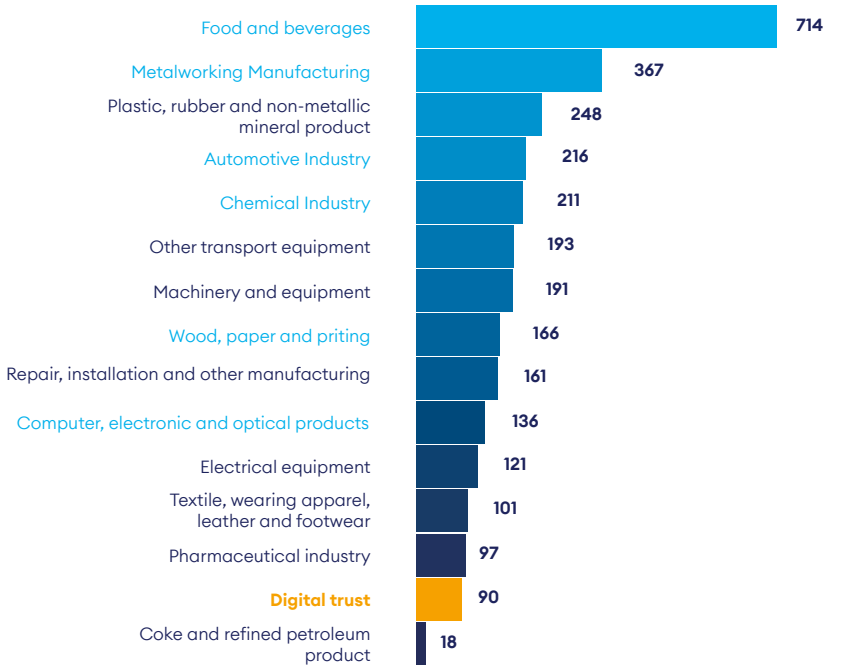
2.3 DIGITAL TRUST IS A FULLY-FLEDGED FRENCH INDUSTRIAL SECTOR

Digital Trust is an industrial sector in its own right. In terms of added value, it is close to the textile and clothing sector. In terms of employment, it is much larger than the coke and refined petroleum sector and is close to the pharmaceutical industry.

Added Values of french industries in 2022 (€ Billion)



Worforce in french industries in 2022 (in thousand)



Source : DECISION, Eurostat, OCDE

2.4 FRENCH PLAYERS ARE AT THE TOP LEVEL IN TERMS OF SKILLS AND R&D

Thanks in particular to French excellence in research and development, the vast majority of French Digital Trust companies are positioned in the high-end segments of their markets, offering solutions at the cutting edge of what technology makes possible today.
France excels in particular in the following areas:

• **Artificial Intelligence & Machine learning:** France excels in deep learning. For several years, the GAFAM companies have established research centers dedicated to this field and have been actively recruiting French talent. France is also witnessing the emergence of leading players in generative AI, such as Mistral AI, which has become a French unicorn. In the field of specialized AI, France benefits from a broad ecosystem offering business-specific solutions across various sectors, including healthcare, insurance, and logistics. On the public R&D side, INRIA notably has dedicated teams working on defense and attack strategies based on deep learning.

• **Cryptography:** France has historically been one of the world leaders and is maintaining its position.

• **Post-quantum technologies (including cryptography):** France remains in the top three worldwide. In a few years, quantum computers should reach operational stages. Post-quantum cryptography is therefore one of the most critical research topics for France.
France is also well positioned in blockchain and in securing connected objects. However, public research suffers from the lack of staff dedicated to Big Data. France has nearly 1,000 full-time academic researchers working on cybersecurity issues, particularly on the Rennes, Paris-Saclay, Brest, Grenoble and Lyon campuses.

2.5 THE GROWTH IN DIGITAL TRUST IS PART OF A GLOBAL DYNAMIC

At the global level, the growth of Digital Trust is driven by four factors, the first three of which are not specific to France:

1. Miniaturisation along with the falling cost of electronic components. This long-term trend makes it possible to integrate electronic security equipment on a large scale and therefore contributes to a strong growth in volume of electronic security equipment. In the short term, the growth of electronic components is cyclical and the 2020-2022 period was instead marked by a surge in semiconductor prices. Since the beginning of 2023, the decline in semiconductor prices has resumed its course.

2. Digital transformation. Accelerated by the COVID crisis in 2020, companies and administrations around the world are digitalizing their processes, deploying clouds and interconnecting data networks.

3. The growth from emerging countries, led by China, which aims to become a world leader in semiconductor production and innovation in the near future.

4. Finally, numerous technological innovations specific to the Digital Trust sector and in which France is often very well positioned both in terms of industrial players and scientific know-how: behavioural biometrics, innovations associated with secure elements, cryptographic developments, quantum computing, real-time analysis of wide-area observation data, blockchain, etc.

France has historically benefited from a powerful defence and security sector that exports strongly compared to the international average and has been able to take advantage of its excellence in research and development to benefit from these four global trends and thus build a solid Digital Trust industry.

However, growth is even stronger in the US and especially Chinese digital trust industries.

2.6 GROWING COMPETITION FROM FOREIGN PLAYERS

French players generate 74% of the Digital Trust revenue in France, i.e. €15.8 billion in 2024. In other words, foreign players in the sector generate 26% of the sector's revenue in France, i.e. approximately 5.5 billion euros in 2024. This figure corresponds solely to the revenue generated by the subsidiaries of foreign players in France and does not include exports by foreign players to France (which could not be measured in this observatory).

Although the share of wealth generated in France by French players remains relatively high, it has been steadily declining from 2013 through 2024, and this trend is expected to continue. Over the past several years, American players have significantly expanded their presence in France, notably through the establishment of new headquarters: Microsoft, Dell, Palantir, Docusign, AWS, Google, Cisco, Check Point Systems, CrowdStrike International, Juniper Networks, Nutanix, F5 Networks, Palo Alto Networks, Rubrik, Okta, Netskope, Forescout Technologies, Aruba, Tufin Software, Quest Software, Proofpoint, and others.
Chinese players are also expanding, increasingly offering high-level solutions capable of competing technically with French offerings.

Similarly, when it comes to production, the weight of foreign players on the French market remains substantial, estimated at around 40 %. In other words, the national market continues to be heavily influenced by foreign, non-European solutions, despite the fact that the French sector has offerings in all segments and includes technological leaders and many players capable of covering at least the entire national market.

Significant acquisitions of French companies by foreign players took place across most segments of the Digital Trust sector between 2013 and 2021. These include the takeover of Arismore by Accenture (USA), DenyAll by Rohde & Schwarz Cybersecurity (Germany), and Oberthur Technologies (acquired by the American fund Advent in 2011), followed by the acquisition of Safran Morpho (also by Advent in 2018) and its subsequent merger with Oberthur Technologies under the Idemia brand in 2018.
Since 2021, however, the number and size of such acquisitions have tended to decrease. In 2022, the only significant acquisition identified was that of Akka Technologies by the Swiss group Adecco.

Nevertheless, a few targeted smaller-scale acquisitions have been noted, such as Hornetsecurity – a German company backed by American capital – which acquired two French companies specializing in email security, Vade and Altospam, within the span of a year.

Above all, many players in the Digital Trust sector highlight the damaging lack of a culture of purchasing French products, both among businesses and public administrations. This lack of support for French products has naturally led companies and administrations to favor foreign offerings.

In a context of generally stagnant growth (0.8 % annual GDP growth in France between 2018 and 2024), inflation, and budgetary austerity in public services, price often becomes the primary purchasing criterion. On this sole basis, American and Chinese players often prove more competitive than their French counterparts, notably thanks to greater economies of scale and heavier reliance on subcontracting in low-wage countries.

Beyond penalizing French players, the procurement of uncontrolled foreign solutions can threaten France's sovereignty, especially when buyers are public entities, Operators of Vital Importance (OIVs), or Operators of Essential Services (OSEs).

Despite growing awareness around sovereignty and strategic autonomy issues, the lack of a culture favoring French-made solutions remains particularly evident in the public sector and among major French corporations.

The triptych of standardization, certification, and regulatory requirements, notably promoted by ANSSI, helps guarantee the use of reliable and secure solutions while shifting competition away from pure price considerations toward technical excellence – naturally benefiting French players.

2.7 A SECTOR WITH GREAT POTENTIAL IF THE RIGHT STRATEGIC CHOICES ARE MADE

Digital Trust is a strategic industry because:

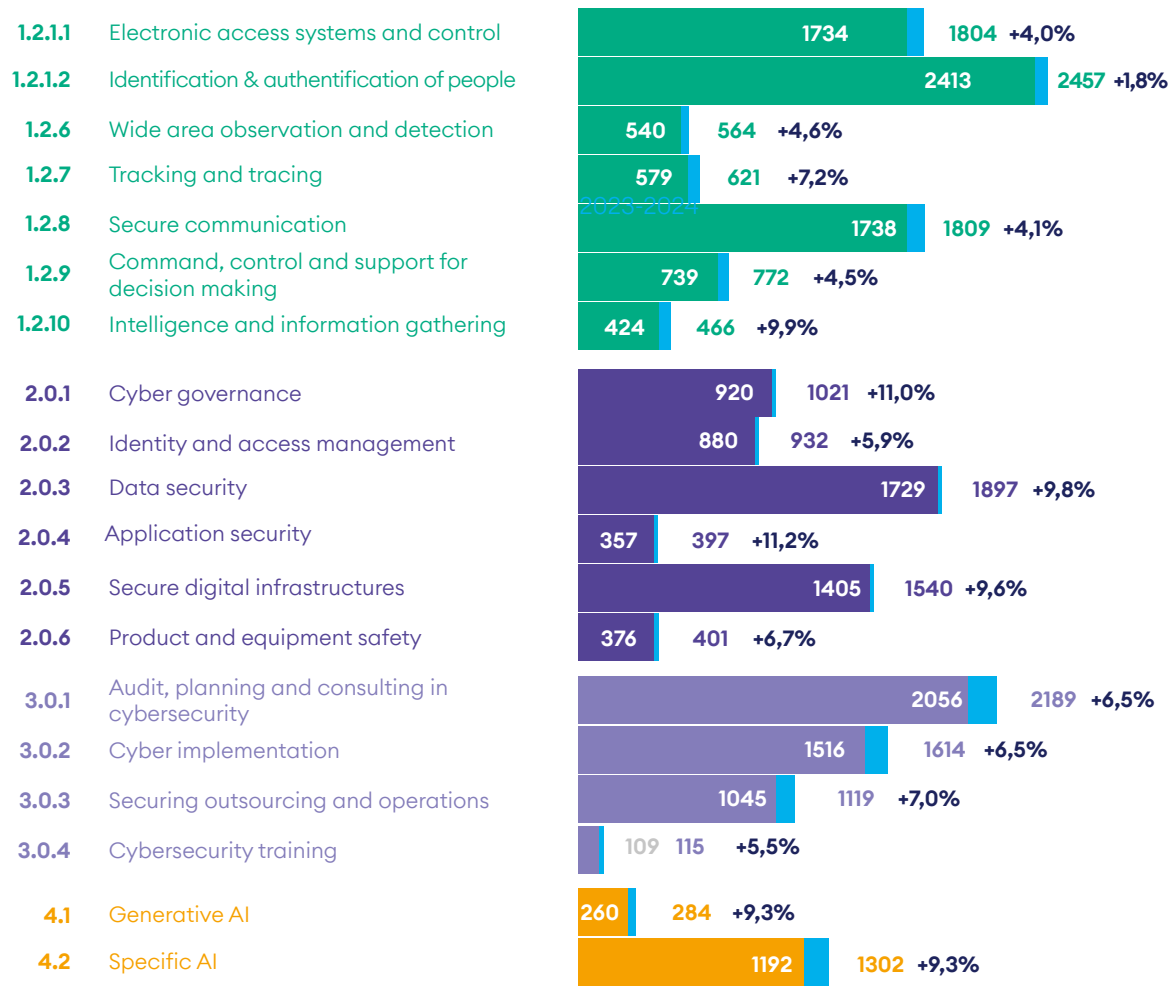
- The **growth** is sustainably higher than that of any other French industry;
- Digital Trust is already of significant size;
- French players are at the forefront in terms of skills and R&D;
- This sector is essential to **national digital sovereignty** and **Europea, strategic autonomy;**
- The growth potential risks being under-exploited due to **strong international competition,** particularly from China and the United States.

The conditions are in place for the leverage to be achieved if a proactive industrial policy is put in place to generate a maximum return on investment, both in terms of employment and added value on French soil and internationally.

3. KEY FIGURES OF THE INDUSTRY

3.1 SIZE AND GROWTH

Revenue per segment in Digital Trust : €21.3 B in 2024



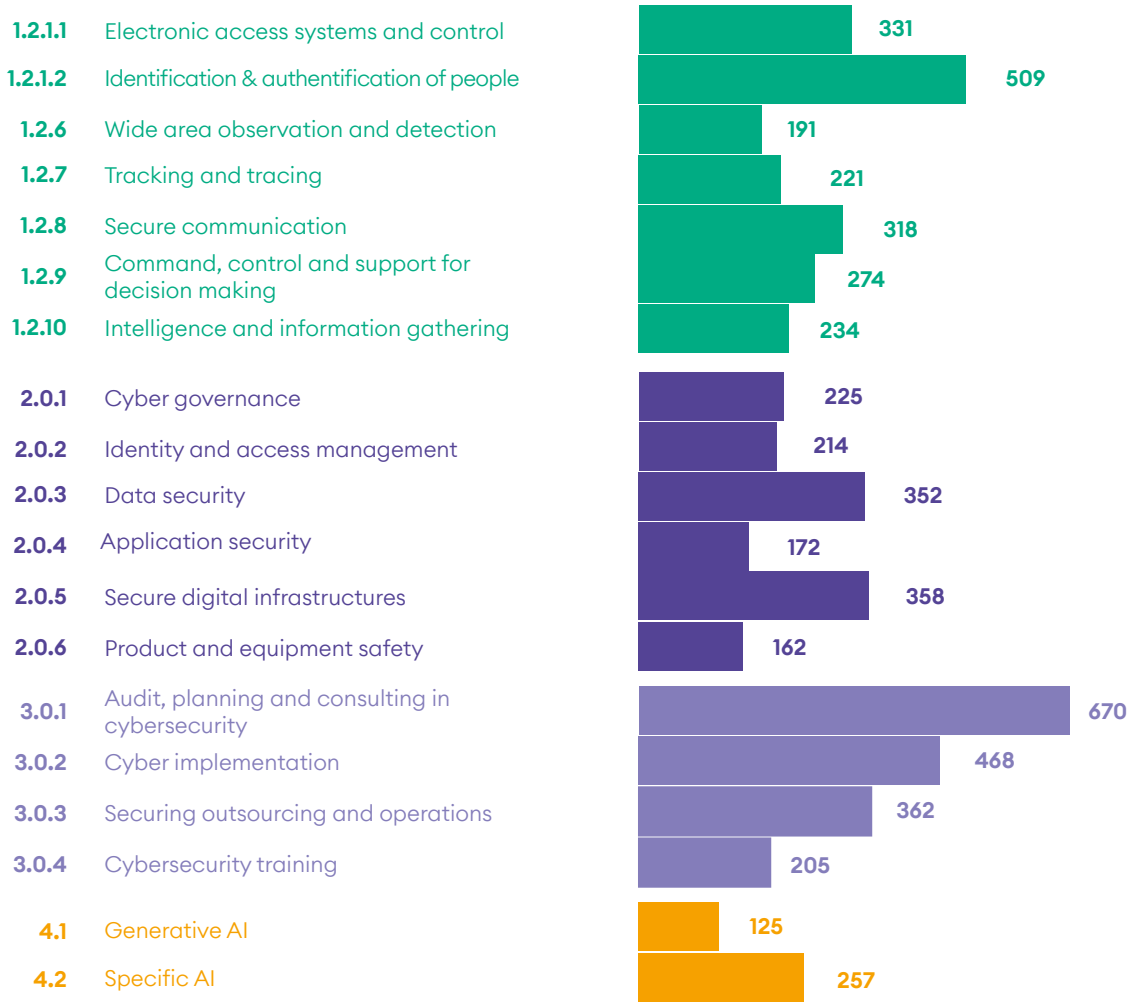
Digital security	Cyber products & softwares	Cyber services	Trustworthy AI
8,493 M€ of revenue	**6,188 M€** of revenue	**5,036 M€** of revenue	**1,586 M€** of revenue
+4% in 2024	+9,2% in 2024	+6,6% in 2024	+9,3% in 2024

21,304 M€ revenue
in digital trust in France

+6,5% in 2024

Source : DECISION Études & Conseil

3.2 NUMBER OF COMPANIES

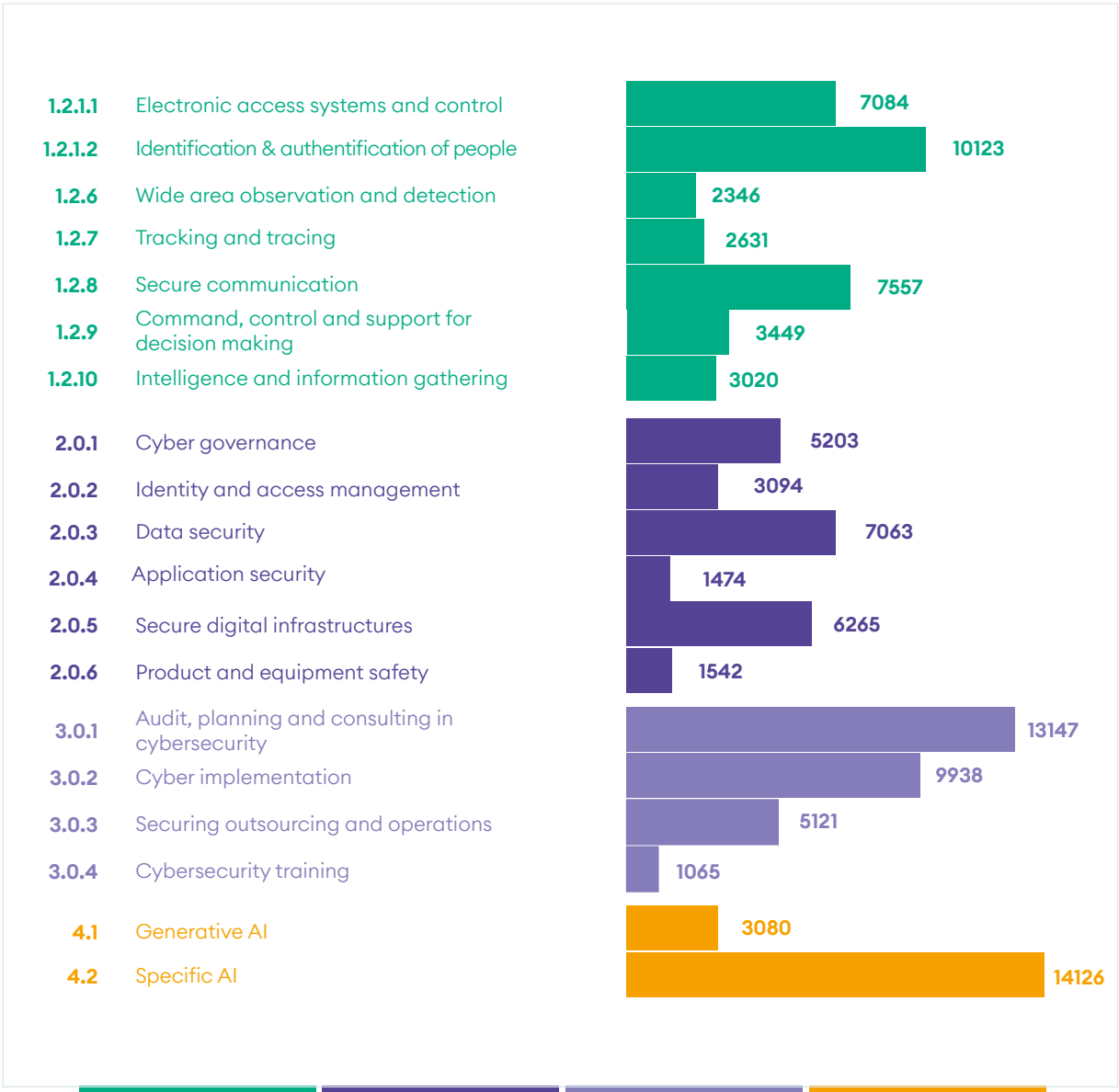


Digital security	Cyber products & softwares	Cyber services	Trustworthy AI
1,770 companies	**739** companies	**717** companies	**315** companies

2,499 companies
in digital trust in France

Source : DECISION Études & Conseil

3.3 JOBS

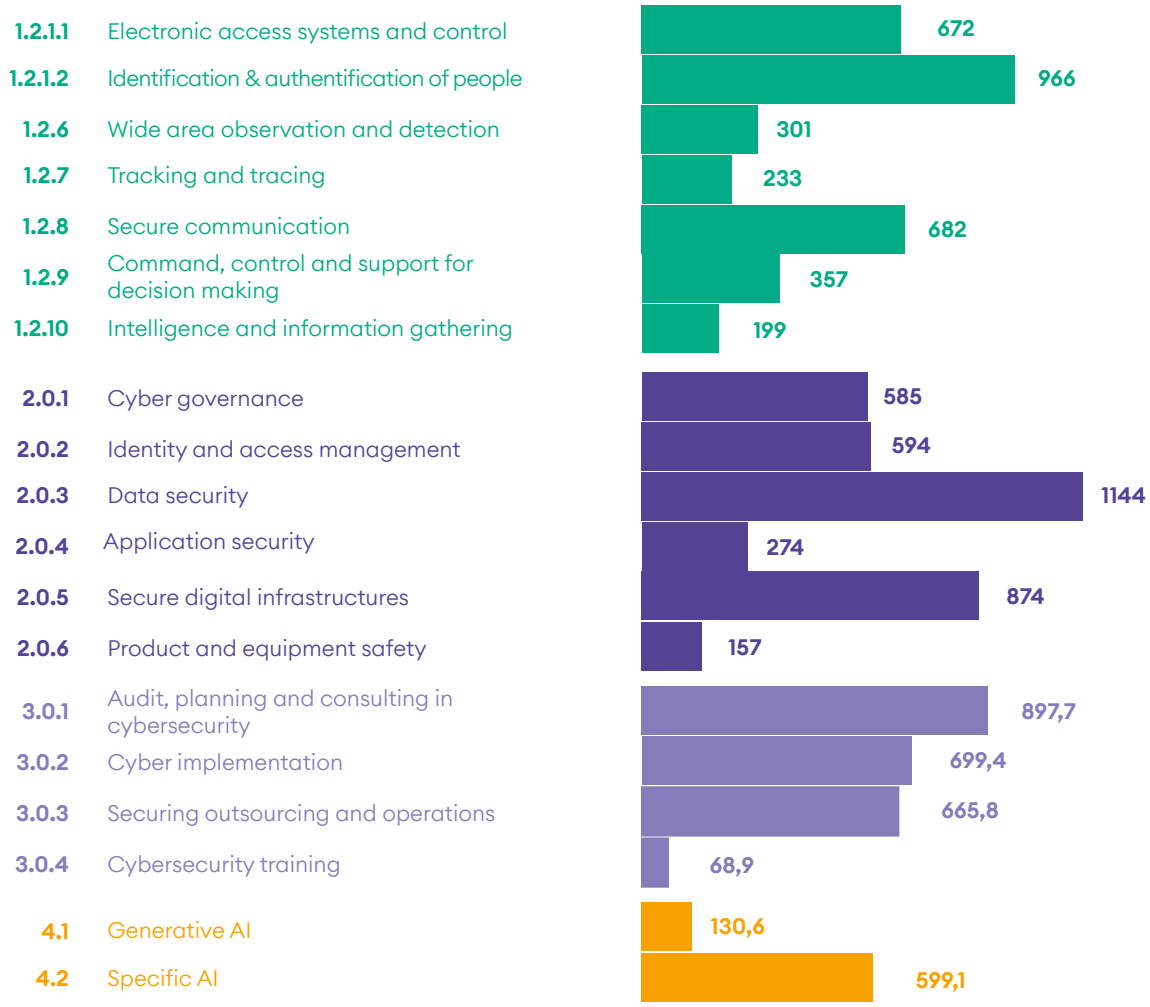


Digital security	Cyber products & softwares	Cyber services	Trustworthy AI
36,212 jobs	**24,641** jobs	**29,271** jobs	**17,206** jobs

107,330 jobs
in digital trust in France

Source : DECISION Études & Conseil

3.4 ADDED VALUE



Digital security	Cyber products & softwares	Cyber services	Trustworthy AI
3 410 M€	**3 627 M€**	**2 332 M€**	**730 M€**
added value	added value	added value	added value

10,099 M€ added value
in digital trust in France

Source : DECISION Études & Conseil

3.5 MERGERS AND ACQUISITIONS

Within the Digital Trust industry, 37 company buyouts concerning headquarters located in France have been identified from January 2023 to March 2025 (i.e. an average of 17 buyouts per year). These buyouts are both inter-company purchases and purchases of companies by financial funds and purchases between financial funds.

Among them:

- 16 buyouts of French companies by other French companies (43%);
- 11 buyouts of foreign companies by French companies (30%);
- 10 buyouts of French companies by foreign companies (27%).

The vast majority of companies acquired are SMEs (64%), confirming buyers' interest in growing structures. Compared with the 2017-2020 period, the frequency of buyouts remains broadly comparable, but the size of target companies is smaller on average.

The year 2024 stands out for its lower transaction volume (14 deals), below the annual average observed over the 2020-2023 period (around 20 deals per year). This downturn is in line with an economic climate that is generally less favorable to mergers and acquisitions.

In 2024-2025, the fast-growing mid-sized companies - Nomios and I-Tracing - engaged in European expansion strategies through acquisitions, reflecting a new dynamic of market consolidation driven by a new generation of French players generation.

Over the past two years, cross-flow between France and other countries has tended to balance out. While the 2017-2020 period was marked by a clear dominance of foreign takeovers of French companies, this dynamic now seems less marked, thanks in part to a few emblematic operations carried out by French groups in neighboring markets - such as the acquisitions of Imperva and Tesserent by Thales in 2023. Nevertheless, in 2024, the United States remained the main buyer of French companies in the sector, with three notable deals: Expert Lines acquired by Neverhack (a French company with majority American capital since its fund-raising with Carlyle in 2023), Vade Security acquired by Hornetsecurity, and PingCastle acquired by Netwrix. This trend continued in early 2025, with two new deals: Secure-IC acquired by Cadence, and Altospam again by Hornetsecurity.

The 37 buyout movements are summarized in the diagram below:

Overview: companies takeovers over the period 2023-2025

A• Main acquisitions since 2023 from the french digital trust leaders

IN Groupe prepares strategic takeover of IDEMIA Smart Identity division to consolidate its global position in digital identity

In September 2024, IN Groupe entered into exclusive negotiations with IDEMIA Group to acquire IDEMIA Smart Identity, one of the company's three divisions. This major operation would enable IN Groupe to pass a strategic milestone by reaching critical mass on a global scale, with combined sales exceeding one billion euros. The acquisition would strengthen IN Groupe's positions in the physical and digital identity markets, with an extensive geographic footprint in Europe, Africa, the Middle East, Latin America and Asia. By gaining access to cutting-edge technologies such as chip design and security software, IN Groupe would acquire enhanced capabilities to meet growing requirements in terms of sovereignty, cybersecurity and compliance with European data protection standards. This operation is in line with the Group's strategy of external growth, which has been underway for over ten years.

Neverhack (ex-Pr0ph3cy) leads ambitious acquisition campaign in 2024

Since raising €100 million in 2023 from US fund Carlyle, which became a 55% majority shareholder, Neverhack has accelerated its external growth strategy to create a one-stop cyber services provider. In 2024, the group made three major acquisitions: French company Expert Line, Estonian specialist Cybers, and Italian multinational Innovery. These operations strengthen its skills in SOC, offensive security and IT architecture integration, while extending its presence in Southern Europe, the Baltic States and the Americas.

ChapsVision continues its external growth strategy in AI and crisis management

ChapsVision made two further acquisitions in 2024 and 2025, consolidating its position in data processing and artificial intelligence. In November 2024, the group announced the acquisition of Sinequa, a global specialist in AI-enhanced enterprise search, in order to integrate its technologies into the ArgonOS platform and accelerate its international expansion. The deal is accompanied by the raising of €85 million from investors including Jolt Capital. In March 2025, ChapsVision acquires IREMOS, a crisis management software publisher and specialist in defense secrecy protection. This operation strengthens ChapsVision's leading position in this field, combining specialized software and business expertise, notably through the integration of RDI+, a subsidiary of IREMOS.

Safran positions itself in defense AI with the acquisition of Preligens

In September 2024, Safran announced the acquisition of Preligens, a French established company in artificial intelligence applied to the defense and aerospace sectors, for 220 million euros. The company, now renamed Safran.AI, is part of Safran Electronics & Defense. Through this acquisition, Safran intends to accelerate the integration of AI into its surveillance, inspection and decision-making systems, while leveraging Preligens' expertise in automated image and signal analysis. Beyond military applications, the group also plans to transpose these technologies to industrial uses as part of its Industrie 4.0 strategy.

French acquisitions in Europe

Several French companies are strengthening their presence in Europe through targeted acquisitions. In 2024, I-Tracing stood out by acquiring Bridewell, a British company specializing in strategic cybersecurity consulting. This operation, backed by Eurazeo, Sagard NewGen and Oakley Capital, enabled I-Tracing to reach over 1,000 consultants and extend its coverage in the United Kingdom and the United States. Two other acquisitions in the UK also marked the year: Nomios acquired Dionach, a company specializing in penetration testing and compliance auditing, while Keensight Capital acquired a majority stake in MetaCompliance, a Northern Ireland-based player specializing in human risk management and cybersecurity training.

B• The main acquisition of French companies by foreign investors

American players strengthen their presence in the French market

American-owned companies were particularly active in France in 2024 and the first quarter of 2025, with five notable acquisitions. The American-owned Hornetsecurity Group acquired the French companies Vade and Altospam, strengthening its presence in France and its European positioning.

American electronic circuit design specialist Cadence acquired Secure-IC, a Telecom Paris spin-off and French flagship in embedded cybersecurity. This acquisition will enable Cadence to expand its portfolio of secure IP and evaluation solutions.

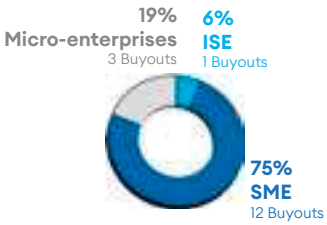
In the field of identity security, Netwrix has acquired PingCastle, renowned for its Active Directory vulnerability analysis solution. This operation enables Netwrix to enhance its vulnerability detection and remediation capabilities in hybrid environments.

These deals demonstrate the continuing interest of American groups in the cybersecurity technologies developed in France.

European groups expand their presence in France

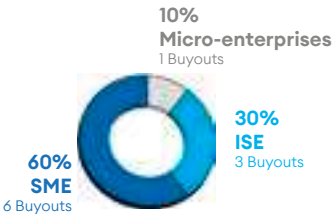
European companies have also consolidated their presence in France through a number of strategic acquisitions. Norwegian group Visma has acquired MyCompanyFiles, a specialist in secure exchange platforms for accountants, continuing its growth strategy in secure cloud services for professionals. In the cybersecurity sector, Ireland's Integrity360 has absorbed Holiseum, a recognized French player in critical infrastructure security (IT/OT). This alliance will enable Integrity360 to strengthen its industrial expertise and accelerate its deployment in France.

16 Buyouts of french companies by french companies



11 Buyouts of foreign companies by french companies

10 Buyouts of french companies by foreign companies



3.6 DESPITE A SLOWDOWN IN 2024, FRANCE REMAINS EUROPE'S TOP FUNDRAISER IN DIGITAL TRUST

As in previous years, DECISION relies on Tikehau Ace Capital's European Cybersecurity Investment Barometer, which it complements with its own research, taking into account ACN's specific segmentation, which encompasses all digital security activities beyond cybersecurity.

After several years of continuous growth, 2024 marks a downturn in the number and total amount of fundraisings in the Digital Trust sector (excluding AI) in France. Over the year, 27 deals were recorded for a total of 352 million euros, compared with 42 deals for 456 million euros in 2023. However, this drop in volume can to be mitigated: the average amount per issue reached 13 million euros in 2024, compared with 11.1 million euros the previous year.
The trend was confirmed in the first quarter of 2025, with only 5 transactions recorded for a cumulative amount of €75 million. Despite this more difficult context, the industry continues to distinguish itself through significant fund-raising: as in every year for the past four years, major deals have been completed, notably by ChapsVision (87 million euros) and Zama (67 million euros).
In 2024, ACN members accounted for almost 60% of the amounts raised, for a total of 209 million euros over the year. This dynamic underlines the growing importance of ACN members in the French digital trust landscape.

Among the French investors who backed startups in the industry in 2024 were major players such as Bpifrance, Tikehau Capital, Alven, SWEN Capital Partners, Hi Inov, Adelie, Shapr Venture, Auriga Cyber Ventures, Kreaxie, Super Capital, Qualium Investissement, GENEO Capital and Elaia.

In an economic and financial climate that remains unfavorable to investment, France has shown remarkable resilience. According to Tikehau Ace Capital's European barometer, amounts raised in cybersecurity fell for the second year in a row across Europe. However, in contrast to its neighbors, France is maintaining a solid momentum, and this year ranks first in Europe in terms of amounts raised, ahead of the UK.

This position confirms the attractiveness of the French ecosystem and its ability to attract significant funding, even in an uncertain economic climate.

Amount of founds raised by french Digital Trust startups

Amounts of funds raised in AI in France

In comparison, fundraising in artificial intelligence reached significantly higher levels in 2024. Over the year as a whole, investments in French AI companies amounted to €1.114 billion, more than three times the amount raised in cybersecurity over the same period (€352 million). This momentum was largely driven by a number of exceptional deals, notably Mistral AI, which has raised a total of 1.09 billion euros since 2023, including 600 million euros in 2024. Another example is H Company, which raised 200 million euros in May 2024.

This imbalance between the two sectors does not undermine the strategic importance of cybersecurity, but reflects the attraction that AI exerts on investors, in a context of strong media coverage and promises of cross-cutting economic transformation.

List of fundraising activities of French Digital Trust startups

2023

	Company	Organisation	Year	Amount (M€)
1	Ledger		2023	100
2	ChapsVision	**ACN**	2023	90
3	DataDome		2023	38.6
4	sekoia.io	**ACN**	2023	35
5	Egerie		2023	30
6	HarfangLab		2023	25
7	Provenrun		2023	15
8	Dattak		2023	11
9	CryptoNext		2023	11
10	Sesame IT	**ACN**	2023	10
11	Stoïk	**ACN**	2023	10
12	Cybervadis		2023	7
13	Ecole 2600	**ACN**	2023	6
14	Filigran		2023	5
15	MiTrust		2023	5
16	Astran	**ACN**	2023	4.7
17	Qevlar AI		2023	4.5
18	NANOCORP	**ACN**	2023	4.2
19	CSB school		2023	4
20	VSORA		2023	4
21	OverSOC		2023	3.8
22	Escape		2023	3.6
23	Narval		2023	3.6
24	Zygon		2023	2.8
25	Dotfile		2023	2.5
26	Bastion Technologies	**ACN**	2023	2.5
27	elba		2023	2.5
28	ShareID	**ACN**	2023	2
29	Defants		2023	2
30	Alcyconie		2023	2
31	VeriQloud		2023	1.9
32	Qontrol	**ACN**	2023	1.5
33	Naaia		2023	1.3
34	Mithril Security		2023	1.2
35	BonjourCyber	**ACN**	2023	1
36	Legapass		2023	0.6
37	Inspeere		2023	0.6
38	Escape		2023	0.5
39	OneWave		2023	0.4
40	Bastion Technologies	**ACN**	2023	
41	Kubo Labs		2023	
	Total ACN			**167**

2024

	Company	Organisation	Year	Amount (M€)
1	ChapsVision	**ACN**	2024	85
2	Zama	**ACN**	2024	67
3	Filigran		2024	32.3
4	YesWeHack	**ACN**	2024	26
5	Stoïk	**ACN**	2024	25
6	Filigran		2024	15
7	Dfns		2024	15
8	BforAI		2024	14.4
9	Patrowl		2024	11
10	BforAI		2024	9.6
11	COMAND AI		2024	8.5
12	Tenacy		2024	6
13	Anozr Way	**ACN**	2024	6
14	Dotfile		2024	6
15	Probabl		2024	5.5
16	Mindflow		2024	5
17	Finovox		2024	3.9
18	Nijta		2024	2.1
19	Dipeo		2024	1.8
20	Alcyconie		2024	1.4
21	Kamae		2024	1.4
22	Nestor		2024	1.2
23	Daspren		2024	1
24	Soteria Lab		2024	0.8
25	Edamame		2024	0.4
26	Alphaguard		2024	0.2
27	LookUp Space		2024	
	Total ACN			**209**

2025

	Company	Organisation	Year	Amount (M€)
1	Riot		2025	27.7
2	Sekoia.io	**ACN**	2025	25
3	Cryptio		2025	15
4	CyGo Entrepreneurs		2025	5
5	Akidaia		2025	1.3

3.7 THE EMERGENCE OF A STRONG ECOSYSTEM OF DIGITAL TRUST MICRO-ENTERPRISES

As shown in the infographic below, the French Digital Trust ecosystem is built around large historical players, often from the digital security and/or digital services sectors, and often linked to the sovereign and defence ecosystems. These major historical players, who are strong exporters, have offers geared towards governments, Operators of Vital Importance (OIVs), and large international companies. They represent €17.3 billion in revenue in 2024.

However, an ecosystem of Micro-enterprises specialized in Digital Trust started to emerge in the 1990s. During the decade of the 2010s, this ecosystem gradually grew in importance and now includes many large SMEs, some of which have already exceeded the €50M revenue mark and have become Intermediate Size Enterprises (ISEs) with an international focus.

This ecosystem is composed mainly of cybersecurity startups, many of which have offers aimed at addressing new markets such as Micro-enterprise/ SMEs and small local authorities. The strong growth of this ecosystem is driven by fund-raising for increasingly large amounts year after year. This ecosystem represents an estimated revenue of between €2.5 and €3.5 billion in 2024 (adding together Micro-enterprises with a revenue of more than €5 million, companies that have raised funds of €5 million or more, and Micro-enterprises that have become ISEs since 2000).

Major historical players

17,3 Mds € in 2024

Emergence of a strong ecosystem of SMEs

2,5 to 3,5 Mds € in 2024

Note : The companies whose logo is present in the box on the SME ecosystem correspond to the most remarkable: ISEs, companies that have benefited from the largest fundraising or SMEs with the largest turnover.

POINT OF VIEW

HENRY MARCOUX

• GENERAL MANAGER

TIKEHAU CAPITAL

“ The year 2024 saw a spectacular overall rebound for the cybersecurity investment sector, with amounts invested up 30% on 2023 to €12.1 billion, corresponding to 687 funds raised in the USA, Israel and Europe. After a decline in cybersecurity investment in 2023 due to an unfavorable economic climate, investor interest is growing.

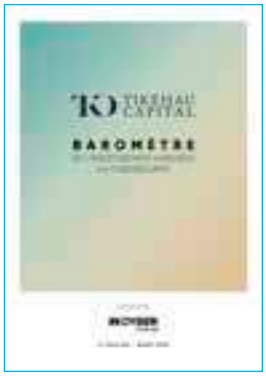
The United States confirms its dominance with massive fund-raising and sustained momentum in advanced financing rounds (Series C, D, and E), while Israel suffers a sharp drop in investment, impacted by geopolitical tensions.

Europe maintains a significant share of 25% of total amounts raised, and over the past decade, the European cybersecurity market has continued to assert itself as a key investment opportunity, with a 1.6-fold increase in the number of rounds and a 12.5-fold increase in amounts invested. These trends bear witness to a changing sector, which remains attractive despite a complex global economic context, and confirm the market’s shift towards financing more focused on companies in an advanced growth phase.

With €342m in amounts raised and 25 rounds of financing in 2024, France is demonstrating its resilience and retaining its singularity in the European cybersecurity ecosystem by occupying first place in Europe in amounts raised, ahead of the UK.

Lastly, the sector’s consolidation momentum accelerated in Europe in 2024, with 134 European cybersecurity companies acquired, 71% of them by European players, a notable 19% increase on 2023. In France, 12 acquisitions took place, 92% of them by French companies. ”

Tikehau Capital, a global alternative asset management group with €49.6 billion in assets under management (as at 12/31/2024), has become one of Europe’s leading players in cybersecurity investment since 2019. In particular, Tikehau Capital’s portfolio in the cybersecurity and trust technologies fields includes the following French holdings: ChapsVision, Claranet, Egerie, Ekimetrics, Glimps, QuarksLab, Oodrive, ProvenRun, Tehtris, TrustInSoft, Trustpair, Yogosha.



The main trends in cybersecurity investment revealed by **the 6th edition of the barometer published by Tikehau Capital** in partnership with InCyber Forum.

available at the following link:
https://urlr.me/h6BRMC

“ Investment in cybersecurity in 2024 ”

“ France leads European countries in amounts raised. ”

+ 30%
Investment in cybersecurity in 2024

25%
of amounts raised in Europe in 2024

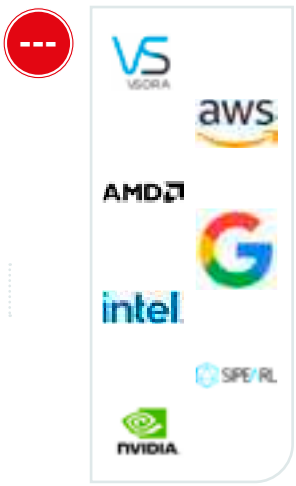
1st european rank
of amounts raised

4. TRUSTED AI: CHALLENGES AND PROSPECTS FOR THE FUTURE

4.1 THE ARTIFICIAL INTELLIGENCE VALUE CHAIN

Trusted Artificial Intelligence makes its appearance in 2024 as a new segment of the French digital trust industry, alongside digital security and cybersecurity products and services.
This chapter positions the French industry along the Trusted Artificial Intelligence value chain (1), distinguishes between general-purpose AI and specific AI in terms of data requirements (2) and value creation for the French industry (3). Finally, this chapter outlines the prospects for structuring a French trusted cloud industry to serve the French specific trusted AI industry.

Positioning of the French industry along the artificial intelligence value chain



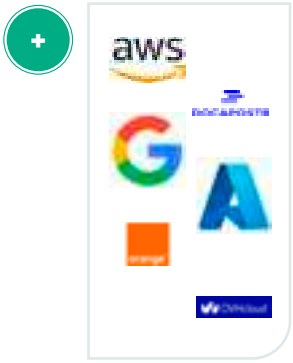
Processor manufacturers: structural dependence on American players

Artificial intelligence production relies upstream on manufacturers of the specialized processors - GPUs, NPUs, ASICs, etc. - needed for training and model inference. This segment is dominated by American companies such as NVIDIA, AMD and Intel.
These companies, often fabless, focus on the electronic design of chips, which they then have produced in foundries, mainly in Asia, notably at TSMC in Taiwan. Hyperscalers such as Google and AWS are investing in this segment by developing their own chips (TPU, Trainium).
France is virtually absent from this critical stage. A few rare fabless companies such as SiPearl, VSORA and Kalray are trying to position themselves, but the ecosystem remains modest and nascent. The major European semiconductor producers (ST Micro, NXP, Infineon) are concentrating on embedded markets (automotive, aerospace, defense, etc.), and are not aiming to invest to compete with the American giants in artificial intelligence chips.

Data center equipment manufacturers, supercomputers, etc. a limited French presence

The hardware segment - high-performance servers (HPS) and supercomputers - is dominated by American and Chinese players such as HP, Dell, IBM and Lenovo. These players source processors from manufacturers to assemble infrastructure solutions tailored to the needs of artificial intelligence. The two French players playing a significant role in this segment are Atos - through its Bull subsidiary - and, to a lesser extent, OVH. These two companies design the architecture of their servers and assemble them. However, this French presence remains isolated and fragile in a sector where international competition is intense. French capacities are far from matching those of the major American and Chinese manufacturers.

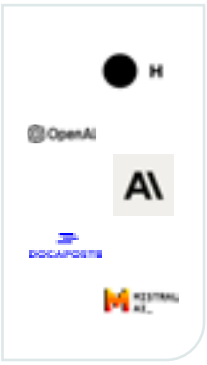
Note : This visual shows the most emblematic French or foreign players in each segment. Consequently, the absence of a company's logo in a segment does not mean that it is absent from that segment.
For example, Thales is positioned in the AI publishers, ESN and integration segments.
Source : DECISION Études & Conseil



Cloud service providers : a market dominated by hyperscalers

Cloud service providers offer the infrastructure needed to train and deploy artificial intelligence models. The world leaders - AWS, Microsoft Azure, Google Cloud - have massive computing capacities and offer their own AI technology bricks (GPT, Vertex AI, Azure OpenAI, etc.), becoming both hosters and publishers. France is attempting to build an alternative ecosystem, with players such as OVHcloud, Numspot, Outscale, Docaposte, Platform.sh and Scaleway. These initiatives offer a sovereign alternative to American solutions, although for the time being they remain far from the capabilities of hyperscalers.

generative AI



Artificial intelligence publishers: a fast-growing French dynamic

Publishers develop software solutions based on artificial intelligence, most often marketed as application services (SaaS). This segment covers two main categories of players:

- Generic model vendors, who design fundamental models (LLM, diffusion, etc.), intended to be used or adapted in a variety of contexts,
- And business solution vendors, who develop customized models to meet specific needs in each sector.

In France, Mistral AI - which develops open source LLMs for general use - is one of the few players in the first category.
In the second category, we find several French companies that design their own models adapted to specific data and problems: Shift Technology (insurance fraud), Gleamer (radiology), Exotec (logistics robotics), Dental Monitoring (orthodontic monitoring), and Wintics (video analysis for cities and infrastructures).
These solutions are sometimes based on the adaptation of external models but are always conceived as products.Internationally, we can observe a similar structuring: generalist model editors such as OpenAI, Anthropic or Cohere, and specialized editors such as Tempus (healthcare), Darktrace (cybersecurity), Trax (retail intelligence), or SambaNova (scientific and industrial analysis).

specific AI

Digital services companies (DSC)

DSC's play a key role in the practical deployment of artificial intelligence in companies. They develop customized models, based on their customers' data, information systems and business objectives.
They also provide integration, consulting and support in the implementation of artificial intelligence. France boasts a very solid network, with companies such as Sopra Steria, Capgemini, Atos, Thales, Orange Business and Wavestone.

Integrators

Integrators provide the link between technologies (models, software, APIs, etc.) and concrete business use cases, particularly in industrial or sovereign sectors. They deploy solutions in specific business environments, often combining them with other technology bricks or embedded systems. These players play a structuring role in the dissemination of artificial intelligence within the economic fabric, by integrating it directly into complex systems or equipment. Thales, Airbus Defence & Space, Idemia and Safran are just some of the major integrators in the digital trust sector. France also has major integrators in other sectors (energy, automotive, healthcare, etc.).

4.2 ARTIFICIAL INTELLIGENCE FOR GENERAL OR SPECIFIC USE : DIFFERENT DATA REQUIREMENTS

General-purpose artificial intelligence is mainly made up of generative AI solutions, and refers to models capable of producing new content - text, images, sound or video - from textual, visual or vocal instructions. These models, such as LLMs (Large Language Models) or SLMs (Small Language Models), are pre-trained on huge volumes of general-purpose data. They can then be adapted to different uses: text generation, information classification, planning, product or service recommendation, or even chatbots and virtual assistants. The French industry has several players positioned in this segment:

• **Mistral AI** is the emblematic French startup specializing in the development of general-purpose open source LLM models, used for generation and dialog tasks.

• **DALVIA Santé** is Docaposte's medical assistant based on generative AI, enabling hospitalization reports to be produced from audio notes and documents from the patient's history. Hosted on the NumSpot sovereign cloud, the solution is designed to guarantee data security and to integrate with hospital business software. Its aim is to save time for healthcare professionals, while improving coordination between the various players involved.

• **Assist'Act** is Docaposte's administrative document drafting tool for local authorities, featuring a conversational assistant based on artificial intelligence. It enables the generation, search and optimized management of public documents.

• **IRIS**, developed by Sopra Steria in partnership with IBM and IVèS, is the first conversational assistant in sign language. This " signbot " enables real-time interactions in LSF, LSQ, LSA and LST, by combining conversational AI (via IBM Watson) and accessibility solutions developed by IVèS.

Specific artificial intelligence, on the other hand, refers to solutions designed for specific use cases in defined business environments. These AIs are based on highly targeted input data (texts, sounds, images, videos, signals, time series, etc.) and are trained on more limited but highly qualified volumes.
They can be used, for example, to automate document reading, detect visual anomalies, predict breakdowns or detect risky behavior.
The French industry boasts many very well-positioned players in this segment:

• **Safran AI** develops algorithms for the automatic analysis of high-resolution satellite images, full-motion video and acoustic signals. These solutions, designed for the defense sector, enable the detection of objects or events of military interest. They are based on a secure processing chain, with full data traceability, and are designed to be integrated into mission-critical systems.

• **Gleamer** offers a solution for analyzing bone lesions from medical images, and generates an automated pre-diagnosis for radiologists. The practitioner retains control over the validation of the report. The solution is deployed in over 50 hospitals and clinics in France, including Hôtel Dieu and Ambroise Paré, and was awarded the Best New Radiology Vendor Award at Eurominnies 2023.

• **Wintics** offers intelligent video analysis solutions to improve infrastructure safety, traffic flow and urban planning. These tools enable local players (airports, ports, public transport operators, local authorities, etc.) to make decisions based on the analysis of behaviors, flows or anomalies detected in public spaces.

Data requirements vary according to whether we're talking about generative or specific AI. Generative AI relies on access to immense volumes of heterogeneous data, often from the web or large textual corpora. The aim is to maximize data coverage and diversity, enabling models to learn how to generate relevant content in a wide range of contexts. This Big Data approach raises major challenges in terms of access to large sets of data in order to remain competitive with American or Chinese solutions - particularly in the sensitive sectors of healthcare, education and transport.

Specific AI, on the other hand, relies on targeted, highly qualified business data. These models are designed for restricted use cases, and require smaller datasets that are perfectly structured, annotated and contextualized. The emphasis is on data quality, rather than quantity. In this context, training can often be carried out locally, without massive computing infrastructure.

One example is Safran AI, whose teams include specialized analysts responsible for manually annotating the satellite images used to train the algorithms. This human annotation guarantees maximum accuracy, enabling the models to finely distinguish objects or anomalies of interest. This iterative approach, based on data quality and business expertise, limits the need for massive infrastructures, while ensuring high performance in critical contexts such as defense or security.

4.3 SPECIFIC AI GENERATES MORE VALUE THAN GENERAL-PURPOSE AI IN FRANCE

Within the framework of this Observatory, the analysis of artificial intelligence production in France focuses on "trusted" artificial intelligence, i.e. artificial intelligence designed and deployed in compliance with a set of legal, technical and ethical criteria. This notion combines the principles defined in the Alliance for Digital Trust (ACN) white paper - transparency, explicability, robustness, security, respect for privacy, human control - with a dimension of sovereignty, by integrating the notion of corporate nationality.

Despite the media and financial hype generated by generative AI - particularly since the emergence of LLMs like GPT or open source models like Mistral AI - specific AI accounts for 82% of sales generated from France in 2024 (€1.3 billion), compared with just 18% for generative AI (€280 million).

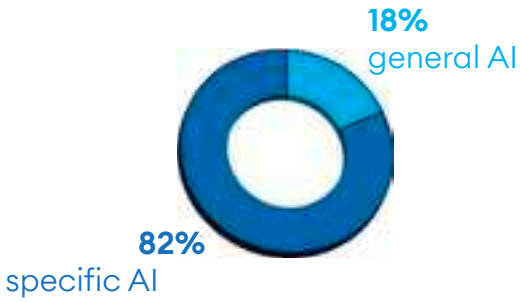
This gap between visibility and economic reality can also be seen in fund-raising. If we consider only the main rounds of financing carried out in 2024, generative AI has concentrated more than €820 million in investments, led by players such as Mistral AI (€1.09 billion since 2023, €600 million in 2024), H Company (€200 million), Dust (€20 million), or Lighton (€12 million). Conversely, although more numerous and active in a wide range of use cases, companies focused on specific AI have raised more modest amounts : just over €130 million in total for the main rounds.

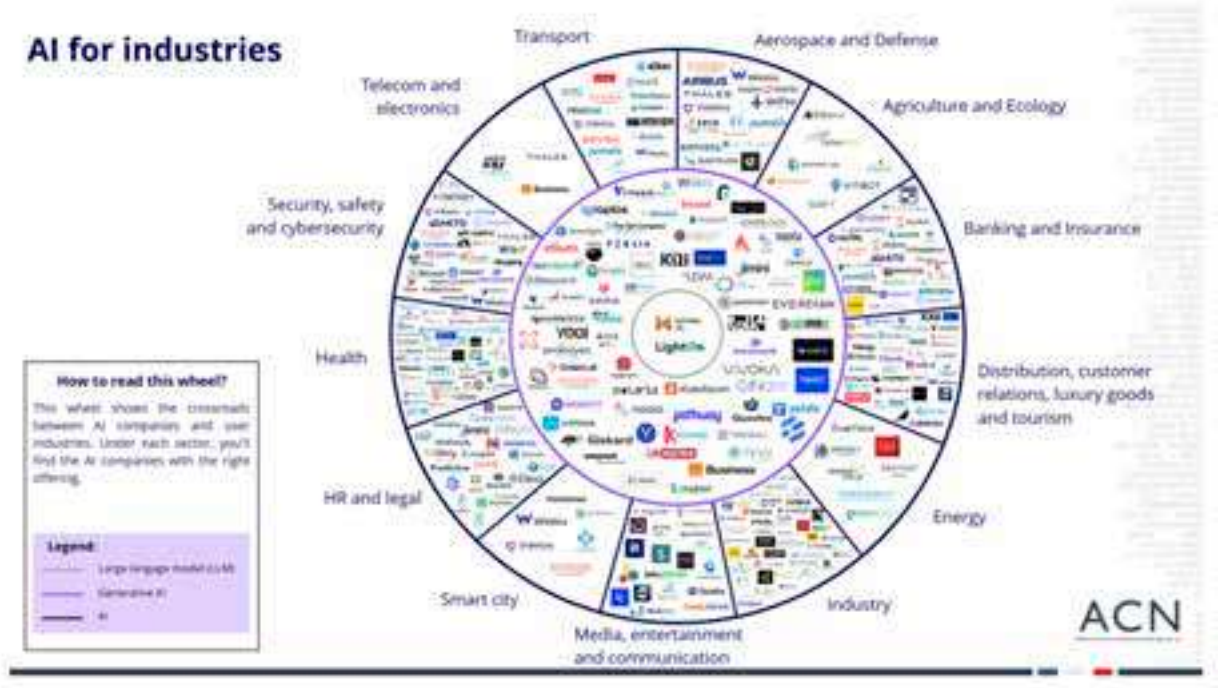
These include Photoroom (€59 millions), Gleamer (€36 millions) and Pollen Robotics (€24 millions).

Finally, this observation is echoed in the financial analysis of French AI startups. In 2024, the immaturity of business models was particularly pronounced among generative AI publishers, with a much wider gap between fundraising and sales than among specific AI publishers.

Beyond this, the trust AI segment remains immature overall in 2024, with average sales per employee much lower than in other digital trust segments (€92,000).

Proportion general AI / specific AI





4.4 TRUSTED CLOUD AND TRUSTED AI: OPPORTUNITIES FOR THE FRENCH INDUSTRY

There is a division in the trusted AI value chain between:

- **A generative AI value chain,** which raises ethical and technical issues linked to access to the largest possible data sets, and in which the American Hyperscalers appear difficult to circumvent.

- **A specific AI value chain,** which requires access to specific data available to many French integrators, and whose sensitivity makes it essential to use trusted French cloud players. By 2024, this second value chain will account for 82% of the French industry's sales and will be one for which end-to-end control is feasible.

Although mastering the value chain of generative AI promises to be an uphill battle, the prospects for value creation - in France and abroad - for the French industry today seem to lie in the structuring of an integrated "trusted cloud dedicated to a specific trusted AI" offering.

5. CURRENT STATUS OF ONLINE THREATS

5.1 ANSSI 2024 THREAT PANORAMA

The ANSSI's 2024 annual report highlights an intensification of the cyber threat, marked by three dominant axes: conjunctural opportunities (Paris Olympic Games), persistent technical vulnerabilities, and the increasingly industrialized means of attackers, whether state or cybercriminal.

ANSSI 2024 threat panorama

available at the following link:
urlr.me/Zpqtk3

The year was marked by major events such as the Paris Olympic Games, which were the catalyst for numerous cyberattack attempts. Although none of the attacks prevented the competitions from taking place, the number of espionage, destabilization and extortion operations was significant, particularly in view of the tense geopolitical context.

One of the most striking findings concerns the exploitation of vulnerabilities in security equipment, notably VPN gateways and firewalls. These devices, exposed on the Internet, have become privileged points of entry for attackers. The report highlights the fact that known vulnerabilities are sometimes exploited several months after patches have been released, underlining a lack of responsiveness in risk management within organizations.

Supply chains, another sensitive area, are targeted for their rebound potential towards strategic targets. Attackers exploit relationships of trust and interconnections between companies and service providers to gain access to end-user systems.
The case of the attack against a French manufacturer through a subcontractor perfectly illustrates this latent threat.
The attack did not result in lateralization but demonstrates persistent attempts.
The report also highlights the rise of cyber mercenarism and the commercialization of large-scale offensive capabilities. State actors and cybercriminals are increasingly using the same infrastructures, open-source tools and even ransomware, making attribution difficult.
The ADINT phenomenon, exploiting advertising flows for surveillance or espionage operations, opens worrying new prospects for the cybersecurity of citizens and businesses.

Finally, attacks are multiplying according to three main logics: profit-seeking (ransomware, data extortion), strategic intelligence (espionage targeting telecoms and institutions), and destabilization (sabotage, DDoS, influence operations). ANSSI calls for a general strengthening of supervision, increased IS security and greater responsiveness to published vulnerabilities.
The next few years will see a growing demand for cyber resilience, for both public and private entities.

“ Attackers linked to the cybercrime ecosystem or reputedly linked to China and Russia are the top three threats. ”

“ In 2024, attacks aimed at destabilization increased, particularly by hacktivist groups. ”

4386

security events handled by ANSSI in 2024, an increase of 15 % on 2023.

50% +

more than half of the ANSSI’s cyberdefense operations were triggered by the exploitation of vulnerabilities in edge equipment.

x2

the number of distributed denial-of-service (DDoS) attacks doubled in 2024 compared to 2023, with increased activity during the Paris 2024 Olympic and Paralympic Games period.

For the first time, France officially attributes cybercriminal activities (APT28) to Russian intelligence services !

In April 2025, the French government, through the Ministry of Europe and Foreign Affairs, for the first time attributed criminal activities (APT28) to Russian intelligence services. In a communication dated April 29, 2025, the Ministry states that “ France condemns in the strongest possible terms the use by the Russian military intelligence service (GRU) of the APT28 attack modus operandi, which is behind several cyberattacks against French interests» and adds that «since 2021, this attack modus operandi (AMO) has been used in the targeting or compromise of around ten French entities.

These entities are players in the lives of French people : public services, private companies, as well as a sports organization linked to the organization of the 2024 Olympic and Paralympic Games. In the past, this modus operandi has also been used by the GRU in the sabotage of the TV channel TV5Monde in 2015, as well as in the attempt to destabilize the French electoral process in 2017. ”

The APT28 attack modus operandi against French entities since 2021 has been described in a technical document drawn up on the basis of findings by the Cyber Crisis Coordination Center (C4), which in its technical-operational form brings together ANSSI, DGSE, DGSI, COMCYBER and DGA. Ministries, companies in the defense sector, think tanks, entities involved in the organization of the JOP24...

The recent French targets of APT28 are numerous, and mainly aimed at spying or even destabilization.

5.2 INSIGHTS FROM INDUSTRY EXPERTS

Maxime ALAY-EDDINE
CEO

2024: a record year for vulnerabilities

“The year 2024 stood out with over 40,000 new entries in the CVE database. Faced with this avalanche - more than 100 vulnerabilities a day! - it is crucial to adopt a clear, actionable prioritization strategy to prevent teams from drowning in information. CISOs can rely on modern approaches such as 3D prioritization, which combines the analysis of technical scores (CVSS, EPSS) with official data from recognized authorities (ANSSI’s CERT-FR, CISA KEV in the USA). Easy to automate and integrate, these methods can eliminate up to 90% of vulnerabilities that have not been identified. This frees up teams to focus on the real threats: good vulnerability management means capturing the signal and eliminating the noise.”

Roland ATOUI
CEO

IoT manufacturers: facing cyberthreats and new obligations

“Connected objects are invading our daily lives, but behind this innovation lie new threats. In November 2024, the Matrix group exploited poorly secured devices to carry out massive DDoS attacks. With the RED Directive (2025) and the Cyber Resilience Act (2027), manufacturers and notification bodies face stringent security and certification requirements. CyberPass, our SaaS platform, enables them to automate and simplify the compliance of connected products, while reducing costs, effort and time.”

Frédérique BAJAT
Product Owner Surveillances et Remediations

The importance of protecting yourself against the growing practice of cybersquatting

“Cybercriminals are increasingly using domain names to carry out their attacks, often registering legitimate-looking names to facilitate the perpetration of fraud. The targeted company is exposed to financial losses, reputational damage and security risks. This practice, known as cybersquatting, is proving very easy, and is marked by the growing use of new generic extensions (poker, .music, .paris...). The challenge for companies is to protect their customers and their brand by securing their domain names, at the risk of weakening their image. It is therefore essential to put in place monitoring strategies to detect fraudulent domain names as early as possible, and to react with appropriate measures in the event of usurpation.”

THALES

Walter CAPILATTI
VP Cybersecurity Premium Services Business Line Thales

A rapidly changing cyber landscape, characterized by the sophistication of attack strategies

“In 2025, our global Cyber Threat Intelligence (CTI) team Thales predicts a sophistication of attacks and the increased integration of artificial intelligence into attackers’ procedures. Key trends include the rise of ransomware campaigns, supply chain risks and the exploitation of vulnerabilities related to connected objects and physical equipment. Organizations need to adopt a holistic cyber approach by monitoring their IT and OT infrastructures through Security Monitoring Centers. They need to develop incident response strategies, supported by threat intelligence via cyber intelligence services to proactively identify vulnerabilities and reinforce their security posture.”

iDAKTO

Stéphane CAUCHIE
Security Innovation Officer

Proactive identity protection in the face of fraud

“In 2025, cybercriminals will continue to adapt and refine their techniques, exploiting the vulnerabilities of traditional authentication systems and the advanced capabilities of AI to bypass existing protections. With the democratization of identity wallets, a new approach to user protection is emerging. A proactive Wallet integrating advanced fraud detection mechanisms is an innovative approach. Thanks to real-time analysis of suspicious behaviour, these solutions aim to anticipate and neutralize attacks before they affect the user, while guaranteeing confidentiality. In the face of increasingly sophisticated attacks, innovation remains our best defense.”

Phragma

Frédéric CERCLET
Manager

The rise of digital identity fraud: the challenges of uniform, interoperable security

“Identity theft continues to progress, keeping pace with technological advances that make these attacks increasingly accessible to cybercriminals. This phenomenon is particularly evident in the growing use of deepfakes, designed to bypass facial recognition authentication systems or make online scams more credible. The development of regulatory and technical frameworks is fundamental to the development and credibility of the digital identity market. Progress has been made, such as PVID certification, while the adoption of the EUDI Wallet scheduled for 2026 represents a promising step forward, offering new uses to citizens while guaranteeing control of their data thanks to the ZKP principle.”

rubycat

Jonathan CLAIREMBAULT
CTO

Achilles heel: the supply chain

“The numerous disclosures of personal data in recent months, combined with the rise of AI-assisted social engineering, will intensify the risk to the supply chain. What’s more, in this international context where the cards have been reshuffled, we can expect state-sponsored attacks assisted by certain suppliers. In the face of this, digital sovereignty, training, third-party supervision, zero-trust and behavioural analysis will be essential to secure the digital ecosystem.”

AIRBUS

Benjamin COSTÉ
Cybersecurity researcher

The rise of the information threat

“ Digital infrastructures are no longer the only targets of the attackers who now threaten our brains. As recent events (elections in Romania, overload operation against journalists, RRN campaign targeting European media, etc.) show, the threat is becoming more widespread and intense. The challenges are immense: hybridity of cyber and informational modes of operation, democratization of generative AI that blurs our relationship to information, management of the human factor... In response, the defense industry is struggling to structure itself, notably because of the multiple fields of expertise involved (IT, law, psychology, geopolitics, etc.). This process of global change is set to continue until 2025, with calling for a global effort in adaptability and resilience. ”

board of cyber

Luc DECLERCK
General manager

Controlling third-party risk : the key challenge of NIS 2 and DORA

“ With NIS 2 and DORA, the evolution of the regulatory framework comes as no surprise in response to an acceleration in the state of the threat, with a growing number of successful cyberattacks involving the compromise of a third party (supplier, partner, customer). Faced with this reality, it is urgent to offer efficient solutions, capable of helping organizations and businesses to scale up their control of third-party risk. ”

sekoia

François DERUTY
Chief Intelligence Officer

Edge equipment: a prime target for threat actors

“ In recent months, a notable trend in cybersecurity has been the intensification of attacks targeting edge devices, illustrated by threats such as Volt Typhoon and PolarEdge. Led by sophisticated groups of attackers, they particularly target devices produced by smaller players in the industry.
Cybercriminals exploit AI to conduct automated recognition of vulnerabilities present on these mid-range devices, enabling them to deploy malicious infrastructures more effectively. This trend underlines the urgent need for companies to reinforce the security of their peripheral devices, to ensure extensive supervision of their information systems, and to ensure the resilience of their supply chain. ”

unumkey

David DUBUS
President

The need for a systems approach to cybersecurity

“ Long considered a technical issue, recent years have seen the human factor being considered, as it is essential for optimal information systems security coverage. However, this rebalancing, however necessary, must not overshadow the need to continue identifying vulnerabilities in deployed services and applications. In addition to these two inseparable pillars, it is vital to set up governance: the only way to check that’s level of cyber maturity is in line with the objectives set. ”

Khadija HUEBRA
Executive Vice President

When phishing is AI-powered, DMARC is the bulwark of choice

“According to ANSSI, phishing accounts for the largest proportion of cyber incidents recorded by French companies. Its strike force is now reinforced by the capabilities of generative AI. Digital identity theft is therefore becoming a major strategic challenge for companies, whose reputations can be damaged. Given this situation, the implementation of a rigorous DMARC protocol is imperative. There is an urgent need to support security experts by analysing DNS configurations and identifying vulnerabilities likely to be exploited, while providing precise recommendations for strengthening domain security. In the face of diversified and sophisticated threats, proactively securing digital identity is becoming essential.”

Philippe LOUDENOT
Director of cybersecurity strategy

Your data, a crucial issue

“Your data is a treasure trove of valuable information that needs to be protected. Yet every day, sensitive data is transferred and exchanged without protection. French, sovereign solutions designed to meet corporate requirements for security and confidentiality of sensitive data do exist. Combining ease of use, advanced security and regulatory compliance, they offer a reliable alternative to traditional file transfer tools, while guaranteeing optimum protection of exchanges. Choosing them means opting for solutions that protect your data, comply with European regulations and give you total peace of mind when managing your sensitive files.”

Philippe LUC
CEO and Co-Founder

Human vulnerabilities: the primary attack vector

“The cyber threat is evolving rapidly, with the rise of automated social engineering. Cybercriminals are using AI to orchestrate sophisticated attacks exploiting all aspects of digital identity, both professional and personal. 70% of executives’ exposure comes from their personal lives and those around them! These attacks can range from presidential fraud to information manipulation via DeepFakes. It is therefore essential for organizations to involve their teams in a tool-based digital footprint protection approach: with a triple benefit: protecting companies from attacks, protecting employees from personal fraud and complying with NIS2 regulations.”

Jean-Yves MARION
Professor

AI Cyberoffensive: Autonomous Cyber Weapon Systems

“The objective of the M32 autonomous agent is to infiltrate a high-tech company; it embeds the latest updates and can be considered one of the most advanced Autonomous Cyber Weapon Systems (ACWS). M32 studied its target and launched the attack. After several weeks of infiltration, the M32 agent exfiltrates relevant information and corrupts sensitive data. AI’s capacity for analysis, generation and decision-making makes it possible to envisage the construction of SACA, like the fictional M32 agent. cyberattack campaigns could then be fully automated, amplifying the number of attacks, their speed of execution, and amplifying the consequences and damage.”

Catherine NOHRA CHINA
CEO

Securing supply chains to protect against cyberthreats

“The IT threat in 2024 will affect the entire supply chain (suppliers, partners and subcontractors). This supply chain is increasingly targeted by cybercriminals, who exploit vulnerabilities in one link to gain access to the systems and data of another. In most cases, attack techniques target data and access rights, exploiting misconfigurations. Identifying and assessing the risks associated with partners and subcontractors is therefore becoming more than crucial for better protection, and this is one of the aims of the NIS 2 directive, which aims to reinforce supply chain security through the implementation of security controls, including audits and contractual requirements.”

Benoit PARIZET
Executive Vice-President - Public Sector

Putting digital trust back at the heart of public uses

“Data is at the heart of the transformation of public action. The uses it enables are manifold: optimizing business processes, strengthening budgetary control, improving relations with users, facilitating the allocation of public subsidies... But they are not without their challenges. First and foremost: the protection of data, which is often sensitive. From collection to storage and processing, every stage in the data value chain must be mastered. Smaller, and often less protected, local authorities are particularly at risk. Although the French government widely encourages the use of the cloud, through the “Cloud at the center” doctrine, which aims to reinforce security, this approach is neither an obligation for small local authorities, nor a guarantee of the protection of their data. It is therefore essential that departments handling sensitive data, whatever the size of the administration concerned, give preference to SecNumCloud-certified solutions, to ensure the highest level of security and guarantee digital confidence in our public services.”

Dr. Florin PAUN
President Co-Founder

The sovereignty of our industries and societies depends on access to relevant data

“The future of our industries will be built on relevant and reliable data, or no future at all! Industrial sovereignty is built on innovative solutions for accessing relevant data and reducing the flow of false and biased data in all uses of AI. The quality and relevance of data cannot be imposed on all stakeholders, but is the result of cognitive processes, of innovative abilities to democratically integrate all the diversity of opinions and perceptions of data impacts in a highly inclusive process, thanks, for example, to the new typology of Qualificative AI - QuAI, recognized by the scientific community having completed the Condorcet Paradox and the Arrow Theorem.”

Caroline RESTOUX
Manager & Lead Consultant
Compliance & Governance
Cybersecurity

2025: a strategic year for information security managers

“In addition to dealing with threats that are constantly evolving in terms of both number and type, organizations are faced with an ever-increasing number of strategic and regulatory challenges. NIS2, DORA, CRA, IA Act, or the subcontractor certification project currently being studied by the CNIL: the year 2025 promises to be rich and compliance-oriented! These various regulations are forcing organizations to take a multi-referential approach to security. A good basis for implementing all these regulations? Implementing ISO/CEI 27001 by taking risks into account, and in a continuous improvement approach.”

Bertrand SERVARY
CEO

Regaining control over our technological dependencies

“Recent crises - health, energy, geopolitical - have revealed an undeniable fact: technological dependence is a systemic vulnerability. In 2025, many organizations will still find themselves captive to infrastructures, software or services developed outside their sphere of sovereignty. This dependence conditions our ability to protect data and ensure business continuity. Regaining control means identifying the critical points in the digital value chain, supporting European alternatives and investing in long-term independence. This is not a matter of technological retreat, but of emancipation. Digital sovereignty begins with the ability to choose freely, without external constraints.”

FOCUS DOCAPOST-CYBLEX CYBERSECURITY BAROMETER 2024

This national barometer was born of a desire shared by Docaposte and Cyblex Consulting to measure the evolution of cyber maturity in companies and public organizations, year after year.
The results are based on telephone interviews conducted in 2024 with over 450 respondents, 27% of whom work for the public sector and 53% of whom are IT specialists.
Results and comparison with the first edition.

Docaposte cybersecurity barometer - Cyblex 2024

available at the following link:
urlr.me/RXcF89

The 7 key findings of the Docaposte-Cyblex 2024 barometer:

1. Companies feel more at risk than last year (+10pts)
The risk varies according to company size and sector of activity:
The top 5 sectors that feel most at risk are : finance, administrative services, accommodation and catering, water and electricity production services, and the public sector.
The larger the company, the more exposed it feels (29% between 50 and 249 employees vs 57% over 1000 employees).

2. Efforts to reduce risk are on the increase (+8 pts)
Budget disparities can be observed depending on the size of the company or organization. 2/3 of companies are increasing their cyber budget:
• An increase that concerns many more companies than in the last edition (+21 pts).
• An increase driven by companies with over 50 employees.

3. The number of cyber-attacks is higher than in 2023 (+11 pts), with 1/3 of respondents saying they have been the victim of a cyber-attack in the last 12 months.
Attack typologies vary according to company size, reflecting the professionalization of attackers and the implementation of targeted actions.
From now on, the 1st impact is no longer data theft, which was in the lead in 2023, but the blocking of information systems (18%):
• VSEs and SMEs suffer from phishing (33%) and ransomware (27%).
• ETIs and large corporations suffer more from: president scams (3 times more than other types of company) and DDOS denial-of-service attacks.

33% Phising

27% Ransomware

24% Theft/loss of data

4. Doubts about the effectiveness of actions remain unchanged from last year, with 1/3 of companies having no confidence in the actions implemented.

The top 3 actions undertaken are:
• Secure workstations,
• Regular software updates,
• Reinforced password mangement.

The strongest increases were:
• Physical access security,
• Securing the corporate network,
• Securing workstations,
• Les exigences vis-à-vis des fournisseurs.

5. Corporate interest in a sovereign system is clearly on the rise, with 52% of respondents considering it important or very important to have a sovereign solution (vs. 20% in 2023). More than companies, public sector players consider the sovereignty of solutions to be " very important ".

6. Support from a specialized partner is becoming the norm: 2/3 of companies say they call on an outsourced resource, reflecting the fact that cybersecurity is a real area of business expertise.

7. The cloud is still outside the scope of cybersecurity for the majority of companies: only 1/3 of companies extend their cybersecurity actions into the cloud.

Olivier Vallet

Chairman and Chief Executive Officer of Docaposte

“ Digital technologies are at the heart of social, geopolitical, environmental and economic issues.

These major developments are accompanied by a rise in cybercrime, which today represents a pressing challenge for all players.

While the reality of this threat is now indisputable, large entities have reacted accordingly by investing massively in their security and integrating cutting-edge technologies to anticipate and counter cyberattacks.

However, smaller players such as VSEs, ETIs and local authorities, lacking the necessary resources and expertise, find themselves helpless in the face of these challenges. The subject of cybersecurity will become even more crucial with the rise of emerging technologies such as artificial intelligence. These innovations, while promising, broaden the attack surface for cyberthreats.

We need to support these less well-protected structures in order to limit our over-reliance on foreign technology giants to master cybersecurity infrastructures, especially when it comes to sensitive data. ”

Christophe Vendran

Chairman and CEO of Cyblex

“ Every year, the challenges of cybersecurity take on a new dimension, reflecting the growing complexity of an increasingly interconnected world. A notable disparity persists between large organizations, which are often well equipped, and very small businesses, which remain highly vulnerable.

This barometer invites all players to fully appreciate the importance of a proactive posture, so that cybersecurity becomes a lever of confidence and growth, rather than a hindrance.

Cyber threats now play a structuring role in essential sectors driven by rapidly expanding digital ecosystems.

Security grows when it is shared. Together, let’s share this knowledge and strengthen our resilience to the challenges of cybercrime. ”

6. MARKET TRENDS

6.1 GENERAL TRENDS

6.1.a. Growth in the French industry

The year 2024 confirms the slowdown initiated in 2023, following two years of strong growth. Overall annual growth reached 6.4% in 2024, a level similar to that of 2023 (6.8%), but significantly below the exceptional performances recorded in 2021 and 2022 (11.3%).

This deceleration is partly due to an uncertain economic and political climate. The year 2024 was marked by persistent budgetary pressures, early legislative elections, and a change in government–all of which negatively impacted public procurement decisions. Yet, the public sector accounts for a significant share of demand in the Digital Trust ecosystem, particularly among local authorities and smaller state structures.

Digital Security continues its muted trajectory: after moderate growth of 3.8% in 2023, the segment grew by 4% in 2024. The slowdown in large-scale projects related to identity and biometrics, combined with weaker public demand, contributed to this stagnation.

Cybersecurity posted stronger growth, though slightly down from the previous year: 9.2% in 2023, then 8% in 2024. The segment remains driven by products (software, hardware, secure elements), which increased by 9.2%, while services slowed to 6%, affected by clients' budget constraints in a tighter economic environment.

Among industrial players, the sector's leaders also reported more moderate growth in 2024. For example, Thales recorded around 1% growth in its digital identity business. A few exceptions stand out, particularly among emerging service providers such as Nomios and I-Tracing, which continue to post growth above the sector average.

The year 2022 remains a high point in the sector's recent trajectory, with overall growth exceeding 11%.

Cybersecurity returned to its long-term trend (11.5%), while Digital Security reached an exceptional level (11%), driven by major projects in identification and access control led by Thales, Airbus, IN Groupe and IDEMIA.

Several factors contributed to this momentum: a post-COVID rebound, price increases linked to the global semiconductor shortage (which positively impacted the value of secure products), and a favorable context shaped by rising geopolitical tensions, border security initiatives, and preparations for major events such as the Paris 2024 Olympic Games.

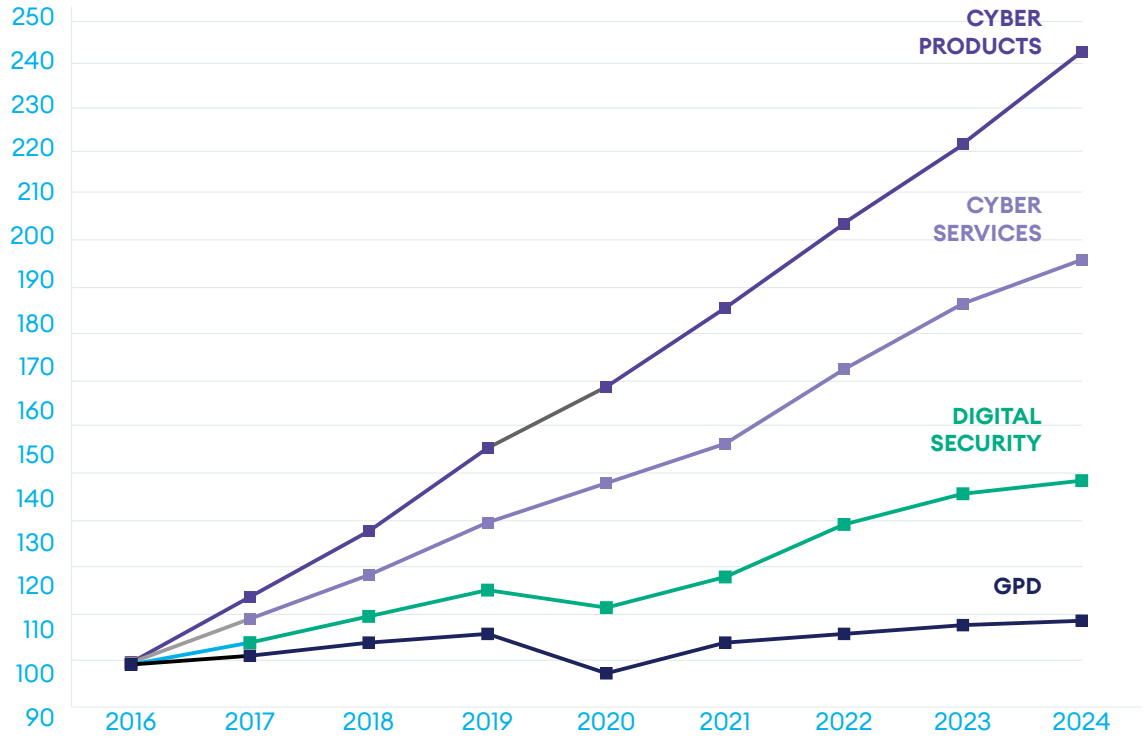
" Overall growth in the sector will stabilise in 2024 at around 6%. "

The graph below shows the comparative growth of the three main segments of the Digital Trust industry and GDP over the 2017-2024 period.

France growth comparison 2017-2024

Growth							
Segments	2018	2019	2020	2021	2022	2023	2024
Digital trust	8,2%	8,5%	3,6%	7,3%	11,3%	6,8%	6,2%
Cyber products	13,9%	14,0%	10,9%	8,8%	12,6%	9,0%	9,2%
Cyber services	9,9%	10,3%	5,8%	8,9%	10,3%	9,4%	6,6%
Digital Security	4,7%	4,8%	-1,7%	5,2%	11,0%	3,8%	4,0%
Trustworthy AI							9,3%
GPD	1,9%	1,8%	-7,8%	6,8%	2,5%	0,9%	1,1%

Source: INSEE, FMI pour 2024



Source : DECISION Études & Conseil

6.1.b. Markets in the industry

I / Markets in 2024

As the diagram shows, the public sector in the broadest sense, i.e. including transport and healthcare, accounts for almost a third of the French market (€6.3 billion in 2024), with the remaining two-thirds coming from the private sector (€13.3 billion). The weight of the private sector is set to grow year on year. The Digital Confidence sector was born out of the French government's need to secure its Vital Information Operators (VIOs/ OIVs). The need for digital trust then spread to large companies in general, beyond the OIVs. The current trend is to develop the market for SMEs and micro-enterprises, most of which are helpless in the face of the risk of cyber-attacks that now affect them, in particular the risk of being subjected to ransomware.

In addition to the public sector, which remains the leading market and a major growth driver, the banking/finance/insurance and energy sectors have been the main drivers of the industry for over three years, ahead of healthcare.

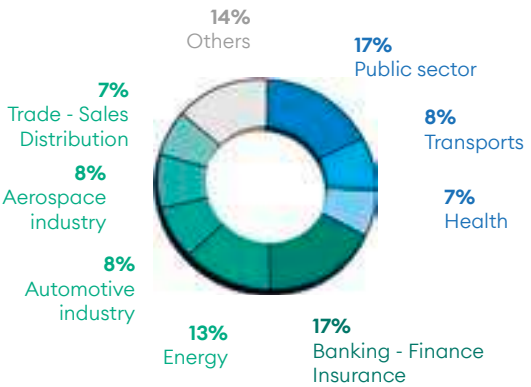
II / The emergence of a market for Micro-enterprise/ SMEs and small local authorities

The following series of diagrams, taken from the 2025 edition of the online survey of industry players, shows the segmentation of the French industry market according to the type of company supplying trust solutions (large-scale enterprise versus micro-enterprises / SMEs).

The French government, Vital Information Operators (VIOs/ OIVs) and large companies (excluding OIV) account for over 80% of the market for large companies in the sector, and nearly 80% of their growth prospects for the coming years.

These large-scale suppliers of trust solutions will account for 48% of the industry's sales in France in 2023 (77% if activities outside France are included). Here, we find the traditional markets around which the industry was built: the French government, OIVs and major private accounts.

Main markets for the industry in 2024



Source : DECISION Études & Conseil, questionnaire completed by companies in the industry from 2022 to 2025. Response in % of respondents weighted by their weight in the industry. The sample represents 8% of the industry in terms of sales.

In contrast, the State and the OIV only represent 19% of the market for SMEs and Micro-enterprises in the sector. Large enterprises (31%), Micro-enterprise/SMEs (28%) and local authorities (20%) account for the bulk of the market and growth prospects for SMEs and Micro-enterprises providing trust solutions in France. In other words, through this vision of SMEs and Micro-enterprises in the sector, we can see the emergence of two markets:

• That of local authorities, including small local authorities. By extrapolation, the market for small local authorities can be estimated at €3.5 billion in 2024.

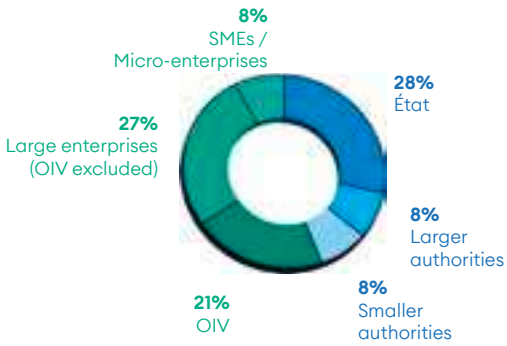
• But most of all, the development of the market associated with the need for trusted products and services from French SMEs and Micro-enterprises. By extrapolation, this market can be estimated at €3.3 billion in 2024.

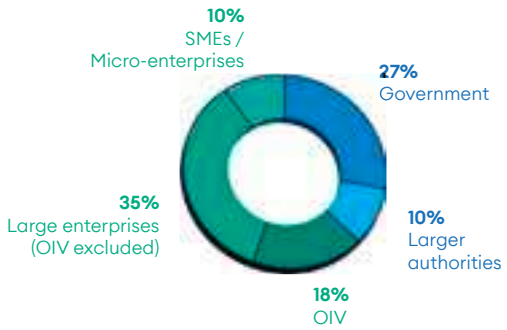
This market is characterized by dedicated offers: standardized offer, rapid deployment, low cost, often without hardware support, etc.

The development of this market for French SMEs and Micro-enterprises was slowed down in 2020 by the COVID crisis. Indeed, French SMEs and Micro-enterprises were more affected by the restrictions associated with COVID than the traditional large customers of the Digital Trust sector (State, IGOs, large companies), which are particularly focused on the supply of essential needs (Banking/Finance/Insurance, Energy, Health, etc.).

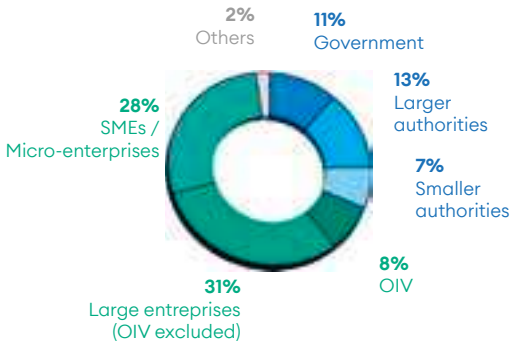
However, the structural trend is indeed towards the development of this SME and Micro-enterprise market, which is destined to become one of the major markets of the sector and will underpin its growth in the years to come.

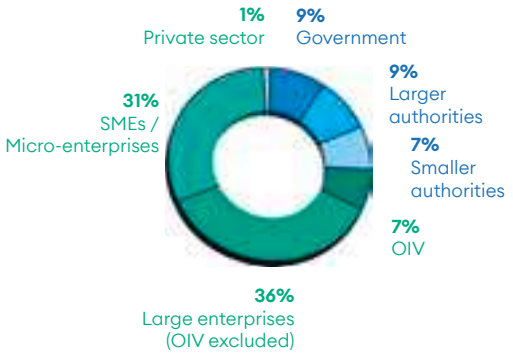
Large enterprises





Micro-enterprises / SME





Source : DECISION Études & Conseil, questionnaire completed by companies in the industry from 2022 to 2025. Response in % of respondents weighted by their weight in the industry. The sample represents 8% of the industry in terms of sales.

POINT OF VIEW

CHRISTOPHE HUSSON

• DIVISION GENERAL
• HEAD OF COMCYBER-MI

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

“ The *Alliance pour la Confiance Numérique* (ACN) plays a major role in structuring, coordinating and representing digital companies, helping to consolidate a strategic industrial and technological sector in a rapidly changing field.

Against this backdrop, the Ministry of the Interior’s Command in Cyberspace (COMCYBER- MI) is a key player in the fight against cybercrime. COMCYBER-MI is a national service reporting to the Director General of the Gendarmerie Nationale and is based on four key pillars: threat anticipation, ministerial strategy to combat cybercrime, operational support for investigative services, and training. In less than two years of existence, it has demonstrated its ability to mobilize rare skills, to act in support of major events such as the Paris 2024 Olympic and Paralympic Games, to project experts in metropolitan France and overseas, and to raise awareness among economic players via tools such as the Sensycrise MOOC, for example.
However, cybercrime is constantly changing. Criminal networks are becoming more professional, exploiting digital vulnerabilities and threatening the security of citizens, businesses and institutions.

In the face of this, the response must be collective. This is why collaboration between COMCYBER-MI and ACN is so important. It is embodied in an agreement structured around four axes: information sharing, joint participation in work, reciprocal exchange of products, and implementation of targeted actions. The agreement will enable public and private sector organizations to work together to build trust-based solutions that meet the challenges of today’s sovereignty, security and competitiveness.

By combining the strength of public action with the agility of industrial innovation, this partnership strengthens our collective ability to anticipate threats, respond effectively to cyber crises and build national resilience. Together, we share a common ambition: to make cyberspace a safe and trustworthy space, in the service of our freedoms, our economy and the values of the French Republic.

“ Our forces, for your cyber protection. ” ”

6.2.a Europe: a single trusted digital market

Digital transformation continues to take place within the EU. In a geopolitical context where tensions are running high, the creation of a trusted digital single market is more than ever a necessity for all players in the industry. The new risks arising from new uses are prompting European institutions and member states to reflect on how to adapt their legislative arsenal to these developments and enable the European Union to better master its digital future. The "For a Digital Europe" program, through which this response is taking place, aims to make Europe a major player in this field, strengthening its technological sovereignty and ensuring its resilience in a context of growing tension in cyberspace. Once again, this year, numerous draft European texts are continuing their legislative journey and are on the verge of completion. These projects concern cybersecurity, and more specifically the strengthening of resilience, digital identity, market regulation and the establishment of a legal framework for artificial intelligence.
All this work is a priority for the digital trust industry.
Like 2024, 2025 is a pivotal year from an institutional point of view in Europe.

All this work is a priority for the digital trust industry. Like 2024, 2025 is a pivotal year from an institutional point of view in Europe. In April 2024, in partnership with its German counterpart Teletrust, ACN published its European priorities and recommendations for accelerating the transition to a single market for digital trust and passed them on to all MEPs. ACN hopes to build on the success of this cooperation with its German counterparts to extend it and aims to forge partnerships with representatives of the digital trust industry in several other European countries. The aim of this inter-European cooperation between industry representatives is to get to know each other better, and to develop common messages that can be put across more forcefully.

ACN document "Digital trust industry priorities for the 2024 European elections"

available at the following link:
urlr.me/rwy7zJ

Implementing an interoperable European digital identity

Work on revising the eIDAS regulation to implement a secure, interoperable digital identity in Europe culminated on April 30, 2024 with its publication in the EU Official Journal. Europe is thus on the verge of enabling all its inhabitants to have a personal digital wallet that can be used throughout its territory. Implementation will be based on common technical standards (Architecture and Reference Framework - ARF), which are still under discussion. By 2027, member states will have to provide every European citizen with a free digital identity wallet.

The creation of a European legal framework for artificial intelligence

The Artificial Intelligence Regulation (AI Act) was adopted by the EU Parliament and Council in early 2024, after 3 years of negotiations. The AI Act was published in the EU Official Journal on July 12, 2024, and came into force on August 1, 2024. The first bans provided for in the regulation are now applicable, and the scheme will gradually be extended to other categories of use, depending on the level of risk associated with them.
On February 4, 2025, the European Commission published guidelines on article 5 of the regulation concerning prohibited practices, and on March 7, 2025, the implementing act setting up the scientific group was adopted. Full implementation of this text, under the guidance of the AI Office, which is becoming more structured, is scheduled for 2026.

ACN report "Detailed Analysis - Artificial Intelligence Regulation - AI ACT"

available at the following link:
urlr.me/SJU2sj

Strengthening cybersecurity

The Cyber Resilience Act (CRA) was adopted by the European Parliament in March 2024, and numerous amendments were made to the text, with a view to bringing its provisions into line with existing texts (NIS 2 Directive, Cybersecurity Act, etc.). On November 20, 2024, the regulation was published in the Official Journal of the European Union and came into force on December 10, 2024. It aims to establish common European cybersecurity standards for products to be placed on the internal European market. The CRA also aims to reinforce the responsibility of manufacturers and suppliers of products with digital elements (PEN) by requiring the implementation of adequate cybersecurity guarantees.
Implementation of the ARC will be gradual: 18 months after its entry into force, i.e. a priori in spring 2026, assessment bodies will be empowered to verify product conformity. From summer 2026, manufacturers will have to report vulnerabilities and incidents. By 2027, all ARC requirements will apply, including minimum pre-market standards, vulnerability management and the duty of transparency towards users.

ACN report "Detailed analysis - Cyber Resilience ACT"

available at the following link:
urlr.me/urQveD

Furthermore, in the face of growing cybersecurity risks, European solidarity in this field has also been legislated through the Cyber Solidarity Act to implement a "European Cyber Shield", a cyber emergency mechanism, notably creating a "European Cyber Reserve", and a cybersecurity incident analysis mechanism. After a trialogue that reduced the original budget allocated to the European Cyber Reserve, the text was adopted by the EU Council on December 2, 2024, with the accompanying amendment to the European CyberSecurity Act. It came into force on February 4, 2025.
Finally, member states are in the process of transposing several texts into national law. The NIS 2 Directive, the Directive on the Resilience of Critical Entities (REC Directive), and the requirements of the DORA Regulation, which were due to be implemented between the end of 2024 and the beginning of 2025, are currently being examined and transposed by EU member states.

ACN report "detailed analysis of NIS 2 directive"

available at the following link:
urlr.me/VWAHzj

Digital operational resilience in the financial sector

The DORA regulation and associated directive came into force on January 16, 2023. They provide an innovative regulatory framework that addresses the risks posed by the profound digital transformation of financial services, the growing interconnection of networks and critical infrastructures, and the increasing number and sophistication of cyberattacks on financial sector players. At the same time, the revision of the REC (Resilience of Critical Entities) and NIS2 directives has strengthened the general cybersecurity framework.
The Digital Operational Resilience Regulation (DORA) defines uniform requirements to strengthen and harmonize risk management related to information and communication technologies (ICT) and the security of networks and information systems at EU level. It also provides for the establishment of a mechanism for the direct monitoring of critical ICT service providers at EU level.
The regulation applies to all EU member states from January 17, 2025. Over the next two years, the Commission will issue delegated acts on the basis of final drafts of technical and implementing regulatory standards.

ACN report "Detailed analysis of the DORA regulation"
available at the following link:
urlr.me/9M2Ubf

6.2.b National digital trust initiatives

Bill on the resilience of critical infrastructures and the strengthening of cybersecurity (transposition REC-NIS2-DORA)

On January 17, 2023, the NIS 2 Directive came into force, having been published in the Official Journal of the European Union by the European Commission on December 27, 2022. The purpose of this directive is to ensure a high common level of cybersecurity throughout the European Union, in order to guarantee a trusted cyberspace for citizens and businesses, and to strengthen cooperation between member states.

Member States had 21 months to transpose the directive into national law: it should therefore have been transposed by October 17, 2024. Many European countries, including France, are behind schedule.

In July 2023, the Commission also issued guidelines clarifying the application of the Union's sectoral legal acts.

On October 15, 2024, during the Council of Ministers, the Minister for the Economy, Finance and Industry, the Minister for Higher Education and Research, and the Secretary of State to the Minister for Higher Education and Research, responsible for Artificial Intelligence and the Digital Economy, presented the bill on the resilience of critical infrastructures and the reinforcement of cybersecurity, enabling the transposition of the NIS 2 directive into French law, as well as the REC and DORA texts. The bill was submitted to the Senate on the same day, which set up a special committee to examine it.

>>> January 24, 2025: ACN was interviewed by Senator Olivier Cadic, Chairman of the Special Committee on Cybersecurity, and Senators Hugues Saury, Patric Chaize and Michel Canevet, rapporteurs for the draft law on the resilience of critical infrastructures and the strengthening of cybersecurity.
The integration of the REC/NIS2/DORA texts into a single transposition bill demonstrates a clear effort at coherence, which ACN welcomes. Indeed, the legibility of the requirements and the clear understanding by regulated entities of the whole edifice is a major element of success in the general objective of improving our country's level of security and resilience.

To achieve this objective, ACN calls for the provisions adopted to be transposed and implemented as quickly as possible, to respond as quickly as possible to the two challenges facing us collectively, namely strengthening our collective resilience and our strategic autonomy. Indeed, it is essential that this text be a lever for the development of the French and European digital trust ecosystem, thus combining sovereignty and resilience.
France has a highly efficient and agile digital trust sector, made up of companies of all sizes (large groups, ETIs, SMEs and start-ups) offering solutions that are adapted and immediately available to meet the needs generated by this bill. It also seems essential that the implementation of this text be accompanied by a massive effort in communication, awareness-raising, dissemination of best practices, support and training for regulated entities, many of which will be subject to cybersecurity obligations for the first time.

ACN has been a driving force behind proposals to disseminate the industry's priorities in parliamentary proceedings. We have proposed that the measures be supplemented by a financial incentive mechanism of the "cybersecurity tax credit" type, in order to lighten the burden of investment on regulated entities (particularly VSEs and SMEs) and put them in a position to meet their obligations. Such public support for the country's security efforts is likely to deliver a high return on investment, especially when compared with the cost of inaction and its effects on the entire national economic and social fabric. In addition, European subsidy schemes dedicated to helping companies, especially SMEs, comply with the new cybersecurity requirements could also be put in place.

ACN would also like to see the creation of a body, including industry representatives, to contribute to the drafting of the decrees, and to monitor their implementation and effectiveness over time, to be able to adapt them to changing techniques and threats. To achieve the objectives of the text, additional provisions could be put in place to:

- Reinforce consideration of the human factor in the bill.
- Require regulated entities to adopt a vulnerability disclosure policy.
- Provide a legislative framework for OSINT activities.

On March 12, 2025, the bill on the resilience of critical infrastructures and the reinforcement of cybersecurity was adopted by the Senate and sent to the National Assembly for examination. A special commission to examine the bill was set up on April 8, 2025. The bill is expected to be passed in the summer of 2025.

POINT OF VIEW

OLIVIER CADIC

- **CHAIRMAN OF THE SENATE SPECIAL CYBERSECURITY COMMISSION**
- **SENATOR REPRESENTING FRENCH NATIONALS LIVING OUTSIDE FRANCE**
- **VICE-PRESIDENT OF THE FOREIGN AFFAIRS COMMITTEE, DEFENCE AND ARMED FORCES**

SÉNAT

“ For me, chairing the special commission charged with studying the bill on “ the resilience of critical infrastructures and the strengthening of cybersecurity ” was a demanding but essential responsibility. The bill, which was passed by the Senate on March 12, 2025, is the fruit of a rigorous and concerted effort, deeply rooted in the realities of the field. It aims to transpose three major European directives: REC, NIS2 and DORA. But beyond transposition, we wanted to convey a vision: one of solid, shared cybersecurity, built with professionals for professionals.
My mindset has always been clear: it’s not a question of preventing cyberattacks - they’re inevitable - but of limiting their impact, guaranteeing continuity and building genuine resilience. This means avoiding contradictory injunctions, such as the introduction of “backdoors” in encryption systems, which would weaken rather than strengthen our defenses. Thanks to an amendment I tabled, this drift has been prevented: the Senate remains, in my view, the home of freedoms.

Throughout our work, I wanted to closely involve economic stakeholders, local authorities, experts, and regulatory bodies. Public-private dialogue is not a luxury; it is a condition for success. We organized seven public hearings, consulted cybersecurity representatives, elected officials, and companies to build an operational text while avoiding any unnecessary over-implementation. Because although security is imperative, it must never become an unreadable or unachievable burden.
I raised concerns about the risk of an imbalance between the obligations set by law and the details left to around forty decrees: too many gray areas, with the administration in sole control.
That is why we made clear recommendations: simplify the implementation measures, avoid over-implementation or under-implementation, support local authorities in this transition, and ensure real clarity of standards.

This text is only a starting point. Its success will depend on the quality of its implementation. It needs to be supported politically, not simply managed technically. That’s the price we’ll have to pay to strengthen confidence in our digital ecosystem.
Moreover, our work is not yet done, as we need to reach agreement with the French National Assembly on a joint text in the joint committee. It is an important objective that this bill be adopted by the largest possible majority, as the issue of cybersecurity concerns all French citizens.

I salute the exceptional work of the three rapporteurs of the special committee I chaired to prepare this text: Michel Canévet, Hugues Saury and Patrick Chaize. Clara Chappaz, Minister Delegate for Artificial Intelligence and Digital Technologies, has always been attentive to our needs, and has been a welcome element of continuity in this process, which I would like to highlight at. ”

POINT OF VIEW

PHILIPPE LATOMBE

- **CHAIRMAN OF THE NATIONAL ASSEMBLY'S SPECIAL CYBERSECURITY COMMISSION**
- **MEMBER OF PARLIAMENT FOR THE 1ST CONSTITUENCY OF VENDÉE**
- **VICE-PRESIDENT OF THE STUDY GROUP ON DIGITAL ECONOMY, SECURITY AND SOVEREIGNTY**

"The Critical Infrastructure Resilience and Cybersecurity Reinforcement Bill has arrived in Parliament at an opportune moment, when transatlantic relations and the international geopolitical context have heightened awareness of cybersecurity issues, even within companies and local authorities that do not belong to the so-called " strategic " sectors and have not yet taken the step of securing their information systems. It's about time. This transposition of the NIS 2 directive and its corollaries, REC and DORA, is not simply a regulatory change imposed by a European Union obsessively seeking to complicate the lives of the players concerned. It represents a major turning point in the way digital risks are managed, at all levels, by the 15,000 structures it concerns (compared with only a few hundred for NIS 1).

What everyone needs to realize above all is that the protection of all data, however seemingly innocuous it may often be, represents a major challenge for citizens, businesses and the State, all the more so with the very rapid rise in power of artificial intelligence and quantum technology, which enable a considerable mass of information to be processed very rapidly. This is a vital risk for our societies and economies.

Being chairman of this special commission is a continuation of the parliamentary work I've been carrying out for almost eight years, and represents a major milestone. I've long been convinced that we need to get economic players, local authorities, experts and regulatory authorities to work together. This means involving the entire value chain, which is no mean feat, simplifying application procedures and striking the right balance between under- and over-transposition. However, this should serve as a guideline for legislators.

ASSEMBLÉE NATIONALE

It is essential that the transposition of a European directive should be experienced not as an additional bureaucratic constraint, but as a reasoned management of risks that concern everyone. It also means realizing that this is both an obligation and an opportunity to develop sovereign French and European solutions capable of protecting us from external threats, be they state and/or criminal, and to strengthen our confidence in our digital ecosystem.

I'd also like these discussions to be an opportunity to look at the place of OSINT (Open Source INTelligence), a practice governed by a few special texts that deserves the development of a common law to provide legal clarification for all those situations that are still too numerous not to be recognized.

Contrary to what some might think, the Critical Infrastructure Resilience and Cybersecurity Enhancement Bill is first and foremost a highly political text, not a mere technical or administrative adjustment. It is therefore up to politicians to take control.

A subject such as this, whose purpose brings people together, should not be the subject of parochial quarrels, but, on the contrary, should enable us to work calmly for the common good. This is an opportunity for me to continue a practice that is dear to me, that of transpartisan dialogue."

FOCUS

LEGAL SECURITY FOR OSINT: PRESENTATION OF THE WORK OF THE WORKING GROUP

ACN - IHEDN CYBER CHAIR PARTNERSHIP

Professor Michel Séjean, Professor Bertrand Warusfel and Doctor of Law Emilie Musso have been co-leading a working group on OSINT since 2023. We asked them about the path their work has taken, and the outcome of these two years of reflection.

“ First, can you explain what OSINT is?

There are several definitions of OSINT (Open-Source Intelligence). For example, the CNIL explains that it is the practice that “ consists of identifying individuals or entities, using publicly available information. ”

OSINT is used in a wide range of sectors, from investigative journalism and genealogy to the government and cybersecurity sectors.
Our working group has come up with a definition that covers a wide range of situations. We do not speak of OSINT, but of “ open-source information gathering ”, and we have, for example, clarified that this activity even encompasses the gathering of information obtained because of “ logging into an account ”.

Why was this working group set up?

Our starting point was the observation that the only people who can perform OSINT in complete safety are fortunate enough to benefit from a law that expressly states so and sets the limits of their practice.

For example, VIGINUM has a decree allowing it to use OSINT to accomplish its mission, but its freedom does not extend to introducing facial recognition or voice identification into its OSINT techniques.

So much the better for VIGINUM: this service benefits from a clear framework! But what about the others? All those people and entities who cannot rely on a legal text specially written for them; how can they use OSINT without feeling that they are taking a risk of condemnation? No general rule clearly states the freedom to use OSINT methods.

This legal uncertainty is such that several OSINT solution providers in the French ecosystem have expressed their dismay to the *Alliance pour la Confiance Numérique* (ACN).

Who’s going to buy French OSINT products if the salesperson can’t reassure customers that there’s no risk if the product is used sensibly? That’s what’s happening today, and customers are buying from abroad; all OSINT users not covered by a special text have the impression that they are in breach of French law, whereas this is not even the case in many situations!

This dissatisfaction gave rise to a partnership between ACN and the “ Digital Sovereignty and Cybersecurity ” Chair of the Institut des Hautes Etudes de Défense Nationale (IHEDN). This group brought together practitioners from several sectors, including the government, business, the bar and university research.

How did you go about your work?

We did apply legal research. It’s a process of creation by induction.

We start from factual situations, such as instances of technology use, and bring all these case studies together to produce a rule.
In other words, we start from the fact and work our way up to the law (induction), rather than starting from the general rule and applying it to the facts (deduction).

“ We’re not talking about OSINT, but open-source information gathering. ”

Émilie Musso
Doctor of Private Law and Criminal Sciences
Cybersecurity law Legal manager at Anozr Way

Michel Séjean
Professor of Digital Law, Private law, Comparative law

Bertrand Warusfel
Professor at Paris 8 University, Lawyer, Feltesse Warusfel Pasquier & Associés

Admittedly, we didn't study every case of OSINT use - that would have been too tedious - but we did try to step back and find a common thread, a shared logic.

As a result of this exercise, we have drawn up a proposal for a common law regime applicable to OSINT.

What are the results of your two years of work?

We have proposed the creation of a common law framework to bring real legal certainty to all those who explore open sources without being covered by a special law on OSINT.

Our proposal has two main thrusts.

The first aims to define OSINT, clearly stating that its practice is free, while respecting texts on privacy, personal data, intellectual property and secrets protected by law. This first text concludes with the articulation of this freedom of principle with special texts that may restrict this freedom by legislative or regulatory means.

The second proposes the creation of an offence accompanied by a justifying fact, as already exists in criminal law, which aims to punish OSINT activities based on information made available following the commission of an offence such as theft, for example, except when this collection is carried out for legitimate purposes, notably research and computer security.

In so doing, we aim to bring legal certainty to this activity, which is necessary for the accomplishment of cybersecurity missions (vulnerability research, penetration testing, digital footprint audits, etc.). This is the start of a new collective conversation on OSINT.

We hope that the sectors of activity that depend on open sources will, next, solicit the democratic circuits to have their specificities recognized and to obtain a text of special law if this is useful and fair. ”

Actions for the AI Summit - February 2025

From February 6 to 11, 2025, the Summit for Action on AI was held in Paris. On this occasion, thousands of players representing some 100 countries and belonging to the artificial intelligence sector gathered in Paris, at the Grand Palais, to take part in this international Summit.
The aim of the Summit was to promote a French and European strategy for AI, by showcasing the know-how of Europe's AI players.

At the end of the Summit, 100 concrete actions and commitments were announced to promote AI that is trusted and accessible to all.

These actions focus on three main areas:
• Giving everyone the means to make the AI revolution their own.

• Promoting our confidence in sustainable AI that respects the environment, social cohesion and our democracies.

• Strengthen the international AI governance system to make it more effective and inclusive.

Among these announcements, we particularly note:
• The government's announcement of the creation of the National Institute for the Evaluation and Security of Artificial Intelligence (INESIA) to scientifically study the effects of this technology, including in terms of security. The institute's mission is to bring together the major national players already specializing in this field.

• The French President's announcement that private companies in France will invest 109 billion euros in AI over the next few years. Much of this investment will be directed towards the construction of data centers.

• The creation of a new international foundation on AI of general interest "Current AI" has also seen the light of day, to reorganize the generative AI landscape by developing and supporting initiatives that serve the public interest, particularly about data quality. It is led by France and brings together nine countries, companies and philanthropic organizations, notably American.

• A declaration on the international governance of AI has been made public. This was drawn up by a working group over a period of more than 7 months, bringing together 29 States, 6 international organizations, 7 tech companies and 10 civil society organizations. Its work aims to identify points of consensus to map out AI sectors and governance needs.

• As part of an inclusive and sustainable AI for people and planet: 58 countries, including France, China and India, have signed a joint declaration to promote open, transparent, ethical and trustworthy AI. To complement this declaration, a Coalition for environmentally sustainable artificial intelligence has been launched. It comprises governments, international organizations, business leaders, academics, artists and members of civil society.

• The launch of a Coalition for environmentally sustainable artificial intelligence. It comprises governments, international organizations, business leaders, academics, artists and members of civil society.

ACN organizes the 1st Rencontres de l'IA de Confiance (RIAC)

As part of the AI Summit in France in February 2025, ACN organized its first Rencontres de l'AI de Confiance (RIAC). They were held on February 3, 2025, at Campus Cyber.

The aim of the event was to explore the notion of Trusted AI to raise awareness of the AI ecosystem and contribute to its structuring, thus making a positive contribution to the public debate by crossing the views of state, industrial and academic players around three round tables.

In line with the White Paper on Trusted AI, published by ACN in March 2024, the debates focused on the criteria for characterizing trust in AI, exploring the legal, technical and ethical dimensions required for this trust.

The event generated a broad consensus around the need to place the notion of trust at the heart of AI deployment, and encouraged the players involved to structure this approach around the joint work initiated by ACN, by mapping these players, listing them in the Observatory, drawing up a charter of ethics for the industry, etc.

ACN white paper "Trustworthy Artificial Intelligence"

available at the following link:
urlr.me/Kr6S4J

6.3 TECHNOLOGY TRENDS

Technological innovation has been the main driver of growth in French and global Digital Trust for more than 10 years and this trend is expected to continue at least for the next 10 years. Technological developments affect Digital Trust in different and complementary ways.

6.3.a Electronic and digital innovations that generate new markets

Innovations in the electronic and digital industries are impacting almost all sectors of modern economies and are thus generating new markets for Digital Trust.

• **Electronic systems and components are characterized by miniaturization and lower costs.** This trend, epitomized by Moore's Law, has shaped the global economy for the past 50 years, and is set to continue for at least the next decade, with the development of multilayer 3D memories and the miniaturization of processors. However, this trend is coming to an end. Investments to continue Moore's Law and keep pace with innovation are growing exponentially, and have already reached such levels that only seven companies are holding their own worldwide: Samsung (South Korea), TSMC (Taiwan) and Intel (USA) in processors, and Samsung (South Korea), SK Hynix (South Korea), Micron (USA), Western Digital (USA) and Toshiba (Japan) in memories. Today, however, there are alternatives to the development of Moore's Law, such as advanced packaging and heterogeneous integration, which are seen as alternatives to the production of increasingly high-performance chips at lower investment cost.

As a result of miniaturisation and falling costs, electronic products are becoming more democratic, including digital trust: sensors, tracking and tracing systems, and all the sub-systems included in the electronic segments of the industry.
This is a long-term phenomenon. In the short term, the growth of electronic components is cyclical and the 2020-2022 period was instead marked by surge in semiconductor prices. Since the beginning of 2023, the decline in semiconductor prices has resumed its course.
Over the next five years, only increases in energy prices are likely to counterbalance the price decline associated with the further miniaturisation of electronics, depending on the magnitude of these increases, particularly in Europe.

• **Digital transformation, i.e. the digitalisation of tools, products and services in all sectors of the economy.** This digitalisation process is still in its beginnings on a global scale. It is leading to an ever-increasing share of digital issues and this trend is expected to last for at least the next 20 years through the deployment of the Cloud-to-Edge continuum and its outlets in industrial IoT (embedded software, connectivity, cloud).

The intersection of these two trends is generating many emerging and promising markets for digital trust.

1. Security of connected objects

Eventually, if every object becomes connected, every object will need a cyber tool to secure it. Moreover, the interconnection of connected objects increases the cybersecurity risks by making entire networks vulnerable. Consequently, the interconnection of objects represents a huge growth potential for the associated cybersecurity products and services: identification and authentication of IoTs, secure elements, security of communications (5G / 6G, long-distance IoT communication protocols such as LoRa and Sigfox or short-range protocols such as Wi-Fi, Z-Wave, Bluetooth Low Energy, etc.), infrastructures, applications (hypervisors, etc.). Until now, the growth resulting from connected objects has not yet impacted the French security industry, although many of them have already been working on a dedicated offer for several years. Progress in the standardisation and interoperability of IoT architectures is likely to accelerate future growth.

• **Connected car.** The main segment, which is already growing strongly, is that of securing cars and their communications: Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I: toll, etc.), Vehicle-to-Device (V2D: smartphone, etc.).

• **Smart & Safe City.** The development of connected objects in cities for security purposes is the second segment that has generated the most significant growth worldwide among digital security and cybersecurity players in connected objects since 2015. The players that have benefited most from the Safe City theme are the major integrators (Thales, Accenture, Capgemini, etc.). Safe City is generally less successful in France than abroad (whether in China, the United States or in many emerging countries) for three main reasons: the French administration, which was built around non-digital processes, the great diversity of public players in France (central state, regions, departments, municipalities, communities of municipalities, etc.), and budgetary austerity.

• **Securing Industry 4.0.** The growth associated with the deployment and securing of Industry 4.0 is expected to be increasingly felt over the coming years. However, installing connected objects inside a factory does not necessarily require the development of dedicated connected object solutions from cyber suppliers as the objects can all be connected to the central factory server. In other words, the classic and slightly older IT-OT technology is sufficient. As a result, the development of connected objects in Factory 4.0 does not result in a significant increase in orders for the implementation of specific solutions for securing connected objects in these factories.
France has major players in all the security segments associated with securing IoTs, but lacks national players of significant size for the deployment of service platforms associated with connected objects (of the type of GAFAMI in the USA or BATX in China).

2. Data sovereignty and sovereign clouds

In parallel with the technological proliferation in electronics for data storage and processing (3D NAND, neuromorphic chips, quantum computing, photonic computing, integrated photonics, photonic interconnection networks, high-performance computing (HPC), etc.), the number and volume of databases is growing exponentially (big data). The issue of securing these data sets is becoming increasingly important, whether for sovereign reasons (public services, critical databases), economic reasons (protection of sensitive company data), or for citizen reasons (citizen's rights, protection of personal data, right to be forgotten, etc.).

Launched in May 2021, the national " Trusted Cloud " strategy has had the merit of laying the foundations of a legal framework aimed at ensuring that French government data cannot be hosted directly by companies that are not under the exclusive control of French jurisdictions. This strategy is built around three pillars:

a/ The " Cloud de confiance " label, issued in accordance with the standards of the Agence nationale de sécurité des systèmes d'information (ANSSI).

b/ The " Cloud au center " policy for the public sector (based on the SecNumCloud standard).

c/ An industrial policy implemented as an extension of France Relance.

In this regard, NumSpot, a collaboration between Docaposte, Banque des Territoires, Dassault Systèmes and Bouygues Telecom, aims to establish an independent, sovereign cloud offering in France. This initiative uses Dassault Systèmes' OUTSCALE cloud infrastructure, qualified as SecNumCloud, to offer services that meet performance, security and environmental responsibility standards. Since its launch in autumn 2022, NumSpot has trained a team of one hundred experts and established partnerships with major cloud players.

3. Digital identities

Closely linked to the theme of data sovereignty, the redefinition of digital identities also stems from digital transformation and the widespread adoption of remote services. The current landscape in France remains characterized by the coexistence of multiple digital identities with varying levels of security: strong identities (SIM cards, bank cards, passports), substantial identities (such as La Poste's Digital Identity), and weaker identities, often provided by non-European actors (such as the GAFA). This fragmentation raises significant issues regarding personal data protection and technological sovereignty.

The alternative promoted by European authorities focuses on the deployment of a strong, certified, unique, and sovereign digital identity, associated with each user, from which secondary identities could be derived according to different use cases.

The French industrial sector possesses all the necessary expertise to support this ambition (secured elements, Identity & Access Management (IAM), integration, cryptography, biometrics, PVID, etc.). Initiatives in this direction are multiplying, both nationally – with the deployment of the Electronic National Identity Card (CNIe) and FranceConnect – and at the European level, through the eIDAS2 regulation and the European Digital Identity Wallet.

The European Digital Identity Wallet represents a major step forward in the standardization and security of digital identities across the European Union.

Piloted under the POTENTIAL project, coordinated by the French Ministry of the Interior and bringing together 20 countries, the wallet aims to enable every European citizen to access public and private services through a certified and interoperable identity. The tested use cases include access to public services, banking and telecom services, electronic prescriptions, driving licenses, and electronic signatures.

Common technical components for the issuance and verification of attestations are currently being deployed, particularly within a shared environment hosted by ANTS and open to the broader ecosystem. Two new European projects, APTITUDE and WEBUILD, will extend this dynamic from September 2025, focusing respectively on use cases related to natural persons and legal entities.

Beyond its technological dimension, the European Digital Wallet also raises challenges related to adoption, trust, and digital inclusion. Its widespread adoption will depend on public awareness initiatives, the creation of integrated service ecosystems, and strict compliance with European regulatory frameworks (notably for age verification services, as required under the French law of May 2024).

As an example, several French players, including Docaposte, are actively participating in these initiatives, notably through the POTENTIAL project, by developing components for the issuance and verification of attestations and contributing to public education around digital identities and the European digital wallet. In parallel, Docaposte is also developing practical solutions for identity verification and age verification in line with new French regulatory requirements, notably through its 18Connect platform.

4. Digital transformation in particular is driving most cybersecurity segments: securing corporate clouds, telecommuting, intelligence and information gathering software that benefits from large digitally generated databases, etc.

FOCUS

RESEARCH : PROGRAM AGENCIES AND CYBERSECURITY

According to a commonly accepted vision, the digital world is gradually evolving towards a generalization of computing and communications, in the form of a continuum where computing is universally distributed. Such a scenario would lead to a considerable increase in the attack surface, and therefore in the vulnerability of the digital universe.

Moreover, the geostrategic developments of recent years require France and Europe to be able to make independent decisions, without outside interference. This applies, of course, to all decisions relating to the digital world. Cybersecurity is an essential element of digital sovereignty, since it is precisely this that protects infrastructures and data from external threats.

Research is fuelling future sovereign technologies in fields as varied as cryptography, evaluation and supervision.
Here are just a few of the key issues that need to be addressed today to ensure a sovereign role in the years to come:

• control over the evaluation and certification of digital systems, at both hardware and software levels, including their interactions the mutual consequences of disruptions of one on the other

• confidence in encryption protocols, including and especially post-quantum algorithms, which have now been adopted internationally, but whose soundness has yet to be established with a high degree of certainty

• confidence in electronic voting procedures

• the ability to finely control personal and industrial data in all circumstances, even in environments where trust is limited.
These subjects, which are just a few examples, still require research work, the results of which will be binding in the years to come, both for the national industry and for citizens.

Following on from the PEPR programs, and particularly the cybersecurity PEPR presented in the 2024 edition of the ACN Observatory, the French government has decided to give national research organizations the task of forecasting and steering strategic research actions within their areas of competence. The Program Agencies created for this purpose are to propose the follow-up to the major PEPR-type programs, and to identify and map French expertise in each of the disciplines within their area of competence.

These agencies were announced by the President of the Republic in December 2023:

" Each agency must be increasingly strategic in its field, helping to define priority research themes, organize scientific intelligence for all researchers in its area of competence, interact with international European counterparts and oversee the development of research infrastructures.
Each ONR transformed into an agency will thus have a real mandate and the resources to steer the programs entrusted to it. "

Of the 7 agencies created, two cover the field of cybersecurity:

• ASIC agency, from components to digital systems and infrastructures, operated by CEA, covering hardware evaluation and all applications to components, infrastructures, firmware and embedded software of technologies for design, programming, evaluation, detection and response to attacks, as well as infrastructure security.

• Agence du numérique - algorithms, software and uses, operated by Inria, which includes a cybersecurity program that aims to produce research results and innovation across the spectrum of software cybersecurity, and to foster and support technology, skills and knowledge transfer operations from academic research to use cases and industry.

The role of the agencies' cybersecurity programs is thus to propose a vision of developments in the field of cybersecurity, to ensure the scientific supervision and coherence of actions undertaken within the framework of the PEPR cybersecurity program, and to set up and operate future programs in line with the national strategy.

For further information, please contact:

• ASIC agency:
Géraud Canet • geraud.canet@cea.fr
• Digital agency:
Ludovic Mé • ludovic.me@inria.fr

6.3.b Innovations specific to the sector that generate new products

At the same time - and given that digital trust is made up entirely of electronic and digital solutions - innovations from digital trust itself generate new products, new applications and thus growth.

1. Cryptography

Cryptography groups together all the processes aimed, for example, at encrypting information to ensure confidentiality between the sender and the recipient. There are many technological developments in cryptography and French industry and its training and research ecosystem are at the top of the world in this field. In addition to the technological fields that are already fairly mature (public key cryptography, etc.), the main fields of innovation are as follows:

• Lightweight cryptography.
The rapid development of the IoT has a huge impact on all aspects of cyber security. Recent massive attacks on IoT configurations have shown that strong cryptographic techniques must be used to ensure overall system security. Unfortunately, regarding the IoT, where cost is an important parameter, the use of cryptography can be limited by the size, power and local computing performance of the objects. This has given rise to a very active research field around so-called lightweight cryptography. In short, lightweight cryptography seeks new cryptographic algorithms or protocols suitable for implementation in restricted environments, including RFID tags, sensors, health and care devices. Lightweight cryptography will progressively be used in all IoT domains where the SWAP (size, weight and power) concept tends to become critical. The first industrial applications are being developed and implemented.

• Post-quantum cryptography.
Communications, whether terrestrial or satellite, are central to our society and effective tools have been developed over the last few decades to secure the data exchanged and to protect against attacks. However, the quantum computer and its potential computing power represents a threat to data encrypted with these methods, which it could decrypt in record time. In response to this threat, post-quantum cryptography is based on new mathematical concepts to encrypt messages and thus secure the transport of information. In this context, The RESQUE consortium, which includes six French entities (Thales, TheGreenBow, CryptoExperts, CryptoNext Security, ANSSI and Inria with six affiliated academic institutions), has embarked on a three-year project to develop a post-quantum cryptography solution. The project aims to secure communications and infrastructures against potential attacks from quantum computers. Funded by the French government and the EU, with additional support from Bpifrance, it focuses on the creation of a post-quantum hybrid VPN and high-performance HSM. These projects extend beyond France's borders, as demonstrated by the partnership between Thales and leading Korean mobile operator SK Telecom to develop post-quantum cryptography for 5G networks.

• Homomorphic encryption.
The rise of cloud computing has generated a highly active research field around functional encryption and homomorphic encryption. Functional encryption is a new paradigm of public-key encryption that enables both fine-grained access control and selective computation on encrypted data. In its most advanced form, Fully Homomorphic Encryption (FHE) allows computations to be performed directly on encrypted data without ever decrypting it: one party can encrypt the input data, another party – without access to the decryption key – can process the encrypted data, and only the holder of the private key can decrypt and access the final result. This field holds strong potential, and the first industrial applications are beginning to emerge. Iliadata is part of this momentum: by combining secure multiparty computation (MPC) and homomorphic encryption technologies, the company offers solutions for the confidential pooling of data, enabling multiple stakeholders to collectively leverage data without compromising its confidentiality. This innovation was recognized with the Research Award at the Forum InCyber 2025, highlighting the growing relevance of these technologies in highly regulated or sensitive environments.

• DNA based Cryptography.
This is a new branch of cryptography. It uses DNA as a carrier of information and computation using molecular techniques. It is a relatively new field that has emerged following discoveries about the great storage capacity of DNA - which is the basic computational tool in this field. One gram of DNA stores about 108 TB of data, which exceeds the storage capacity of any electrical, optical or magnetic storage medium. The first industrial applications should emerge in the next few years.

Cryptography using generative adversarial neural networks (GAN cryptography).
Generative adversarial neural networks are a recent innovation in artificial intelligence. The use of these algorithms in cryptography makes it possible to improve the quality of certain systems. This field is still at the development stage and the first industrial applications should emerge in the next few years.

2. Secure elements.
This innovative field is particularly important for France because all the underlying technologies are born there, allowing the development of three world leaders from France: Thales, Idemia and ST Microelectronics. Secure elements are micro or nanoelectronic components comprising a combination of secure embedded software (SW) and hardware (HW) and designed to be integrated into communicating devices in order to securely manage all interactions between the latter and the outside world by storing dedicated applications and confidential data in an encrypted manner (SIM cards, bank card chips, etc.).

In May 2021, the ACN published a report on advanced cryptographic processes, which describes the state of the art for each of these technologies.

ACN Report "Advanced Cryptographic Processes"
available at the following link:
www.confiance-numerique.fr

In the context of the development of IoT, the secure elements segment is marked by the replacement of SIM cards (Universal integrated circuit card) by miniaturized secure elements directly embedded or integrated in the systems to which they are attached, or even without any hardware component (soft secure elements, Trusted Execution Environment). The deployment of embedded secure elements (e-UICC) and Soft secure elements has begun and the massive deployment of integrated secure elements (i-UICC) is not expected to take place before 2024, i.e. once the problems of assurance and standardisation have been resolved. France currently leads the world in this sector with Germany and ahead of China, the United States and South Korea. The main competitors of the French players at world level are the Dutch NXP, the Germans Infineon and Gieseke & Devrient, the South Korean Samsung and the Chinese Shanghai Huahong and Shanghai Fudan Microelectronics. There is a potential medium-term threat to French players due to the lack of skills in Europe and France in More Moore technologies which is likely to lead to American and Asian manufacturers acquiring dominant positions in the i-UICC segment.

Soft secure elements also represent a strong threat to French players, mainly through the American GAFAMs and the Chinese BATXs which can take advantage of their dominant position to impose their solutions.

3. Artificial Intelligence (AI).
Artificial intelligence covers the development of machine learning algorithms (artificial neural networks, multi-layer or not, supervised or not, generative adversarial networks, etc.) for prediction or classification purposes, generative text AI such as ChatGPT, and the issue of edge AI, i.e. the design of chips and embedded systems dedicated to the operation of machine learning algorithms (which are very greedy in terms of computing and memory capacity). Developments in the field of artificial intelligence are not specific to the security sector, but the theme does involve setting up a framework for trustworthy AI.

• **The need for a legal framework:** to ensure that its development and use are in line with society's fundamental values. This involves European legislative work to establish a stable legal framework that protects both the rights and freedoms of citizens while enabling technological innovation. This framework must take into account several aspects of AI, such as its technical nature and liability, and be drawn up in a concerted manner to form a coherent and solid foundation. The challenge is to regulate, by eliminating potential risks, without preventing innovation, so as not to deprive society of essential tools for its digital sovereignty and strategic autonomy.

• **A definition of trustworthy AI:** AI systems must be designed to be transparent, explainable and secure. Trust in these systems can be enhanced by strict cybersecurity standards and rigorous development processes to anticipate potential flaws and abuse. In addition, the data used for the learning phase of these AI models must be managed ethically, with clear standards to avoid the introduction of discriminatory biases, to ensure that the decisions made by these models are fair and equitable.

• **Social acceptance of AI:** essential, it must be cultivated through an ethical approach to its deployment. Respecting ethical principles, protecting human rights and prioritizing human well-being in the development of AI are fundamental. Public education and awareness, combined with transparent demonstrations of the usefulness and safety of AI, such as at major events, can facilitate better understanding and acceptance of these technologies.

When it comes to artificial intelligence, France benefits from excellence in training and research, and French security players are taking fairly strong positions in security applications (notably Thales Digital Identity & Security and Idemia). Although lagging behind the USA and China, who are leveraging their strong digital industrial fabric, France has a competent industry in industrial AI and generative AI. Despite this, however, there is a brain drain from France to the USA in this field, which threatens French positions in the future, including in the security sector.

4. Blockchain.

Initially associated with crypto-currencies and Bitcoin in particular, blockchain is emerging as a new essential tool for digital trust. This protocol records and stores transactions in encrypted form in a decentralized database.

The information is, in fact, unforgeable and unchangeable. As a distributed and secure register of transactions, the blockchain is both a vector of trust and a tool to fight against fraud. It is either public (all participants can intervene in the process) or private. In the latter case, only certain participants record transactions and authorize or not their reading. There are many developments in the field of digital trust: management of social benefits, protection of the infrastructures of vital operators, but also civil or internal security missions and secrecy management between institutions.

These applications will reduce dependence on a central authority, but they require the evolution of the current centralized trust system towards a decentralized system for sovereign-type applications as well as a new organisation of operations. French players have mastered several of the key technologies in the field of blockchain (cryptography, formal methods, etc.). However, it should be noted that the level of acceptance of the technology by users is still low.

At the global level, all sectors taken together - and although this technological field is still not very mature - the American industrial ecosystem is clearly the most advanced in the development of solutions integrating blockchain. The Chinese ecosystem is also important and growing rapidly. Finally, the German and British ecosystems are at least comparable to the French ecosystem.

5. Open Hardware/Software platforms for edge computing and IoTs.

Sharing software code (Open Software) has been around for some time, but in recent years the trend has been towards sharing electronic component designs (Open Hardware). Open source software and hardware accelerate innovation by allowing developers and designers to share and reuse developments made by others.

The re-publication of new developments in open source fuels the innovation process and benefits the whole community. France's strengths in this area of Open Source are numerous. The national market is highly developed, representing a quarter of the European market.

The community of both researchers and developers is undoubtedly the largest and most advanced.

However, security is not very present in the Open Source world. The security market is still dominated by the major proprietary software publishers, most of them North American. A proactive purchasing policy and incentives for the development of certified technology bricks and platforms oriented towards Open Source would help to strengthen this field, particularly for innovative applications associated with edge computing or IoTs, where American domination is not yet too strong.

6. Real-time analysis of local and wide area observation data.
In terms of local observation and surveillance, real-time analysis will eventually be the keystone of the future video surveillance ecosystem. Coupled with artificial intelligence, it will make it possible to identify wanted individuals in real time or to make certain decisions automatically. Real-time satellite imagery is also developing, with numerous opportunities for wide-area observation and intelligence and information gathering. France has the players and the technological know-how to benefit fully from these technological developments.

7. Open Source Intelligence (OSINT).
OSINT has existed for decades in rudimentary form (human sources, documentation, bibliography, etc.).

It was with the explosion in the amount of open data available online since the early 2010s that the OSINT market really took off, through the development of IT tools for collecting and exploiting this data.

These data come from a variety of sources: social networks, websites, media, geospatial imagery, forums, measuring devices, etc., all of which represent a goldmine of information that can be exploited for intelligence purposes. Until the early 2010s, users of OSINT services were limited to government agencies for intelligence purposes or to combat fraud, crime and misdemeanors, as well as a few large corporations, notably through business intelligence agencies.

Today, we can see the emergence of an ecosystem of companies capable of providing OSINT solutions, the most important of which are Chapsvision (notably with the acquisition of Owlint), Palantir, Thales, Athea, Airbus (GEOINT), Anozr Way, Sekoia.io, etc.

8. Other technological developments exist, but do not have the same intensity of impact on the global digital trust industry. Developments around digital identity are an illustrative example: captcha and challenges for software, QR codes, iris recognition, vein recognition, dynamic passwords, etc.

6.3.c Digital transformation & miniaturization : Towards global offers of Security as a Service

1. The security sector as a whole is in the process of standardizing its products

At the global level, digital trust is impacted by two major factors:

• Miniaturization coupled with the falling cost of electronic components, leading to an ever-increasing share of electronic systems or sub-systems in security products.

• Digital transformation, leading to an ever-increasing share of software in security tools. In particular, producers of physical and electronic products - where margins are on average lower than in cybersecurity - are progressively trying to move up the value chain by developing skills in software. The latter - such as Thales, Idemia and Naval Group - are positioning themselves more and more strongly in the development of software dedicated to application security.

The intersection of the two trends described above is therefore gradually leading the players in the industrial sector to position themselves in all segments: physical, electronic and cyber. The physical/electronic/cyber distinction is consequently progressively going to have less and less meaning and in the long term it is likely that each product architecture will be global with a physical component, an electronic component and a cyber component.

This trend even affects private security services. Whereas the physical security of premises used to be made up solely of human resources, its technological and electronic content is continually increasing (SOC, video surveillance cameras, etc.), thanks to the miniaturisation and falling costs of electronic products.

In human surveillance, net profitability is very low (only 1% on average in 2021 and artificially boosted by the CICE). In electronic security, it is higher, although with varying levels depending on the company. The desire of a large number of private service providers is therefore to diversify their services by integrating electronic and cyber products and by moving upmarket.

For example, the large Spanish company Prosegur, one of the European leaders in security, has created an investment fund with €30 million to invest in electronic and cyber security.

Since 2016, this fund has acquired the companies Dognaedis, Innevis and Cipher, all of which specialise in cyber security and are grouped together within Prosegur under the Cipher brand.

Securitas, another European leader in private security, acquired the electronic security business of the American Stanley Security in January 2022 and is expanding in this segment.

Finally, this trend is also felt by the buyers in the industry. All players concerned by security issues (and OIVs in particular) must now also integrate cyber security as a strategic issue

Suez is an emblematic example of a player traditionally concerned with security through the management of drinking water networks and which now considers cybersecurity to be a strategic issue.

Calls for tender for the digitalisation of drinking water management increasingly include cyber-security aspects of the data generated.

2. This standardisation is leading manufacturers to develop more and more global turnkey offers...

Global turnkey cybersecurity offer, global Safe City offer, global security offer, etc. more and more players in the sector are positioning themselves on this type of global offer by following the product standardisation dynamic mentioned above. Thales, through the acquisition of Gemalto in 2019 and the creation of the " Digital Identity & Security " Business Unit bringing together Gemalto, the Thales Digital Factory, Guavus (an American specialist in Big data analytics acquired in 2017) and Thales eSecurity (following the acquisition of Vormetric in 2015), is the most emblematic example of this type of strategy, with the aim of providing and securing the entire critical decision chain in a digital environment. Atos, Orange, Equans and IBM are also positioned on global offers.

3. ...open source...

Some players offer turnkey approaches with proprietary systems. These approaches are less and less favoured by customers who find themselves dependent on a single private player for the maintenance and future improvement of interfaces. As a result, the development of open source solutions is increasing.

In the particular field of national identity management systems (civil status) operated by states, the trend towards the use of open source solutions is also noticeable.

However, there is also a very strong trend towards modularity in terms of distinct functional bricks, as States wish to avoid being dependent on a single supplier or service provider so as not to be locked in. This is reflected in particular in the use of standardized APIs (Application Programming Interfaces) for each functional brick, ensuring complete independence in their design, while allowing them to be interconnected in an interoperable manner.

This trend is combined with that of open source, as functional bricks are increasingly based on open source solutions. This issue of API standardisation is gaining momentum on many subjects, for example with the concept of Open-Services Cloud (OSC) aiming to make cloud services interoperable, reducing the dependence of cloud users on hyperscalers (see the DECISION Études & Conseil study carried out at the beginning of 2023 on the subject: *Open-Services Cloud (OSC) Unlock Cloud interoperability to foster the EU digital market*.

4. ... And *As a Service*

At the same time, we are seeing the gradual end of the simple purchase of products (software in licence mode, etc.), and the development of sales in the form of services (SaaS: Software as a Service, etc.), guided by the need for constant adaptation of security tools to deal with new threats in a context of constant technological change.

In 2020, the provision of software in SaaS mode already represented 40% of the total value of the European enterprise software market (DECISION Études & Conseil, SITSI).
This proportion is growing year on year and should approach 80% by 2030.

As far as solution providers are concerned, this change in usage does not offer new markets or opportunities. On the other hand, it is changing the way companies design their solutions.

As a result, it offers an opportunity to reshuffle the deck in all markets, as current leaders who fail to reshape their solutions and the business models based on these solutions will lose their leadership positions in the coming years.

On the customer side, security is gradually becoming an organizational skill that is found in all the people involved in the design of products and services, and no longer just a separate function isolated from the application development process or associated skills.

One of the consequences is the progressive development of dedicated internal teams in each of the clients' operational units.

ABOUT ACN

ACN
Alliance pour la confiance numérique

The *Alliance pour la Confiance Numérique* (ACN) represents companies (world leaders, micro-companies, SMEs and ISEs) in the digital trust industry, and particularly those in digital identity, cybersecurity and trustworthy AI.

France has a highly efficient industrial fabric in this field and an internationally recognized excellence thanks to world leaders, SMEs, ISEs and the various dynamic players in the sector.

There are 2,499 companies with a revenue of €21.3 billion in France in this fast-growing sector (7.4% average annual growth since 2016).

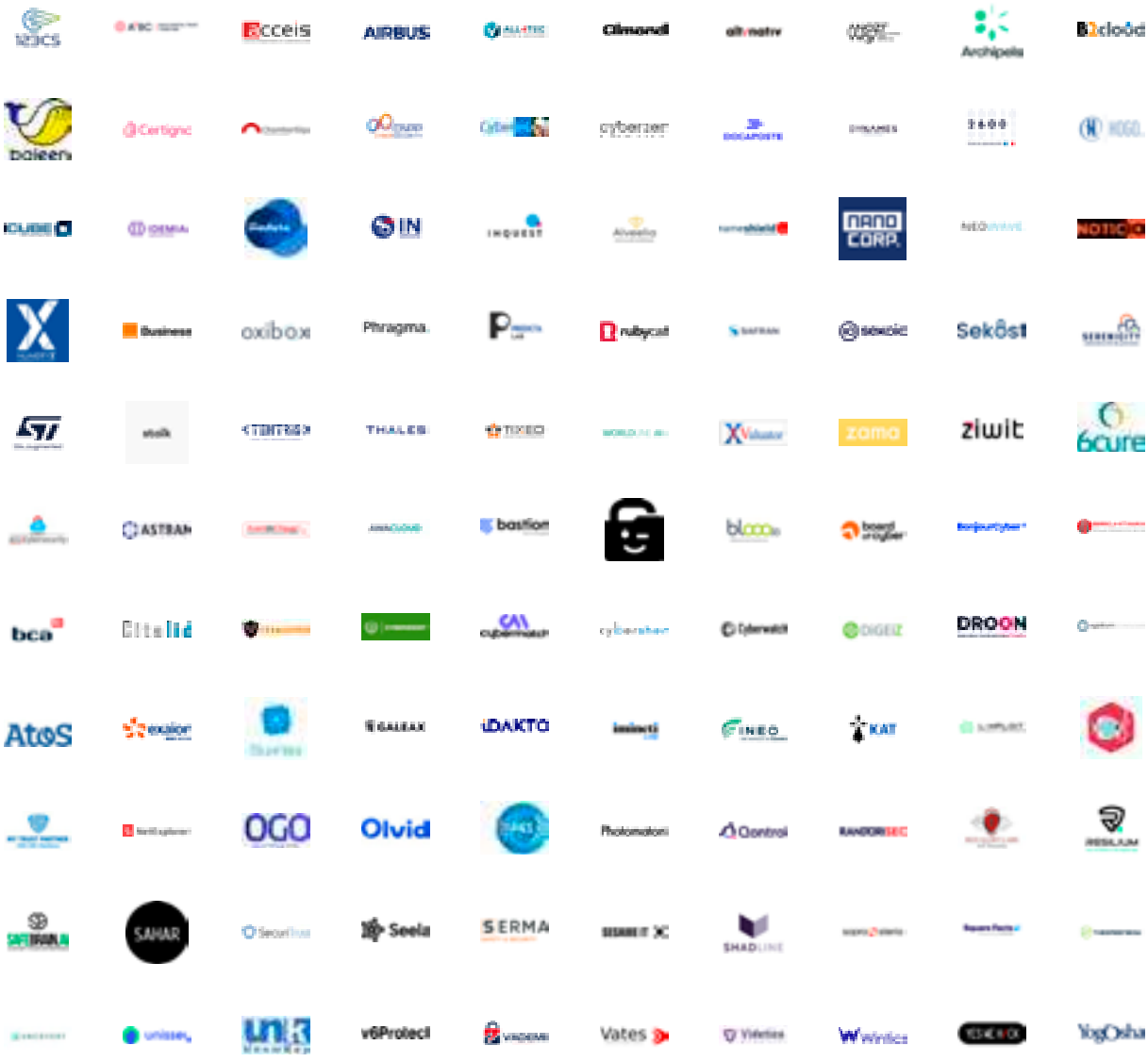
The 114 members of the *Alliance pour la Confiance Numérique* (ACN), 87% of which are Micro-companies/SME-ISEs, account for 2/3 of the revenue of French digital trust companies worldwide (hardware manufacturers, software publishers, integrators, services, security assessment laboratories, research, etc.).

ACN is a member of the FIEEC (*Fédération des Industries Electriques, Electroniques et de Communication*), is an associate member of the Cyber Campus and actively participates in the work of the CSF (*Comité Stratégique de Filière*) of the Security Industries.

ACN is also a founding member of the association representing the European cybersecurity ecosystem: ECSO (European CyberSecurity Organisation).

ACN partners

ACN members



ACN associated members

ABOUT
DECISION ÉTUDES & CONSEIL

Since 2017, DECISION has been conducting the Digital Trust Industry Observatory on behalf of ACN.

DECISION is a research and consulting firm specializing in economic studies (market analysis, forecasts, value chains, etc.) and consulting and strategy assignments, in the fields of:

- electronics (components, equipment, systems),
- aeronautics, defense, security,
- electricity, renewable energies and industry of the future.

Our customers include private companies, whether start-ups/SMEs/ETIs, major industrial groups, professional organizations or financial institutions and investment funds, as well as local and national public authorities (governments, ministries, etc.) and the European Commission.

In 2009, DECISION initiated and conducted the first study for the European Commission on the security industry, and is one of the partners in the framework contract (2010-2015) on the security industry (including cybersecurity) for the European Commission's DG ENTR.

Since then, DECISION has also carried out studies to assess the economic weight of the security industry for the French government:

- In 2015 under the aegis of PIPAME (Pôle Interministériel de Prospective et d'Anticipation des Mutations Economiques), an inter-ministerial structure bringing together the Ministry of the Economy (DGE), the Ministry of the Interior (DMISC) and the SGDSN.

- In 2018 under the aegis of CoFIS (Comité de la Filière Industrielle de Sécurité), bringing together the Ministry of the Economy (DGE), the Ministry of the Interior (DMISC), SGDSN, CICS (Conseil des Industries de la Confiance et de la Sécurité), GICAT and Milipol.

- In 2020, under the aegis of the Conseil Stratégique de Filière (CSF) des Industries de Sécurité, bringing together the Ministry of the Economy (DGE), the Ministry of the Interior (DMISC), SGDSN, CICS (Conseil des Industries de la Confiance et de la Sécurité), and GICAT.

- In 2022, through a consortium including GICAT, ACN, the Ministry of the Interior, the Ministry of the Economy (DGE) and SGDSN.

For more information
www.decision.eu

DECISION
ETUDES & CONSEIL

NOTES

Production - Layout
Agence Verveine

ACN

English version available at :
www.confiance-numerique.fr

Press
Partnership