HarfangLab

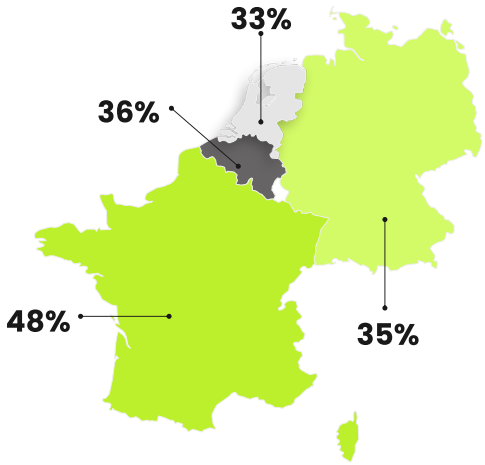
HARFANGLAB STATE OF CYBERSECURITY REPORT

CYBERSECURITY AMONG EUROPEAN BUSINESSES IN 2025: FROM RELIANCE TO RESILIENCE

SUMMARY

1 P.3	**KEY** FINDINGS
2 P.4	**THE STRATEGIC IMPERATIVE OF CYBERSECURITY** IN 2025
3 P.5	**THREAT LEVELS** AND THE ROLE OF AI
4 P.12	**CYBER RISK** PREPAREDNESS AND RESPONSE
5 P.15	**SOVEREIGNTY AND TRUST** ARE SHAPING A NEW AGE OF CYBERSECURITY
6 P.19	**CYBERSECURITY** MADE IN EUROPE
7 P.21	**CONCLUSION**

KEY FINDINGS

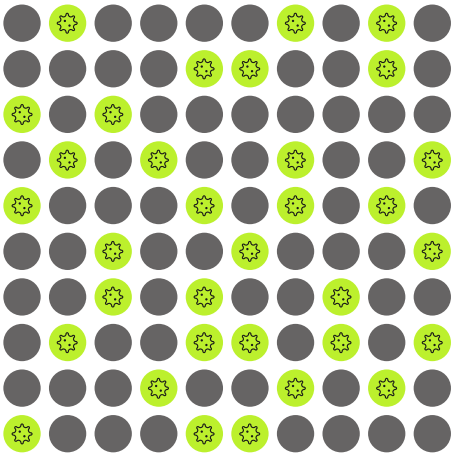


01

CYBERTHREAT EXPOSURE

On average, 40% of respondents rated their organisation's current cyberthreat level as extreme or severe.

02



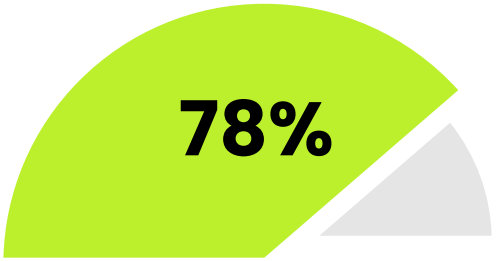
Over half (53%) of European businesses say that data leaks are the worst possible consequence of an attack.

03

58%

58% of surveyed companies believe that the main risk factor for them is AI development supporting cyber criminals.

04



78% of business leaders in Europe are more concerned about digital sovereignty than they were a year ago.

05

Only 1 in 5 businesses (19%) report they have full control over their deployments and security infrastructure.

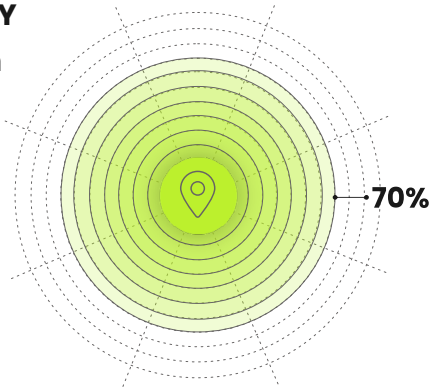
06

70% of respondents believe that European organisations are overly dependent on foreign technologies and should actually reduce this dependence.

EUROPEAN BUSINESSES ARE CONCERNED ABOUT EXTERNAL THREATS, SOVEREIGNTY, GEOPOLITICAL TENSIONS, AND THE IMPACTS THEY MIGHT HAVE. **HOW ARE THEY REACTING?**

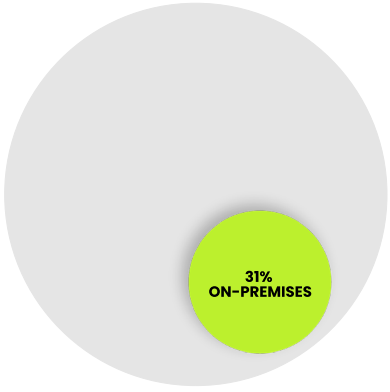
BUYING LOCALLY

7 in 10 European businesses are considering shifting to European cybersecurity providers.



RUN LOCALLY

On-premises is making a comeback: 31% prefer an on-premises EDR solution over a cloud-based one, to gain greater control.



THE STRATEGIC IMPERATIVE OF CYBERSECURITY IN 2025

Cybersecurity might not be a new concern, yet it has become increasingly central to the strategies and conversations of organisations across the globe. Rising awareness of the challenges companies face, fuelled by the real-life examples of numerous companies devastated by cyberattacks, has finally pushed corporate decision-makers to integrate cybersecurity at the core of their business strategies.

Awareness, however, is only the first step on the path to cyber resilience. The challenge lies in execution. Implementation of effective cybersecurity strategies is often inadequate, hindered by a lack of financial resources, a global shortage of skilled professionals and the complexity and fragmentation of protection technologies. These obstacles make it difficult for many organisations to respond to threats and invest in strategies at levels that align with the scale of risk they face.

Looking ahead to 2025, several factors are expected to further exacerbate cyber risk. Heightened geopolitical tensions and ongoing armed conflicts around the world are increasingly spilling into cyberspace. Cybersecurity has become a strategic tool capable of destabilising adversaries or delivering decisive strategic advantages. As a result, states are engaging in cyberwarfare campaigns that are growing in sophistication and stealth. In this digital battleground, where influence is as critical as infrastructure, control over data, platforms, and digital sovereignty becomes paramount. Issues of trust, autonomy, and strategic independence now intersect with traditional notions of cybersecurity.

This geopolitical turmoil has led both countries and companies to consider some fundamental questions:

- How can organisations maintain control over their data, tools, and partners in such a volatile environment?’
- Should organisations prioritise trust over performance?
- What responsibility do European entities have to help build a competitive, sovereign technological ecosystem in the face of dominance by American, Russian, and Israeli giants?

To respond to these challenges, governments and multilateral organisations are attempting to regulate cyberspace. The European Union has led the way delivering regulatory frameworks like the GDPR and NIS2 that are designed to improve protections and help organisations build cyber resilience. However, these regulations also introduce new compliance burdens for IT leaders and executives.

So, what role should Europe's cybersecurity ecosystem play in helping organisations achieve the critical transformation of their cyber strategies in 2025? What is the future of cybersecurity, and in what context and with what tools, will it unfold?

This second edition of HarfangLab's State of Cybersecurity Report aims to answer those questions. It will identify the priorities and barriers that European organisations face when confronting the 2025 cybersecurity landscape.

Through this report, we aim to articulate the needs and expectations of companies, while providing concrete and actionable guidance.

A WORD FROM THE CEO

Grégoire Germain
CEO, HarfangLab

"Cybersecurity is not just about risk management, it's about freedom. In today's international context, organisations should not have to choose between peace of mind and security. Protection should never come at the cost of control or autonomy.

At HarfangLab, we believe high-performance cybersecurity must be sovereign, transparent, and adaptive. Our responsibility is to give organisations the ability to secure their ecosystems without sacrificing independence. Strategic autonomy must be a reality, not a trade-off."

THREAT LEVELS AND THE ROLE OF AI

For European businesses, AI is no longer a distant disruptor on the horizon. It is a present and active agent of both threat and defence. Cybercriminals are starting to weaponise generative AI to accelerate attacks, evade detection, and manipulate human behaviour with alarming precision.

Yet at the same time as creating potentially existential problems, AI is also delivering cybersecurity solutions. Teams are racing to harness AI's capabilities for rapid threat identification, automated response, and predictive analysis.

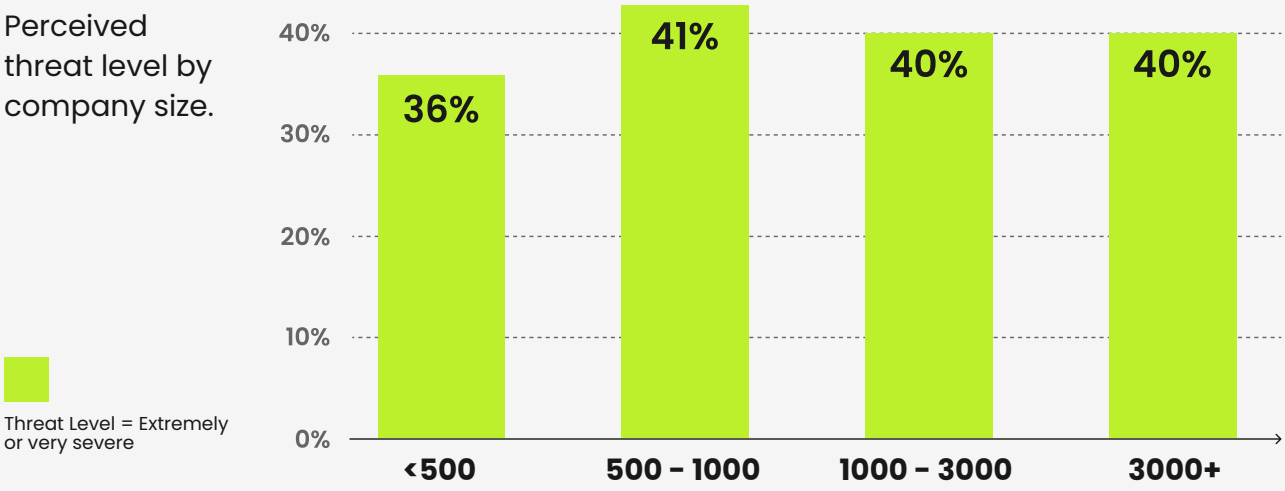
This dual role of AI as both a danger and a potential solution sits at the heart of today's cybersecurity climate. Our research reveals a continent coming to terms with this paradox, as organisations reassess their vulnerabilities and redefine what resilience looks like in an AI-driven threat landscape.

A CONSISTENTLY HIGH, BUT EVOLVING, THREAT PERCEPTION

Across sectors and company sizes, organisations are grappling with an increasingly volatile threat landscape, where risks are not only more pervasive but also more complex, fluid, and difficult to anticipate.

According to our findings, 40% of European companies rate their cyber threat level as “extremely” or “very” severe, a daunting figure that holds steady across both small and large businesses. Among SMEs with fewer than 1,000 employees, 38% report this heightened threat awareness, closely mirroring the 40% of large enterprises (3,000+ employees) who say the same.

Perceived threat level by company size.



Interestingly, this marks a notable shift from last year’s landscape. The proportion of compagnies perceiving severe threats has remained constant, while among large companies, the perception of risk has declined significantly from 53% to 40%.

There could be many reasons for this apparent drop-off in concern. Perhaps the larger players have already invested heavily in cyber security and feel more comfortable with the defence mechanisms they have created. There may also be a greater optimism among big players, possibly due to the experience of seeing their systems rebuff attacks.

Yet, beneath the surface, the marginal drop in concern might actually be masking something entirely different, a subtle normalisation of risk. In other words, a recalibration of what constitutes “severe” in an environment where threats are no longer exceptional but endemic.

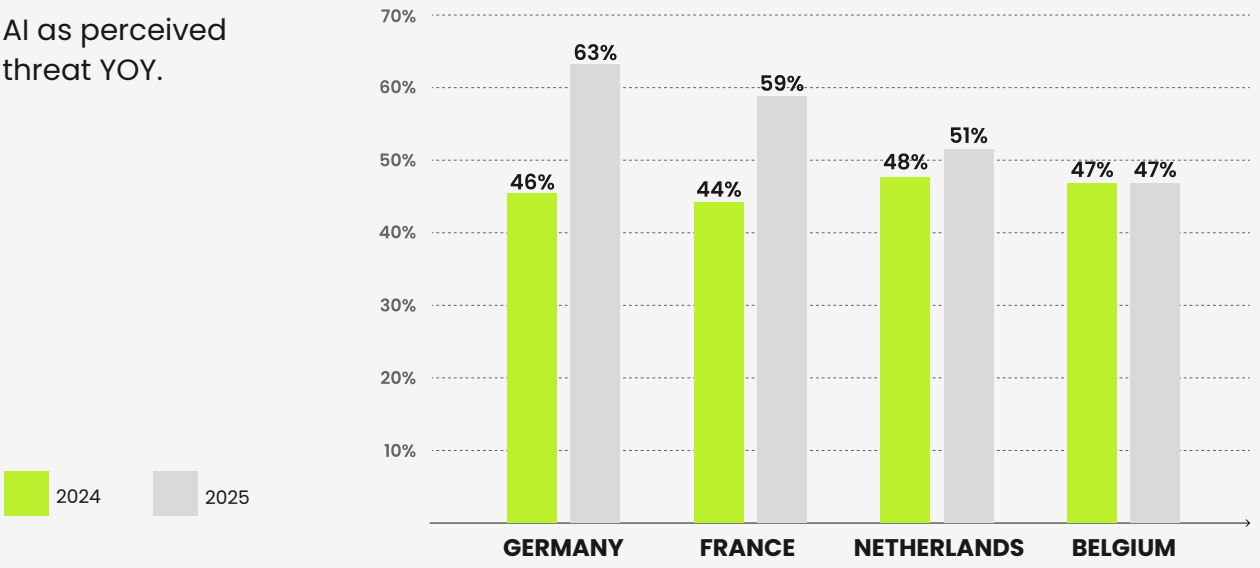
There is also some regional differences at play here too. Just under half (48%) of French companies rate their cyber threat level as “extremely” or “very” severe, which is notably more than in Germany (33%) or Belgium (36%). One factor may be recent high-profile breaches, such as Free telephone operator in France, which came under attack with the company database of 19.2 million French customer datapoints compromised and attackers demanding €10 million ransom.

Léna Jakubowicz
Head of Presales, HarfangLab

"The threat landscape has evolved, but the threat actors tend to keep using the old techniques, like ransomware attacks. As they’ve been making headlines for years, companies took action to cope with them. The problem is now that in addition to encrypting the computers, the attackers also steal the data, leak it, and even blackmail the organisations. Hence, even if the businesses feel like they now have backups for their systems, they are still exposed to the data leaks. That’s potentially why the biggest fear for businesses is now more about data protection and confidentiality issues than the encryption itself."

THE DRIVERS BEHIND RISING RISK

AI as perceived threat YOY.



When our respondents were asked what is fuelling the current risk climate, one factor towered above all others: artificial intelligence in the hands of cybercriminals. A striking 58% of respondents cite the use of AI by threat actors as a key contributor to increased cyber risk. This is up sharply from 46% last year. AI is especially worrying companies in Germany (63%), France (59%), and the Netherlands (51%). The higher figure clearly reflects growing concern over the accessibility and power of generative AI. Malicious actors are becoming ever more adept at crafting convincing phishing lures, automating vulnerability scanning, and obfuscating malware with unprecedented efficiency.

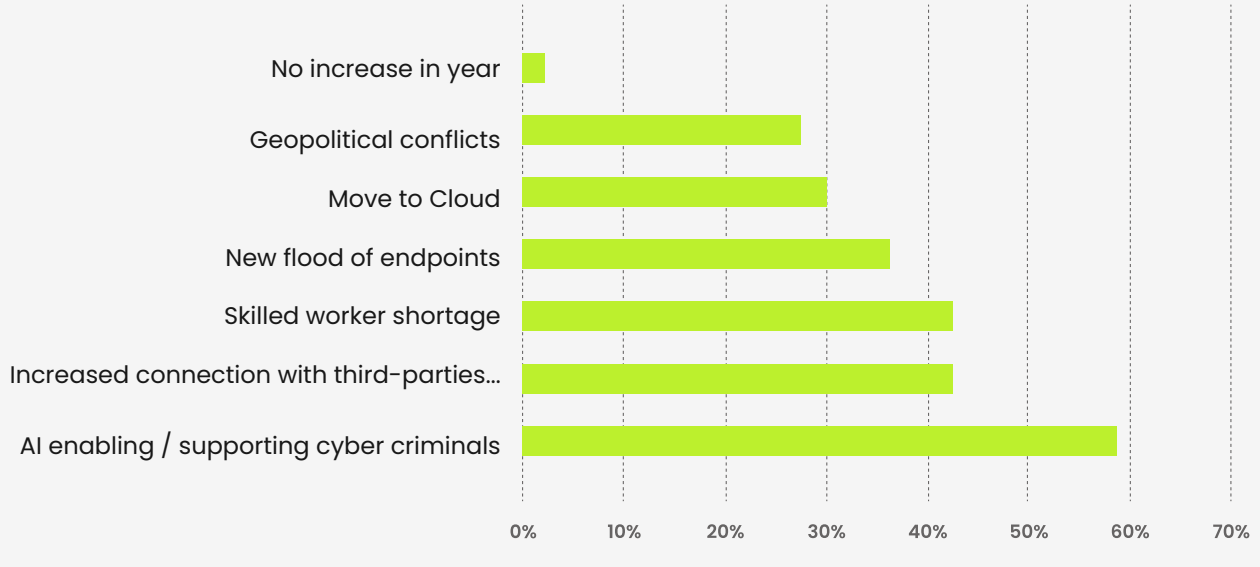
The AI-driven threat does not exist in isolation. It is compounded by systemic vulnerabilities in modern enterprises, especially those who are becoming ever more data driven. Nearly half of our respondents (44%) point to increasingly porous data ecosystems, where third-party integrations and cross-border data flows widen the attack surface.

There are also growing concerns about the talent crisis in cybersecurity. Macro-economic and employment-based trends have clearly widened the potential employer base for talented cybersecurity professionals. Many of those who might have worked for European companies might now be lured into working remotely for American or Middle Eastern enterprises, with the promise of higher salaries. This has created a talent crisis, particularly in Europe, that leaves teams stretched thin and slow to respond. The concern is most pronounced in Germany and Belgium, with 47% of respondents in both countries citing the talent crisis as a major concern. Interestingly, France's figures were lower at 37%, which may reflect a mature talent market for cybersecurity professionals.

Add to this the proliferation of endpoints including mobile devices, IoT nodes, and remote access points, and it becomes clear that organisations are not just fighting smarter attackers, but also defending a battlefield that is vastly more complex than even a year ago. This concern was reflected by our survey respondents with over a third in each country (apart from The Netherlands which was slightly lower) citing it as a reason for increased threats.

Another constant amid all this flux is geopolitical conflict, cited by 28% of respondents, a figure unchanged from last year. That said, the recent escalation of conflict in the Middle East might make this even more worrisome for companies, especially those businesses headquartered in countries whose governments might be playing an active role in the ongoing skirmishes.

Factors increasing the level of cyber risks in European organisations.



THE IMPORTANCE OF MAPPING AN INFORMATION SYSTEM

The aim of mapping is to represent an organisation's information system and its connections with the outside world. It provides insights into all components of the information system and gives a clearer picture of what is involved.

This mapping is essential for controlling, protecting, defending, and ensuring resilience in the event of a cyberattack.

It may concern IT infrastructure, applications, network connections, processes, and resources involved in information system managemen. It is this diversity of information system viewpoints that enables effective monitoring, and optimal reaction time in the event of a security event.

Although there is no single reference, mapping is as much a part of ANSSI's "Information Hygiene Guide" as it is of the French Military Programming Law, or NIS 1 and 2.

Nevertheless, it can be a thorn in the side of security organisations. Mapping can reveal technical debt or obsolete architectures that are ill-suited to security challenges. It can also reveal gaps in documentation, loopholes, and even actions that have slipped under the radar.

Mapping an information system is essential for good IT hygiene, and a valuable tool for identifying and remedying vulnerabilities in applications.

THE SHIFTING ANATOMY OF RISK

Beyond broad risk drivers, organisations are re-evaluating the specific threats that concern them the most, chief among these is the fear of collateral damage from critical infrastructure attacks. **Over one-third (34%) say they worry that a breach targeting power grids, telecoms, or transport systems could indirectly but significantly impact their own operations.** That is more than double last year's figure (16%). This may reflect not only a greater awareness of supply-side interdependence but also a wake-up call from recent high-profile incidents that disrupted services far beyond their immediate victims.

Other fears remain persistent but have shifted slightly in intensity. Concerns about human error, whether through negligence or insider threat, have dipped slightly to 27%, while technical vulnerabilities now worry only 23% of respondents (down from 33%). This could point to increased investment in patching and code security, but it may also signify a dangerous complacency. Supply chain vulnerabilities, similarly, hover at 19%, barely changed from the previous year, which perhaps reflects that the concern had been growing last year and has not abated.

REAL-WORLD CONSEQUENCES: WHAT IS AT STAKE?

If the sources of cyber risk are evolving, so too are its consequences, and European companies are under no illusion about what a breach can mean. The most commonly cited consequence is the leak of sensitive data and information which is feared by 53% of respondents. From reputational damage to regulatory penalties, the ripple effects of data exposure are not just understood but front of mind for many security executives.

More visceral forms of disruption also loom large. Wiping or destruction of information systems (40%), espionage, and intellectual property theft (36%), ransomware lockouts (35%), and outright financial theft (33%) are no longer edge cases. They are core threats. And 30% of respondents warn of a chilling possibility: a complete shutdown of production operations. In sectors like manufacturing, healthcare, and logistics, such disruptions can have immediate and far-reaching societal impacts.

Even when systems stay online, the scars caused by a breach may linger. Nearly one-third (29%) fear damage to their public image, an especially acute concern in industries where trust is paramount.

Léna Jakubowicz
Head of Presales, HarfangLab

"A badly handled cyber crisis can do more than disrupt operations, it can permanently damage customer trust, regulatory standing, and long-term brand reputation.

In the heat of the moment, unclear roles, lack of communication, or uncoordinated technical responses can turn a manageable incident into a strategic failure.

To cope effectively, companies need to embed cybersecurity into every level of decision-making, not just in technology, but in governance, communication, and leadership readiness."

AI: THE DOUBLE-EDGED SWORD

Amid this threat landscape, organisations are not only wary of AI's dark side, they are also pinning their hopes on its potential to tilt the balance back in their favour. An overwhelming 82% believe that AI-enhanced cybersecurity solutions can help defend against AI-enhanced threats.

The confidence in AI as a cyber tool is highest in France (87%) and Germany (85%), with companies in Belgium (71%) and the Netherlands (74%) marginally less optimistic.

Yet the optimism is tempered by realism and an understanding that AI is at its most potent when operated by a human who knows how to make the system work at its optimum. Almost four in five respondents (79%) say that human analysts will remain indispensable, even in an AI-augmented future.

There is also some degree of scepticism about the full potential of AI with 59% saying they are concerned that security vendors overpromise what the technology can deliver. It seems that AI is no longer perceived as a silver bullet, but rather a key weapon in the cybersecurity armory, effective only when integrated into human-led workflows and overseen by skilled practitioners.

This nuanced stance reflects broader shifts in the cybersecurity field. The age of AI security evangelism is giving way to an era of practical implementation, where companies seek solutions that are smart, explainable, fast, and trustworthy.

Joséphine Delas
AI Engineer,
HarfangLab

"As companies rush to harness the power of AI, they're also expanding their attack surface in ways that traditional security models aren't prepared for. The opportunity is immense, from faster detection to smarter automation, but then so is the risk, from model corruption to data leakage.

Cybersecurity teams have a responsibility not just to protect AI systems, but to embed security into their design from the ground up. That means auditing training data, securing inference pipelines, and understanding how adversaries can exploit or manipulate models."

FROM RELIANCE TO RESILIENCE

As European organisations navigate the dual threats and opportunities posed by AI, they are beginning to rethink what security means in a post-linear risk environment. Resilience is replacing reliance, not just on tools, but on trusted partners, robust processes, and an adaptive mindset.

The need for transparent, AI-integrated, and human-driven cybersecurity strategies has never been greater. The research shows that Europe's businesses are under no illusion about the road ahead. But they are also not standing still. The journey from reliance to resilience is underway.

CYBER RISK
PREPAREDNESS AND RESPONSE

As European organisations adapt to an increasingly AI-fuelled threat environment, the question becomes not just whether they are at risk, but whether they are ready to confront that risk. HarfangLab's latest research reveals a paradox at the heart of cybersecurity strategy: while companies largely feel confident in their ability to prevent and detect cyber threats, they remain less certain about how effectively they can respond to incidents once they occur. This gap between anticipation and action could prove critical in an era where the speed and sophistication of cyberattacks are escalating.

STRONG ON PREVENTION, LESS CERTAIN ON RESPONSE

According to our data, 69% of European businesses report feeling well-prepared to prevent cyber incidents, and 70% express confidence in their ability to detect them. These numbers, though slightly down from 72% the previous year, suggest that core cybersecurity frameworks, such as firewalls, threat monitoring and endpoint protection, are widely deployed and reasonably trusted. Many organisations appear to have invested in early warning systems and perimeter defences that give them a sense of initial control.

However, confidence begins to waver when the focus shifts from prevention to response. **Only 65% of businesses say they feel well-equipped to respond to cyber incidents in ways that limit damage, down from 72% in 2024.** This marks a significant drop and indicates a growing recognition that containment and recovery are often the most challenging aspects of cyber defence. In practical terms, this means that while businesses may spot a breach quickly, they may still be vulnerable to operational disruptions and any ensuing financial loss and reputational harm if their response processes are not agile and robust.

This imbalance between detection and response capabilities may reflect several structural issues including fragmented incident response plans, lack of cross-functional coordination during crises, and overreliance on manual processes in a world demanding rapid, automated reactions. It also underscores the reality that as threats evolve, so must the speed and cohesion of the enterprise response.

Part of the problem is the increasing complexity of the cybersecurity landscape as it continues to rapidly evolve. The proliferation of tools, technologies, and acronyms can overwhelm even experienced IT teams, and bamboozle less-technical decision makers. Ultimately this confusion means it is often challenging to discern which solutions are truly necessary. Sadly, many organisations fall into the trap of assuming that a comprehensive platform with dozens of features automatically equates to stronger protection. But more is not always better, at least in this instance. True cybersecurity is about understanding specific vulnerabilities and selecting tools that address those risks with precision.

This is where the role of a trusted cybersecurity partner becomes pivotal. Efficiency and control are not achieved through volume but through clarity. An experienced MSSP (Managed Security Service Provider) can identify real threats and tailor protections to an organisation's unique risk profile. Instead of chasing every new capability, businesses should ask themselves existential questions... "Where is our greatest value? Where are we most likely to be attacked?" With the right guidance, cybersecurity becomes not only more effective, but also more manageable.

Joséphine Delas
AI Engineer,
HarfangLab

"AI can accelerate threat detection and automate responses, but it doesn't replace human expertise.

Behind every intelligent system, you need experienced professionals who understand context, nuance, and the evolving tactics of real-world attackers. Without that human oversight, even the most advanced AI risks making critical misjudgements or being exploited.

In cybersecurity, it's not just about having the smartest algorithm, it's about having the smartest people guiding it."

REMOTE WORK: A WEAK SPOT?

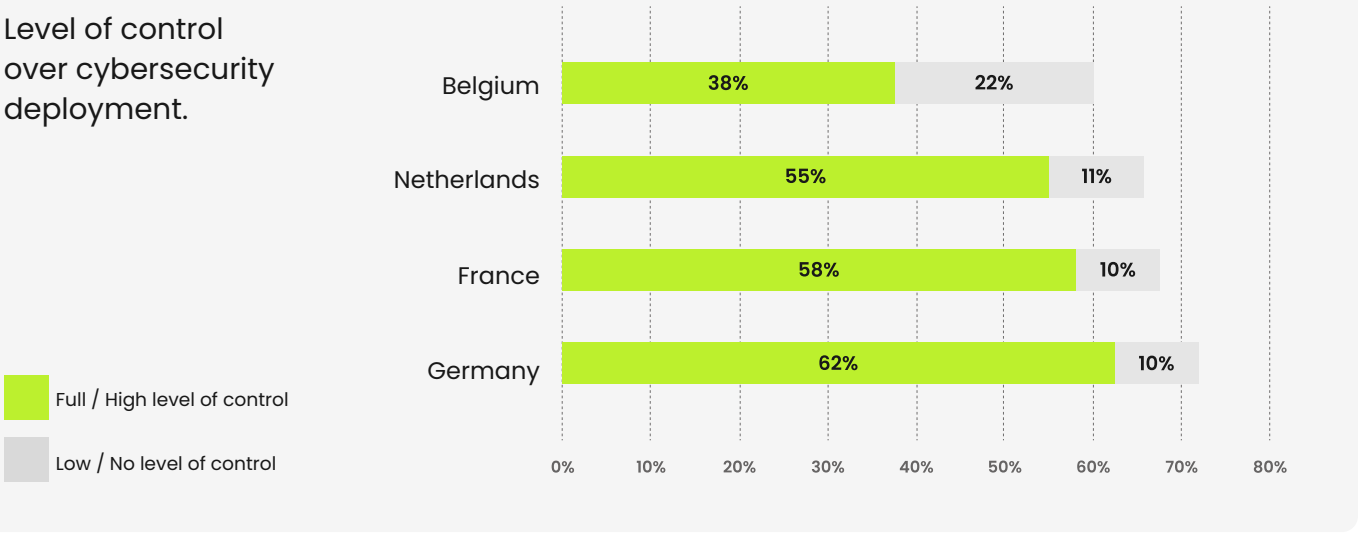
One area where concerns are especially pronounced is remote work. Hybrid and distributed models have become a permanent feature of the post-pandemic workplace, and in some European countries as many as one quarter of employees now work this way. Yet only recently have companies really begun to think through and ultimately tackle the cybersecurity implications of disparate workforce. It has become a key trend in the last year, with the research highlighting that remote work security is now the top driver of a increased cybersecurity investment, with a 28% projected growth in spending.

Home and hybrid working present some very tangible vulnerabilities. Hackers may find it easier to access home networks, personal devices, and unsecured Wi-Fi connections than they do well-protected, on-site networks. Consequently, endpoint management, user authentication, and data loss prevention strategies must now extend well beyond the corporate office. This issue is that not all companies are keeping pace with the new working paradigm and its cybersecurity anomalies. It could be that companies who have already enhanced the security of the remote workforce have done so as a response to an attack where compromised home setups served as entry points for broader network breaches. Other companies who have not experienced this type of cybersecurity challenge might be slower to adapt their systems and policies. Ultimately IT monitoring tools must have a full overview of all potential vulnerabilities on each endpoint, and this can include everything from apps through to upgrades.

THE CONTROL CONUNDRUM

One of the most telling findings of the research is that just 57% of businesses feel they have a “full” or “high” level of control over their cybersecurity deployment and infrastructure updates. In other much more worrying words, nearly half of the organisations surveyed admit to having only limited control over the very systems designed to protect them.

Level of control over cybersecurity deployment.



This gap in control can stem from a number of factors: decentralised IT environments, inconsistent patching and upgrade practices, legacy systems that are difficult to integrate, or reliance on third-party managed services that limit visibility. It is possible, even likely, that this lack of control is directly driving the increased focus on remote work and supply chain security, two domains where visibility and influence are traditionally hardest to maintain.

Moreover, insufficient control raises serious questions about resilience. In a crisis scenario, a delayed or partial response due to weak governance structures can turn a manageable breach into a full-scale disaster. Cybersecurity readiness is not just about having tools in place; it is about being able to coordinate and execute across the organisation in real time.

Most importantly, the concern is not just about the vulnerability introduced by outsourcing or decentralising infrastructure. Rather it is about the deeper implications for compliance and trust. When an organisation lacks control over its critical infrastructure, it naturally raises the question: who does have control? And is that third party secure, transparent, and accountable?

Without clear visibility, it becomes nearly impossible to fully understand what needs protecting, let alone ensure its security. How can a business guarantee the safety of its assets, data, and people if it cannot even define the perimeter of its responsibility? If you are not in control, are you certain someone else is, and are they only acting in your best interest?

SOVEREIGNTY AND TRUST
ARE SHAPING A NEW AGE OF CYBERSECURITY

As European organisations become more attuned to the risks posed by cybercriminals, systemic dependencies, and geopolitical turbulence, the concept of sovereignty in cybersecurity is taking centre stage.

Sovereignty, in this context, refers to the ability of a business, an organisation (like the EU), or a nation, to exert full control over its data, its systems, and the infrastructure supporting them. It is a concept rooted in autonomy and trust. Given the chaotic nature of global politics, its relevance is growing by the day.

Recent years have brought sharper focus to the risks stemming from extraterritorial data access. As conflicts sharpen, so too does the possibility of state-aligned cyber interference, surveillance, or disruption. And it would be short-sighted to think that bad actors were only interested in disputing public entities; companies also need to rethink what tools they use, and where and how those tools operate.

Anouck Teiller
CSO, HarfangLab

"In today's interconnected world, digital sovereignty has become a cornerstone for both nations and enterprises.

As cyber threats escalate in sophistication and frequency, over-reliance on external technologies can expose critical infrastructures to vulnerabilities.

Ensuring control over digital assets and infrastructures is not just a matter of national security but also of maintaining trust and resilience in the face of evolving cyber challenges."

Cloud-based solutions remain popular for their scalability and speed. But their globalised architecture has a downside. The adoption of cloud technology has largely been driven by Silicon Valley with the key global players being Amazon Web Services, Azure (Microsoft), and Google. Yet increasingly companies have been developing concerns over foreign access to sensitive information.

After months of championing sovereignty, IT specialists in the EU have begun switching from US cloud providers to French competitors in order to maintain greater control over their organisations' digital infrastructure and data. **These concerns are backed up by our data which illustrates that over a third (37%) of European businesses say they are extremely or very concerned about foreign access when using cloud-based cybersecurity services.** The concern is even higher among large enterprises, where 47% cite this as a serious issue, compared to 35% of smaller businesses. Ultimately, the driver for digital sovereignty for companies is control and transparency. Organisations increasingly want to be the only decision makers when it comes to their data protection.

Anouck Teiller
CSO, HarfangLab

"The cloud only becomes a problem when it's imposed without strategy or transparency.

From a cybersecurity perspective, what matters is that using the cloud is a conscious choice, not a default, and that organisations retain control over their data, configurations, and threat detection."

A strong 78% of respondents say their leadership is more concerned with digital sovereignty today than a year ago, and 54% say it is a top priority. This is particularly true in France (83%) and Germany (81%). Belgians (71%) and Dutch (64%) are slightly more ambivalent in their views. This rise in C-suite focus reflects a wider awareness that control over digital infrastructure, from cloud servers to cybersecurity solutions, is essential to long-term business continuity and legal resilience.

70% agree that European businesses are too dependent on foreign technology, and 69% express concern that cybersecurity products from outside the EU may be subject to foreign surveillance laws. This is especially sensitive in regulated sectors such as finance and healthcare, where the risk of outsider access is not just hypothetical, but potentially catastrophic.

As a result, there is growing demand not only for local vendors, but for greater investment from the European Union itself. A resounding 79% of businesses want to see the EU invest more in building sovereign cybersecurity infrastructure, signalling that sovereignty is not only a private priority but also a public expectation.

However, some respondents (59%) say they would like to work with European companies, but that unfortunately they often lack features compared to American companies.

Pierre-Louis Mauratille
Operations Director, HarfangLab

"European cybersecurity solutions have a technical level that's equivalent to their American counterparts, and sometimes even better! Look at the latest MITRE Evaluations results, it speaks for itself. Still, if we want to build a strong European ecosystem, increasing their visibility and incentives to purchase them is critical. This requires easier access to financing to support publishers capable of competing with the US market.

The harmonisation of the legislative and regulatory framework and the pooling of certifications currently underway will also contribute to greater clarity regarding constraints and supply.

The key point to remember is that without European purchases, there can be no robust sovereign ecosystem. It is therefore our collective responsibility to build this ecosystem together."

THE STRATEGIC PIVOT TO ON-PREMISES

This unease is already reshaping cybersecurity purchasing strategies. On-premises capability has emerged as the top purchasing criterion for cybersecurity solutions, and 54% of businesses now say that data sovereignty is a critical driver in vendor selection. The perception is clear: security is not just about stopping threats, it is about knowing who can see what, and from where.

One way of gaining greater levels of control is for all a company's data, and the mechanisms that protect it, to be stored locally. This pivot to on-premises cybersecurity started slowly, yet it has been gathering momentum. Most businesses are still tied to either hybrid (42%) or cloud-based solutions (35%) and seem content with those solutions. Yet a notable 17% of businesses are now actively planning a shift to on-premises cybersecurity models.

Feeling like the company has control over its own data is a recurring theme for companies who have shifted to on-premises. In our survey, 31% of respondents cited the desire to manage their own deployments, updates, and infrastructure as a key factor.

Another 28% harbour concerns about sovereign control of data. They want to ensure it remains within national or EU jurisdiction. A similar proportion are looking to sever dependence on foreign cloud providers, while 26% explicitly seek to reduce exposure to foreign surveillance laws or geopolitical instability.

Unsurprisingly, it is the business areas utilising the largest amounts of sensitive data that are leading the pivot to on-premises. Government organisations (27%), followed by healthcare and pharmaceutical firms (24%) and IT companies (17%), are most likely to favour a shift. In these sectors, trust is not optional, it's mission-critical. Sensitive health records, classified data, proprietary algorithms simply cannot be risked in cross-border infrastructures, no matter how sophisticated the cloud security layer may be.

WHY ON-PREMISES IS BECOMING A SOUND CHOICE FOR SOME BUSINESSES

Over the past two decades cloud-based cybersecurity solutions have emerged as the default answer to scale, flexibility, and cost-efficiency of data storage. Yet today, on-premises deployment is experiencing a revival, and for some companies it is the best choice to address their risk analysis requirements.

01

On-premises solutions boast one major advantage over more commoditised cloud-based solutions, and that is control. They enable businesses to manage security architecture internally, without relying on external providers for updates, patches, or uptime. This local control is particularly valuable in incident response scenarios where speed and autonomy are paramount.

02 Another potential advantage on-premises systems offer is more advanced compliance alignment in jurisdictions with strict data localisation laws. These include regulations mandated by GDPR or through national health data regulations. Systems can be developed from day one to meet those requirements. This is less complex and more efficient than having to patch solutions into systems that have been built for universal applications.

03 **On-premises also reduces third-party risk exposure. In a cloud-based setup, a vendor breach could compromise multiple clients across regions. With on-premises, the damage is likely to be more contained.**

Anouck Teiller
CSO, HarfangLab

"On-premises isn't automatically the 'secure' option! It's just one option. Like the old Westerns, there's the good, the bad, and the ugly. Done right, with clear strategy and skilled teams, on-premises can give you tight control and complete cybersecurity.

But without that, it quickly becomes a patchwork of blind spots and outdated assumptions. Security isn't about location. It's about how well you manage and monitor what you've got."

SOVEREIGNTY IN THE AGE OF CYBER RISK

A European context, sovereignty has become a foundational element of digital trust. It speaks to the right of nations and organisations to control their own data infrastructure, independent of external political or corporate influence. Growing international tensions are compelling nations to keep, or gain, autonomy in critical areas like cybersecurity.

This is especially critical in an era where legal frameworks such as the US CLOUD Act allow foreign governments to compel access to data stored on servers operated by companies under their jurisdiction, even if that data resides in Europe. For European businesses, this represents a direct conflict with GDPR principles and has sparked a renewed focus on sovereign cloud initiatives and data localisation.

Digital sovereignty is not simply about where data is stored, but also who controls the software supply chain, how encryption keys are managed, and whether third-party code introduces hidden dependencies. Sovereignty encompasses everything from governance structures to the geopolitical alliances of vendors.

Ultimately, sovereignty is about trust. In cybersecurity, that trust must be earned not only through technical excellence, but through jurisdictional clarity, operational transparency, and legal alignment.

CYBERSECURITY
MADE IN EUROPE

Amid mounting global cyber threats and a shifting regulatory landscape, European businesses are voicing strong support for frameworks that protect their sovereignty and create trust across borders. While regulation can add layers of complexity and responsibility, the overwhelming consensus from our survey makes it clear that European cybersecurity rules are worth it.

An overwhelming 94% of respondents said European and local cybersecurity regulation is necessary, with more than half (58%) calling it absolutely essential. one-third (36%) suggested the regulations be scaled back slightly.

EUROPE AS A STANDARD BEARER

Businesses across the continent recognise that European cybersecurity regulations, such as GDPR, have evolved into global benchmarks. **70% of respondents agreed that Europe has become a role model for the world in cybersecurity and data protection regulation.**

It is not only European companies that appreciate the continent's cybersecurity framework. Indeed, 71% say their business partners who operate outside of the continent actively appreciate the European level of digital protection, and 67% believe it gives them a competitive edge. This suggests that compliance with European standards is increasingly viewed as a trust signal in B2B relationships across supply chains and sectors.

European cybersecurity today is competing to be more trusted, equally (or more) capable than their American or Asian counterparts, and wholly aligned with local values. When companies choose sovereign cybersecurity vendors, they are not rejecting global innovation. Rather they are choosing solutions that respect European governance and the values and traditions underpinning it.

From a business standpoint, this positioning matters. Clients and partners increasingly ask detailed questions. Where is the data stored? Who owns the infrastructure? What are the levels of compliance? Sovereign vendors have clear answers to these questions. And that builds trust.

Moreover, European vendors are proving that sovereignty does not mean compromise. Whether in threat intelligence, automation, endpoint defence, or incident response, European-built tools are now competing on features, scalability, and ease of integration. They offer support that is culturally and linguistically attuned to their markets, and product development cycles that are rooted in EU norms and standards.

Anouck Teiller
CSO, HarfangLab

"Being sovereign means offering an infrastructure and tools that adapt to the client's expectations, compliance rules, and values – no matter what they are. The client should stay in control, not the security provider. Technologies should be an asset, not a source of further fears and breaches.

That's what sovereignty'sabout: restoring power to the hands of the end-client."

WHAT BUSINESSES WANT IN A CYBERSECURITY PARTNER

So how do these attitudes translate into buying decisions? And what do companies actually look for in cybersecurity vendors? Here, the research challenges some widely held assumptions.

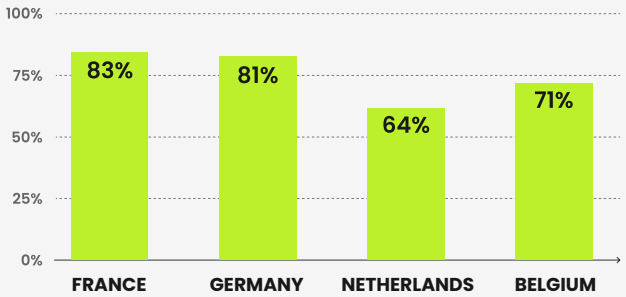
Performance is certainly important, but not always the top priority. Only 22% of respondents say performance (or proof of it) is their leading selection criterion when choosing a vendor. Instead, businesses are placing increased emphasis on sovereignty, control, and alignment with operational models.

For example, 26% say the capacity to deliver on-premises deployments with equivalent functionalities is a key factor in vendor selection. This reflects a deeper concern for compatibility with internal systems, autonomy in deployment, timely updates, and legal jurisdiction over data handling.

Following performance and on-premises deployment that delivers features equivalent to cloud deployment, the 3rd top criterion on the list is the quality of customer service and the human factor. Feeling like they can communicate, ideally during the same working hours with experts who are responsive, reactive, and accessible is particularly critical in today's environment where human resources are missing. This human factor is particularly important for French respondents, who put the quality of customer service as their number one top priority.

In other words, European buyers are no longer just comparing feature sets, rather they are evaluating strategic fit, long-term control, human expertise, and understanding of context and geopolitical risk. Vendors that align with these priorities, especially those rooted in or fully committed to Europe, are gaining ground in a market increasingly shaped by values as much as by technology.

Decision makers are more interested in sovereignty than one year ago.



RECENT MOVES IN EUROPEAN CYBERSECURITY CONSOLIDATION

There is clear momentum behind the "Cybersecurity Made in Europe" movement.

In recent months, several consolidation efforts have reinforced the depth and scalability of European cybersecurity expertise. A standout example is HarfangLab's collaboration with Austrian antivirus provider IKARUS, combining endpoint detection and response with legacy malware defence to offer enhanced protection for both public and private clients.

Similarly, the joint move between Sekoia, HarfangLab, and Infinigate to bundle their solutions is a signal of European vendors working together to create sovereign, interoperable security stacks capable of rivalling the best of what the US and Asia have to offer.

CONCLUSION

It is no surprise that the findings of this report underscore the urgent need for European organisations to prioritise cyber resilience in the face of an increasingly volatile threat environment.

In light of rising threats driven by AI, geopolitical tensions, and growing complexities created by changing workplace practices, businesses should adopt a proactive and adaptive approach to cybersecurity.

Yet, as our research reveals, awareness alone is not enough. Organisations must bridge the gap between threat detection and effective response. Sure, they need to be able to identify risks, but they also need the tools to mitigate them swiftly and decisively.

Central to this transformation is the growing importance of trust and strategic autonomy and, in particular, control and sovereignty. Can European companies rely on providers from the US and Asia in the way they used to?

The clamour for sovereign cybersecurity providers reflects a broader shift toward reclaiming digital independence. Europe is leading by example. Regulations like GDPR and NIS2 have set global standards. Now the continent needs to take these strong foundations and build on them.

Resilience is not just about defence, but about creating an ecosystem where innovation, security, and trust coexist.

This report serves as both a call to action and a roadmap. It highlights the critical steps needed to move from reliance to resilience. By harnessing the right strategies, partnerships, and tools, European organisations can turn challenges into opportunities. By making the right decision now they can ensure they remain secure, sovereign, and ahead of the curve.

METHODOLOGY

The report is based on research conducted by Sapio Research, commissioned by HarfangLab. The interviews took place in Q2 2025 and surveyed over 800 IT and cybersecurity leaders across France, Germany, Belgium, and the Netherlands. Business sizes ranged from 300 to 5,000 employees, covering sectors including healthcare, manufacturing, technology, and government services.

ABOUT HARFANGLAB

HarfangLab is a global cybersecurity provider specialized in endpoint protection against known and unknown threats.
Founded in 2018, HarfangLab detects 100% of attacks and neutralizes them on workstations and servers, all while providing a comprehensive mapping of your IT infrastructure. As the European leader in the latest MITRE ATT&CK Evaluations, its EDR was the first to be certified by the French National Cybersecurity Agency (ANSSI). Together with its EPP, HarfangLab protects hundreds of customers worldwide, including public administrations, companies of all sizes, and international organizations across highly sensitive sectors.

Your security, your choice. Deploy via the Cloud or On-Premises. The HarfangLab platform integrates natively with industry-leading security tools, leverages in-house AI technology, is fully operable via API, and ensures complete transparency into data and detection rules – delivering strategic autonomy for SOC teams and the organizations they defend.

For more information, visit us harfanglab.io

Press contact:
Noemie Minster
noemie.minster@harfanglab.fr

Marketing contact:
marketing@harfanglab.fr

HarfangLab