InfoBrief, sponsored by Microsoft | January 2026

Preparing for NIS2 and Beyond: The Next Phase of Cyber Resilience in EMEA

Progress Since 2024, Emerging Pressures, and the Role of Modern Security Platforms

Mark Child
Associate Research Director,
European Security, IDC

Ralf Helkenberg
Senior Research Manager,
European Privacy and Data Security, IDC

Table of Contents

CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

Executive Summary 3

Pan-European Overview 7

Country Snapshot 27

Executive Summary

Europe’s NIS2 Readiness at a Turning Point

- In the 18 months between the first and second survey cycles, the direction of travel became clear: European organizations are now more aware and more ready to comply with the NIS2 directive, with **greater board engagement, budget allocation**, and **resources for implementing changes**.

- Despite this visible progress, **a readiness gap persists**, with many organizations seeing cyber-risk management as recommended rather than mandatory. Additionally, organizations operating across multiple EU member states find it difficult to stay abreast of all the unique requirements.

- Complexity and a lack of integration between solutions are seen as the enemies of security: the majority of organizations are focused on **consolidation** to improve overall security posture and capabilities. Many organizations are exploring – or already using – **GenAI-augmented solutions** to improve their security capabilities across multiple areas.

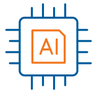
- Based on the full survey data, IDC segmented all 2,000 respondent organizations into five maturity tiers for NIS2 readiness: Aware (the least mature), Capable, Equipped, Advanced, and Ready (the most mature). From 2024 to 2025 the share of organizations in the bottom two tiers has decreased while **the share in the top two tiers has increased**.

Executive Summary

Member state readiness has improved, but more than **1 in 5** organizations still say they lack timely and clear guidance from their national cybersecurity authorities.

Data security and cloud security are the top two modernization priorities for 2026, each mentioned by a third of respondents. AI security risk management follows, at **29%**.

17.5% of organizations believe they are already compliant with NIS2. A further **67.4%** expect to be within 12 months.



Across multiple security fields, from cloud security and IAM to data protection and information governance, more than **40%** of organizations have already implemented GenAI solutions.

Vertical market highlights: progress is uneven by sector	Banking	Energy	ICT Service Management	Healthcare	Manufacturing	Public Administration
By when does your organization expect to have all required security measures in place for NIS 2 compliance? – Already compliant	20.6%	17.9%	17.0%	13.0%	17.6%	14.3%
To what extent has using GenAI improved the efficiency and effectiveness of your security operations? - Significant improvement	18.6%	16.8%	19.1%	8.8%	11.1%	12.0%

Vertical Highlights

	Aerospace & Defense	Digital providers	Digital infrastructure	Energy	Banking	Financial market infrastructures	Public administration	Health	ICT service management	Manufacturing	Transport and logistics	Water, wastewater, waste mgmt
Q3. BARRIER - Lack of resources for implementing changes to policies, practices, or processes	15.8%	21.6%	24.4%	26.9%	24.1%	36.1%	23.2%	21.4%	25.8%	24.9%	23.5%	21.1%
Q3. BARRIER - A lack of capable and knowledgeable technology partners to guide and support us	21.1%	25.6%	27.6%	17.9%	21.2%	19.3%	22.3%	20.1%	25.8%	21.5%	25.4%	26.3%
Q7. When compliant - Already compliant	33.3%	19.9%	13.5%	17.9%	20.6%	19.3%	14.3%	13.0%	17.0%	17.6%	17.8%	21.1%
Q7. When compliant - Longer than 18 months	3.5%	2.8%	3.3%	2.1%	2.9%	1.2%	4.5%	3.9%	1.1%	3.6%	2.8%	10.5%
Q10. Digital sovereignty is a primary factor shaping our technology choices and deployment locations	19.3%	11.4%	17.1%	15.2%	22.9%	20.5%	11.6%	11.7%	23.6%	15.5%	19.7%	10.5%
Q11. Consolidation - Yes, we are significantly reducing vendors	38.6%	23.9%	16.0%	26.2%	19.4%	12.0%	8.0%	18.2%	19.8%	15.0%	17.4%	26.3%
Q13b. To what extent has using GenAI improved the efficiency and effectiveness of your security operations? - Significant improvement	12.7%	9.8%	12.5%	16.8%	18.6%	16.0%	12.0%	8.8%	19.1%	11.1%	13.2%	10.5%
Q14. How ready is your organization to adopt autonomous AI agents within security tools ...? - Actively evaluating or piloting	8.8%	14.8%	21.8%	22.1%	23.5%	21.7%	13.4%	18.2%	29.7%	20.0%	21.1%	15.8%
Q15. How would you rate your organization's current level of security for AI environments - Advanced	3.5%	8.5%	10.2%	11.7%	15.9%	13.3%	8.9%	11.7%	17.0%	7.5%	13.6%	10.5%
Q19. To what degree does your security modernization align with your organization's overall business modernization goals? - Fully aligned	10.5%	6.3%	7.6%	7.6%	12.4%	10.8%	5.4%	5.8%	14.8%	8.5%	9.9%	21.1%

Pan European Overview

The Evolving NIS2 Landscape

From Directive to Operational Reality

COUNTRY	EXPECTED DATE	STATUS / NOTES	"Lack of timely and clear advance guidance from our national security authorities"*
Belgium		Transposed	21.4%
Croatia		Transposed	Not surveyed
Czech Republic		Transposed	30.0%
Cyprus		Transposed	Not surveyed
Denmark		Transposed	23.1%
Finland		Transposed	23.1%
Germany		Transposed	26.4%
Greece		Transposed	20.0%
Hungary		Transposed	8.0%
Italy		Transposed	27.0%
Latvia		Transposed	Not surveyed
Lithuania		Transposed	Not surveyed
Malta		Transposed	Not surveyed
Romania		Transposed	21.4%
Slovakia		Transposed	18.0%
Slovenia		Transposed	Not surveyed
Austria	January 1, 2026	Imminent	20.0%
Estonia	January 1, 2026	Imminent	Not surveyed
Ireland	Late 2025 / Early 2026	Imminent	34.0%
Poland	End of 2025	Imminent	19.3%
Sweden	January 15, 2026	Imminent	23.1%
Bulgaria	Mid-2026	In progress	36.7%
France	Q1 2026	In progress	32.0%
Luxembourg	January 2026	In progress	Not surveyed
Netherlands	Q2 2026	In progress	27.1%
Portugal	April 1, 2026	In progress	22.9%
Spain	Q1 2026	In progress	21.0%

- Despite transposition delays, most EU member states are on course to ensure that the NIS2 Directive will be in force in 2026, with completion of the process imminent in multiple states. Organizations no longer have the safety blanket that the law is not in force yet: readiness is now a requirement!
- Regulatory clarity is improving as more and more member states complete transposition of the Directive. However, many organizations still feel they lack guidance from the authorities. That challenge is multiplied for organizations operating across more countries.
- Despite these challenges, there is an increase in organizational confidence and activity compared to 2024, with fewer organizations struggling for budget or resources, and greater awareness of how their existing capabilities map to requirements.

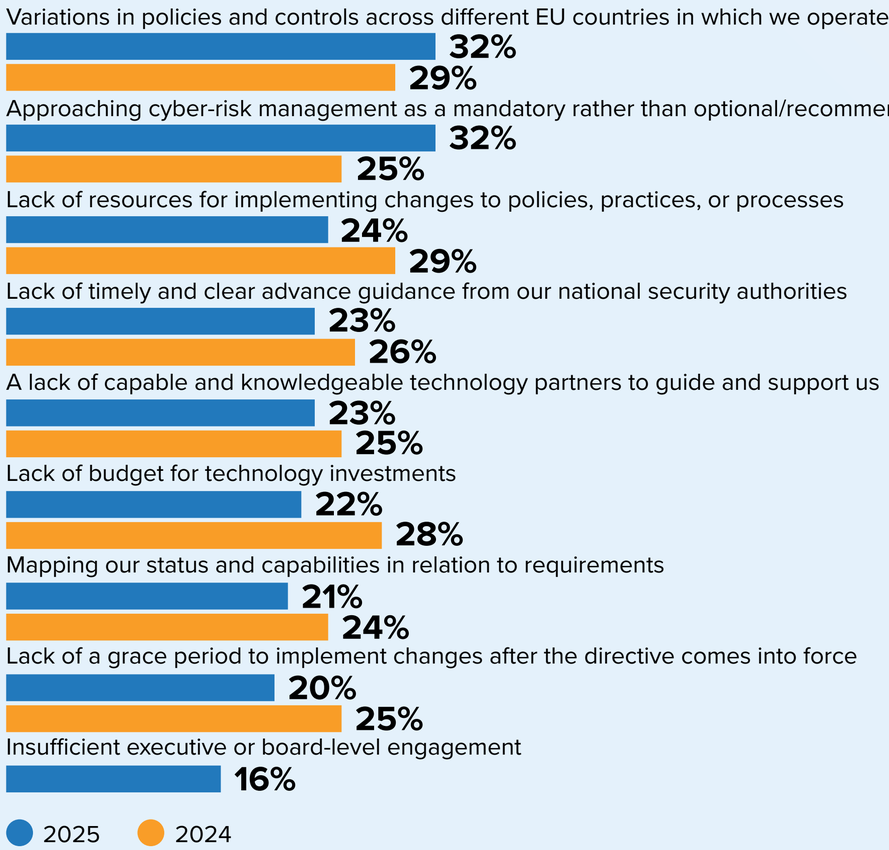
*Share of organizations citing lack of timely and clear advance guidance as a top 3 challenge to achieving NIS2 compliance

The Evolving NIS2 Landscape

From Directive to Operational Reality

How Challenges in Achieving NIS2 Compliance Have Shifted from 2024 to 2025

Which of the following issues present the greatest challenges for your organization in achieving NIS2 compliance?



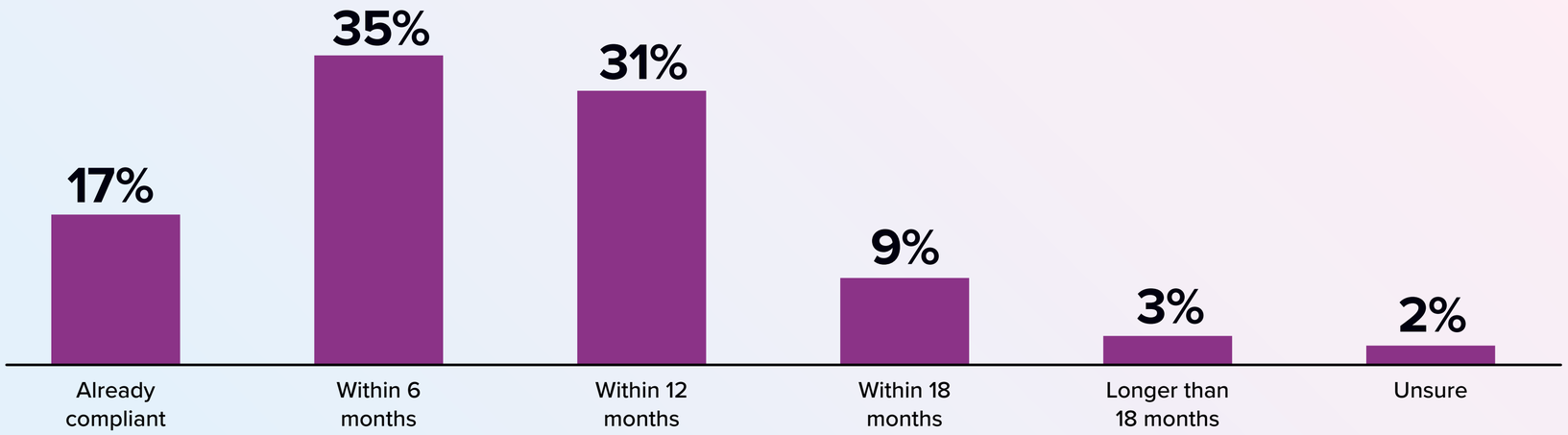
- Two factors have emerged as the top challenges for achieving NIS2 compliance: the **difficulties of managing varying requirements across multiple countries**; and the **shift from perception of security as "recommended" to "mandatory"**.
- Year-on-year, the share of organizations struggling with lack of budget or lack of resources has dropped by 5-6 percentage points. Similarly, the number of organizations looking for a grace period to implement changes has also dropped. Lack of board-level engagement was the lowest ranked response.
- The bottom line is that **organizations are ready to take actions and implement changes** – they just need guidance and support to ensure those changes are the right ones.

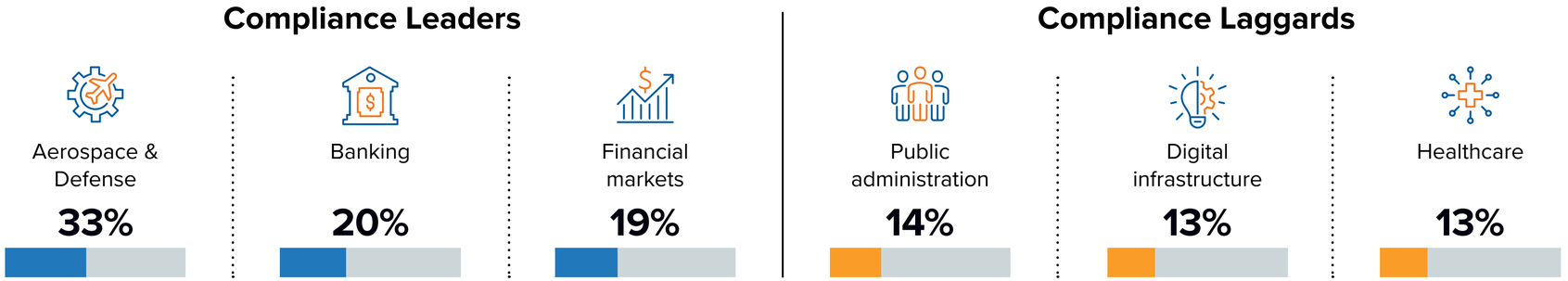
The Evolving NIS2 Landscape

From Directive to Operational Reality

Timeline Optimism

By when does your organization expect to have all required security measures in place for NIS2 compliance?





Share of organizations in each sector stating they are Already Compliant with NIS2

- With transposition of the Directive completed or imminent in the majority of member states, the outlook is generally positive, with **53.3%** of organizations either **already compliant** or expecting to be **compliant within 6 months**. However, that still leaves a substantial share of organizations facing the risk of **compliance penalties**.
- Having a supportive partner can be critical. Among organizations that rated the support of their lead NIS2 partner as Very High, 49.7% say they are already compliant. Among those that rated the support as Low, only 16.0% are already compliant.

Maturity in Motion

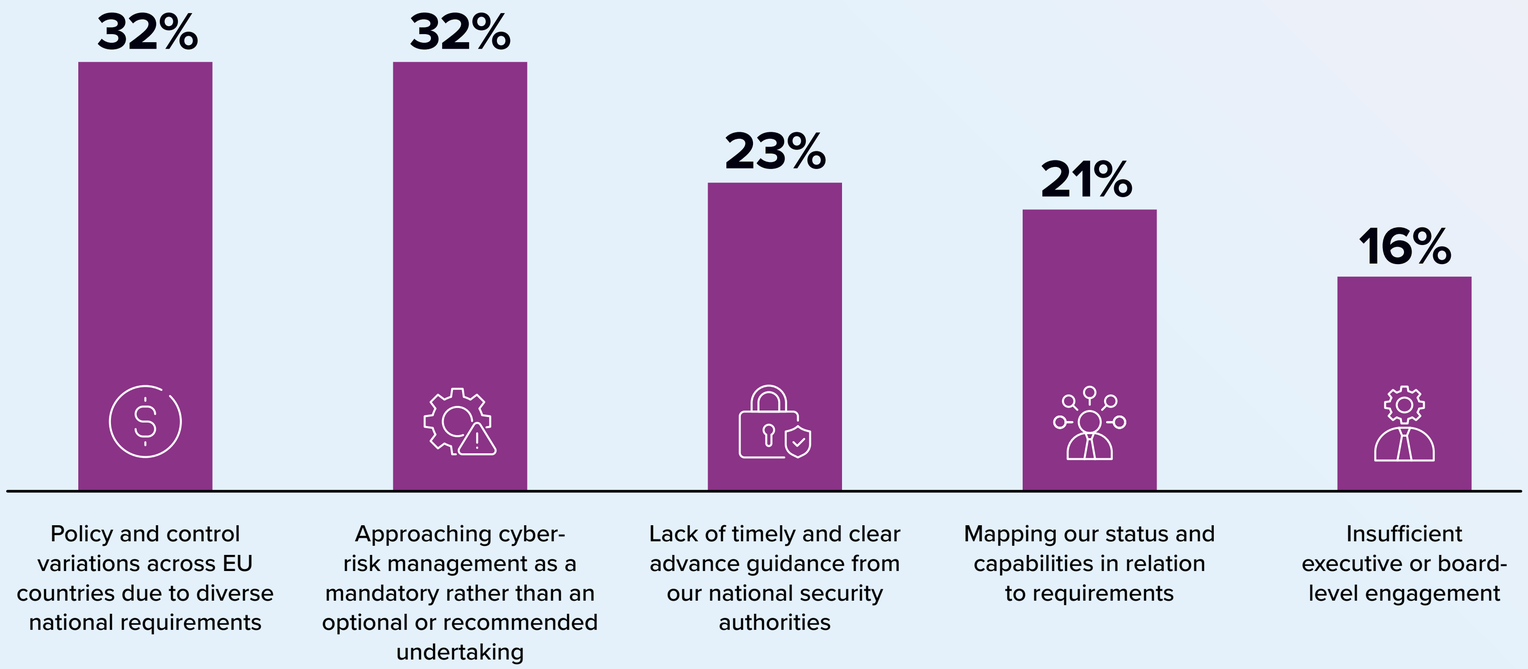
The Five-Tier NIS2 Readiness Model

Aware	Capable	Equipped	Advanced	Ready	
5%	14%	35%	30%	17%	2025
-4pp	-3pp	+2pp	+3pp	+3pp	
9%	17%	33%	27%	14%	2024
Organizations at this level have a basic understanding of NIS2. They are beginning to recognize its importance and are aware of the need to align with its requirements. This stage is about gaining knowledge and understanding the scope of what needs to be done.	At this stage, organizations have moved beyond basic awareness and are capable of taking action. While they have started to put policies and procedures in place to meet some NIS2 requirements, there is still work to be done to ensure full compliance.	Organizations scoring in this range are equipped to handle most of the challenges presented by NIS2. They have a solid grasp of the directive and have implemented a significant number of measures. They are well on their way to achieving a strong cybersecurity posture.	These organizations are advanced in their preparedness. They have not only addressed the majority of the NIS2 requirements but also put robust processes and technologies in place. They are likely to be seen as leaders in cybersecurity within their industries.	Organizations at the ready level exhibit the highest degree of preparedness. They have fully integrated NIS2 requirements into their operations and are continuously improving their cybersecurity measures. They serve as benchmarks for best practices in the field.	

Awareness & Knowledge

Progress but Not Yet Universal

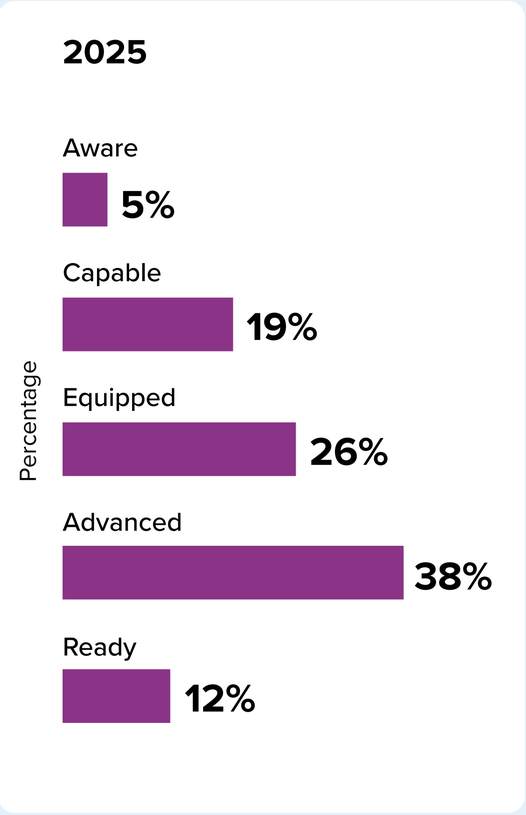
Which issues present the greatest challenges for your organization in achieving NIS 2 compliance? [Selected responses]



- The first question any Board should ask its CISO in relation to NIS2 is “Are we compliant?” The survey data shows that for the majority of organizations (88.3%), mapping their status and capabilities in relation to requirements is not a major barrier.
- At the same time, almost a quarter of organizations say their national security authorities are not providing enough timely and clear guidance: this needs to be addressed.
- Compared to the 2024 survey, executive or board-level engagement is now much stronger – this was the lowest-ranked barrier of all the responses.
- At the same time, almost a third of organizations still need to get over the hurdle of viewing cyber-risk management as recommended rather than mandatory.
- Overall, the awareness metrics are improving year by year. This puts organizations in a position to assess their technical readiness and look at the investments necessary to accelerate their journey to compliance.

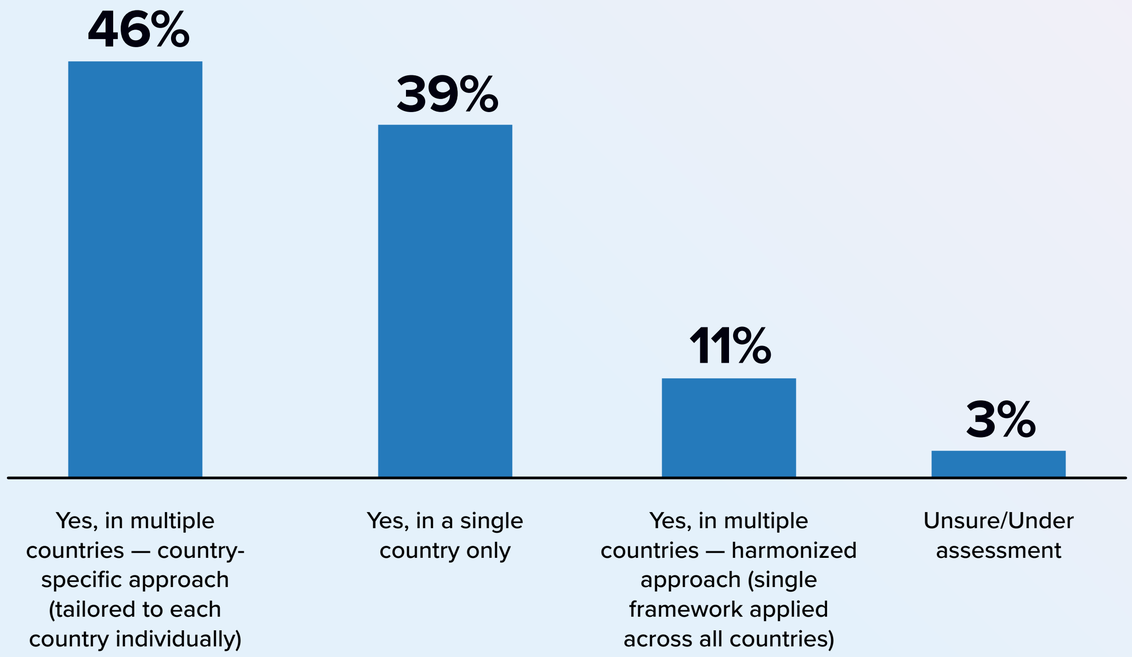
Awareness & Knowledge

Multi-Country Compliance



Seeking Multi-country compliance

Is your organization seeking to achieve NIS 2 compliance in one or more countries?



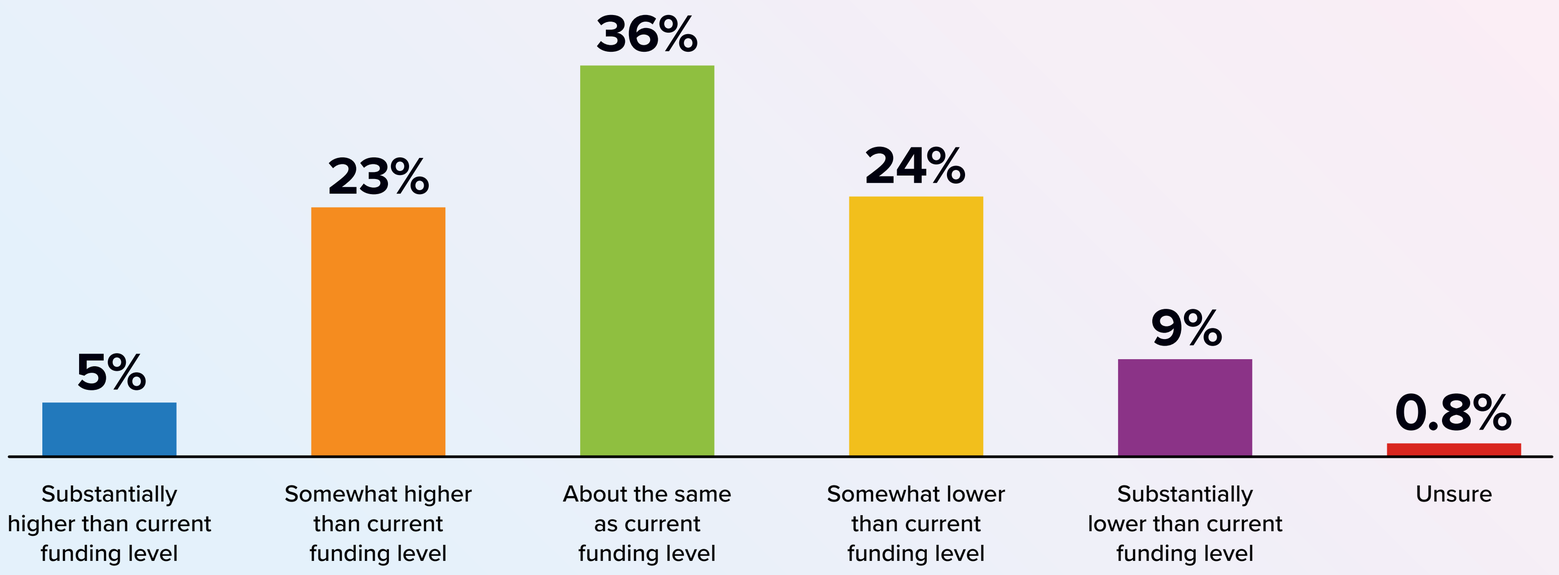
- The majority of organizations (57.3%) need to be NIS2 compliant across multiple countries; yet this complexity is one of the top challenges (cited by 32.0%) in achieving compliance.
- Within certain vertical sectors, that share is even higher:

35%	Manufacturing
35%	ICT Service Management
35%	Healthcare
34%	Financial markets

Governance & Compliance

Strong Intent, Uneven Execution

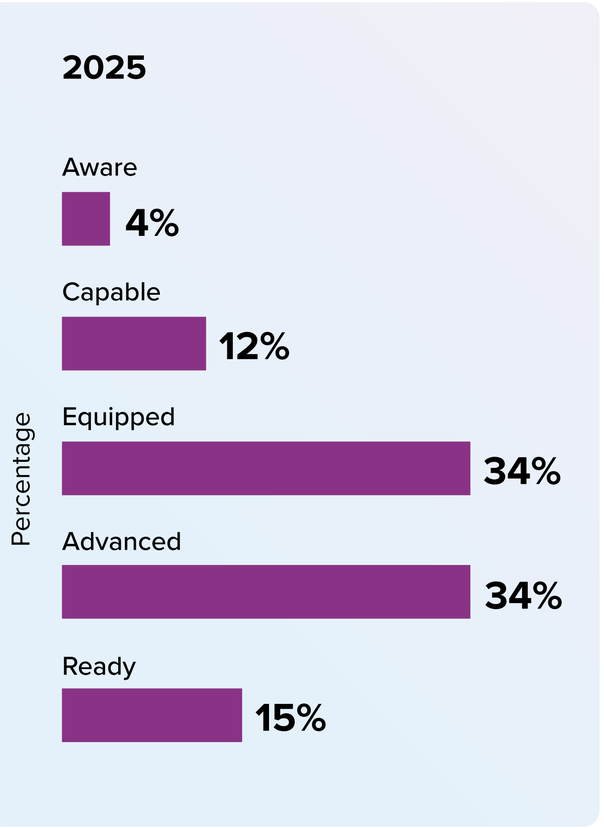
Twelve Months NIS2 Funding Outlook



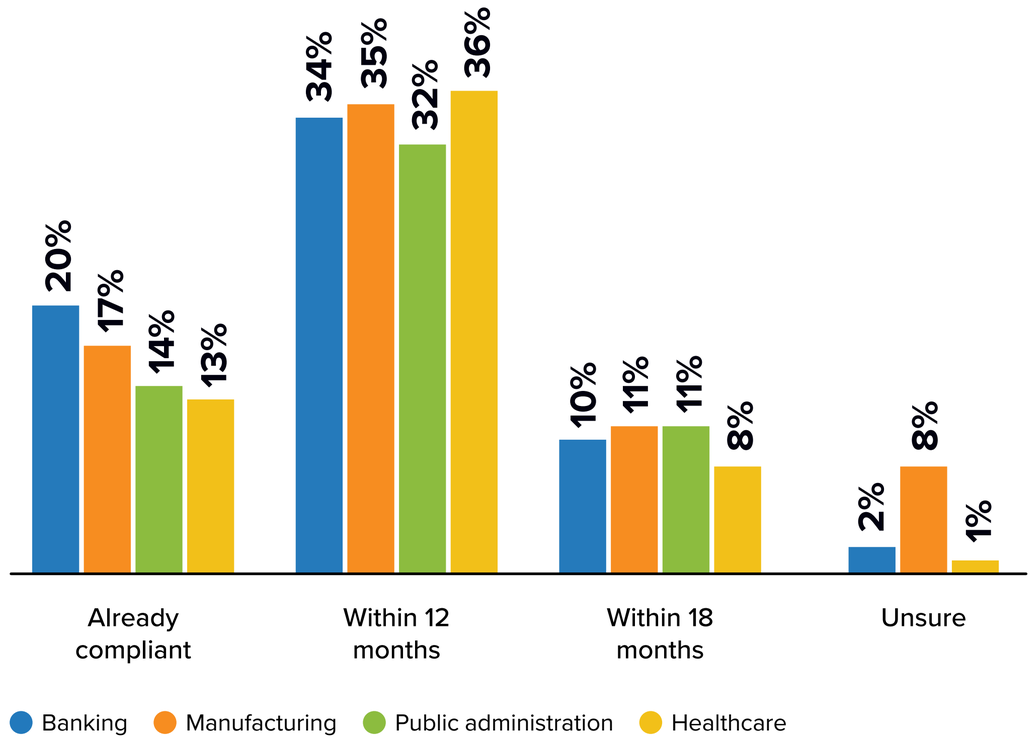
- Overall, 30% of European organizations are increasing their funding for NIS2 compliance over the next 12 months, with a further 36% maintaining spending.
- The investment outlook is even more positive in the Financial Markets (34.9% increasing), Digital Infrastructure (33.8%), and ICT Service Management (38.5%) verticals.
- Perhaps surprisingly, the biggest share of organizations saying they are seeing reduced funding is the Aerospace and Defense vertical (61.4%). However, as that sector also has the highest share of organizations saying they are already compliant, it appears that those mature organizations are already looking beyond NIS2 to new priorities.

Governance & Compliance

Compliance Timeline



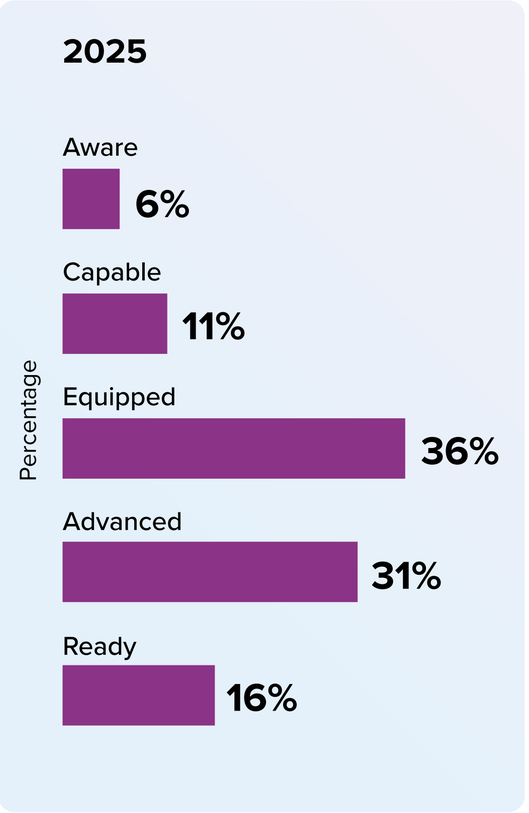
Compliance Timeline by select verticals



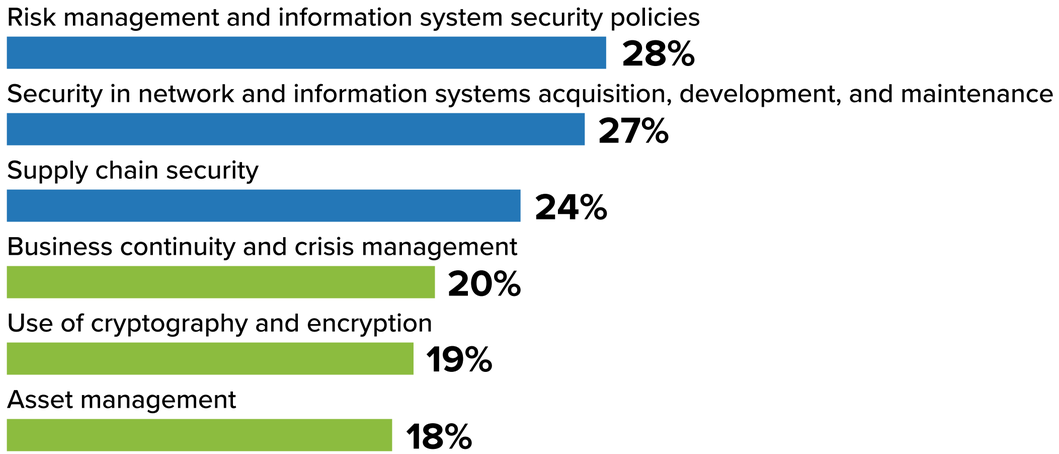
- Compliance timelines are generally positive with 17.5% of organizations claiming they are already compliant and a further 35.8% expecting to achieve compliance within the next 6 months – by which time, the Directive will be in force in most (but not all!) member states.
- There is a gap, however, with more than 40% expecting it will take 12–18 months to achieve compliance and some organizations anticipating even longer than that.

Risk Management & Security Practices

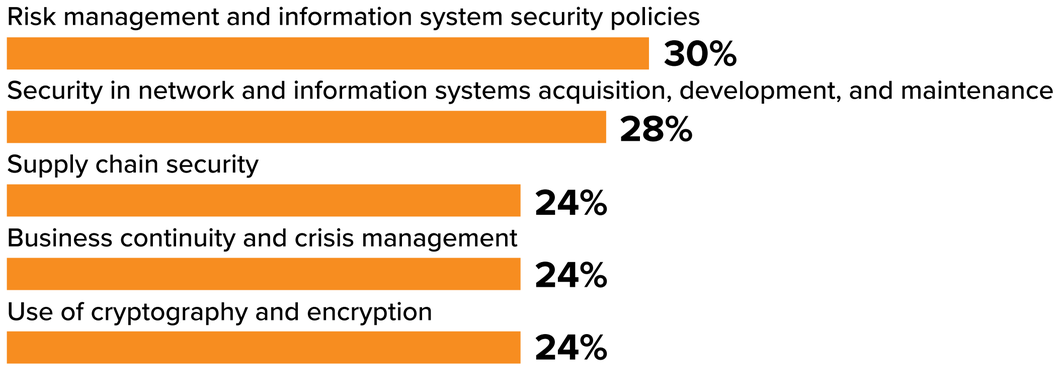
Toward a Technology-Led Compliance Model



NIS2 Requirements: Top 3 and Bottom 3 Gaps



2026 Top 5 Security Technology Priorities



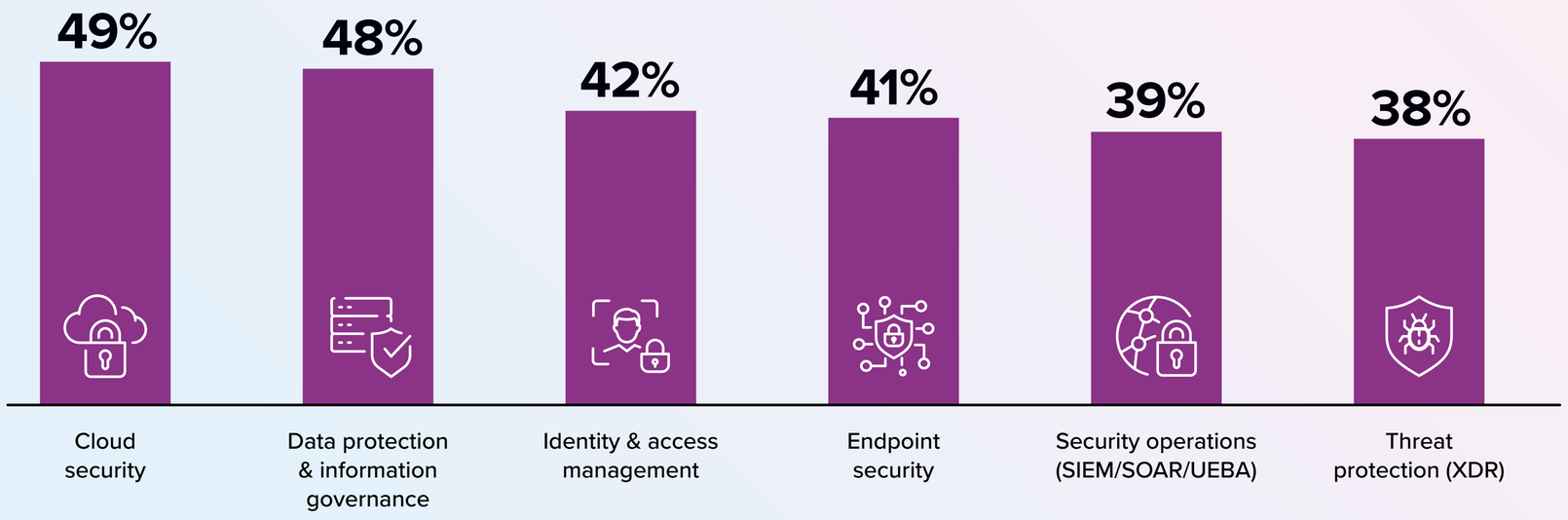
- European organizations are positive about their security readiness, with high confidence levels around business continuity management and incident handling. Concerns persist, however, around core risk management frameworks and the security controls and policies applied around acquiring, developing, and maintaining their networks and information systems.
- Despite those concerns, organizations are moving forwards with security technology adoption plans for 2026 as they strive for NIS2 compliance. Cloud security solutions are the top priority (30.6%), followed by encryption and data security (28.7%). Identity and access management (IAM), security analytics, and backup and recovery solutions are also high on the priority list.
- These technology investments are not just checklist security. European organizations are on a maturity journey towards continuous controls and, with some heavy organizational lifting, a more risk and governance-led approach to security.

Risk Management & Security Practices

Using GenAI for Security Operations

GenAI for Security

In which of the following security product areas has your organization implemented, or is it planning to implement in the next 12 months, GenAI, such as copilots?

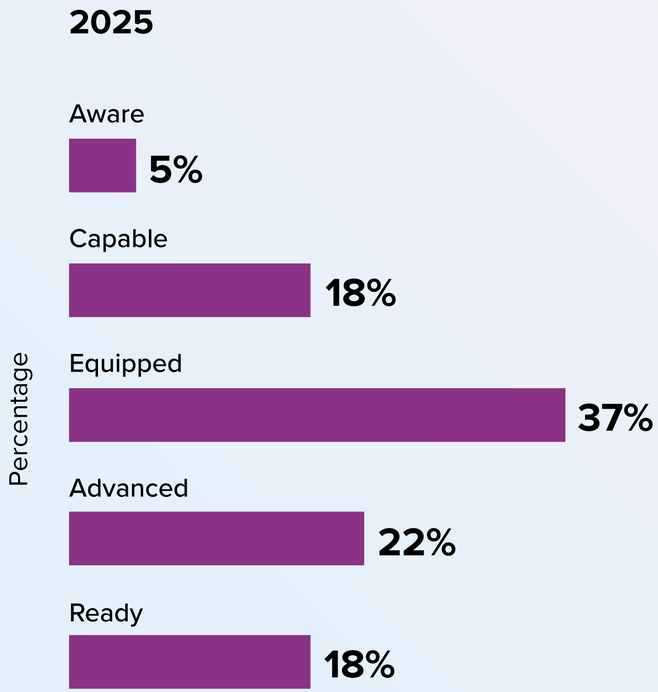


- AI represents a key weapon in the security arsenal and pilots have become reality with GenAI implementation penetration at 40-50% across a range of security disciplines, from cloud security to data protection and information governance.

  However, the AI environments themselves also need protecting and more than half of European organizations state that their level of security is either Basic or Developing (bottom two boxes). **This must be a priority for 2026**.

Strategic Alignment & Information Channels

NIS2 Shaping Enterprise Security Strategy



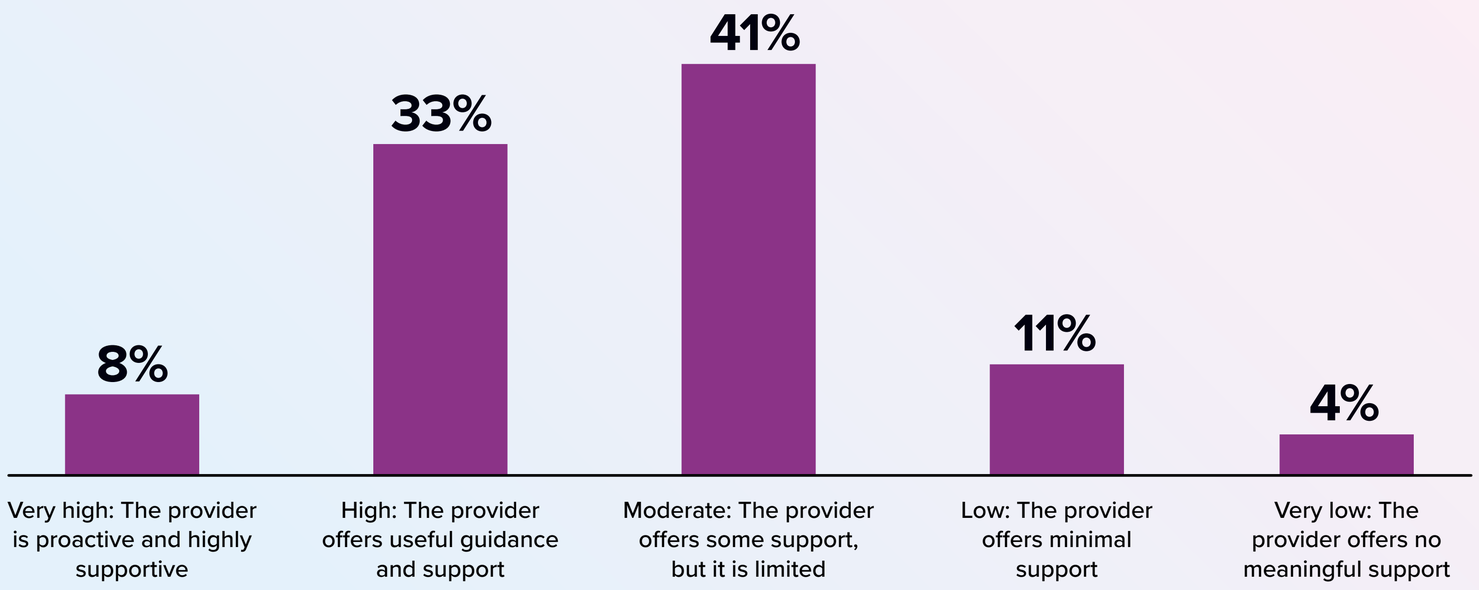
Security Modernization Strategy aligned with Business Goals

- Security modernization has emerged as a strategic imperative, for achieving NIS2 compliance, but also for going beyond that, for robust cyber risk management and continuous improvement of security posture. This is driving increasing alignment of security modernization with business goals.
- Nevertheless, fewer than 1 in 10 European organizations say that their security modernization strategy is fully aligned with their business goals. Although a further 31.0% say they are “mostly aligned”, that leaves 60% of the market with significant room for improvement.
- Consolidation is a significant component of security modernization. Almost three quarters of European organizations aiming to reduce the number of security vendors they work with and consolidate their environments.

Strategic Alignment & Information Channels

Lead Partners

Lead Partner Support for Achieving NIS2 Compliance



Compliance support becomes a crucial aspect of strategic security partnerships

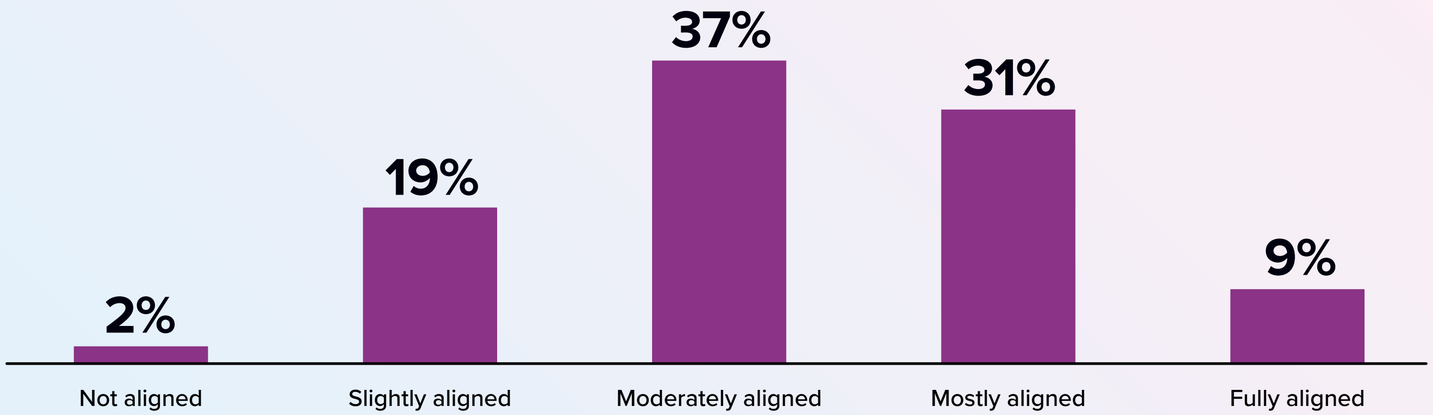
- In addition to their technology platforms and capabilities, strategic security partners are also judged on compliance leadership. The assessments are varied: 58% of organizations say their lead NIS2 partner offers no support or very limited support; conversely, 42% say their partner offers useful guidance or are proactive and highly supportive. The former group stands at a competitive disadvantage. To put it another way, those that are ready to support clients and prospects in their compliance journey have significant opportunities ahead.

The alignment of multiple factors – security strategy, business strategy, and IT strategy – is often what separates Tier 2 or Tier 3 organizations (Capable or Equipped) from Tier 4 and Tier 5 organizations (Advanced and Ready)

Security Modernization

Strengthening Resilience, Efficiency and Compliance

Lead Partner Support for Achieving NIS2 Compliance



Top 5 Expected Benefits of Security Modernization

- Improved resilience to cyberattacks
- Access to advanced technologies
- Cost efficiency and reduced operational overhead
- Better visibility & control across IT and OT
- Stronger alignment between security and business objectives

- Cyber modernization upgrades infrastructure, tools, and processes to maximise value by reducing organizational risk, improving efficiency, and optimising resources through automation and legacy system upgrade. It strengthens governance and leverages advanced technologies, including cloud-native security and AI-driven threat detection, to stay ahead of evolving cyber threats.
- Ensuring security alignment with business strategy further strengthens outcomes. Most organizations report their security modernization efforts to now be either moderately (38%) or mostly aligned(31%) with business strategy. This reflects a shift from reactive, compliance-driven investments toward more deliberate, capability-focused programmes that support digital transformation and operational resilience.
- The expected benefits of security modernization include improved cyber resilience, greater operational efficiency, and access to advanced technologies. It is also expected to better align security initiatives with business objectives, enhancing overall organizational value.

Security Modernization

Strengthening Resilience, Efficiency and Compliance

Top 5 Focus Areas For Security Modernization

1

Data Security

Protecting sensitive information through robust governance, encryption, data loss prevention and real-time monitoring to prevent breaches and meet regulatory requirements.

2

Cloud Security

Securing hybrid and multi-cloud environments by addressing misconfigurations, enforcing consistent policies, and monitoring cloud-native workloads in line with compliance standards.

3

AI Security Risk

Managing risks from AI adoption, including model vulnerabilities, third-party AI components, and adversarial threats, while ensuring transparency, trust, and regulatory adherence.

4

Identity and Access Management

Strengthening oversight of user and privileged access, detecting anomalous behaviour, and enforcing adaptive policies to meet compliance obligations.

5

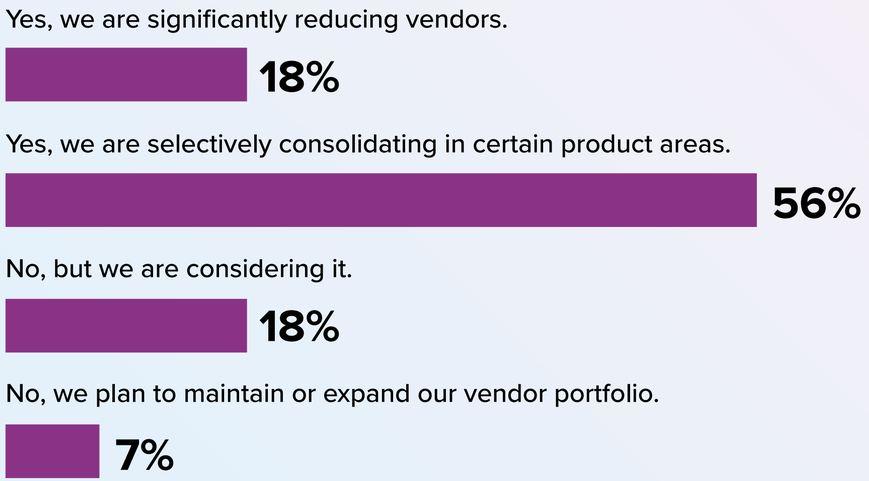
Security Analytics and Automation

Using intelligent analytics and automated workflows to detect, prioritize, and respond to threats efficiently, supporting both operational effectiveness and regulatory reporting.

Security Modernization

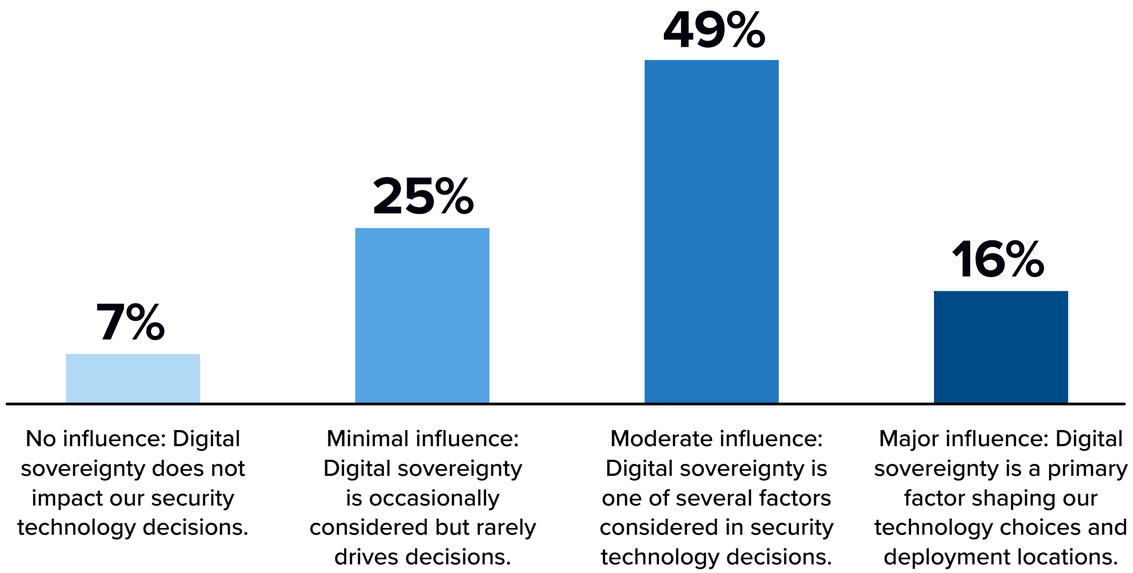
Vendor Consolidation and the Impact of Digital Sovereignty

Organizations' Approach To Consolidating Cybersecurity Vendors



Three-quarters of organizations are pursuing a strategy to consolidate security vendors, with the majority(56%) focusing on selective consolidation in specific product areas. This effort reduces complexity and technology sprawl, drives the adoption of platform-centric architectures, and helps simplify operations, improve integration, cut costs, and enhance overall security effectiveness.

The influence of geopolitics and digital sovereignty on security technology adoption

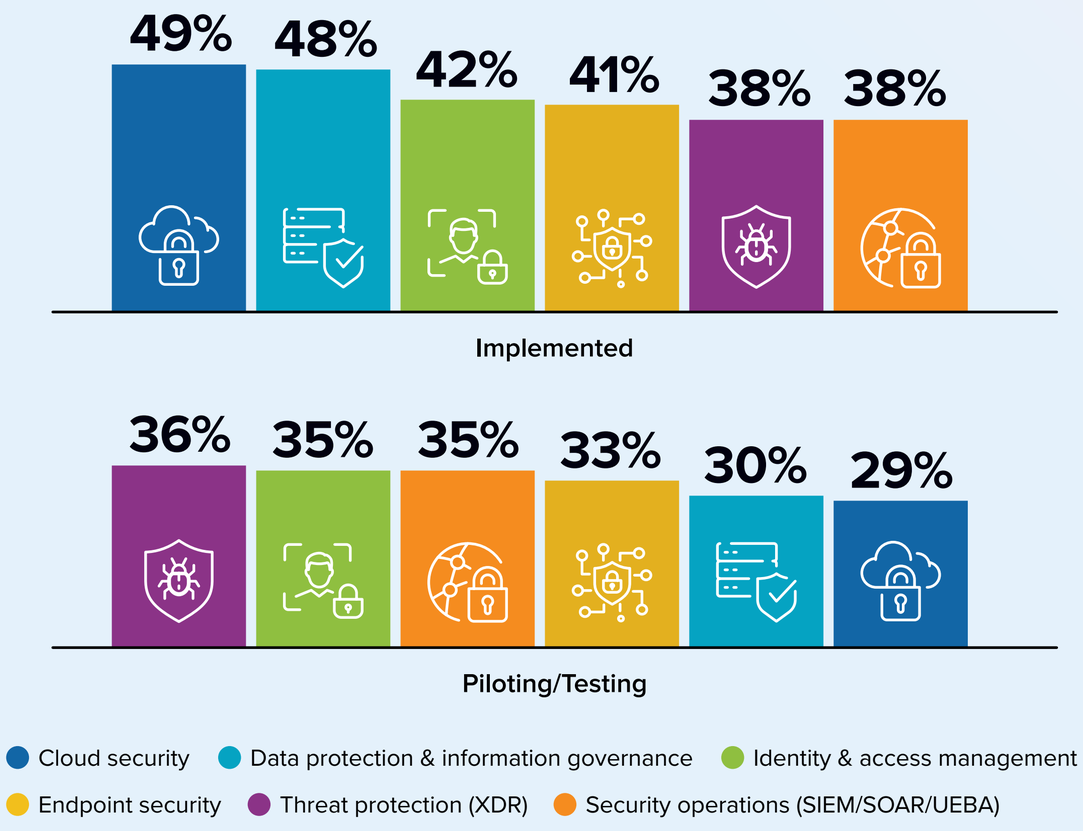


European organizations are increasingly factoring geopolitics and digital sovereignty into their selection of security vendors and technologies. For 17%, digital sovereignty is a primary driver, while for another 50% it is one of several considerations, reflecting heightened focus on regulatory compliance, data residency, and risk mitigation in a complex international environment.

AI in Cybersecurity

Critical Enabler for NIS2 Resilience

GenAI Adoption across Security Domains



AI strengthens core detection, response and governance capabilities, helping organizations meet NIS2's security and reporting requirements more effectively.

Machine learning has long supported cybersecurity, but advances in GenAI and agentic AI are driving deeper integration across security domains.

GenAI use cases center on:

- **Cloud security:** analyse configuration drift, identify misconfigurations at scale, and surface environment-wide risks in real time.
- **Data protection and security:** classify sensitive data, detect anomalous access patterns, and strengthen policy enforcement across distributed data flows.
- **Identity and Access Management:** detect anomalous login behaviour, analyse privilege escalation patterns, and enable adaptive access controls based on real-time risk signals.

GenAI Impact on Security

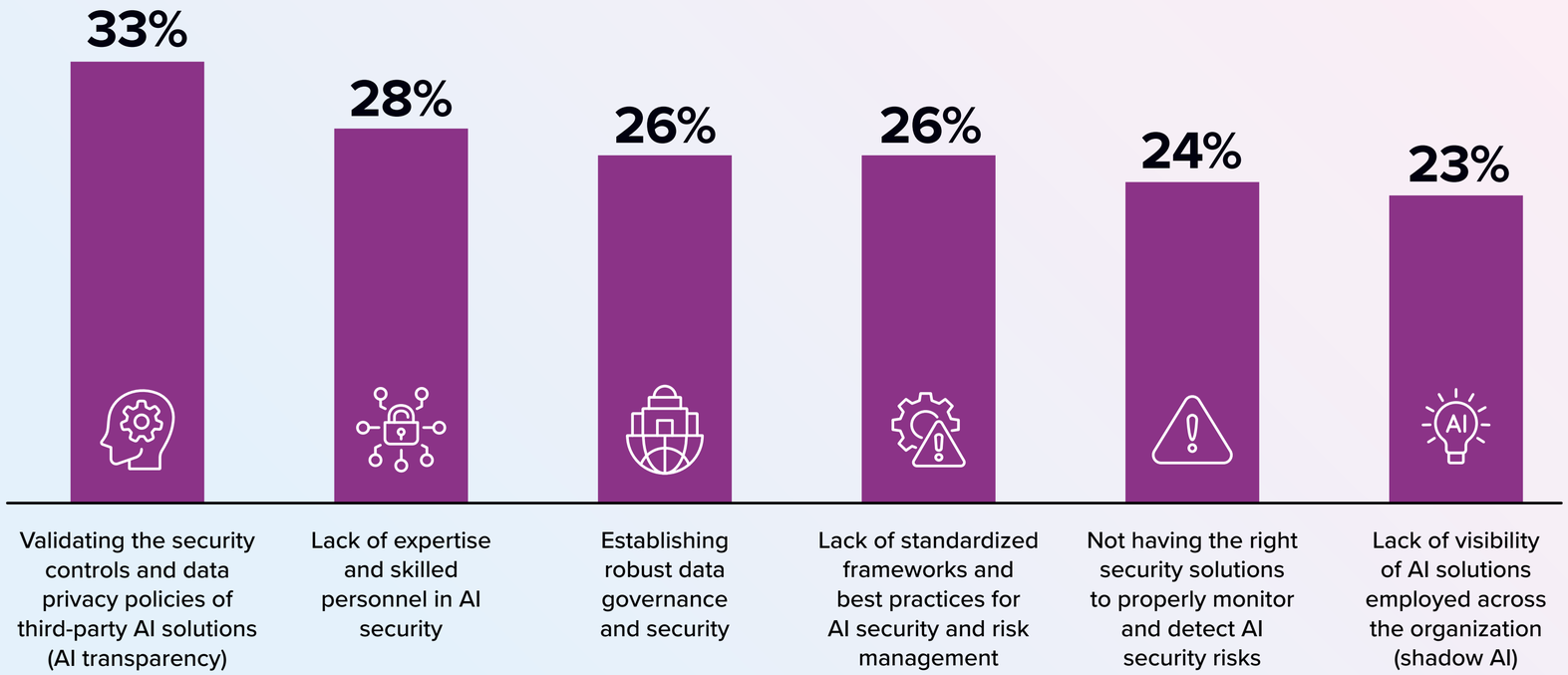
75%

Organizations report measurable gains in security efficiency and effectiveness from GenAI adoption.

AI in Cybersecurity

Critical Enabler for NIS2 Resilience

Lead Partner Support for Achieving NIS2 Compliance



Organizations now operate AI environments that span multiple vendors, architectures, and deployment models, making consistent data protection and the use of context-aware, adaptive controls increasingly essential. Overall, AI security posture remains at an early stage of maturity. The challenges are diverse and extend across technical, organizational, and supply-chain domains. The top three are:

1. **Validation of security and privacy controls of AI solutions**

   Organizations struggle to assess whether external AI solutions meet required security controls and data-privacy standards, creating uncertainty around model integrity, data handling, and trustworthiness.

2. **Shortage of AI-Security Expertise**

   Security teams lack the specialized skills needed to evaluate model behaviour, identify AI-specific threats, and build resilient controls across the AI lifecycle.

3. **Build Robust Data Governance and Security**

   Effective protection of training data, model inputs, and outputs remains challenging, with gaps in lineage, access control, and policy enforcement increasing the risk of over-exposure, leakage and misuse.

Who Leads and Why It Matters

	Observations	Effects
Leaders	• Highly Digital sovereignty conscious – 90% of NIS2 readiness leaders say digital sovereignty has a moderate or major influence • Have seen efficiency gains from AI – 67% of NIS2 leaders have seen a moderate or significant improvement • More AI ready - 71% of NIS2 leaders have a higher level of security for AI environments • Leaders build for resilience – 32% of leaders cite resilience as a key benefit of security modernization	• Have a stable or increased security funding outlook • Build cybersecurity for business outcomes, not for cost savings alone • Are able to leverage AI in security operations
Laggards	• Evaluate partner primarily based on cost– 37% of laggards value cost more than integration capabilities when choosing a partner • Facing compliance delays- 67% of laggards say they are more than 6 months away from compliance with NIS2 or unsure about when • Look primarily for cost savings – 29% modernize for cost efficiency reasons	• Declining security funding outlook with mounting cost pressures • Are not in a position to reap efficiency gains from AI • Struggle with more basic security measures, with less time and money available for innovation

What This Means for 2026

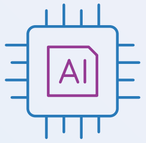
The Road to Technology-Enabled Compliance

The readiness gap affects business impact. Organizations with higher NIS2 readiness, are consistently further ahead with AI and are more actively consolidating and modernizing their cybersecurity.

Organizations that want to succeed in 2026 have to:

Formalize governance

Accelerate modernization



Adopt AI-driven security

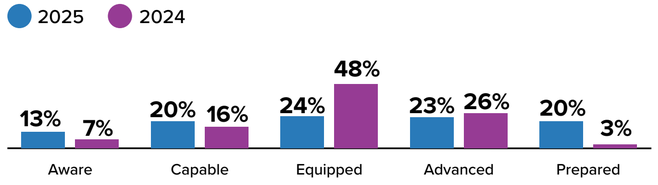
Reduce fragmentation

Prepare for multi-country compliance

Country Snapshots

Austria

Country Snapshot | Sample: n=70



49% of organizations expecting compliance within 12 months
94% working with an external lead partner

Prioritized for Modernization

- **37%** AI security risk management
- **37%** Data Security
- **30%** SIEM/SOAR/UEBA

Top 3 Barriers

37%
Approaching cyber risk management as mandatory rather than mandatory

36%
Policy and control variations across EU countries

31%
Lack of budget for technology investments

Top 3 Drivers – Q20 but potentially Q19

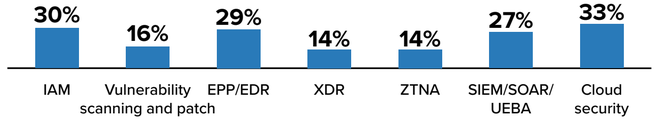
29%
Improved resilience to cyberthreats

29%
Cost efficiency and reduced operational overhead

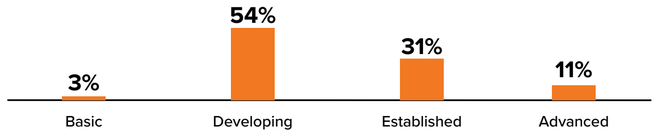
26%
Better visibility and control across IT and OT environments

Technology Readiness Indicators

Prioritized for NIS2 Compliance

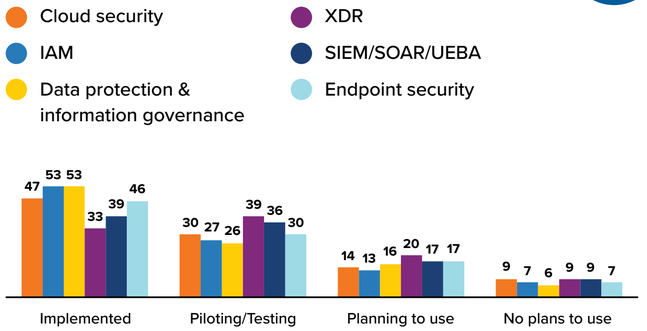


AI Security Posture



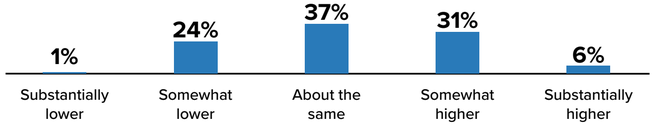
AI Adoption in Security

(Percentage of respondents)

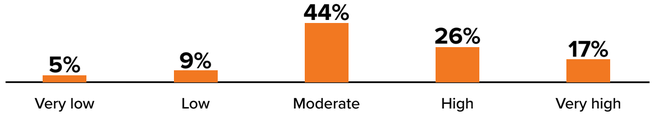


Strategic Alignment

Funding Outlook compared to current level

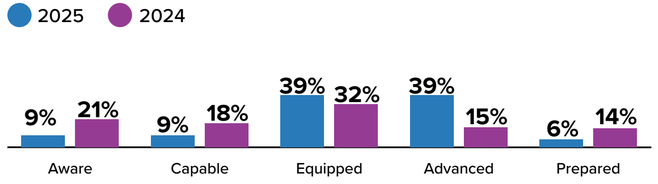


Satisfaction with Lead Partner



Belgium

Country Snapshot | Sample: n=70



69% of organizations expecting compliance within 12 months

100% working with an external lead partner

Prioritized for Modernization

- **41%** Cloud Security
- **36%** Data Security
- **34%** AI security risk management

Top 3 Barriers

40%
Approaching cyber risk management as mandatory rather than mandatory

27%
Lack of capable and knowledgeable technology partners

24%
Lack of budget for technology investments

Top 3 Drivers

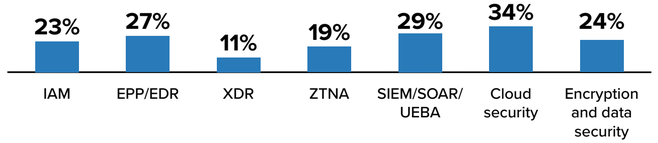
31%
Access to advanced technologies

23%
Reduced complexity and vendor sprawl

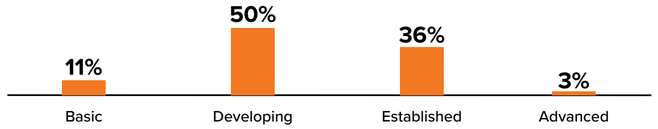
23%
Cost efficiency and reduced operational overhead

Technology Readiness Indicators

Prioritized for NIS2 Compliance



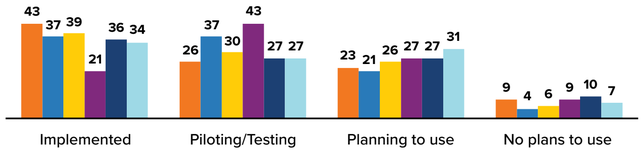
AI Security Posture



AI Adoption in Security

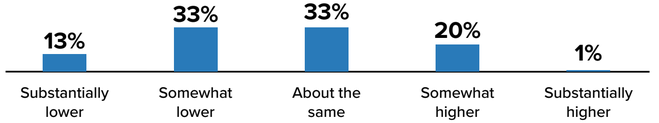
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

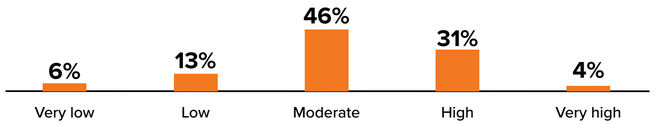


Strategic Alignment

Funding Outlook compared to current level

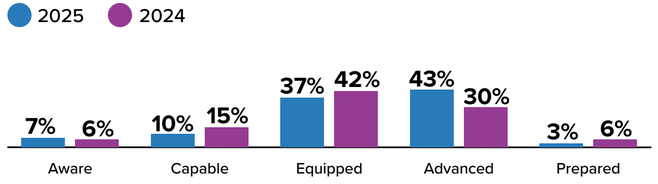


Satisfaction with Lead Partner



Bulgaria

Country Snapshot | Sample: n=30



77% of organizations expecting compliance within 12 months
97% working with an external lead partner
Prioritized for Modernization

- **37%** Data Security
- **33%** AI security risk management
- **23%** Endpoint Security

Top 3 Barriers

37%
Lack of timely and clear advance guidance from national security authorities

30%
Approaching cyber-risk management as mandatory rather than optional

30%
Policy control variations across EU countries

Top 3 Drivers

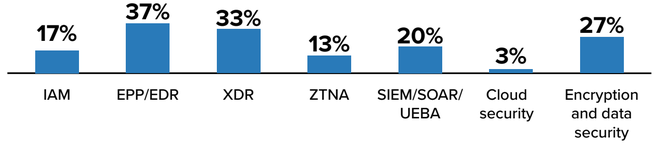
37%
Improved resilience to cyberthreats

37%
Stronger alignment between security and business objectives

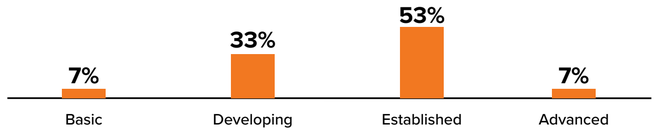
27%
Increased employee and stakeholder confidence in security

Technology Readiness Indicators

Prioritized for NIS2 Compliance



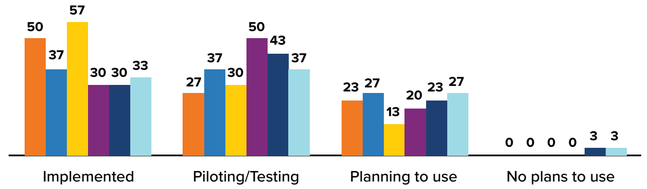
AI Security Posture



AI Adoption in Security

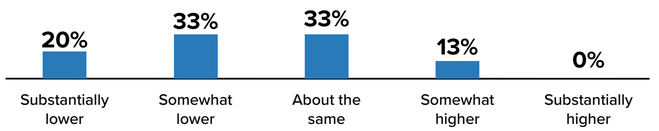
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

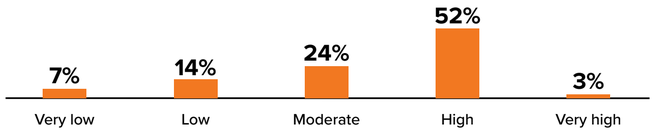


Strategic Alignment

Funding Outlook compared to current level

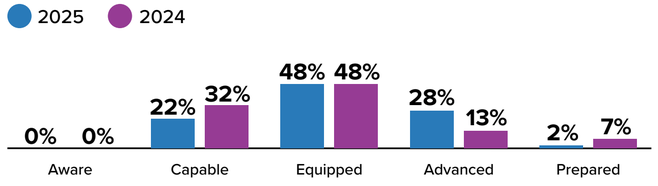


Satisfaction with Lead Partner



Czech

Country Snapshot | Sample: n=50



80% of organizations expecting compliance within 12 months

100% working with an external lead partner

Prioritized for Modernization

- **40%** Cloud Security
- **30%** Data Security
- **28%** Threat Intelligence

Top 3 Barriers

30%
Lack of timeline and clear advance guidance from our national security authorities

26%
Insufficient executive or board-level engagement

26%
A lack of capable and knowledgeable technology partner to guide and support us

Top 3 Drivers

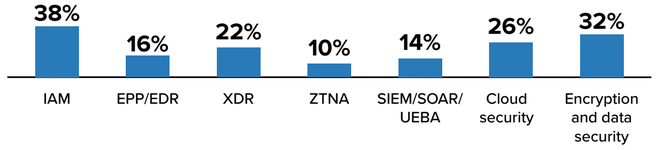
32%
Improved resilience to cyberthreats

28%
Access to advanced technologies

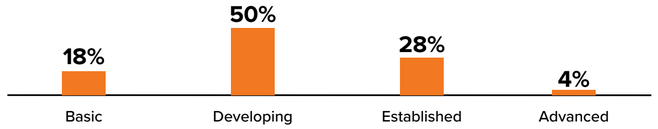
20%
Stronger alignment between security and business objectives

Technology Readiness Indicators

Prioritized for NIS2 Compliance

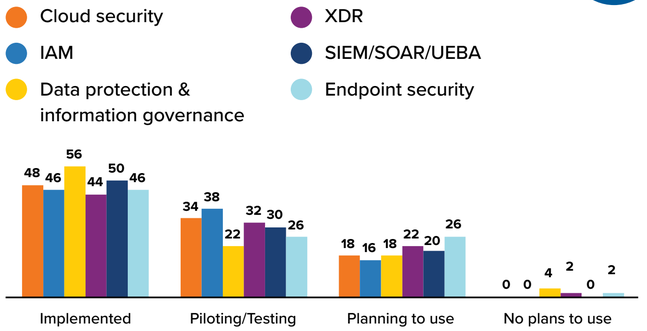


AI Security Posture



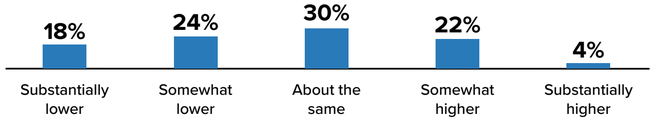
AI Adoption in Security

(Percentage of respondents)

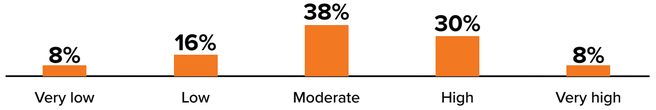


Strategic Alignment

Funding Outlook compared to current level

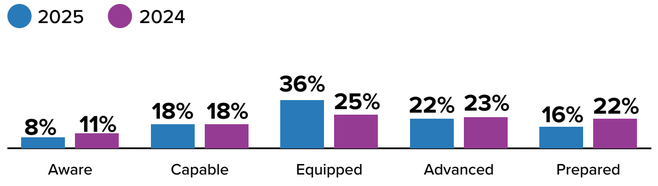


Satisfaction with Lead Partner



France

Country Snapshot | Sample: n=200



68% of organizations expecting compliance within 12 months

98% working with an external lead partner

Prioritized for Modernization

- **34%** Data Security
- **32%** Cloud Security
- **26%** Endpoint Security

Top 3 Barriers

34%
Approaching cyber-risk management as mandatory rather than optional

32%
Lack of timely and clear advance guidance from our national security authorities

28%
Lack of resources for implementing changes to policies, practices, or processes

Top 3 Drivers

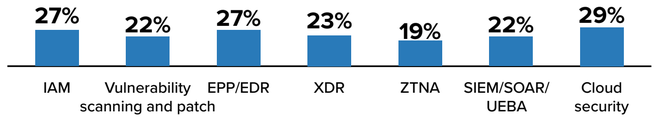
28%
Improved resilience to cyberthreats

27%
Stronger alignment between security and business objectives

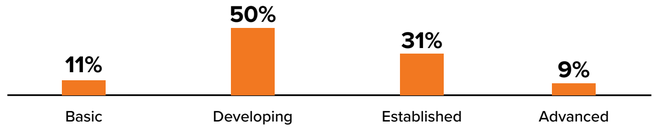
26%
Access to advanced technologies

Technology Readiness Indicators

Prioritized for NIS2 Compliance



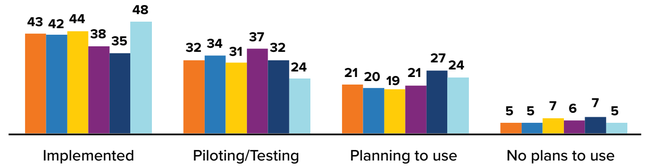
AI Security Posture



AI Adoption in Security

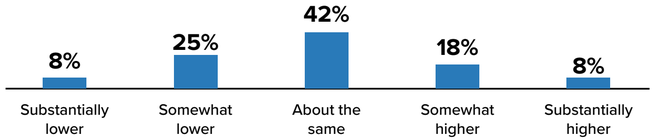
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

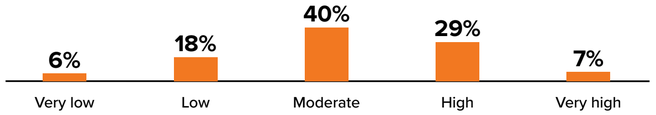


Strategic Alignment

Funding Outlook compared to current level

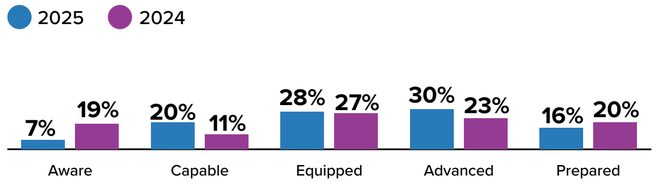


Satisfaction with Lead Partner



Germany

Country Snapshot | Sample: n=220



63% of organizations expecting compliance within 12 months
97% working with an external lead partner

Prioritized for Modernization

- **40%** Cloud Security
- **31%** AI Security Risk Management
- **29%** Data Security

Top 3 Barriers

38%
Approaching cyber-risk management as mandatory rather than optional

31%
Lack of resources for implementing changes to policies, practices, or processes

27%
Policy and control variations across EU countries

Top 3 Drivers

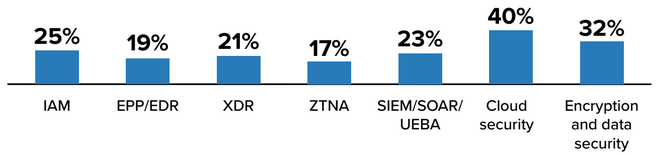
36%
Improved resilience to cyberthreats

27%
Cost efficiency and reduced operational overhead

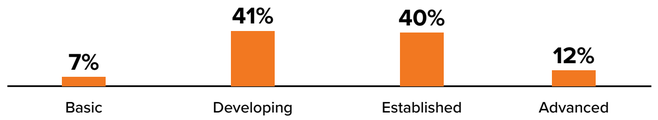
26%
Access to advanced technologies

Technology Readiness Indicators

Prioritized for NIS2 Compliance



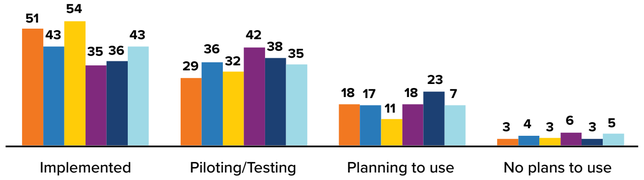
AI Security Posture



AI Adoption in Security

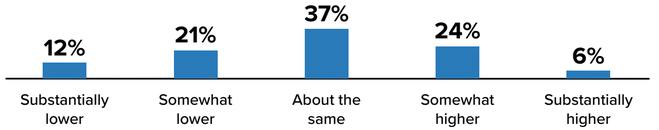
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

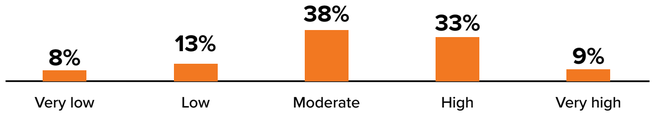


Strategic Alignment

Funding Outlook compared to current level

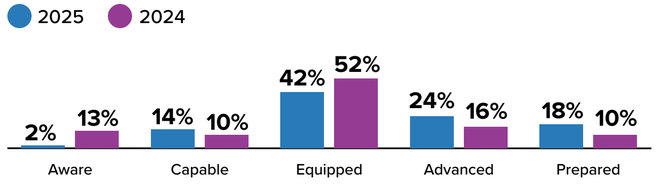


Satisfaction with Lead Partner



Greece

Country Snapshot | Sample: n=50



62% of organizations expecting compliance within 12 months
96% working with an external lead partner

Prioritized for Modernization

- **40%** Data Security
- **30%** Cloud Security
- **30%** Identity and access management (IAM)

Top 3 Barriers

42%
Policy and control variations across EU countries

38%
Mapping our status and capabilities in relation to requirements

24%
A lack of capable and knowledgeable technology partner to guide and support us

Top 3 Drivers

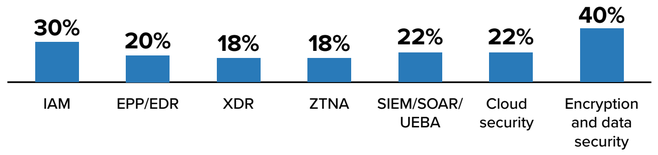
30%
Stronger alignment between security and business objectives

26%
Cost efficiency and reduced operational overhead

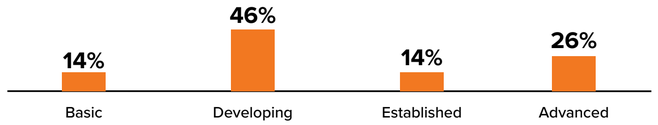
26%
Improved resilience to cyberthreats

Technology Readiness Indicators

Prioritized for NIS2 Compliance



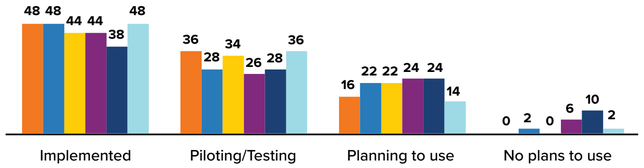
AI Security Posture



AI Adoption in Security

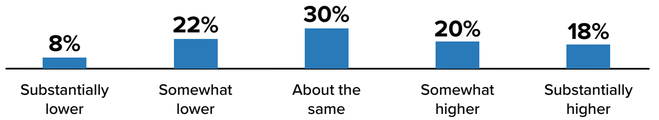
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

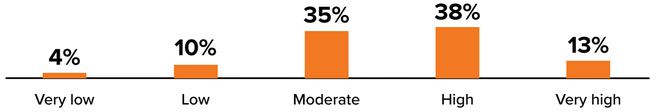


Strategic Alignment

Funding Outlook compared to current level

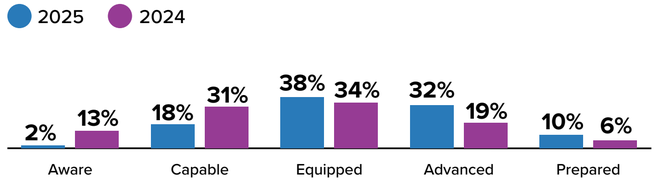


Satisfaction with Lead Partner



Hungary

Country Snapshot | Sample: n=50



56% of organizations expecting compliance within 12 months
98% working with an external lead partner

Prioritized for Modernization

- **30%** AI security risk management
- **24%** Data Security
- **22%** Identity and access management (IAM)

Top 3 Barriers

36%
Policy and control variations across EU countries

28%
Lack of a grace period

24%
Approaching cyber-risk management as mandatory rather than optional

Top 3 Drivers

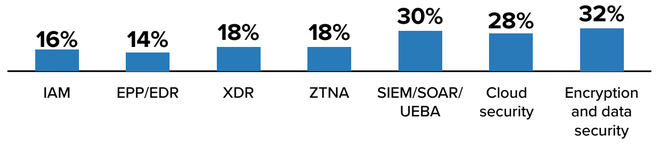
26%
Regulatory and compliance readiness

24%
Improved resilience to cyberthreats

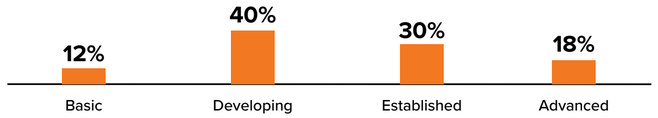
24%
Better visibility and control across IT and OT

Technology Readiness Indicators

Prioritized for NIS2 Compliance

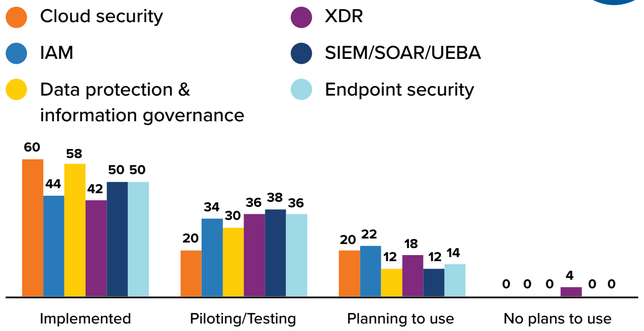


AI Security Posture



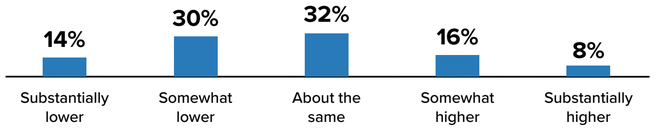
AI Adoption in Security

(Percentage of respondents)

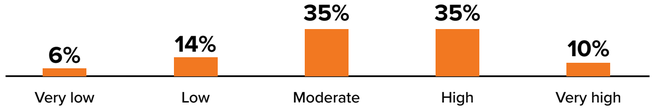


Strategic Alignment

Funding Outlook compared to current level

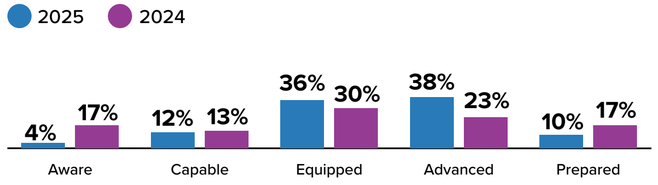


Satisfaction with Lead Partner



Ireland

Country Snapshot | Sample: n=50



78% of organizations expecting compliance within 12 months
92% working with an external lead partner

Prioritized for Modernization

- **38%** Data Security
- **36%** Cloud Security
- **34%** AI security risk management

Top 3 Barriers

40%
Lack of resources for implementing changes to policies

34%
Lack of timely and clear advance guidance from our national security authorities

32%
Policy and control variations across EU countries

Top 3 Drivers

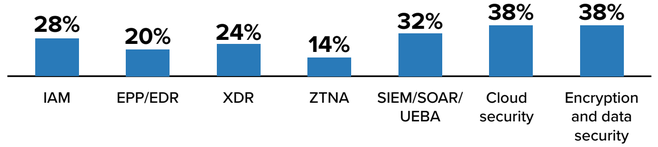
34%
Improved resilience to cyberthreats

32%
Access to advanced technologies

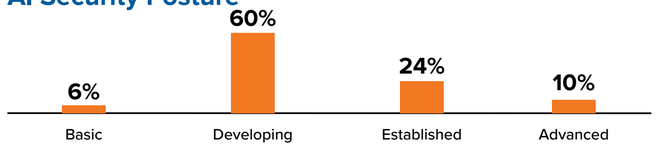
26%
Regulatory and compliance readiness

Technology Readiness Indicators

Prioritized for NIS2 Compliance

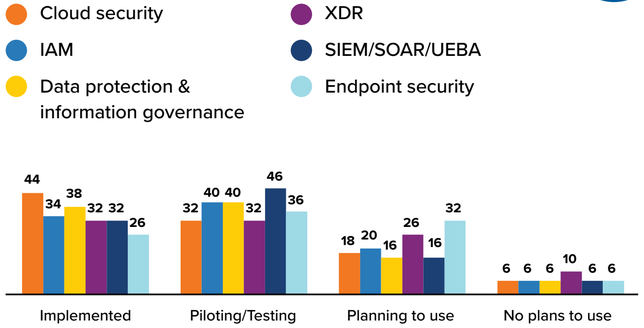


AI Security Posture



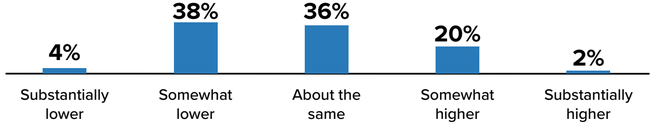
AI Adoption in Security

(Percentage of respondents)

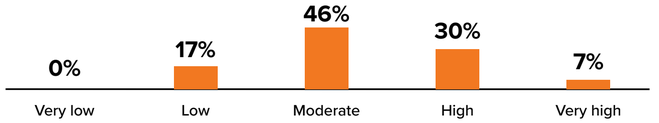


Strategic Alignment

Funding Outlook compared to current level

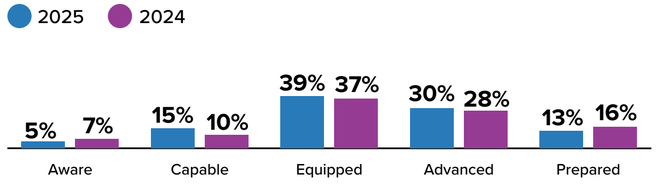


Satisfaction with Lead Partner



Italy

Country Snapshot | Sample: n=200



73% of organizations expecting compliance within 12 months

99% working with an external lead partner

Prioritized for Modernization

- **35%** Data Security
- **31%** Cloud Security
- **26%** Vulnerability Management

Top 3 Barriers

27%
Lack of timely and clear advance guidance from our national security authorities

25%
Lack of resources for implementing changes to policies

24%
Policy and control variations across EU countries

Top 3 Drivers

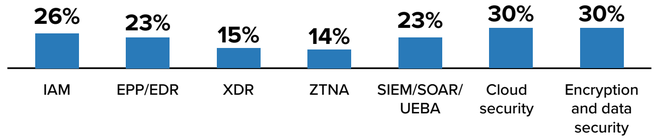
30%
Improved resilience to cyberthreats

26%
Stronger alignment between security and business objectives

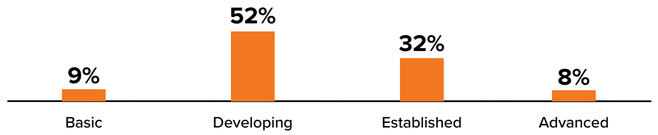
25%
Access to advanced technologies

Technology Readiness Indicators

Prioritized for NIS2 Compliance



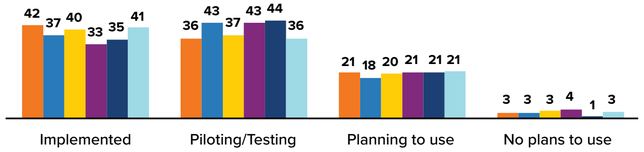
AI Security Posture



AI Adoption in Security

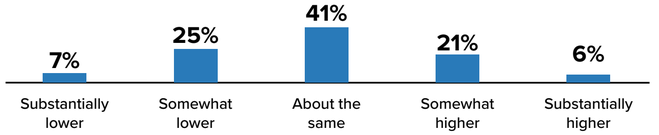
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

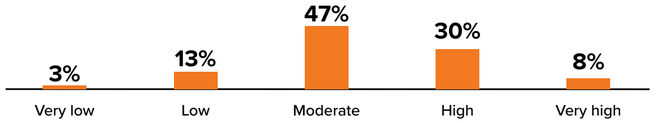


Strategic Alignment

Funding Outlook compared to current level

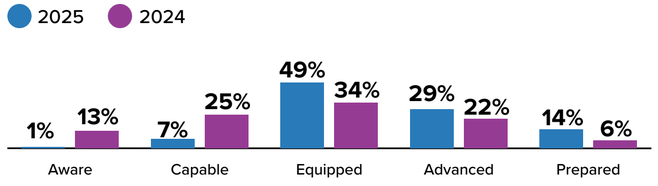


Satisfaction with Lead Partner



Netherlands

Country Snapshot | Sample: n=70



70% of organizations expecting compliance within 12 months
99% working with an external lead partner

Prioritized for Modernization

- **36%** AI security risk management
- **30%** IAM
- **24%** Security analytics and automation

Top 3 Barriers

36%
Apporaching cyber-risk management as mandatory rather than optional

31%
Policy and control variations across EU

30%
A lack of capable and knowledgeable technology partners to guide and support us

Top 3 Drivers

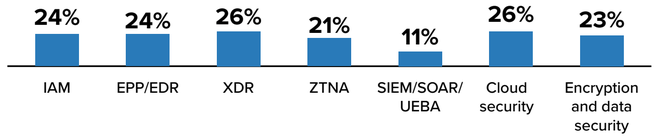
33%
Access to advanced technologies

26%
Better visibility and control across IT and OT

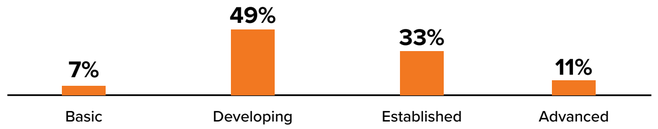
23%
Improved resilience to cyberthreats

Technology Readiness Indicators

Prioritized for NIS2 Compliance



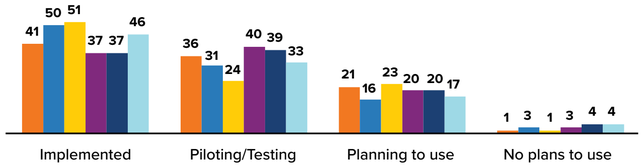
AI Security Posture



AI Adoption in Security

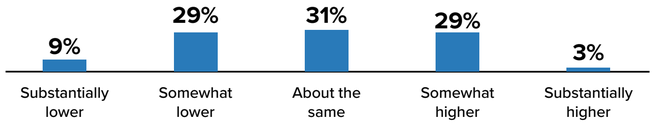
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

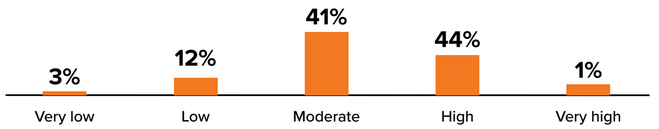


Strategic Alignment

Funding Outlook compared to current level

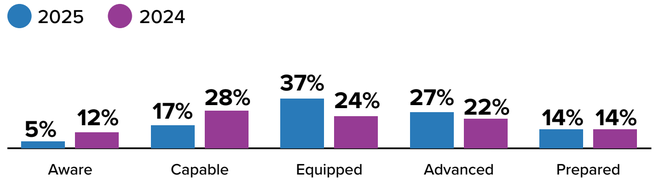


Satisfaction with Lead Partner



Poland

Country Snapshot | Sample: n=150



63% of organizations expecting compliance within 12 months
96% working with an external lead partner

Prioritized for Modernization

- **39%** Data Security
- **37%** Cloud Security
- **25%** Vulnerability Management

Top 3 Barriers

37%
Policy and control variations across EU countries

28%
Mapping our status and capabilities in relation to requirements

27%
Approaching cyber-risk management as mandatory rather than optional

Top 3 Drivers

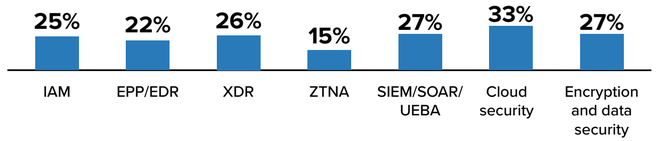
38%
Improved resilience to cyberthrets

26%
Access to advanced technologies

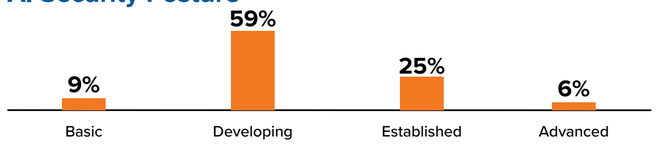
25%
Stronger alignment between security and business objectives

Technology Readiness Indicators

Prioritized for NIS2 Compliance



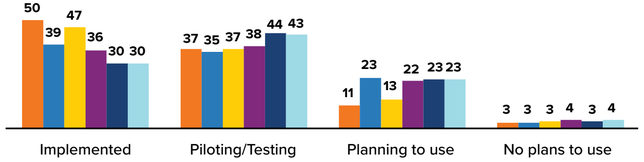
AI Security Posture



AI Adoption in Security

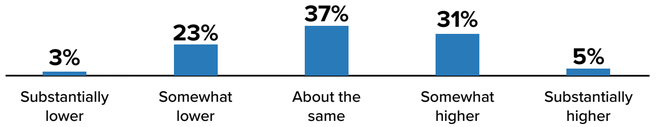
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

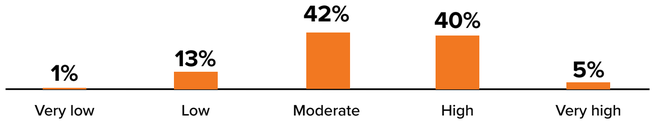


Strategic Alignment

Funding Outlook compared to current level

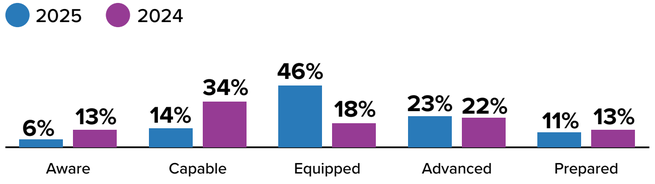


Satisfaction with Lead Partner



Portugal

Country Snapshot | Sample: n=70



63% of organizations expecting compliance within 12 months

100% working with an external lead partner

Prioritized for Modernization

- **39%** Data Security
- **29%** Cloud Security
- **29%** AI security risk management

Top 3 Barriers

44%
Approaching cyber-risk management as mandatory rather than optional

24%
Mapping our status and capabilities in relation to requirements

24%
Policy and control variations across EU countries

Top 3 Drivers

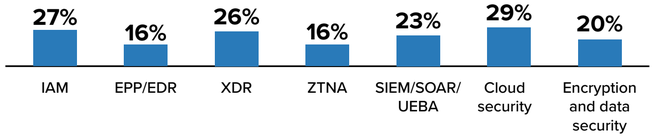
36%
Improved resilience to cyberthreats

29%
Regulatory and compliance readiness

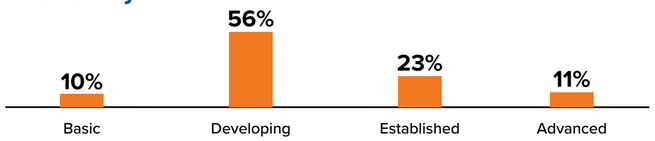
24%
Access to advanced technologies

Technology Readiness Indicators

Prioritized for NIS2 Compliance



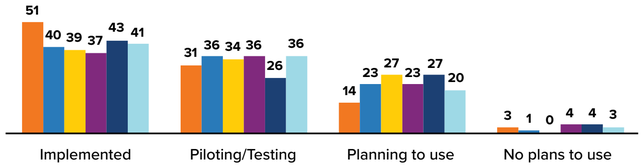
AI Security Posture



AI Adoption in Security

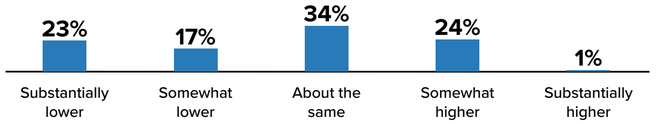
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

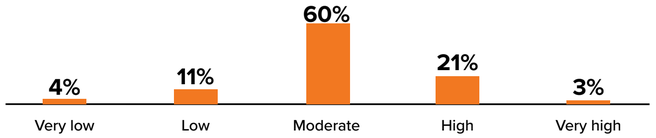


Strategic Alignment

Funding Outlook compared to current level

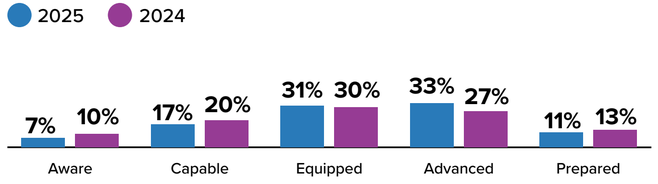


Satisfaction with Lead Partner



Romania

Country Snapshot | Sample: n=70



80% of organizations expecting compliance within 12 months
96% working with an external lead partner

Prioritized for Modernization

- **37%** Cloud Security
- **34%** Security Analytics and Automation
- **31%** Endpoint Security

Top 3 Barriers

41%
Mapping our status and capabilities in relation to requirements

41%
Policy and control variations across EU

30%
Approaching cyber-risk management as mandatory rather than optional

Top 3 Drivers

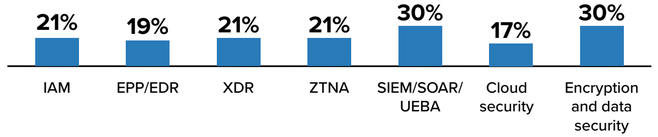
34%
Access to advanced technologies

31%
Stronger alignment between security and business objectives

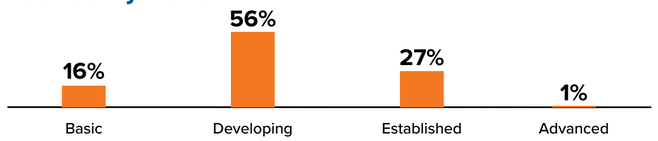
26%
Cost efficiency and reduced operational overhead

Technology Readiness Indicators

Prioritized for NIS2 Compliance

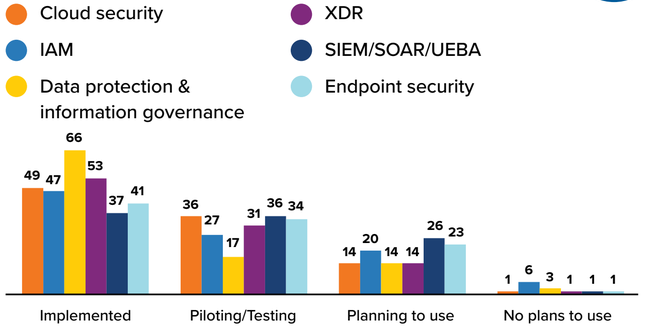


AI Security Posture



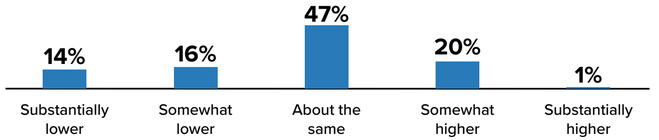
AI Adoption in Security

(Percentage of respondents)

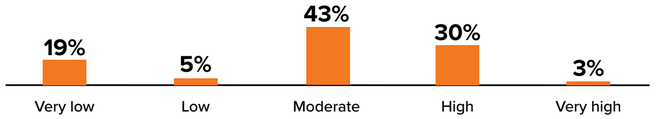


Strategic Alignment

Funding Outlook compared to current level

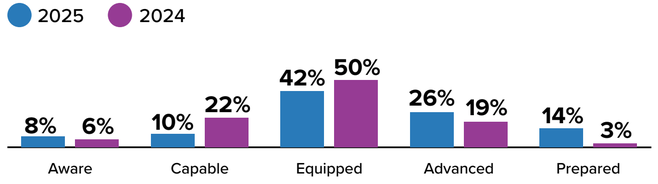


Satisfaction with Lead Partner



Slovakia

Country Snapshot | Sample: n=50



62% of organizations expecting compliance within 12 months
90% working with an external lead partner

Prioritized for Modernization

- **34%** Cloud Security
- **30%** Endpoint Security
- **28%** Data Security

Top 3 Barriers

38%
Policy control variations across EU

28%
A lack of capable and knowledgeable technology partners to guide and support us

26%
Mapping our status and capabilities in relation to requirements

Top 3 Drivers

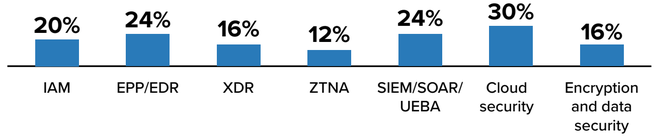
36%
Improved resilience to cyberthreats

36%
Cost efficiency and reduced operational overhead

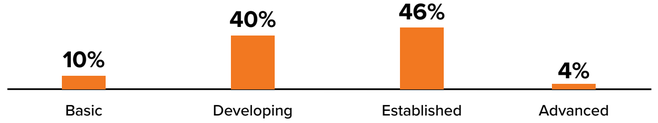
24%
Better visibility and control across IT and OT

Technology Readiness Indicators

Prioritized for NIS2 Compliance

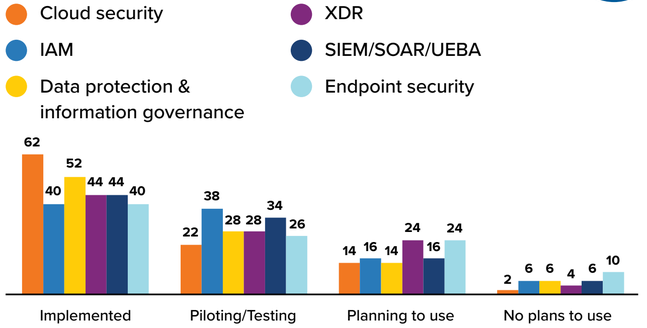


AI Security Posture



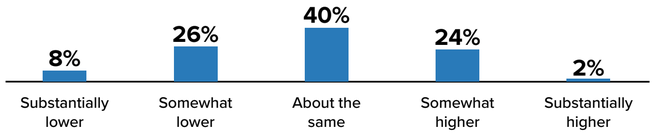
AI Adoption in Security

(Percentage of respondents)

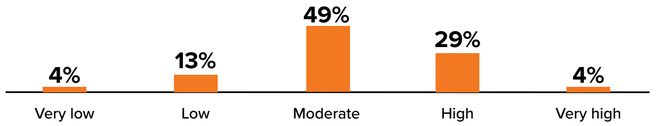


Strategic Alignment

Funding Outlook compared to current level

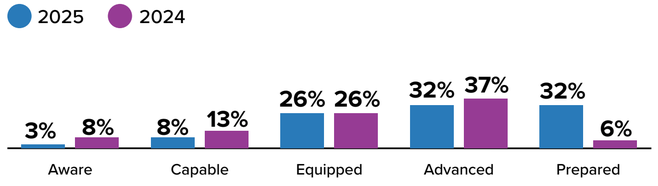


Satisfaction with Lead Partner



Spain

Country Snapshot | Sample: n=200



67% of organizations expecting compliance within 12 months

99% working with an external lead partner

Prioritized for Modernization

- **38%** Data Security
- **32%** Cloud Security
- **28%** AI security risk management

Top 3 Barriers

36%
Policy and control variations across EU

35%
Approaching cyber-risk management as mandatory rather than optional

26%
Lack of budget for technology investments

Top 3 Drivers

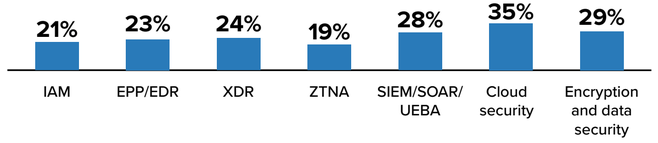
30%
Cost efficiency and reduced operational overhead

29%
Improved resilience to cyberthreats

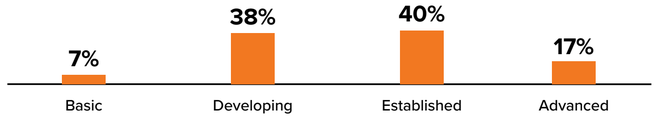
25%
Better visibility and control across IT and OT

Technology Readiness Indicators

Prioritized for NIS2 Compliance

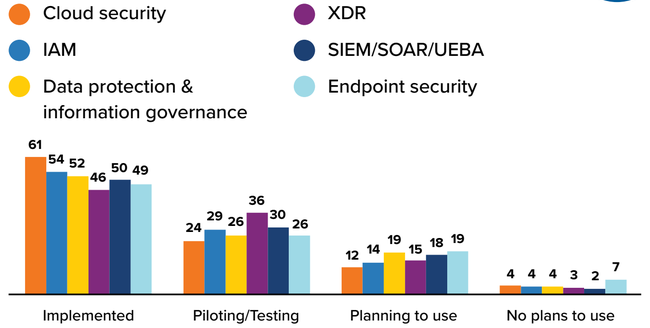


AI Security Posture



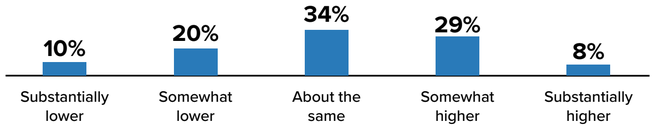
AI Adoption in Security

(Percentage of respondents)

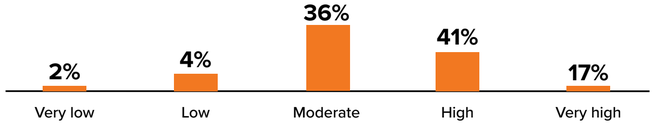


Strategic Alignment

Funding Outlook compared to current level

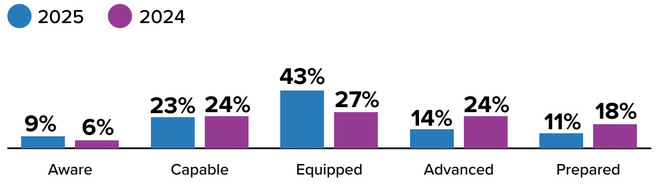


Satisfaction with Lead Partner



Switzerland

Country Snapshot | Sample: n=70



63% of organizations expecting compliance within 12 months

99% working with an external lead partner

Prioritized for Modernization

- **34%** Cloud Security
- **33%** Data Security
- **33%** AI Security Risk Management

Top 3 Barriers

34%
Lack of budget for technology investments

30%
Policy and control variations across EU

29%
Lack of resources for implementing changes to policies

Top 3 Drivers

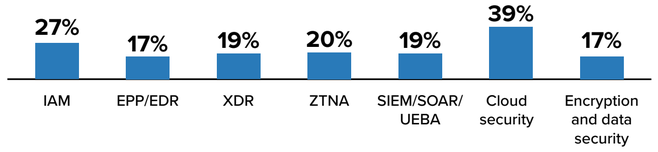
33%
Better visibility and control across IT and OT

24%
Stonger alignment between security and business objectives

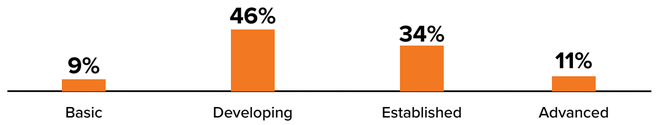
24%
Cost efficiency and reduced operational overhead

Technology Readiness Indicators

Prioritized for NIS2 Compliance



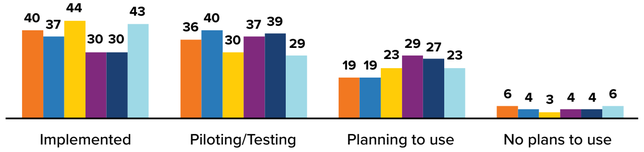
AI Security Posture



AI Adoption in Security

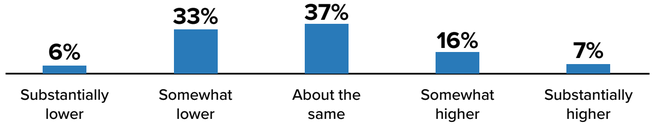
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

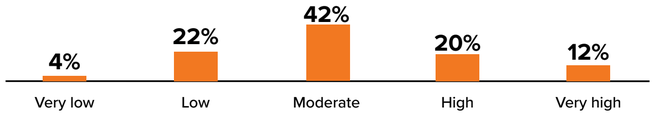


Strategic Alignment

Funding Outlook compared to current level

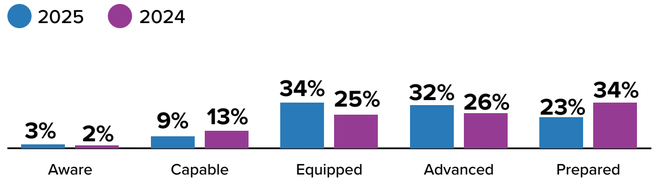


Satisfaction with Lead Partner



UK

Country Snapshot | Sample: n=200



75% of organizations expecting compliance within 12 months

99% working with an external lead partner

Prioritized for Modernization

- **37%** AI Security Risk Management
- **36%** Cloud Security
- **31%** Data Security

Top 3 Barriers

42%
Policy control variations across EU

40%
Approaching cyber-risk management as mandatory rather than optional

28%
Lack of resources for implementing changes to policies

Top 3 Drivers

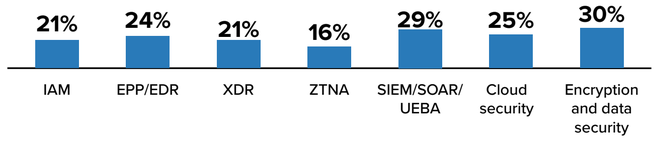
31%
Improved resilience to cyberthreats

26%
Access to advanced technologies

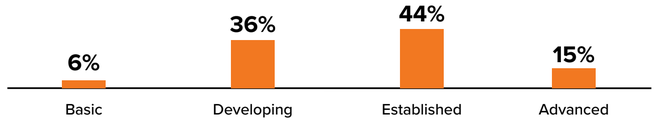
25%
Better visibility and control across IT and OT

Technology Readiness Indicators

Prioritized for NIS2 Compliance



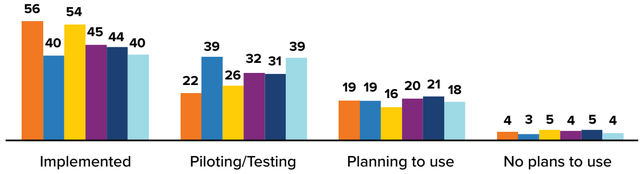
AI Security Posture



AI Adoption in Security

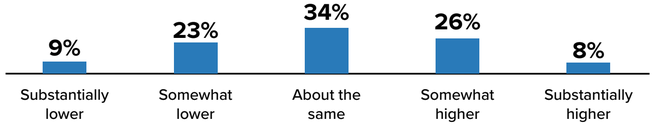
(Percentage of respondents)

- Cloud security
- IAM
- Data protection & information governance
- XDR
- SIEM/SOAR/UEBA
- Endpoint security

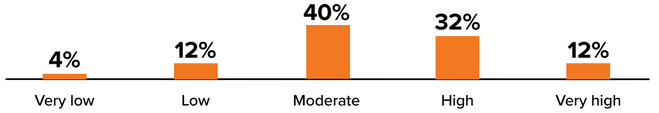


Strategic Alignment

Funding Outlook compared to current level

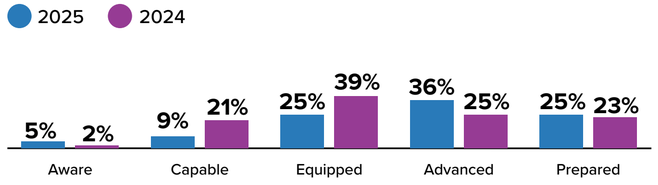


Satisfaction with Lead Partner



Nordics

Country Snapshot | Sample: n=130



71% of organizations expecting compliance within 12 months
98% working with an external lead partner

Prioritized for Modernization

- **39%** AI Security Risk Management
- **36%** Data Security
- **32%** Cloud Security

Top 3 Barriers

34%
Policy and control variations across EU

30%
Approaching cyber-risk management as mandatory rather than optional

26%
Lack of budget for technology investments

Top 3 Drivers

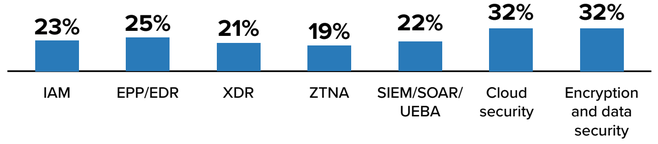
32%
Access to advanced technologies

30%
Improved resilience to cyberthreats

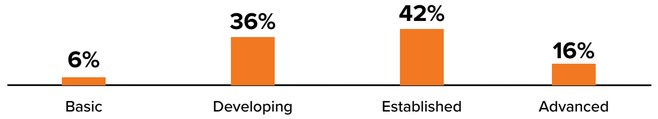
27%
Cost efficiency and reduced operational overhead

Technology Readiness Indicators

Prioritized for NIS2 Compliance

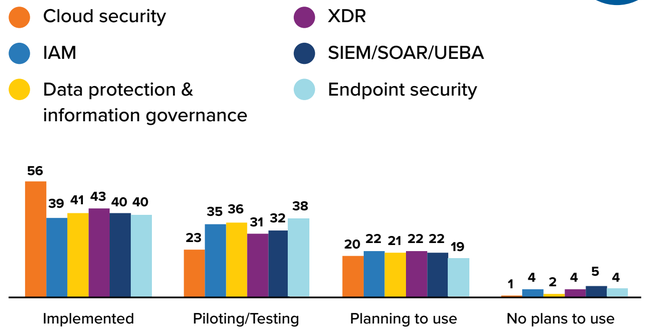


AI Security Posture



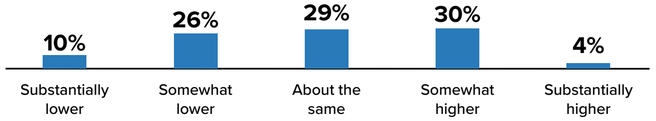
AI Adoption in Security

(Percentage of respondents)

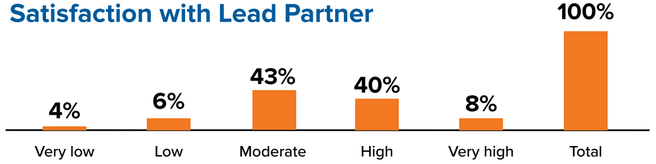


Strategic Alignment

Funding Outlook compared to current level



Satisfaction with Lead Partner



About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data, and marketing services company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC UK
1st floor, Whitfield Street, London, W1T 2RE, United Kingdom
T 44.208.987.7100

@idc | @idc | idc.com