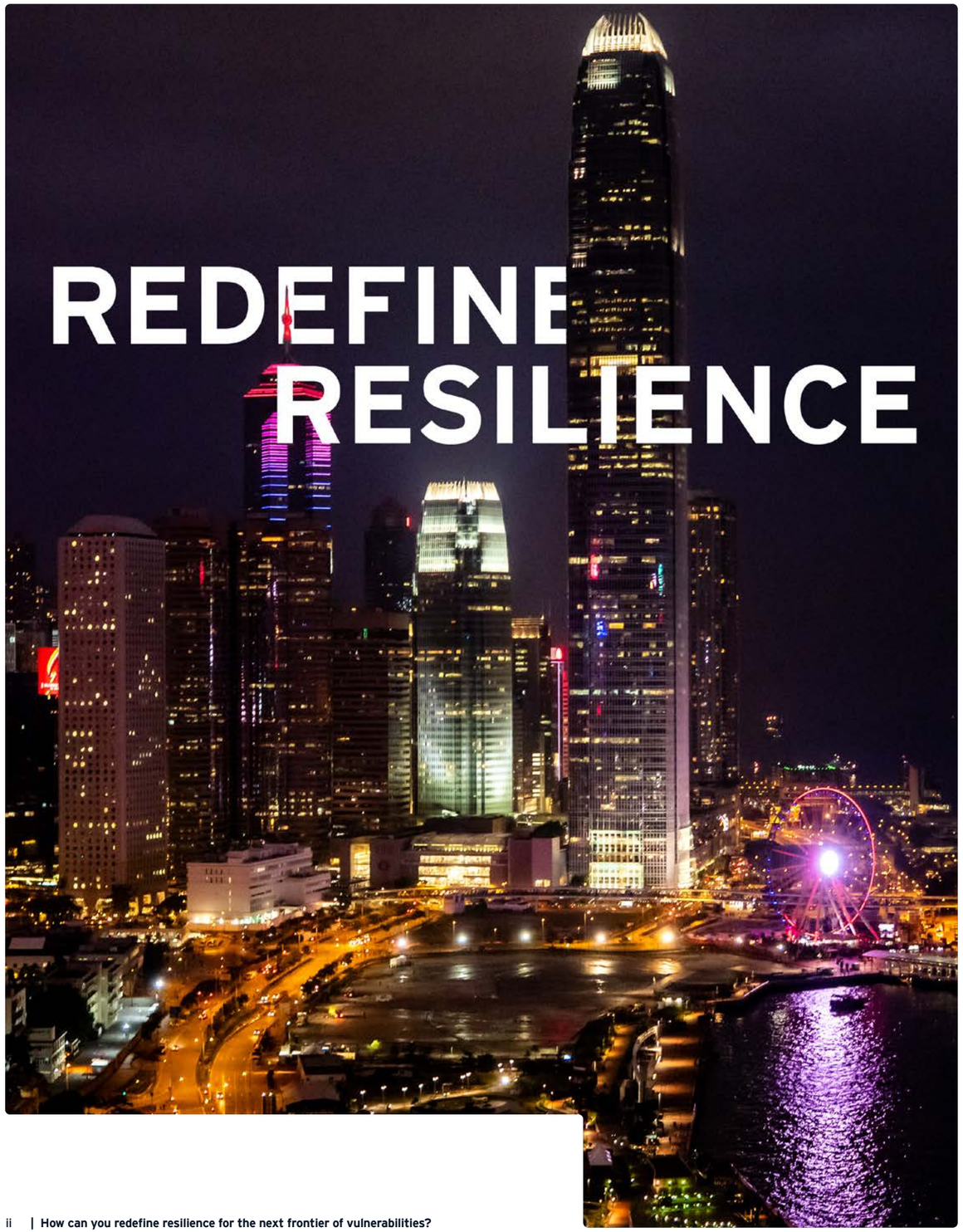
How can you redefine resilience for the next frontier of vulnerabilities?

2026 EY Global Cybersecurity Leadership Insights Study

The better the question.
The better the answer.
The better the world works.

Shape the future with confidence



Foreword

Earlier this year, when we started research for our 2026 EY Global Cybersecurity Leadership Insights Study, we knew that AI was morphing and intensifying the vulnerability landscape more rapidly than most organizations could keep up. We also knew, anecdotally, that CISOs were struggling to gain visibility and cybersecurity coverage of their organizations' assets.

To gain a deeper, more granular understanding of where organizations might be vulnerable in the future, we launched our team's largest – and perhaps most timely – cybersecurity study to date.

Then, the moment many in the cybersecurity industry had been anticipating arrived when revelations about frontier AI models' ability to discover and exploit vulnerabilities came to light. Rarely has there been so much attention – from boards, C-suites, regulators, the media and the public – on cybersecurity.

Cybersecurity leaders should use this inflection point as a springboard to build lasting resilience. Our study's discovery of the "vulnerability zone," or the assets in organizations with below average visibility and cybersecurity coverage, will help leaders do so.

There will be future inflection points. Will your organization be ready for them?

Richard Watson
EY Global Consulting Cybersecurity Leader

Richard Bergman
EY Global Cybersecurity Transformation Leader

Study in brief

CISOs, boards and the C-suite need to take decisive steps over the next 12-18 months to build resilience following recent frontier AI revelations.

EY research found that 36% of organizations' assets have inadequate visibility and cybersecurity controls, making them vulnerable to AI-enabled attacks.

A leading cohort of "Secure Creators" is transforming cybersecurity to move at machine speed and is coordinating better across the enterprise to build resilience.

Contents

Introduction 01

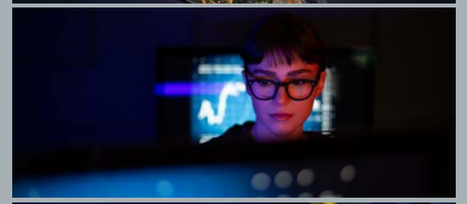
01 Identifying the vulnerability zone 03

02 Gain complete visibility of your organization to minimize the vulnerability zone 09

03 How to build resilience for the next cybersecurity shock 17

04 Steps to minimize the vulnerability zone in the age of frontier AI 21

Appendix Sector vulnerability zone insights 25



Research methodology

About the research

840
survey respondents

17
sectors

128
countries

In March 2026, the global EY organization conducted research to better understand how cybersecurity functions are approaching visibility and coverage of the attack surface. We surveyed 840 C-suite and cybersecurity leaders across 17 sectors and 128 countries covering the Americas, Asia-Pacific, and Europe, the Middle East, India and Africa (EMEIA). All respondents represented organizations with over US$1 billion in annual revenue, including 50% with US$10 billion or more in annual revenue.

Building on the findings of the previous EY Global Cybersecurity Leadership Insight Studies (2023, 2024, and 2025), we repeated the statistical modeling to identify Secure Creators – companies with better cybersecurity outcomes. These high-performing organizations were identified by leaders' evaluation of their organizations against a range of objective and subjective cybersecurity metrics: mean time to detect (MTTD), mean time to respond (MTTR), number of cybersecurity incidents, integration of cybersecurity within the organization, and cybersecurity's impact on innovation and value creation. In the 2025 study, Secure Creators represent 51% of the survey sample while Prone Enterprises (lower-performing organizations) made up 49%.

In addition to these quantitative methods, interviews with cybersecurity professionals, including senior executives at leading organizations, cybersecurity technology companies and the EY Cybersecurity Consulting practice were conducted. Some of these interviews form the basis for guest perspectives that are featured in this article.

Identifying the vulnerability zone

The "vulnerability zone" is based on a survey assessment of 475 asset types that are common across organizations. For each asset relevant to their organization's sector, respondents assessed their cybersecurity functions' level of visibility and coverage (security controls, protection and monitoring), based on four-point scales. Each asset was then plotted based on these two data points.

The aggregated responses across all assets were used to calculate the mean level of visibility and coverage, which define the boundaries of the vulnerability zone. The vulnerability zone includes assets whose average visibility and coverage fall below the aggregated mean.

Frontier AI has changed the enterprise cybersecurity resilience challenge

Organizations must still protect their most critical assets, but resilience increasingly depends on their ability to see, govern and respond across the assets, identities and dependencies that sit outside their clearest line of sight.

Recent revelations about frontier AI models' ability to discover and exploit vulnerabilities caught many organizations flat-footed. Verifying and patching weaknesses remains essential, but the deeper challenge is ongoing and structural. In a nonlinear, accelerated, volatile and interconnected (NAVI) environment, inflection points happen more frequently and rapidly, in ways that cascade across organizations, often pushing resilience to the brink. A future inflection point may take the form of a fully automated cyberattack, a quantum-enabled adversary or a cybersecurity risk we are yet to imagine.

In this environment, resilience must be redefined to encompass more than just incident recovery. Cybersecurity leaders must help their organizations continuously understand where vulnerability is accumulating, prioritize what matters to the "minimum viable enterprise" and respond at a speed closer to the threats now forming.

The 2026 EY Global Cybersecurity Leadership Insights Study shows where vulnerability might be accumulating. Based on a survey of more than 800 cybersecurity leaders and analysis of 475 asset types, we found that 36% of organizations' assets fall into an area we have named the "vulnerability zone," or the group of assets with below-average visibility and cybersecurity coverage.

Why the vulnerability zone matters now

A by-product of the common "crown jewels" approach to cybersecurity – focusing protection on your most valuable assets – is the gradual formation of a segment of assets that aren't adequately protected.

While this trade-off may have been acceptable in the past, adversaries have increasingly found vulnerabilities "on the perimeter," chaining together attacks across organizations to reach more valuable assets. Frontier AI – and already publicly-accessible AI models – accelerates this paradigm, making underprotected assets more easily reachable by a broader swath of adversaries and flattening the time from vulnerability discovery to exploitation. According to the CrowdStrike 2026 Global Threat report, the average eCrime breakout time fell to 29 minutes, highlighting how quickly adversaries can move from initial access to lateral movement.[1]

Encouragingly, the "Secure Creator" cohort, respondents we identified in past studies as organizations with more advanced cybersecurity functions than their peers, again emerged. In this year's study, only 30% of Secure Creators' assets fall in the vulnerability zone on average, compared to 42% of "Prone Enterprises," the lagging cohort.

Secure Creators were better prepared for the frontier AI inflection point because they had strategies that better cover the attack surface (a strategy we covered in our 2023 study). They have been able to respond and adapt to AI-enabled threats more quickly because cybersecurity was already integrated into their organization-wide resilience strategies.

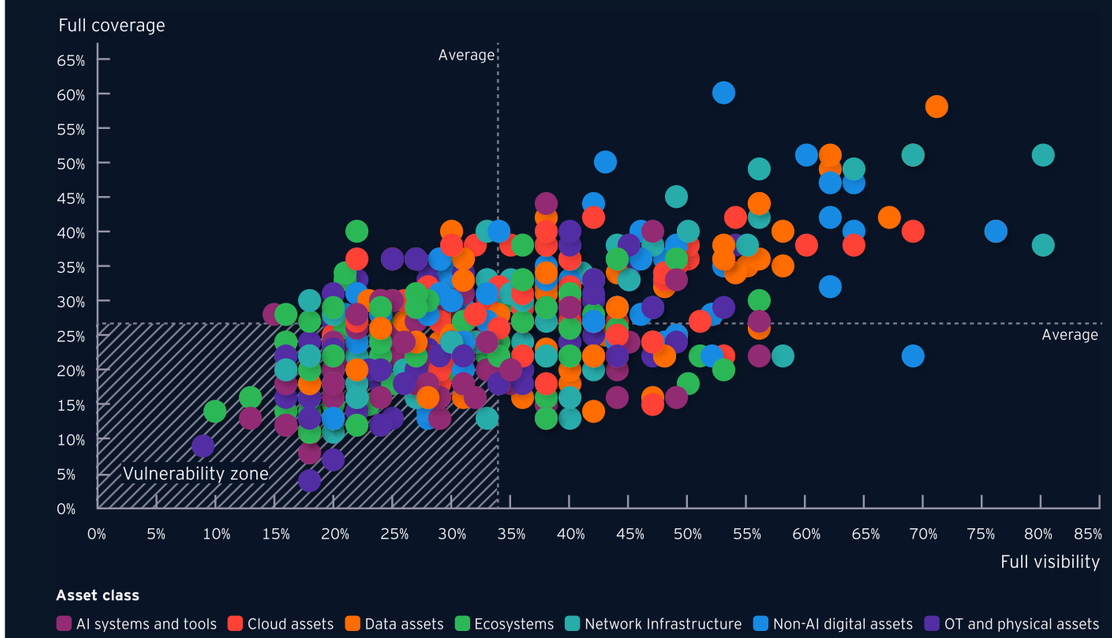
The chief information security officers (CISOs), boards and C-suites who champion these strategies and minimize the vulnerability zone will be better prepared when the next inflection point materializes.

1 2026 Global Threat Report | Latest Cybersecurity Trends & Insights | CrowdStrike

Identifying the vulnerability zone

Across 475 unique assets within seven asset categories, our research sought to understand where organizations are vulnerable, including in areas often outside of cybersecurity's remit.

1. The first dimension we measured was visibility, or the ability to identify and inventory assets.
2. The second dimension is cybersecurity coverage, or the appropriate controls, protection and monitoring of each asset.
3. Where average visibility and coverage are both below average, assets fall into the vulnerability zone.



See appendix for sector- and asset-level analysis | Page 25

Identifying the vulnerability zone

The vulnerability zone is concentrated in certain asset categories and varies by sector. It will evolve as pace of change accelerates.

01

For many boards, C-suites and regulators, revelations about frontier AI risk solidified cybersecurity as a critical facet of resilience. For CISOs, building resilience for future cybersecurity inflection points requires understanding how three shifts are reshaping risk across their organization's assets:

- Rapid AI experimentation and adoption are expanding and augmenting the attack surface.
- Increasingly complex third-party and software supply chains are introducing risk into assets beyond organizations' direct control.
- AI-enabled adversaries can exploit vulnerabilities in underprotected assets to move laterally across organizations.

These shifts do not affect all assets equally. Identification of the vulnerability zone helps CISOs understand these changes on a more granular level and improve visibility and coverage of assets where they see risk accumulating.

Our research also measures how frequently assets undergo changes that require updated security controls. Frequently updated assets, like an AI tool for inventory management or a cloud-hosted administrative system, can create visibility and coverage gaps for cybersecurity functions that are not prepared for a high pace of change. In fact, our survey's respondents cited velocity of technology change as the biggest difficulty in keeping accurate asset registers.

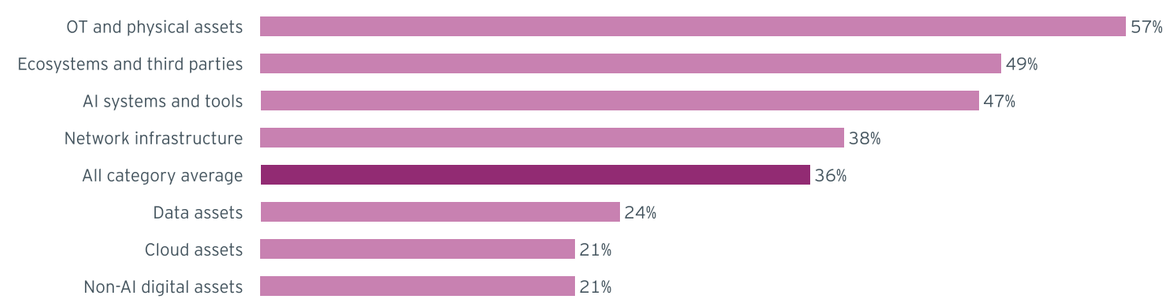
Though respondents from different sectors received sector-specific lists of assets, every respondent's asset list was grouped into the following categories:

- AI systems and tools
- Cloud assets
- Data assets
- Ecosystems and third parties
- Network infrastructure
- Non-AI digital assets
- OT and physical assets

OT and physical assets (57% of assets in the vulnerability zone), ecosystems and third parties (49%), AI systems and tools (47%) and network infrastructure (38%) were most likely to fall in the vulnerability zone.

OT and physical assets are the most likely category to fall into the vulnerability zone

Average percent of assets that fall into the vulnerability zone



Based on 475 sectorized assets. Inclusion in the vulnerability zone defined by below average visibility and coverage of each asset.
See "Identifying the vulnerability zone" for full details.

It is not surprising to see OT and physical assets as the category most likely to fall in the vulnerability zone — these assets are often outside the cybersecurity function's remit. In the past, this might have been an acceptable risk for boards. Now, as physical AI proliferates and previously firewalled assets are increasingly connected to networks — all while the threat to OT from frontier AI grows — CISOs should be leading the effort to protect these assets. This starts by gaining better visibility of the attack surface.

Ecosystems and third parties — the second-most represented category in the vulnerability zone — are increasingly important for organizations' critical operations, from software and cloud infrastructure to logistics and service delivery. As their criticality grows, they increasingly require persistent, privileged access to internal networks and environments, which materially expands the attack surface. Agentic AI may intensify these dynamics, as effective deployment requires AI vendors to have pervasive access across multiple functions or across entire organizations.

Adversaries are capitalizing on this exposure, frequently targeting third parties as an initial access vector before pivoting laterally into primary target environments. To decrease this exposure without limiting critical third-party relationships, CISOs should close foundational control gaps found by our survey: 47% of organizations fail to properly segment their environments, and 59% lack comprehensive asset telemetry, reducing visibility and delaying detection.

AI systems and tools were the third-most represented category in the vulnerability zone. AI poses challenges for both the visibility and coverage elements of the vulnerability zone calculation. Visibility is challenged in multiple ways. The generative AI rollout often creates shadow usage and untracked data flows as employees adopt tools outside approved channels, while agentic AI introduces additional blind spots through proliferating agents, identities, tool connections and autonomous actions that are difficult to inventory and monitor. Coverage gaps compound the issue because many security teams do not yet apply consistent controls, testing, monitoring or governance to AI systems and tools that evolve quickly and connect to sensitive data and workflows.

47%

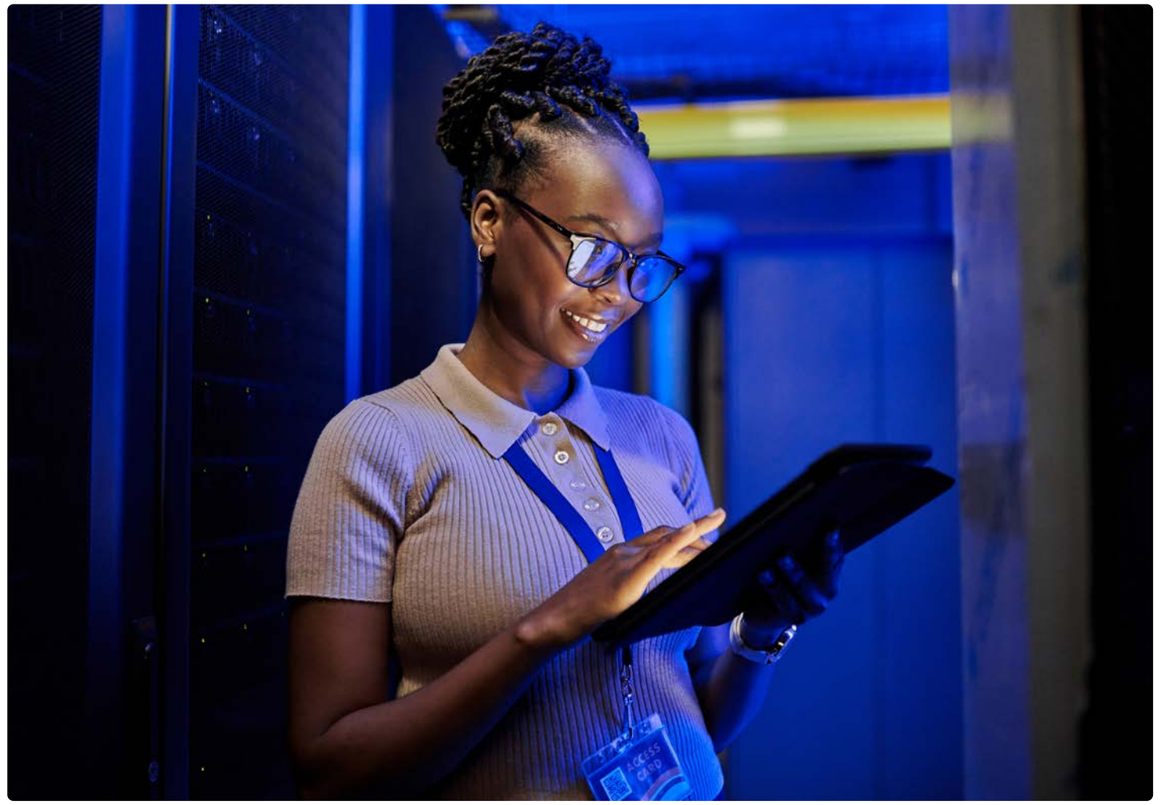
of organizations fail to properly segment their environments.

59%

of organizations lack comprehensive asset telemetry.

Network infrastructure — with 38% of assets in the vulnerability zone — is the fourth-most represented category, but a top concern for CISOs. Adversaries, especially nation-state actors, are increasingly targeting perimeter devices, like VPN gateways, firewalls, routers and edge network appliances, as initial access vectors. Compared to modern cloud services or endpoint software, many of these kinds of networking devices have characteristics like custom firmware or slow patch cycles that will make them even more susceptible to frontier AI-enabled threats. It is critical for CISOs to move these assets out of the vulnerability zone by improving their visibility and cybersecurity coverage.

Network infrastructure is the fourth-most represented category, but a top concern for CISOs.



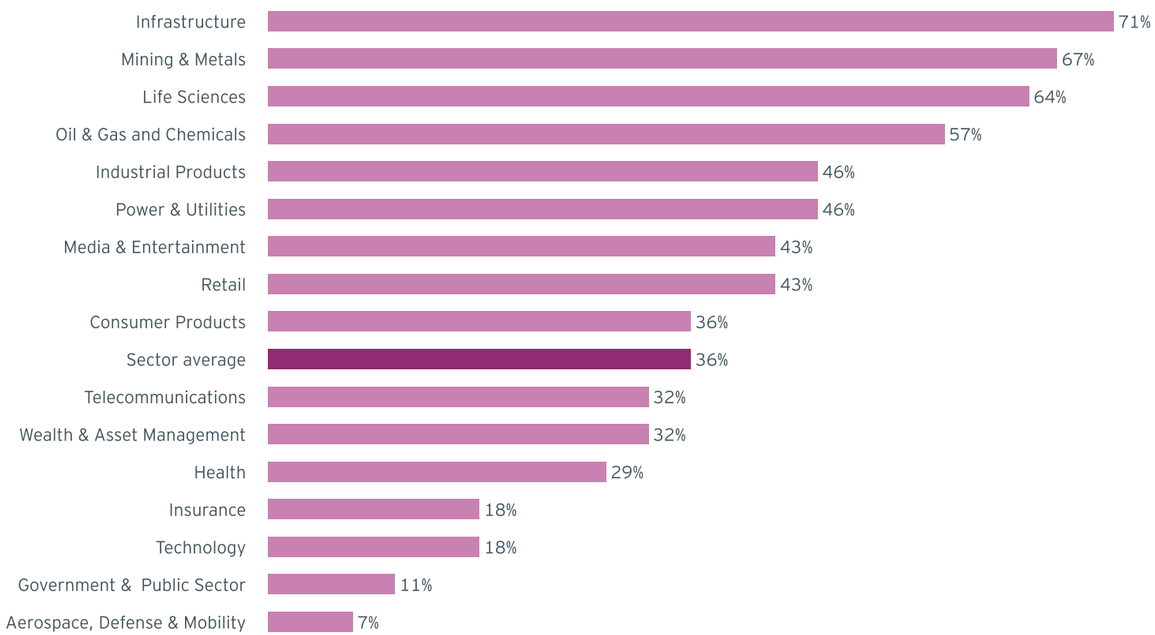
Broadly, sectors more dependent on OT assets have more assets in the vulnerability zone.

Our analysis reveals sectoral patterns in the vulnerability zone. Broadly, sectors more dependent on OT assets – like Infrastructure, Mining & Metals, Power & Utilities, Oil & Gas and Chemicals – have more assets in the vulnerability zone. Most of the sectors with the fewest assets in the vulnerability zone – Government & Public Sector; Banking & Capital Markets; Insurance; Aerospace, Defense & Mobility – typically have regulatory regimes that enforce stricter security rules.

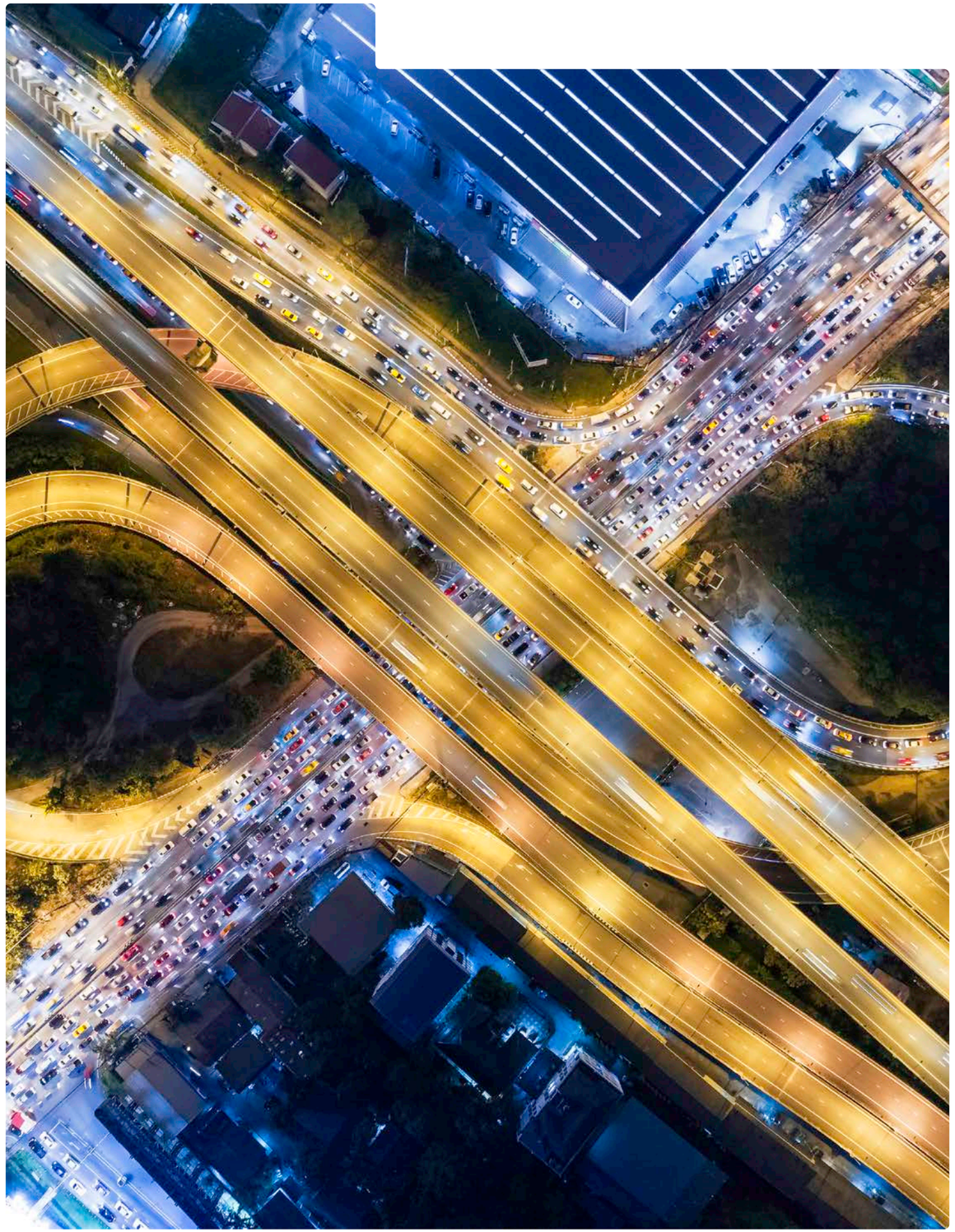
See appendix for a sector- and asset-level analysis of the vulnerability zone.

The size of the vulnerability zone varies significantly by sector

Average percent of assets that fall into the vulnerability zone



Based on 475 sectorized assets. Inclusion in the vulnerability zone defined by below average visibility and coverage of each asset. See "Identifying the vulnerability zone" for full details.



Gain complete visibility of your organization to minimize the vulnerability zone

Partial visibility of your assets is no longer adequate as threats from frontier AI expand the attack surface.

02

The exclusive use of manual, disconnected asset identification methods in a world where adversaries can – in seconds – locate and exploit vulnerabilities in systems invisible to cybersecurity is a threat to enterprise resilience.

These methods are also out of sync with how future, agentic AI-enabled organizations will be organized and operated.

> In agentic environments, visibility must shift to real-time, machine-readable mapping of agents, identities, permissions and execution paths as they form.
>
> **Maez de Guzman**
> EY Global Cybersecurity Managed Services Emerging Markets Leader

In agentic AI environments, where software agents can create and use identities, permissions and tool connections at machine speed, manual asset identification methods are too slow and fragmented to maintain an accurate view of what exists, how it interacts and where risk is accumulating.

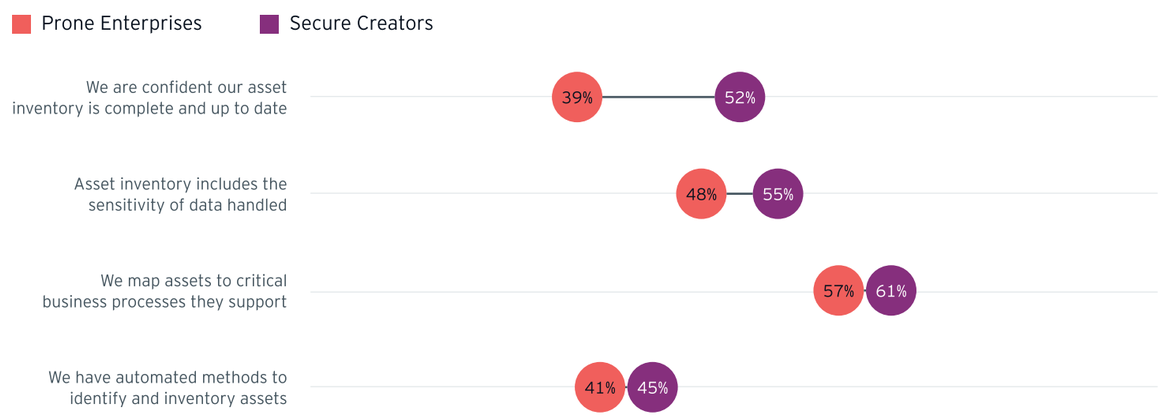
Our study found that 70% of cybersecurity leaders believe their most significant risks are located in blind spots.

With boards and C-suites now more attuned to cybersecurity risk following recent frontier AI vulnerability revelations, CISOs should use this moment to invest in enterprise-wide visibility.

Our research found that many cybersecurity functions are starting from behind. According to our analysis of open text survey responses, respondents' biggest challenges in achieving asset visibility are dependency complexity, resource constraints and asset data governance.[2] Only 43% of respondents use automated methods to identify and inventory assets and 45% said they were confident that their asset inventory is complete and up to date.

Cybersecurity visibility methods must keep up with fast-moving adversaries

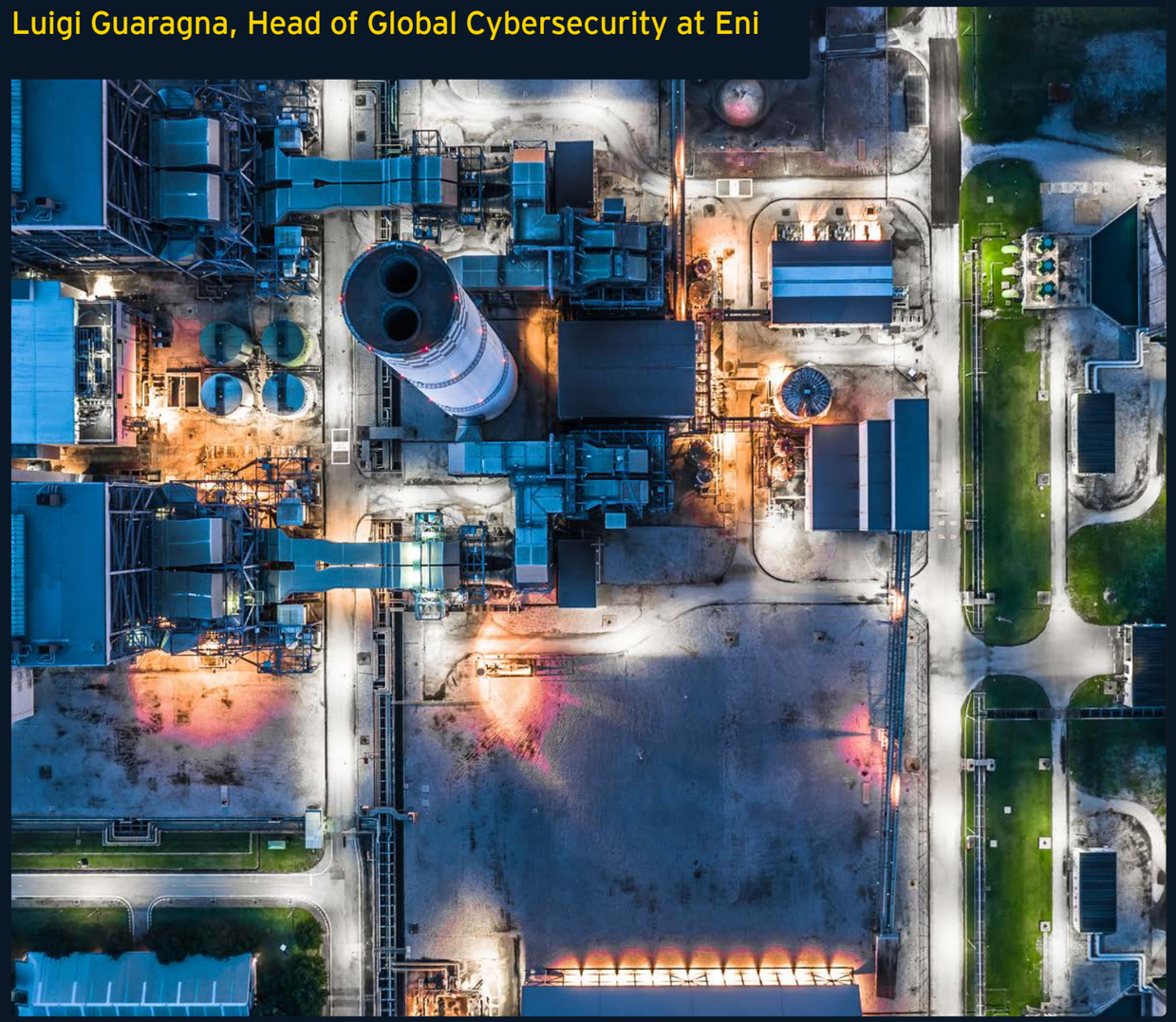
Percent that say the following mostly or completely describes their cybersecurity function's approach



2 EY Insights analysis leveraging an LLM to systematically categorize and tag free-text survey responses according to a predefined curated taxonomy.

Guest perspective

Luigi Guaragna, Head of Global Cybersecurity at Eni



How Eni manages vulnerabilities on a global scale

Eni operates in more than 60 countries, across businesses that range from oil and gas to biorefining, chemicals and renewables. That scale makes asset visibility less about a single central view and more about building a model that works across many operating realities.

Our approach is a distributed model with a strong center. We define policies, rules and security measures centrally, and our IT teams worldwide – including in subsidiaries and locations where assets are managed locally – apply those requirements consistently. To make that governance actionable, local teams provide standardized visibility inputs (for example, comprehensive asset and IP information on a regular cadence), which enables us to run enterprise-wide vulnerability management with confidence that we are looking at the right scope.

Where services are centralized, visibility is naturally easier – our core IT estate is managed through a central CMDB in ServiceNow. We pair that with vulnerability scanning and bring findings into ServiceNow's Security Operations, where we prioritize remediation using a practical set of lenses: the known severity of the issue (common vulnerabilities and exposures-based), the criticality of the asset and the likelihood of exploitation. That shared prioritization model helps align owners across a large organization on what matters most and what must move first.

A key integrator for this distributed effort is our global endpoint configuration program, GeCO, which sits within our zero-trust journey. Endpoints may be supported locally for practical reasons, but GeCO gives us a consistent way to see them, verify their configuration and push centrally defined baseline controls when needed – so local flexibility doesn't come at the cost of uneven security posture.

OT requires a different operating rhythm because the business owns the environment, and our role is to set the framework, perform assessments, identify gaps and rigorously track remediation with the business and OT vendors. We also invest in collaboration and training to keep building shared understanding and capability over time.

Finally, we are strengthening how cybersecurity engages in M&A. In practice, that means getting involved earlier in the deal lifecycle – not only at sign-off – so we can shape integration decisions with risk in mind. At the same time, we are leveraging technology within our zero-trust program, including an SSE solution designed to help incorporate acquired companies and extend our cybersecurity services more quickly once organizations need to interoperate.

> "Where services are centralized, visibility is naturally easier — our core IT estate is managed through a central CMDB in ServiceNow.
>
> **Luigi Guaragna, Head of Global Cybersecurity**
> Eni

Secure Creators, our survey's leading cohort of respondents, appear better prepared for frontier AI-enabled threats because they are closer to full enterprise visibility and better understand the interconnections between their assets. This is reflected in significantly higher satisfaction with configuration management databases (85% versus 45% of Prone Enterprises), giving CISOs a more reliable view of what matters most and where exposure concentrates.

Leading CISOs are building on this foundation by shifting toward autonomous, AI-assisted discovery, prioritization and remediation, supported by continuous telemetry and threat-based exposure monitoring. They pair these capabilities with clear, cross-functional ownership for remediation and integrate security into software development lifecycles. This positions organizations to adopt AI more safely and operate effectively in autonomous, agent-driven environments.

"Leading cybersecurity functions need to use the lessons they learned securing software development by building cybersecurity into AI agent development lifecycles," Ganesh Devarajan, EY Americas Consulting Cyber Risk Leader, said. "This build-out should include automated discovery of AI models and agent-to-agent communications."

Beyond asset visibility, Secure Creators are also more advanced than their peers at network, identity and dependency mapping — a critical capability in a world where AI-enabled adversaries are increasingly targeting identity and trust mechanisms as entry points to quickly move laterally across enterprises. Secure Creators, who are more likely to highly rate their network mapping abilities (67% give high ratings vs. 59% of prone enterprises), are building extended visibility maps across their organizations

As the very concept of an "identity" evolves with the agentic AI rollout, CISOs who have the best fundamental understanding of their attack surface and the interplay between networks and dependencies will be best positioned to manage the proliferation of non-human, dynamic and machine-speed identities.

"

Leading cybersecurity functions need to use the lessons they learned securing software development by building cybersecurity into AI agent development lifecycles

Ganesh Devarajan
EY Americas Consulting Cyber Risk Leader

How to build resilience for the next cybersecurity shock

The current moment is a catalyst for firms to more deeply integrate cybersecurity into enterprise resilience, before the next inflection point hits.

03

In a NAVI world, inflection points beget more inflection points, meaning boards and C-suites need to think beyond the threats posed today by frontier AI models. In our survey, conducted in the weeks before the recent frontier AI revelations, only 45% of cybersecurity leaders felt prepared for AI-enabled threats. Just 21% are prepared for quantum-enabled threats.

To prepare for these risks – and those we are yet to imagine – organizations must build resilience strategies that deeply integrate cybersecurity and allow them to uphold their fundamental promises to stakeholders in the face of disruption. This approach requires defining and defending the minimum viable enterprise (MVE): the critical capabilities, assets and dependencies needed to sustain core commitments. Defending the MVE requires real-time signals that indicate whether it can still function as conditions change, tabletop exercises to validate its architecture, and physical and digital infrastructure to close strategic gaps.

How EY helps define and defend the minimum viable enterprise (MVE)

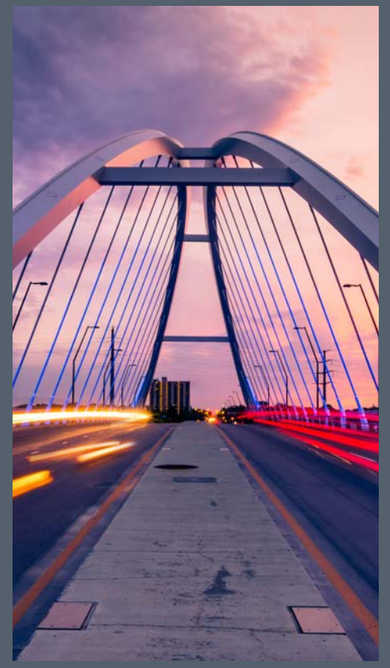
EY helps clients build a minimum viable enterprise (MVE) – the smallest functioning version of the business that can keep serving customers, paying staff and meeting obligations during a major incident. It is not the full enterprise restored to pre-incident state, but the core that must never go dark.

01 **Identify the critical services:** Work with the business to name the products and obligations the enterprise must keep delivering through an incident. This establishes the MVE service list and anchors what continuity requires.

02 **Map the supporting estate:** Trace each service to its applications, data stores, identities and infrastructure. CMDB and SBOM become the source of truth, providing a clear, structured view of what must operate to sustain the MVE.

03 **Surface hidden dependencies:** Resolve identity providers, third-party SaaS and shared platforms. The MVE is only as resilient as its weakest external link, producing a full dependency graph.

04 **Defend the MVE:** Through a phased engagement, we help define the MVE blueprint, run tabletop and rehearse exercises calibrated to likely threats, and build the technical floor – including the immutable backup estate, isolated recovery vault and codified MVE rebuild – delivering a demonstrably recoverable MVE.



For cybersecurity to enhance resilience, defenses need to operate much closer to machine speed and to be structurally aligned with the threat landscape. Resilience depends on continuous monitoring, high-quality intelligence and automated detection and response. With adversaries increasingly moving across legacy systems, internal dependencies, third parties and data access pathways, leaders need a connected view of the attack surface that reflects how systems interact and how failures propagate.

Frontier AI and future inflection points will expose the cost of deferred enterprise modernization. A recent survey supporting the long-term research collaboration between EY and the Saïd Business School at the University of Oxford shows that there has been a 28% increase in the number of organizations motivated to undertake large-scale transformations to improve their cybersecurity. Legacy architectures, accumulated technical debt and poorly-understood complexity are resilience liabilities in the face of faster, more adaptive threats. Sustained resilience will require confronting structural weaknesses directly, rather than continuing to manage around them.

Only

48%

are confident in their ability to quickly detect an incident in their supply chain.

Coordinating resilience outside of your organization

Frontier AI model developers have launched ecosystem-wide initiatives in response to a new reality: vulnerability discovery is accelerating faster than most organizations can validate and remediate issues on their own. Alongside these efforts, initiatives such as CrowdStrike's Project QuiltWorks – an industry coalition that uses AI to identify, validate and prioritize vulnerabilities before they can be exploited – bring together security providers, AI researchers and organizations including EY to accelerate coordinated risk reduction.

"Project QuiltWorks is about using frontier AI to help organizations stay ahead of emerging risk," said Fabio Fratucello, Field CTO World Wide, CrowdStrike. "Powered by leading frontier AI models, QuiltWorks brings together CrowdStrike's security expertise and industry partners like EY to help identify vulnerabilities, understand how they can be chained together by adversaries, and validate risk in real-world environments. The goal is to help organizations prioritize remediation and reduce exposure before vulnerabilities can be weaponized."

For participating organizations, these initiatives can provide earlier visibility into emerging vulnerabilities, faster validation and more coordinated remediation efforts across interconnected ecosystems. More broadly, the industry benefits when vulnerabilities are identified and addressed upstream by technology providers, reducing systemic risk and helping organizations mitigate exposure before vulnerabilities are exploited.

Resilience depends on managing cybersecurity risks from identities and SaaS providers

Only 48% of respondents are confident in their ability to quickly detect an incident in their supply chain.

Resilience and business continuity increasingly depends on trust in third parties that support critical business processes. This arrangement looks precarious in the face of increased identity-based cyberattacks, which prey on identity protocols that require direct interaction between sensitive internal resources and SaaS providers. As highlighted in the CrowdStrike 2026 Global Threat Report, 82% of detections were malware-free, demonstrating that many modern intrusions increasingly rely on compromised identities, legitimate credentials and trusted access pathways rather than malware.

Faster vulnerability discovery and exploitation compound the issue. Many third party vendors — especially smaller, less-resourced firms — may be unable to provide sufficient evidence of remediation or patching of vulnerabilities exposed by frontier AI. Identifying and validating alternative providers is one workaround, but viable substitutes do not exist in many cases, particularly where critical processes rely on a small number of specialized vendors.

To combat this reality, organizations must adapt how they interact with third parties to build resilience and counteract the rise in identitybased threats. This means moving from periodic vendor assessments and "VPN and a contract" to continuous, identity-centric, least-privilege, monitored access patterns paired with supply-chain assurance and runtime guardrails.

Secure Creators are already ahead. They are more likely to have mandated and verifiable security requirements for third parties with access to their organization's environment (55% have these requirements vs. 39% of Prone Enterprises). They are also significantly more confident in their ability to quickly detect a cybersecurity incident in their supply chain (68% vs. 30%) or in a data center (81% vs. 49%).

Expanding the cybersecurity remit over OT and physical assets is critical to enterprise resilience

OT doesn't always fall squarely within cybersecurity's remit, but CISOs need to be consulted when OT and physical assets are being connected to networks or enabled with AI. When consulted on these projects, CISOs should weigh two considerations:

- Don't connect OT by default: every new connection should be treated as a deliberate risk decision, weighing the operational benefits against the cybersecurity threat.
- Assume legacy OT will remain vulnerable: for already connected environments running hardware that is rarely or never updated, CISOs need to defend around unpatchable systems with isolation, monitoring and compensating controls.

"Resilience in OT starts with visibility — asset identification is key," Piotr Ciepiela, EY Global Cyber Architecture, Engineering & Emerging Technology Leader said. "While cybersecurity typically drives that effort, it's impossible without deep coordination with OT. And even then, you have to plan for the reality that much of the OT environment can't be patched, so resilience comes from segmenting, isolating and building controls around what you can't fix."

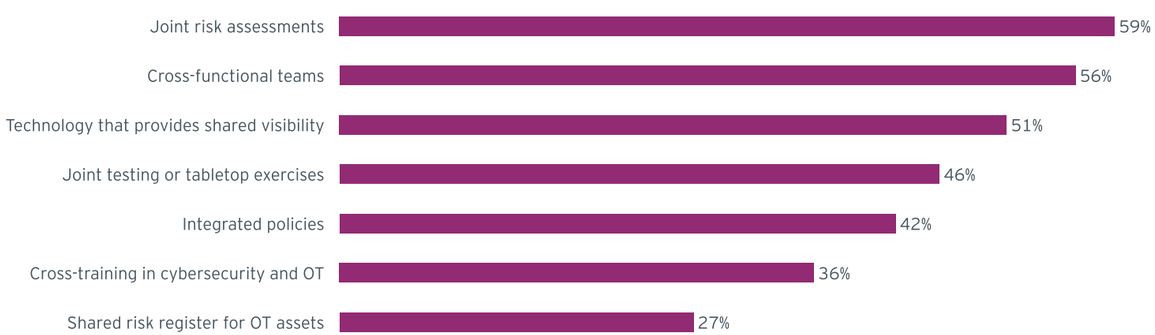
Secure Creator cohort manages OT and physical assets better than their peers by coordinating more closely with the operations function

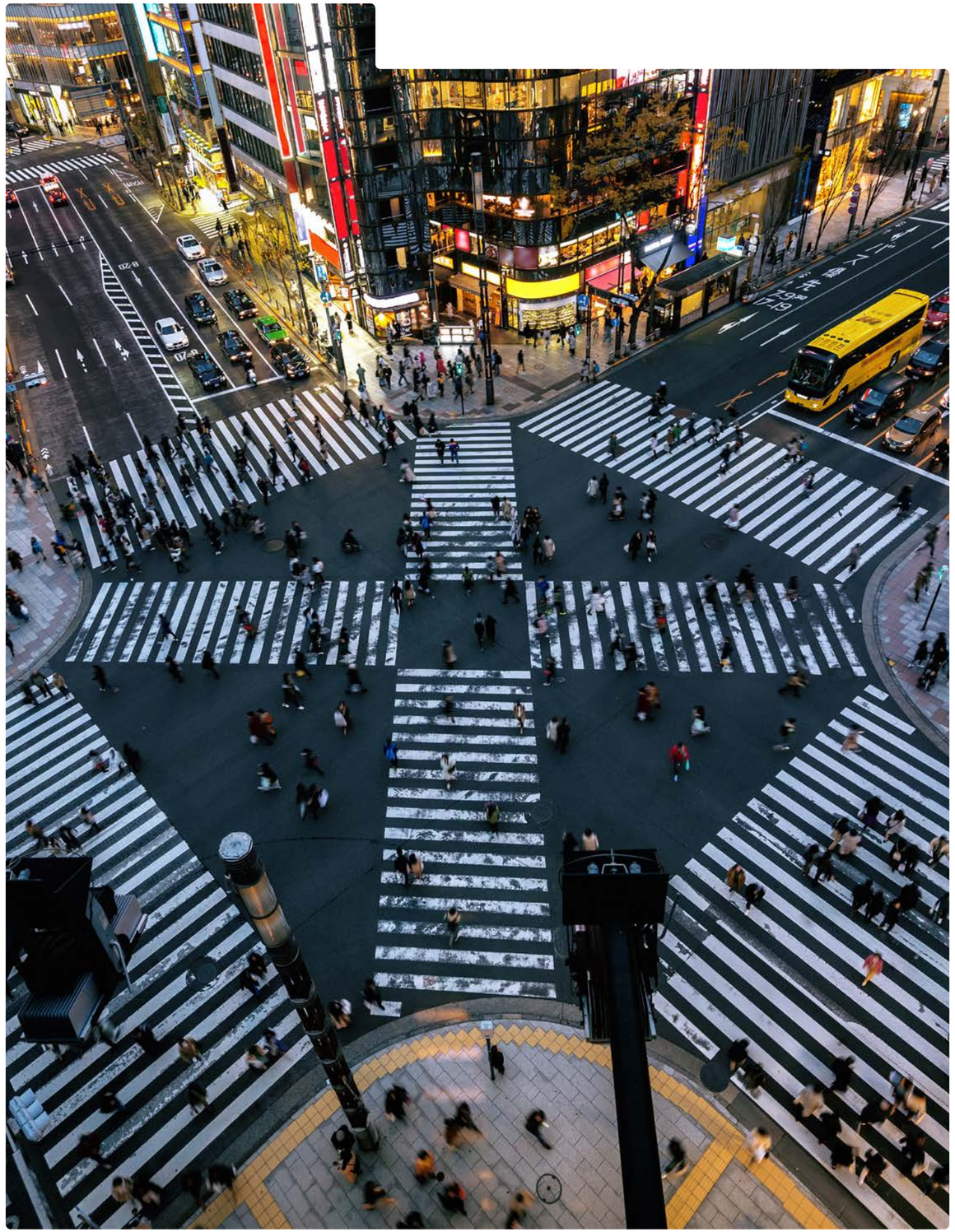
Two shifts in the cybersecurity threat landscape make OT coordination critical for resilience. The first shift is towards OT as a threat vector, with groups like Volt Typhoon demonstrating how adversaries can quietly compromise legacy OT and infrastructure systems to undermine operational resilience over time. The second shift is towards using advanced AI capabilities to identify and exploit weaknesses in connected devices, interfaces and legacy environments that aren't as frequently updated as IT systems.

In our study, the Secure Creator cohort manages OT and physical assets better than their peers by coordinating more closely with the operations function. They are more likely to have cross-functional teams for OT coverage (61% vs. 51% of Prone Enterprises) and are more satisfied with their coordination with operations teams for the security of physical assets and OT (68% vs. 45%).

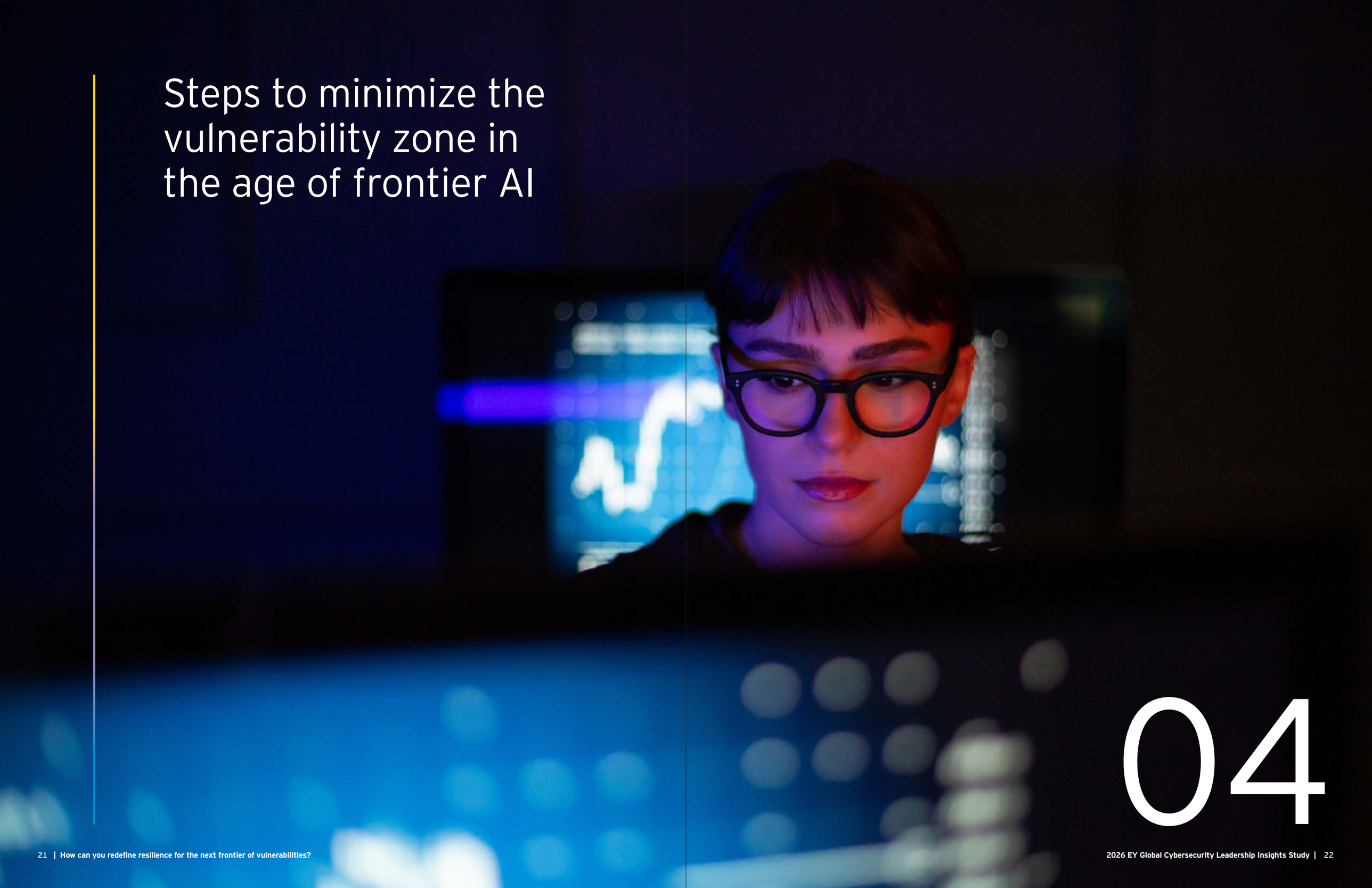
Coordination with OT teams is critical as assets are connected to networks and AI

Percent of organizations with the following in place





Steps to minimize the vulnerability zone in the age of frontier AI



04

CISOs should use the next 12 to 18 months to materially shrink the vulnerability zone

01

Develop continuous, enterprise-wide asset and identity visibility

- Move from fragmented, manual asset inventories to automated, continuous discovery and telemetry across assets, identities and dependencies
- Develop a real-time, integrated view of the attack surface, including non-human identities, service accounts and AI agents
- Improve visibility into perimeter devices such as VPN gateways, firewalls, routers and edge appliances, which are often insufficiently monitored
- Extend visibility beyond core IT into OT, third parties and AI systems, where gaps are most pronounced

02

Close foundational coverage gaps across the attack surface

- Strengthen baseline controls, with a focus on network segmentation and comprehensive telemetry
- Apply consistent security controls, testing and monitoring to network infrastructure and edge devices
- Expand coverage beyond "crown jewels" to include interconnected assets that enable lateral movement
- Ensure that assets with high rates of change, including AI systems, are continuously governed and monitored

03

Define and defend the minimum viable enterprise to bolster resilience

- Identify the critical services, assets and dependencies required to sustain core business operations
- Establish real-time resilience signals, continuous monitoring and automated detection and response to ensure the enterprise can operate through disruption
- Map and manage interdependencies across systems, identities, third parties and infrastructure to reflect how failures propagate across the attack surface
- Use scenario testing and tabletop exercises to validate resilience architecture and prepare for future inflection points, including AI- and quantum-driven threats

04

Accelerate investments in modern cybersecurity defense

- Use frontier AI models internally to strengthen code scanning
- Apply frontier AI to enhance infrastructure vulnerability scanning across the vulnerability zone and prioritize what to fix
- Accelerate the transformation of traditional SOC operations by building an autonomous model that continuously detects, investigates and responds to threats at scale

05

Shift to continuous, identity-centric third-party risk management

- Evolve from periodic vendor assessments to continuous monitoring of third-party access and behavior
- Enforce identity-centric, least-privilege access across employees, partners and machine identities
- Implement runtime controls and guardrails for SaaS and third-party integrations
- Reframe the attack surface around identity pathways and trusted access relationships rather than perimeter boundaries alone

06

Prioritize security of perimeter and network infrastructure in the resilience model

- Treat perimeter devices as priority assets, given their role as common initial access vectors
- Improve visibility, patching discipline and monitoring of devices with slower update cycles and embedded firmware
- Bring network infrastructure into continuous exposure management and broader enterprise security programs
- Reduce implicit trust at the network edge and assume that compromise can originate from perimeter environments

Detailed Sector Breakdown

Appendix

Sector impact

Aerospace, Defense & Mobility

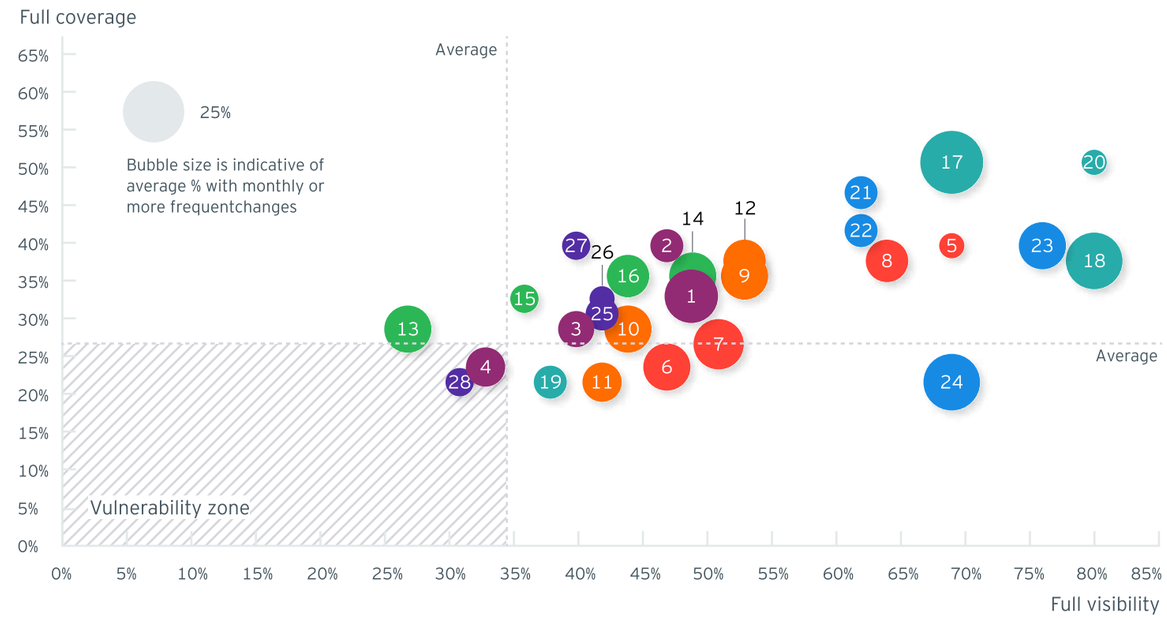
Aerospace, Defense & Mobility organizations appear to have stronger core cybersecurity discipline than most sectors, but they still face pressure from AI adoption, complex supply chains and heightened geopolitical risk.

Many of the most critical functions in the sector depend on external partners, from maintenance and repair to specialty hardware and component suppliers. Cybersecurity resilience depends not only on internal controls but also on how well organizations understand the security of the broader ecosystem around them, especially where suppliers may themselves be targets of state-backed activity. audience engagement and content delivery depend on a wide set of partners.

Key sector insights from the study

- Seven percent of assets in the Aerospace, Defense & Mobility sector fall into the vulnerability zone.
- Broadly, respondents report better visibility and cybersecurity coverage over assets than peers in other sectors, but organizations tend to have less visibility over their ecosystems than over their other assets, including maintenance and repair partners, specialty chip and hardware supply chain partners, and avionics and component suppliers. This is a potential concern as third parties are critical to operations in this sector, particularly for defense companies whose suppliers may be targets for state-sponsored cyberattacks.
- Accelerated pace of change might create new vulnerabilities for the sector. Twenty-two percent of respondents said public and private APIs, remote access and jump hosts undergo monthly or more frequent changes that require updates in cybersecurity controls.

Vulnerability zone



AI systems and tools

1. AI for manufacturing quality inspection
2. AI for mission planning and decision support
3. AI for predictive maintenance of fleets and aircraft
4. **AI for supply chain risk detection**

Cloud assets

5. Backup and disaster recovery storage
6. Cloud compute for simulation and digital twin workloads
7. Cloud storage for design and test data
8. Secure cloud environments for engineering and analytics

Data assets

9. Export-controlled and program data
10. Software source code and build artifacts
11. Supply chain and parts traceability data
12. Telemetry, flight test, and mission data

Ecosystems

13. Avionics and component suppliers
14. Cloud, SaaS, and data center providers
15. Maintenance and repair partners
16. Specialty chip and hardware supply chain partners

Network infrastructure

17. Perimeter controls such as WAF and DDoS protection
18. Remote access and secure jump hosts
19. Satellite and aircraft communications links
20. Segmentation between classified and unclassified environments

Non-AI digital assets

21. Fleet management and maintenance systems
22. Flight software and embedded system toolchains
23. Product lifecycle management and digital engineering systems
24. Public and private APIs

OT and physical assets

25. Aircraft, drones, and vehicle platforms
26. Avionics, sensors, and communications equipment
27. Manufacturing facilities and specialized tooling
28. **Test stands, wind tunnels, and lab equipment**

Asset in vulnerability zone

Sector impact

Banking & Capital Markets

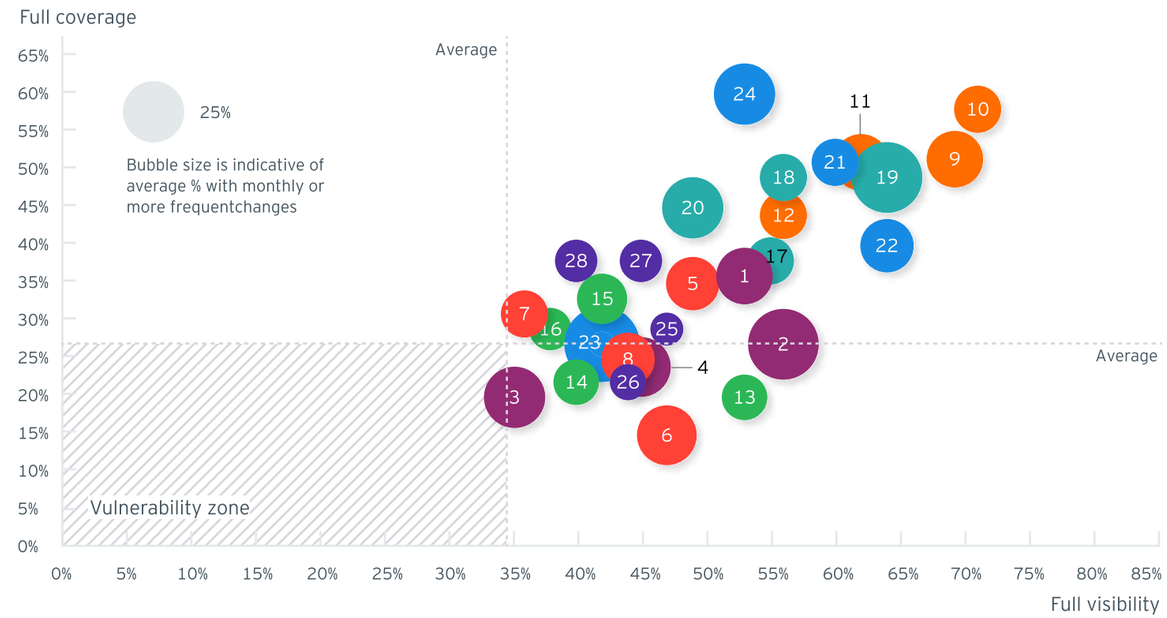
The Banking & Capital Markets sector stood out in our study for the strength of its cybersecurity posture.

This likely reflects the weight of regulatory expectations around operational resilience, incident reporting and third-party oversight. In the United States, banks are subject to formal cybersecurity incident notification requirements, and in Europe, DORA has raised the bar further for ICT risk management, resilience testing and oversight of critical service providers. Even so, the sector is not immune to the next wave of cybersecurity exposure as AI is further integrated into customer interaction and data environments, particularly where new capabilities are introduced through APIs, partner integrations and shared technology platforms.

Key sector insights from the study

- The Banking & Capital Markets sector has above average visibility compared to all other sectors.
- However, many assets have insufficient cyber coverage, especially cloud accounts and landing zones, customer service AI assistants, and data center providers.
- Accelerated pace of change might create new vulnerabilities for the sector. Banking & Capital market assets have higher frequencies of changes that require updates in security controls than average. For example, 35% of respondents said open banking APIs and partner integrations undergo monthly or more frequent changes that require updates in cybersecurity controls.

Vulnerability zone



AI systems and tools

1. AML and sanctions monitoring models
2. Credit risk and default prediction models
3. Customer service AI assistants
4. Fraud detection models for payments and cards

Cloud assets

5. Backup and disaster recovery in cloud
6. Cloud accounts and landing zones
7. Cloud data platforms for analytics
8. Cloud storage and managed databases

Data assets

9. Account and balance data
10. Customer PII and consent records
11. KYC and identity verification documents
12. Payment and card transaction records

Ecosystems

13. Cloud, SaaS, and data center providers
14. Credit bureaus and market data vendors
15. Fintech partners and outsourced service providers
16. Payment networks and processors

Network infrastructure

17. ATM and payments network segments
18. Branch and headquarters networks
19. Internet edge protections for digital channels
20. Remote access for staff and vendors

Non-AI digital assets

21. Core banking system
22. Mobile and online banking channels
23. Open banking APIs and partner integrations
24. Payments processing platforms

OT and physical assets

25. ATMs and self-service kiosks
26. Branches and critical office sites
27. Data centers and communications rooms
28. Teller and trading floor workstations

Asset in vulnerability zone

Sector impact

Consumer Products

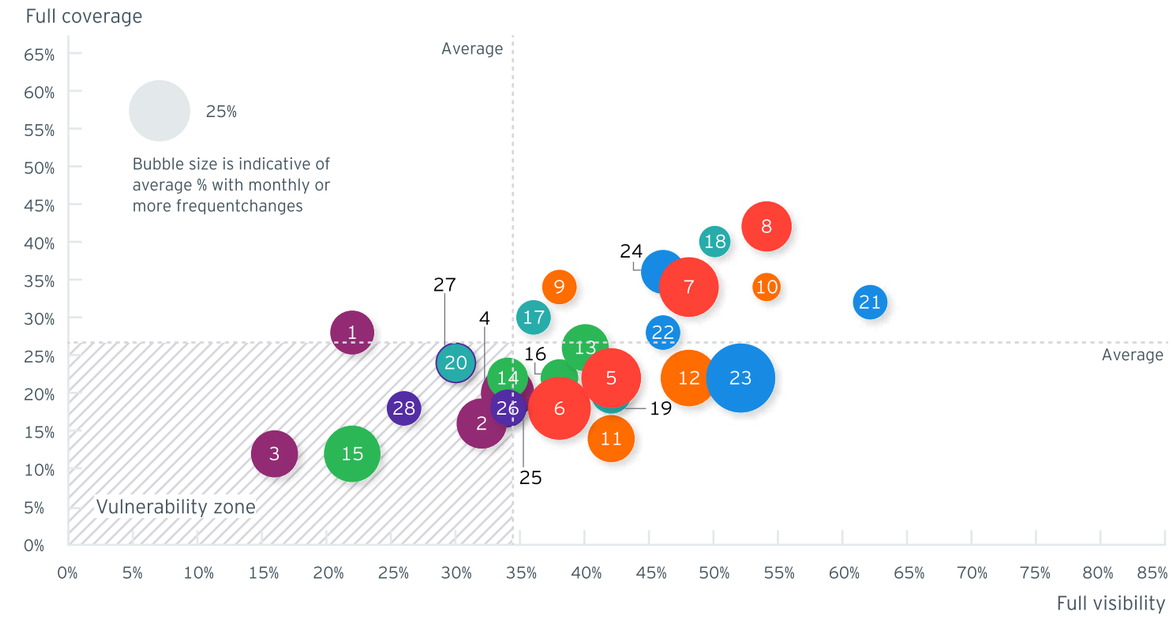
Growth in Consumer Products is increasingly tied to how quickly companies can sense and respond to fast-moving, fragmented demand.

To enable this, organizations are connecting demand creation and fulfilment more tightly, linking pricing, promotion and forecasting directly to manufacturing and logistics. AI is central to this shift, enabling faster and more dynamic decisions across this end-to-end system. At the same time, it is reshaping cybersecurity risk across both commercial systems and physical operations. As connectivity increases across internal systems and external partners, exposure is growing across a highly interdependent ecosystem, often faster than it is being secured.

Key sector insights from the study

- Thirty-six percent of assets in the consumer products sector fall into the vulnerability zone, spanning both AI-driven decision systems and connected operational environments.
- Asset categories most exposed in the vulnerability zone include AI systems and tools, OT and physical assets, and ecosystems.
- In commercial systems, several assets critical to demand creation sit in the vulnerability zone due to low visibility or weak cybersecurity coverage. These include pricing, promotion and revenue optimization models, demand forecasting and supply planning AI, marketing personalization and generative AI tools, and martech, adtech and media agency platforms, where ownership and security are often fragmented across partners.
- In operational environments, the issue differs. Assets such as manufacturing and packaging equipment, robotics, sensors and IoT devices, and connected fleet and handheld devices are generally well understood, but cybersecurity coverage has not kept pace with their increasing connectivity.
- Overall, risk is concentrated in the gap between rising connectivity and decision speed, and the level of cybersecurity coverage across commercial, operational and partner ecosystems. This extends exposure across the full loop from demand creation to fulfilment, making cybersecurity resilience a direct constraint on operating reliably at speed.

Vulnerability zone



AI systems and tools

1. Computer vision and AI-based quality inspection
2. **Demand forecasting and supply planning AI**
3. **Marketing personalization and GenAI tools**
4. **Price, promotion, and revenue optimization models**

Cloud assets

5. Cloud data lakes and analytics platforms
6. Cloud PLM platforms
7. Digital commerce and D2C platforms
8. SaaS platforms for planning, CRM, HR, and finance

Data assets

9. Product formulations, recipes, and intellectual property
10. Quality, compliance, and food safety data
11. Retailer sell-out, loyalty, and shopper data
12. Trade promotion, pricing, and margin data

Ecosystems

13. Cloud, SaaS, and data center providers
14. **Ingredient, packaging, and logistics providers**
15. **Martech, adtech, and media agency platforms**
16. Retailer technology platforms and data-sharing interfaces

Network infrastructure

17. Core networks supporting operations
18. Corporate LAN/WAN and SD-WAN
19. IoT and edge devices in factories and warehouses
20. **Plant-floor OT networks (ICS / SCADA)**

Non-AI digital assets

21. ERP platforms (order-to-cash, procure-to-pay)
22. Manufacturing Execution Systems (MES)
23. Public and private APIs
24. Warehouse and Transportation Management Systems (WMS/TMS)

OT and physical assets

25. **Fleet assets (connected vehicles, handheld devices)**
26. **Manufacturing and packaging equipment, and robotics**
27. **POS systems in owned or franchised retail environments**
28. **Sensors and IoT devices monitoring production**

Asset in vulnerability zone

Sector impact

Government & Public Sector

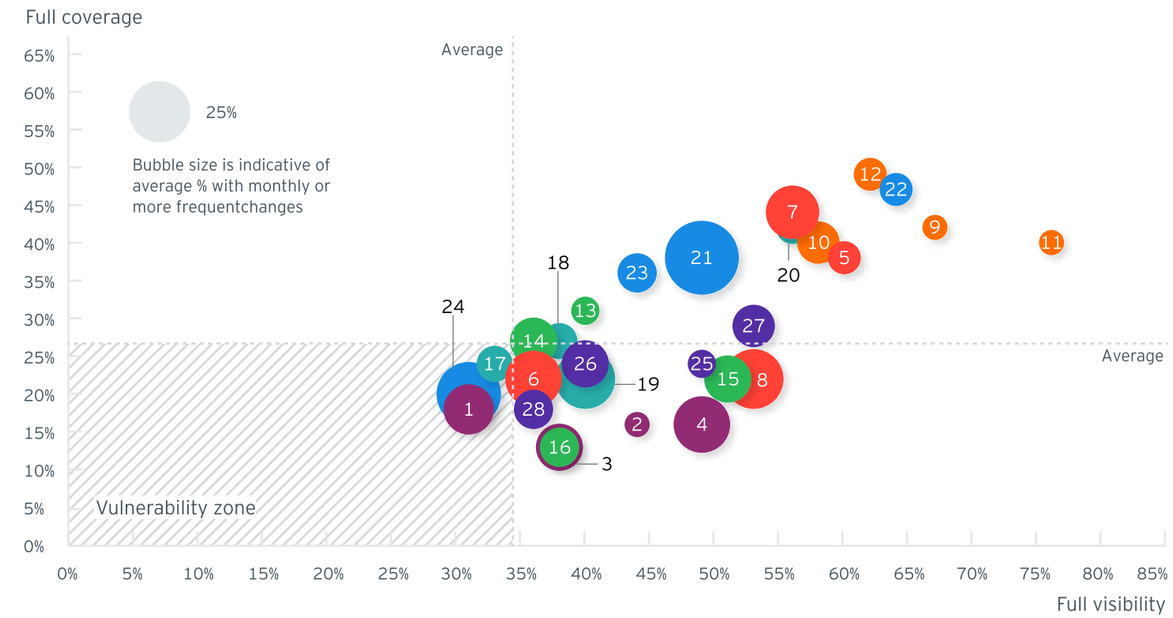
Being a leading target of cyberattacks poses unique risks for Government & Public Sector organizations that are under pressure to modernize services, in part by adopting AI and connecting data to more digital systems.

Constituent-facing AI tools and supplier-connected APIs can improve service delivery but also introduce new points of exposure. Agentic AI can connect disparate legacy systems, but it does not remove legacy vulnerabilities and can increase risk due to the potential blast radius of a compromised agent. For public sector organizations, the main challenge is whether security controls are being updated quickly enough across public services, third-party and supplier ecosystems (including vendor hosted data, software dependencies and outsourced service providers), and the connected interfaces that modernization efforts introduce.

Key sector insights from the study

- Eleven percent of assets in the Government & Public Sector fall into the vulnerability zone.
- This is one of the strongest sectors in the study for visibility and cybersecurity coverage over assets, potentially due to higher baseline security across government and public sector organizations, given the increased likelihood and sensitivity of cybersecurity incidents.
- A possible point of concern is public-facing AI, with only 31% of respondents saying they had full visibility over AI assistants for constituent services, and only 18% saying they had full cybersecurity controls over them.
- Government & Public Sector respondents also report lower-than-average visibility and cybersecurity coverage over public and private APIs (only 31% report full visibility and 20% report full coverage), and over government-wide networks and backbone connectivity (only 33% report full visibility and 24% report full coverage).
- Accelerating internal modernization efforts might create new vulnerabilities for the sector. Only around a third of respondents said constituent service portals, public and private APIs, and remote access platforms for contractors undergo monthly or more frequent changes that require updates in cybersecurity controls.
- Despite reporting relatively low direct exposure, governments may remain highly exposed to cyber risk through critical infrastructure dependencies that are often operated outside of government itself.

Vulnerability zone



AI systems and tools

1. AI assistants for citizen services
2. AI for case triage and workload prioritization
3. AI for fraud detection in benefits and taxation
4. AI for public safety analytics

Cloud assets

5. Backup and disaster recovery storage
6. Cloud storage and managed databases
7. Cloud-hosted identity and access management
8. Data platforms for analytics and reporting

Data assets

9. Citizen identity and demographic databases
10. Law enforcement and criminal records
11. Sensitive communications and classified records
12. Tax records and financial datasets

Ecosystems

13. Cloud and telecom providers supporting government workloads
14. Cloud, SaaS, and data center providers
15. Payment and identity verification service providers
16. Suppliers supporting critical materials and services

Network infrastructure

17. Government-wide networks and backbone connectivity
18. Inter-agency networks connecting ministries and departments
19. Remote access platforms for staff and contractors
20. Secure defense and emergency communications networks

Non-AI digital assets

21. Citizen service portals and mobile apps
22. National ID and identity verification systems
23. Passport and visa management systems
24. Public and private APIs

OT and physical assets

25. Biometric verification systems at borders and airports
26. Endpoint hardware such as desktops and laptops
27. On-premises data centers and server rooms
28. Secure storage and destruction facilities

Asset in vulnerability zone

Sector impact

Health

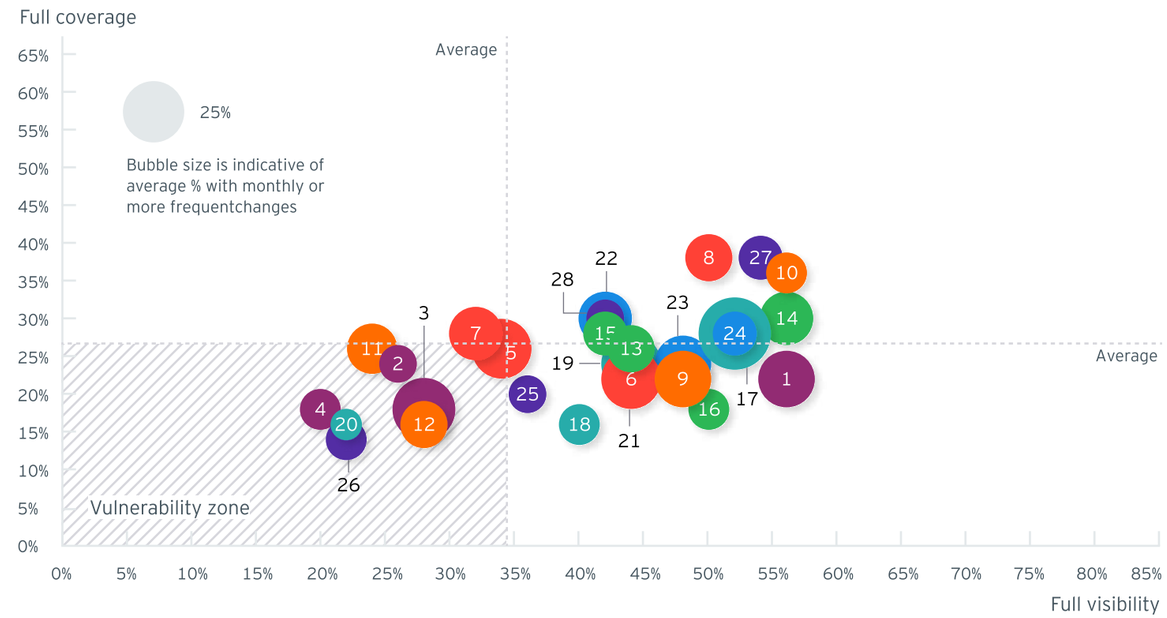
Health organizations are moving from a focus on AI use cases and point solutions, to determining where AI can actually deliver ROI.

While initial uses centered on back-office administrative functions, health organizations are now embedding AI into the clinical space, such as using ambient technology for note-taking during appointments.
The expansion into the clinical space raises risks as it touches onto more sensitive data, creating new cybersecurity exposure in environments where trust and confidentiality are critical. As frontier AI improves the speed of vulnerability discovery and attack development, health organizations must consider whether AI is being introduced into sensitive workflows faster than security teams can build the visibility and controls needed to manage it.

Key sector insights from the study

- Twenty-nine percent of assets in the Health sector fall into the vulnerability zone.
- AI systems and tools are most likely to fall within the vulnerability zone.
- Sector respondents reported the lowest visibility in clinically relevant AI use cases, including automated workflows that operate across clinical systems and AI used to support clinical decisions and risk scoring.

Vulnerability zone



AI systems and tools

1. AI for billing, coding, and claims management
2. AI used to support clinical decisions and risk scoring
3. Automated workflows that operate across clinical systems
4. Patient triage and symptom assessment tools

Cloud assets

5. Analytics platforms for research and population health
6. Cloud-hosted clinical and administrative systems
7. Integration platforms connecting clinical systems
8. SaaS platforms for collaboration and operations

Data assets

9. Billing and insurance data
10. Clinical research and trial datasets
11. Medical imaging and diagnostic data
12. Patient health and identity records

Ecosystems

13. Cloud, SaaS, and data center providers
14. Electronic health record and clinical system vendors
15. Laboratories and health information exchanges
16. Medical device manufacturers and service providers

Network infrastructure

17. Core infrastructure services such as directory services
18. Secure connections between hospitals, clinics, and labs
19. Secure remote access for clinicians and vendors
20. Segmented networks for medical devices

Non-AI digital assets

21. Imaging, laboratory, and pharmacy systems
22. Patient portals and telehealth platforms
23. Public and private APIs
24. Scheduling, registration, and billing systems

OT and physical assets

25. Bedside monitors and connected patient equipment
26. Imaging and diagnostic equipment
27. Laboratory instruments and automation systems
28. Medical devices used in patient care

Asset in vulnerability zone

Sector impact

Industrial Products

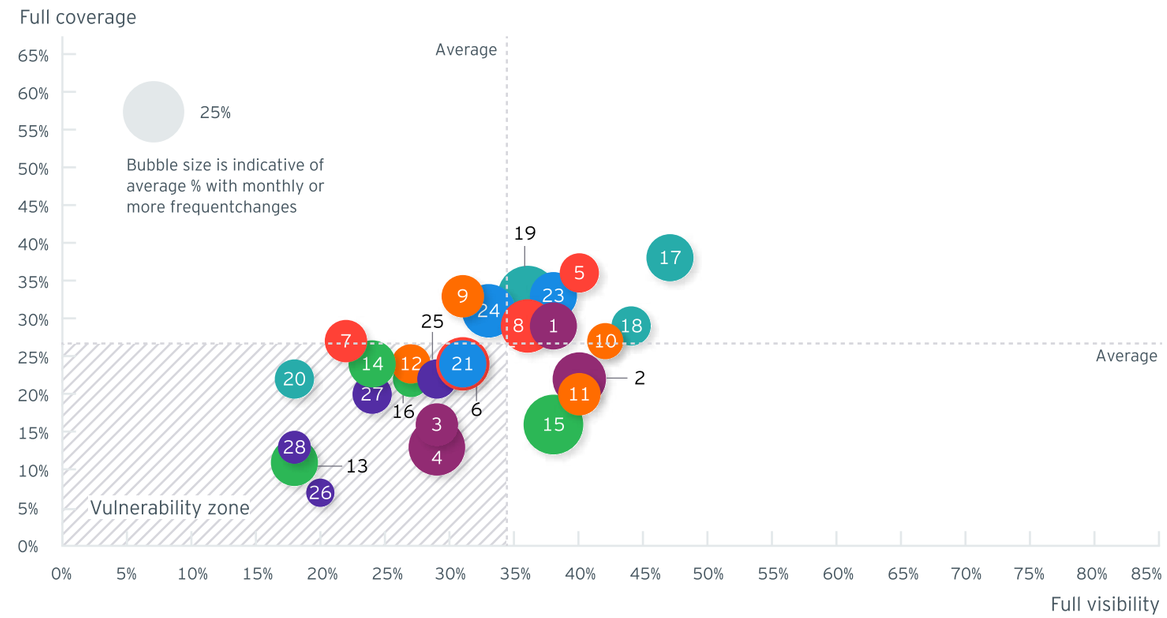
As industrial assets become more connected and AI-enabled, manufacturers are pushing deeper into vulnerability zones.

In these zones visibility gaps and cybersecurity controls lag behind operational integration. At the same time, frontier AI is making it faster and easier to identify and exploit these weaknesses, raising the risk to systems at the core of production.

Key sector insights from the study

- Forty-six percent of assets in the Industrial Products sector fall into the vulnerability zone.
- Asset categories in the vulnerability zone: AI systems and tools, OT and physical assets, and ecosystems.
- Industrial robots and automation systems stand out as a weak point, with only 20% of respondents saying they had full visibility over them, and only 7% saying they had full cybersecurity controls over them. Blind spots and coverage gaps are likely to become more important as these assets are increasingly connected to networks and integrated with AI.
- Supply chains were least likely to be seen as a source of cyber risk by industrial products respondents as compared to other sectors. As industrials seek greater transparency within their supply chains, control of exposure to cyber risk could be prioritized.

Vulnerability zone



AI systems and tools

1. AI for demand forecasting and inventory planning
2. AI for predictive maintenance and equipment health
3. **AI for production scheduling and throughput optimization**
4. **AI for supply chain risk and disruption detection**

Cloud assets

5. Backup and disaster recovery storage
6. **Cloud platforms for analytics and reporting**
7. Cloud storage for engineering files and production data
8. DevOps pipelines for product software and digital services

Data assets

9. Bills of materials and manufacturing recipes
10. Customer orders and service records
11. Maintenance records and equipment configurations
12. **Production telemetry and quality test results**

Ecosystems

13. **Cloud, SaaS, and data center providers**
14. **Contract manufacturers and assembly partners**
15. Software vendors for PLM, ERP, and MES
16. **Suppliers and component manufacturers**

Network infrastructure

17. Network segmentation and industrial firewalls
18. Plant networks segmented from corporate IT
19. Remote access for operations and vendors
20. **Wireless networks and handheld device connectivity**

Non-AI digital assets

21. **APIs and integration platforms connecting plants and partners**
22. Enterprise asset management systems
23. ERP and finance systems
24. Quality management systems

OT and physical assets

25. **CNC machines and production equipment**
26. **Industrial robots and automation systems**
27. **PLCs, HMIs, and control cabinets**
28. **Warehouses and material handling equipment**

Asset in vulnerability zone

Sector impact

Infrastructure

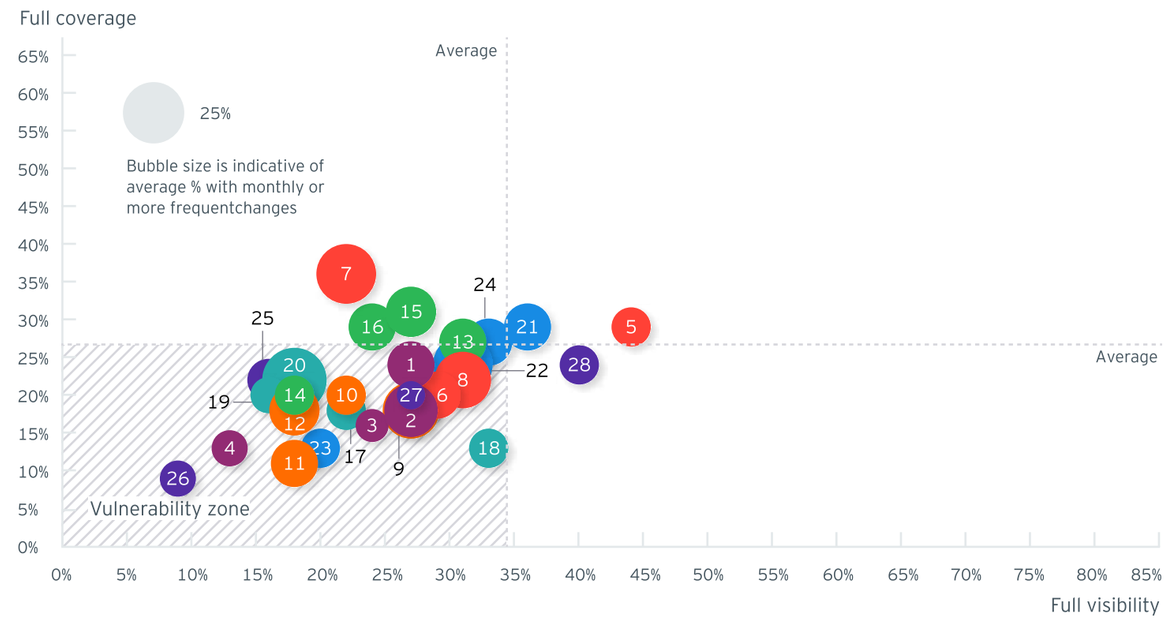
Infrastructure operators face one of the clearest examples of cybersecurity risk moving closer to physical operations.

Rail systems, traffic Infrastructure and structural monitoring assets are increasingly connected to networks, but many remain difficult to monitor with the same rigor as enterprise systems. Frontier AI accelerates vulnerability discovery in these environments, helping adversaries identify misconfigurations, weak authentication, and exposed remote access paths in OT and monitoring systems. As connectivity expands, operators need end-to-end asset inventory, continuous monitoring and segmentation to limit how far an intrusion can spread.

Key sector insights from the study

- Seventy-one percent of assets in the infrastructure sector fall into the vulnerability zone.
- The high share of assets in the vulnerability zone indicates that infrastructure cybersecurity risk is concentrated in physical and operational environments that are often operated outside government, where limited visibility or coverage increases the likelihood that cyber weaknesses translate into public service disruption or safety impacts.
- For rail operators, rail signaling, switches and control equipment are a notable concern, with only 9% of respondents saying they had full visibility over these assets.
- Other physical assets have low visibility including bridges, tunnels, and structural monitoring sensors (16% have full visibility) and traffic signals, controllers, and roadside equipment (27% have full visibility).
- By nature of this sector, infrastructure assets have lower than average pace of change, which provides an opportunity for organizations to improve visibility and coverage.

Vulnerability zone



AI systems and tools

1. AI for fraud detection in tolling and payments
2. AI for predictive maintenance of infrastructure assets
3. AI for scheduling maintenance crews and equipment
4. AI for water leak detection and pressure optimization

Cloud assets

5. Backup and disaster recovery storage
6. Cloud analytics and data platforms
7. Cloud storage for video, sensor, and maintenance data
8. Cloud-hosted public websites and traveler apps

Data assets

9. Engineering drawings and as-built documentation
10. Maintenance records and inspection reports
11. Tolling and fare transaction data
12. Traffic volumes, speed, and incident data

Ecosystems

13. Cloud, SaaS, and data center providers
14. Emergency services and public safety partners
15. Municipal and regional government partners
16. Payment processors and financial partners

Network infrastructure

17. Backbone links to control centers and operations hubs
18. Network segmentation and industrial firewalls
19. OT networks for traffic, water, and facility operations
20. Remote access for operators and vendors

Non-AI digital assets

21. Asset management and maintenance planning systems
22. Public and private APIs
23. SCADA systems for water and wastewater operations
24. Tolling, fare collection, and payment systems

OT and physical assets

25. Bridges, tunnels, and structural monitoring sensors
26. Rail signaling, switches, and control equipment
27. Traffic signals, controllers, and roadside equipment
28. Water treatment plants and pumping stations

Asset in vulnerability zone

Sector impact

Insurance

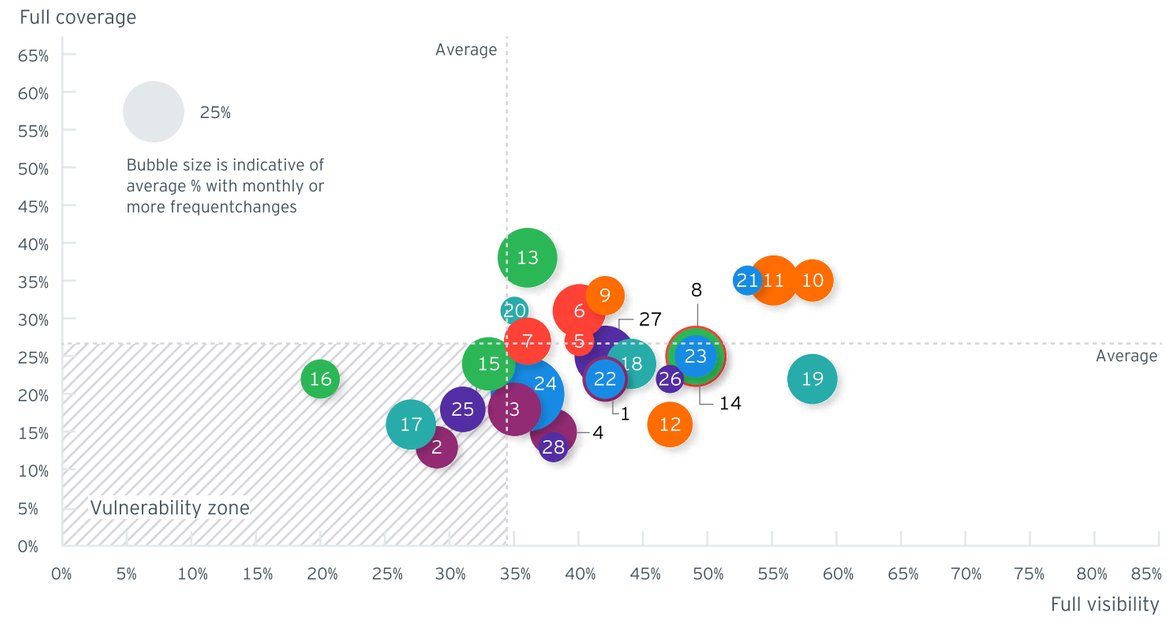
Insurance companies are scaling their digital infrastructure and embedding AI across the value chain — from customer service and claims to fraud detection and core decision-making.

Meanwhile they continue to rely heavily on cloud platforms, data providers and externally managed systems throughout their operations. That increases cybersecurity exposure across customer-facing channels, analytics environments and third-party connections. At the same time, frontier AI is making it easier to identify and quickly exploit vulnerabilities and maintain access through lateral movement and "living off the land" techniques. For insurers, the key challenge lies in securing the entire ecosystem (including distribution channels). Doing this while maintaining strong visibility and control alignment becomes increasingly difficult as AI enabled tools, APIs, and connected platforms evolve at a rapid pace and continuously reshape the attack surface.

Key sector insights from the study

- Eighteen percent of assets in the Insurance sector fall into the vulnerability zone.
- The sector's relative strength may reflect a more mature regulatory environment. However, it is concerning that fewer than half of respondents report complete visibility across critical digital assets, including AI systems, non AI digital assets and broader digital ecosystems. As insurers continue to scale their digital footprint – particularly through deeper AI integration, this lack of end to end visibility materially amplifies cyber vulnerability and risk exposure.
- Another potential point of concern is customer-facing AI, with only 29% of respondents saying they had full visibility over customer service AI assistants, and only 13% saying they had full cybersecurity controls over them.
- Accelerated pace of change may create new vulnerabilities for the sector. More than a quarter of respondents said APIs and cloud storage and managed databases undergo monthly or more frequent changes that require updates in cybersecurity controls. At the same time, over two thirds of respondents indicate that 20%–50% of their cybersecurity operations are outsourced – a reliance that is likely to increase as insurers seek to manage frequent changes across an expanding and increasingly cyber exposed infrastructure.

Vulnerability zone



AI systems and tools

1. Claims automation and fraud detection
2. **Customer service AI assistants**
3. Document intake and classification AI
4. Underwriting and pricing models

Cloud assets

5. Backup and disaster recovery in cloud
6. Cloud accounts and landing zones
7. Cloud compute platforms
8. Cloud storage and managed databases

Data assets

9. Claims files and supporting evidence
10. Customer identity and financial data
11. Payments and billing transaction data
12. Policy and contract records

Ecosystems

13. Brokers, agents, and distribution partners
14. Cloud, SaaS, and data center providers
15. **Data providers and reinsurers**
16. **Third-party claims partners and repair networks**

Network infrastructure

17. **Call center voice and contact networks**
18. Corporate and branch networks
19. Internet edge for portals and APIs
20. Remote access for staff and partners

Non-AI digital assets

21. Billing and payment systems
22. Claims management platform
23. Core policy administration system
24. Customer and agent portals, plus APIs

OT and physical assets

25. **Call center devices and workstations**
26. Data centers and server rooms
27. Employee laptops, mobiles, and VDI
28. Scanners and printers for documents

Asset in vulnerability zone

Sector impact

Life Sciences

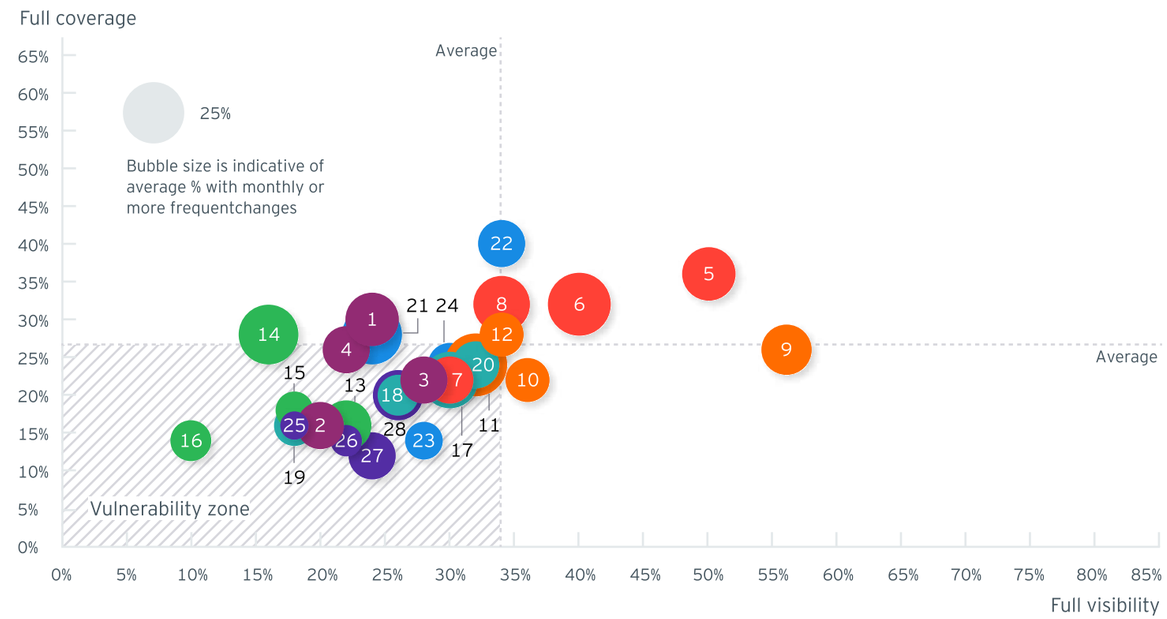
Life Sciences organizations are digitizing across research, clinical operations, manufacturing and laboratory environments while also investing heavily in AI to speed discovery and improve throughput.

That creates a wide attack surface across high-value data, connected operations and partner ecosystems. In a sector where intellectual property, regulated data and operational continuity are critical to enterprise resilience, assets in the vulnerability zone present opportunities for attackers to move from one connected environment to another once access is gained.

Key sector insights from the study

- Sixty-four percent of assets in the Life Sciences sector fall into the vulnerability zone.
- Asset categories in the vulnerability zone: AI systems and tools, non-AI digital assets, network infrastructure, OT and physical assets, and ecosystems.
- Fewer than 30% of respondents say they have visibility over any of the AI assets assessed, including AI for clinical trial matching and protocol design, AI for manufacturing process control and yield improvement, AI for drug discovery and target identification, and AI for lab automation and experiment optimization.
- Organizations report by far the most visibility over clinical trial participant data.

Vulnerability zone



AI systems and tools

1. AI for clinical trial matching and protocol design
2. AI for drug discovery and target identification
3. AI for lab automation and experiment optimization
4. AI for manufacturing process control and yield improvement

Cloud assets

5. Backup and disaster recovery storage
6. Cloud research compute for modeling and analytics
7. Cloud storage for experimental data and omics datasets
8. Data platforms for clinical, safety, and manufacturing analytics

Data assets

9. Clinical trial participant data and study documents
10. Genomics and biomarker datasets
11. Intellectual property such as formulas and compound libraries
12. Manufacturing batch records and quality data

Ecosystems

13. Cloud, SaaS, and data center providers
14. Contract manufacturing organizations and packaging partners
15. Logistics partners for cold chain shipping
16. Raw material and reagent suppliers

Network infrastructure

17. Corporate networks and remote access
18. Laboratory networks and instrument connectivity
19. Manufacturing and plant networks segmented from IT
20. Wireless networks used in labs and warehouses

Non-AI digital assets

21. APIs and integration platforms connecting labs, plants, and partners
22. Clinical trial management systems
23. Laboratory information management systems
24. Manufacturing execution systems and quality management systems

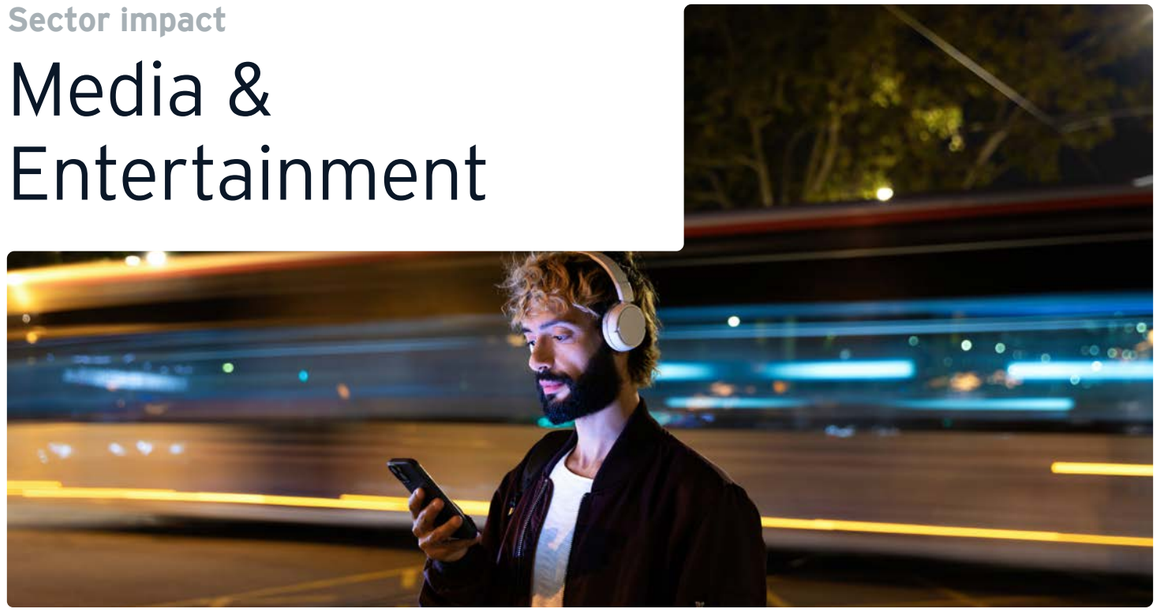
OT and physical assets

25. Bioreactors, cleanroom equipment, and manufacturing lines
26. Laboratory instruments and connected analyzers
27. On-premises servers supporting labs and plants
28. R&D labs and controlled-access facilities

Asset in vulnerability zone

Sector impact

Media & Entertainment



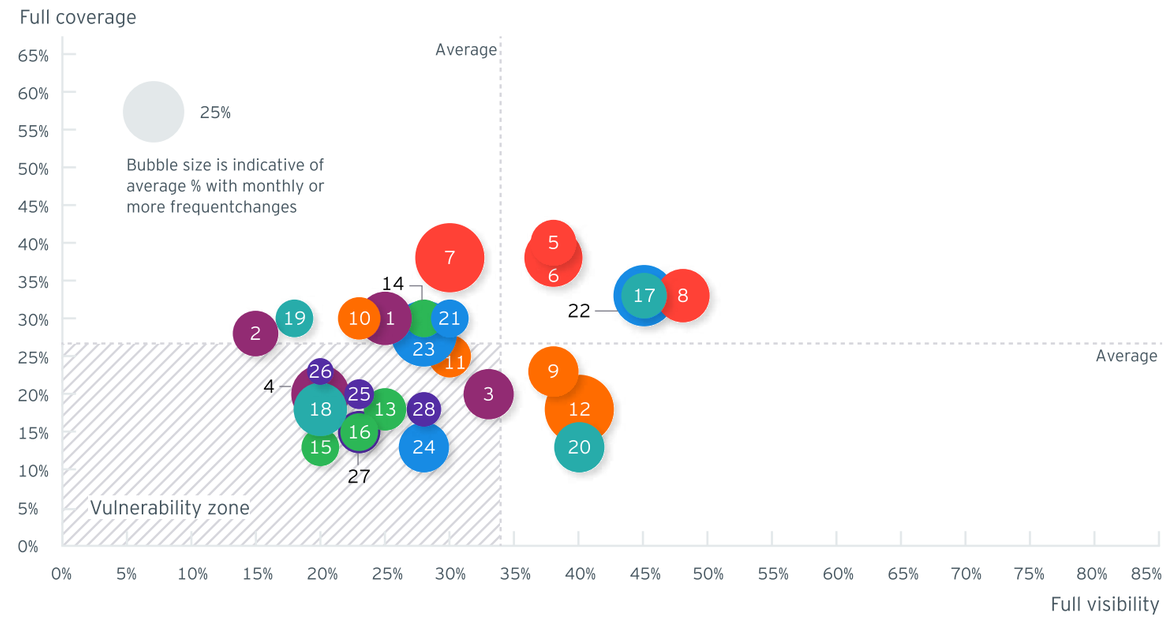
Media & Entertainment organizations are increasingly using AI to enhance content planning, forecasting and audience engagement.

At the same time, their operating ecosystem is becoming more interconnected, creating cybersecurity risks that can originate across agencies, adtech, distribution partners and content workflows, as well as in the organization's own platforms. As frontier AI improves the speed and quality of vulnerability discovery, it can shorten the path from a weak external platform or workflow tool to broader enterprise exposure, especially in environments where revenue, audience engagement and content delivery depend on a wide set of partners.

Key sector insights from the study

- Forty-three percent of assets in the Media & Entertainment sector fall into the vulnerability zone.
- Asset categories in the vulnerability zone: AI systems and tools, non-AI digital assets, network infrastructure, OT and physical assets, data assets, and ecosystems.
- Respondents report better visibility over traditional revenue-driving assets, with 45% saying they had full visibility over customer engagement platforms and 48% saying they had full visibility over content hosting and distribution platforms.
- Visibility is weaker for potential future revenue drivers, with only 25% of respondents saying they had full visibility over AI for content demand and audience forecasting, and 48% stating they have limited to no visibility on AI for crowd management, safety, and incident prediction.

Vulnerability zone



AI systems and tools

1. AI for content demand and audience forecasting
2. AI for crowd management, safety, and incident prediction
3. **AI for dynamic pricing, capacity, and yield optimization**
4. **AI for fraud detection and revenue-leakage**

Cloud assets

5. Business systems, backups, and recovery platforms
6. Cloud storage for content libraries and archives
7. Cloud-based advertising, customer data and analytics platforms
8. Content hosting and distribution platforms

Data assets

9. Final masters and distribution-ready content
10. Guest preferences, itineraries, and loyalty data
11. **Scripts, concepts, and original creative materials**
12. Subscriber, guest, and transaction records

Ecosystems

13. **Cloud, SaaS, and data center providers**
14. Distribution partners, streaming platforms, broadcasters
15. **Equipment suppliers, maintenance providers**
16. **Production partners, content owners, licensors**

Network infrastructure

17. Broadcast, streaming, and delivery networks
18. **Corporate office networks and remote access**
19. Edge and delivery networks for digital experiences
20. Payment and transactional networks

Non-AI digital assets

21. Content planning, scheduling, and rights-management platforms
22. Customer engagement platforms (web, mobile, connected-screen apps)
23. Public and private APIs
24. **Workforce, scheduling, and asset maintenance systems**

OT and physical assets

25. **Broadcast control rooms and transmission facilities**
26. **Cameras, recording devices, and creative equipment**
27. **Point-of-sale terminals and access scanners**
28. **Studios, sound stages, and production facilities**

Asset in vulnerability zone

Sector impact

Mining & Metals

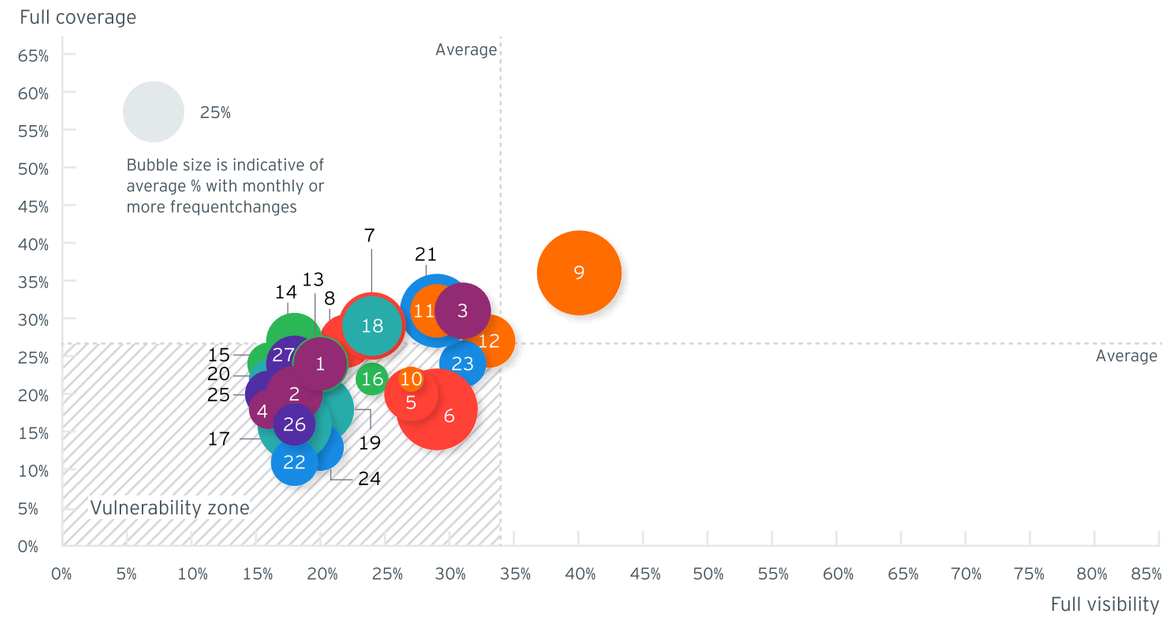
Mining & Metals organizations operate in environments where cybersecurity risk will increasingly reach into core production systems.

As operational technology becomes more connected and more dependent on software and network infrastructure, weak visibility and weak controls can create direct operational exposure. That risk is rising as frontier AI makes it easier for adversaries to find exploits in systems that were often designed or long assumed to be secure, which increases the importance of building monitoring and protection around the industrial assets that support production.

Key sector insights from the study

- Sixty-seven percent of assets in the Mining & Metals sector fall into the vulnerability zone.
- Asset categories in the vulnerability zone: AI systems and tools, non-AI digital assets, network infrastructure, physical assets, data assets and ecosystems.
- Industrial control systems are a major weak point, with only 18% of respondents saying they had full visibility over PLC and SCADA applications, and only 11% saying they had full cyber controls over them.
- OT network infrastructure shows a similar gap, with only 18% of respondents saying they had full visibility over it, and only 16% saying they had full cyber controls over it.

Vulnerability zone



AI systems and tools

1. AI for predictive maintenance of heavy equipment
2. AI for processing optimization in mills and flotation circuits
3. AI for safety monitoring such as gas and vibration detection
4. Autonomous haulage and drilling control algorithms

Cloud assets

5. Cloud hosed mine planning and geological databases
6. Cloud hosted data historians (mill)
7. Core cloud workloads and storage
8. SaaS platforms used by different teams (exploration, engineering)

Data assets

9. Employee Data
10. Geological models
11. Operational performance data
12. Other personal data (investors, partners,etc.)

Ecosystems

13. Cloud, SaaS, and data center providers
14. Logistics providers (rails, port, shipping platforms)
15. OEM digital platforms (equipment health, diagnostics)
16. Power/Utilities and grid operators

Network infrastructure

17. OT network infrastructure including routers, switches, and firewalls
18. Remote access to sites and equipment
19. Site-wide supervisory networks and control centers
20. Wireless networks supporting field operations

Non-AI digital assets

21. Fleet dispatch and production management systems
22. Industrial control systems such as PLC and SCADA applications
23. Maintenance and asset management systems
24. Public and private APIs

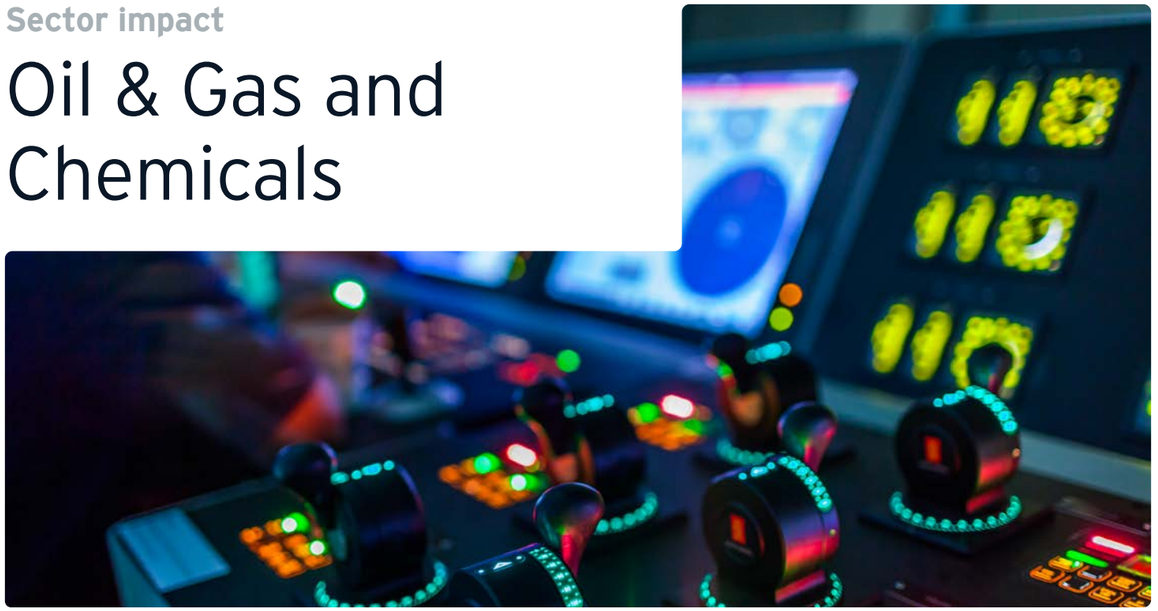
OT and physical assets

25. Autonomous and semi-autonomous mobile equipment
26. Fixed plant equipment (mills, crushers, conveyors)
27. PLCs, SCADA, DCS for processing facilities

Asset in vulnerability zone

Sector impact

Oil & Gas and Chemicals



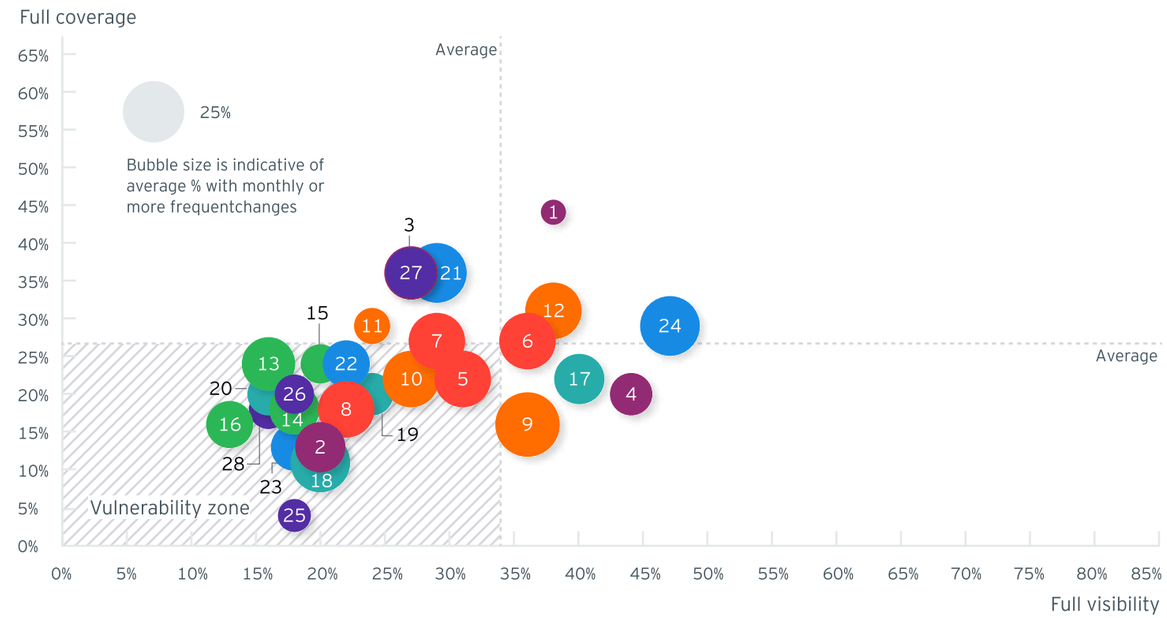
Oil & Gas and Chemicals companies manage cybersecurity risk across distributed field operations, control environments and large contractor and supplier networks.

As these environments become more connected, the consequences of weak visibility or poor controls rise quickly. Frontier AI adds to that risk by making it easier to identify exploitable weaknesses in control systems and supporting assets that were often built for availability and safety rather than persistent exposure to advanced cyber intrusion, which raises the importance of securing field and pipeline environments with the same rigor as the rest of the enterprise.

Key sector insights from the study

- Fifty-seven percent of assets in the Oil & Gas and Chemicals sector fall into the vulnerability zone.
- Asset categories in the vulnerability zone: Non-AI digital assets, network infrastructure, cloud assets, physical assets, data assets and ecosystems.
- SCADA and control applications for field and pipelines are a significant concern, with only 18% of respondents saying they had full visibility over them, and only 13% saying they had full cybersecurity controls over them.
- Industrial control hardware is potentially at risk, with only 18% of respondents saying they had full visibility over PLCs and safety systems, and only 4% saying they had full cybersecurity controls over them.

Vulnerability zone



AI systems and tools

1. AI for process optimization in refineries and plants
2. **AI for production optimization and well performance**
3. AI for seismic interpretation and subsurface modeling
4. AI for trading and scheduling optimization

Cloud assets

5. **Cloud analytics platforms for production and trading**
6. Cloud storage for seismic and engineering data
7. Cloud-hosted historians and data platforms
8. **Edge compute platforms connected to field sensors**

Data assets

9. Environmental monitoring and reporting data
10. **Pipeline pressure, flow, and integrity data**
11. Seismic data and geoscience models
12. Trading positions and scheduling data

Ecosystems

13. **Cloud, SaaS, and data center providers**
14. **Pipeline operators and interconnect partners**
15. **Shipping and terminal partners**
16. **Third-party maintenance and inspection vendors**

Network infrastructure

17. Industrial firewalls and segmentation controls
18. **OT networks segmented from corporate IT**
19. **Remote access for operators and vendors**
20. **Remote site connectivity including microwave and satellite links**

Non-AI digital assets

21. APIs and integration platforms connecting sites and partners
22. **Engineering and maintenance management systems**
23. **SCADA and control applications for field and pipelines**
24. Trading, scheduling, and revenue systems

OT and physical assets

25. **Industrial control hardware such as PLCs and safety systems**
26. **Pipelines, compressor stations, and pumping stations**
27. Refineries and processing plants
28. **Wells, rigs, and drilling control equipment**

Asset in vulnerability zone

Sector impact

Power & Utilities

Power & Utilities organizations face a cybersecurity environment shaped by a decentralizing value chain, increasingly connected operational assets, long-lived legacy infrastructure, and persistent geopolitical risk.

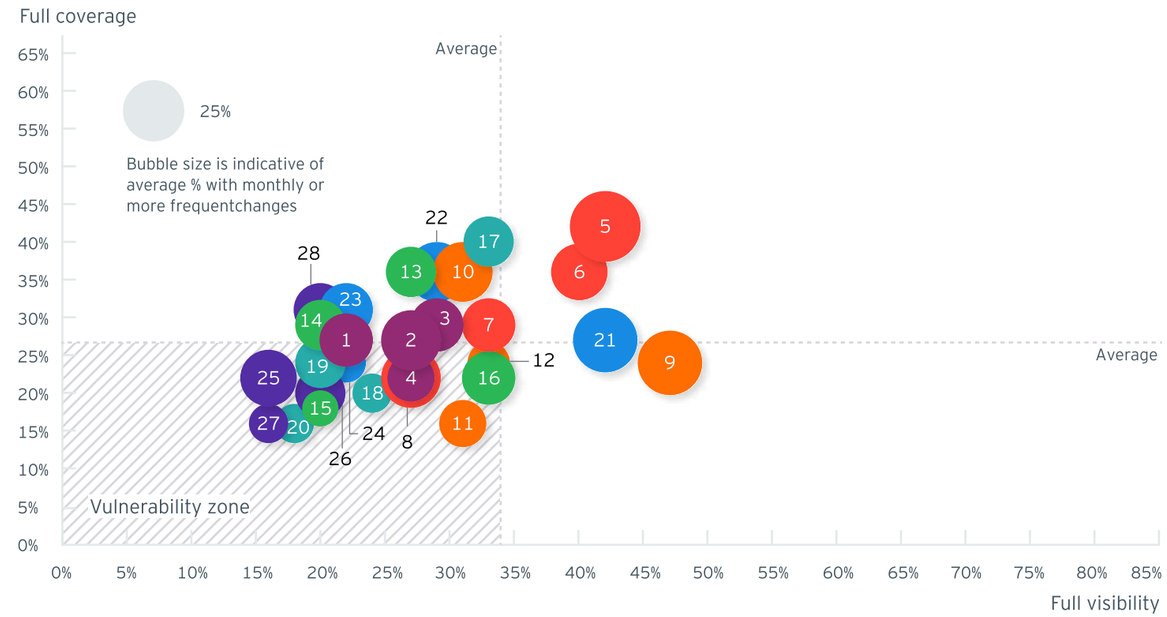
As grids shift from a small number of centralized power plants to a large ecosystem of distributed assets, the expanding cyber-attack surface creates new risks. A coordinated attack on the digital platforms, communications networks or virtual power plants that orchestrate distributed energy resources could be more destabilizing than the compromise of a single physical plant.

This is compounded by deeper IT-OT integration and limited visibility across operational environments. As state-backed actors continue to target critical infrastructure, frontier AI further strengthens the attacker side by making it easier to identify weaknesses in systems historically assumed to be secure because they were specialized, isolated or difficult to access. For utilities, the priority is shifting from protecting individual assets to building visibility, control and resilience across OT networks, edge devices, field communications and third-party ecosystems that increasingly underpin reliable energy delivery.

Key sector insights from the study

- Power & Utilities is one of the more exposed sectors. Seventy-one percent of respondents are classified as "Prone Enterprises" (the laggard group of respondents) and 46% of sector assets fall into the vulnerability zone, indicating broad exposure across the sector's asset base.
- The weakest points sit at the operational edge of the grid. Only 16% report full visibility over smart meters and field communications equipment, and only 16% report full cybersecurity coverage. Substation communications networks are similarly exposed, with 18% full visibility and 16% full coverage.
- OT visibility and control gaps create resilience risk. Only 20% have full visibility over OT networks for generation, transmission and distribution, while just 24% report full cybersecurity coverage, a critical gap as operational environments become more connected to enterprise systems, cloud platforms and AI-enabled tools.
- Cyber controls are not keeping pace with asset change. Only 4% can fully deploy required controls on a newly provisioned asset within 12 hours, while 78% take one to 30 days, a significant lag for a sector adding connected devices, distributed energy assets and third-party integrations.
- AI and geopolitics amplify an already exposed operating model. Eighty percent agree that geopolitical competition over AI technologies is increasing external cybersecurity risk, yet only 38% say they are well prepared for AI-enabled threats and only 29% for threats arising from geopolitics, reinforcing the need to treat cybersecurity resilience as part of grid reliability.

Vulnerability zone



AI systems and tools

1. AI for distributed energy resource optimization
2. AI for fraud and energy theft detection
3. AI for load forecasting and grid planning
4. **AI for predictive maintenance of grid assets**

Cloud assets

5. Backup and disaster recovery storage
6. Cloud analytics and data platforms for grid operations
7. Cloud-hosted customer experience platforms
8. **Integration platforms connecting OT, IT, and partners**

Data assets

9. Customer identity and account data
10. Grid topology and asset configuration data
11. **Outage records and restoration metrics**
12. **Relay settings and control system configurations**

Ecosystems

13. Cloud, SaaS, and data center providers
14. Distributed energy and charging partners
15. **Energy retailers and billing partners**
16. **Regulators and compliance reporting channels**

Network infrastructure

17. Backbone connectivity between control centers and sites
18. **Network segmentation and industrial firewalls**
19. **OT networks for generation, transmission, and distribution**
20. **Substation communications networks**

Non-AI digital assets

21. Customer portals, billing, and payment systems
22. Outage management systems
23. Public and private APIs
24. **SCADA systems and control center applications**

OT and physical assets

25. **Distributed energy resources such as solar and storage**
26. **Protective relays and control devices**
27. **Smart meters and field communications equipment**
28. Substations, transformers, and switchgear

Asset in vulnerability zone

Sector impact

Retail

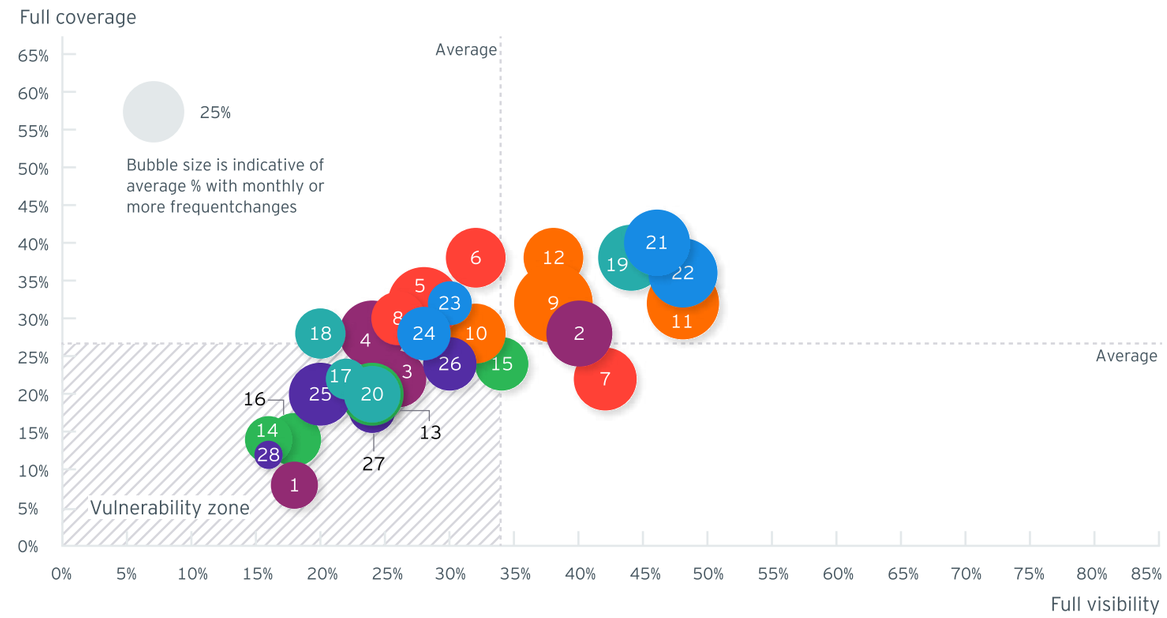
Retail organizations are expanding their use of AI across customer engagement, merchandising and operations while continuing to depend heavily on third parties across payments, fulfillment, logistics and digital marketing.

That combination creates more externally connected systems while attackers are getting better at finding weaknesses in software and digital workflows. In retail, cybersecurity resilience increasingly depends on how well organizations manage the links between core commerce platforms, payment environments and third-party systems that can provide a foothold for fast exploitation or lateral movement into day-to-day operations.

Key sector insights from the study

- Forty-three percent of assets in the Retail sector fall into the vulnerability zone.
- AI systems and tools, OT and physical assets, and ecosystems are more likely to fall in the vulnerability zone.
- Survey respondents report stronger visibility over assets most central to customer interactions and revenue, including ecommerce platforms, digital payment processing infrastructure and payment and transaction data. Yet, material gaps between visibility and coverage remain, heightening both operational exposure and the risk of reputational damage. Given retail's complex ecosystem, third-party exposure is a weak point, with only 18% of respondents saying they had visibility over third-party vendor systems.

Vulnerability zone



AI systems and tools

1. AI-enabled visual recognition and automated loss prevention tools
2. Customer personalization and promotion engines
3. Intelligent inventory, logistics and supply chain platforms
4. Retail media networks and data monetization solutions

Cloud assets

5. Cloud-based customer data platforms (CDPs)
6. Cloud-based inventory and order management systems
7. Cloud-hosted e-commerce platforms
8. Retail analytics and business intelligence dashboards

Data assets

9. Customer data (especially through loyalty)
10. Internal sales and pricing strategy data
11. Payment and transaction data
12. Supplier and vendor contracts

Ecosystems

13. Cloud, SaaS, and data center providers
14. Franchisee and concession partner network
15. Marketplace, delivery, and payment partners
16. Third-party vendor and supplier systems

Network infrastructure

17. Instore and warehousing IoT infrastructure
18. In-store Wi-Fi networks
19. Retail data centers
20. VPNs and remote access systems for remote connectivity

Non-AI digital assets

21. Digital payment processing infrastructure
22. E-commerce platforms and websites
23. Point-of-sale (POS) systems
24. Public and private APIs

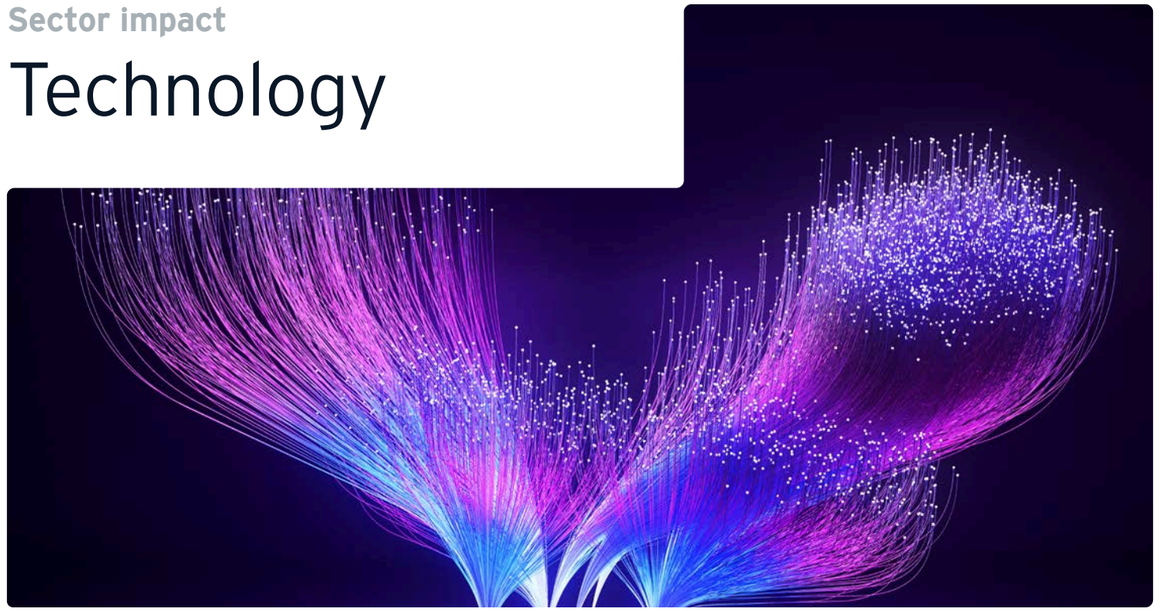
OT and physical assets

25. Autonomous vehicles and warehouse robotics
26. Digital signage and interactive displays
27. Employee handheld devices and scanners
28. RFID-enabled fixtures such as smart shelves or products

Asset in vulnerability zone

Sector impact

Technology



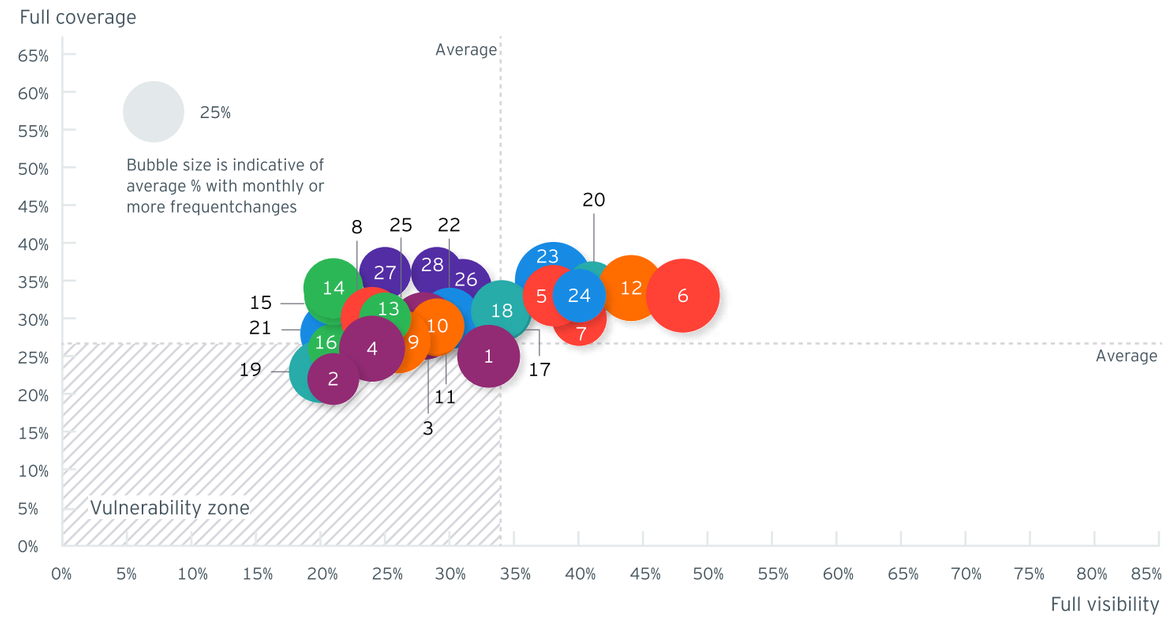
As Technology organizations roll out AI across products, internal tools and customer experiences, they are potentially exposing more software, APIs and data flows to cyber risk.

Recent advances in frontier AI have shown that attackers can identify weaknesses and develop exploits faster than before, which raises the importance of knowing where AI is deployed and what data it touches. That pressure is amplified by reliance on software dependencies, cloud platforms and embedded third-party services, which expands the number of paths into the enterprise and makes it harder to keep controls aligned with how products and services are changing.

Key sector insights from the study

- Eighteen percent of assets in the Technology sector fall into the vulnerability zone.
- Nearly half of tech organizations report US$100 million+ annual cybersecurity spend (vs. 31% in other sectors). Most notably, tech organizations allocate 20% of their overall cybersecurity budget to AI, compared with 14% elsewhere.
- The visibility paradox: while 45% of tech respondents say they have complete visibility over 91%–100% of assets (vs. only 6% of other sectors), the picture changes when looking at asset categories. In particular ecosystems (22%), AI systems and tools (26%), and OT and physical assets (28%), have low visibility. Given how tech companies go to market through ecosystems, this presents opportunities for increased controls for supplier monitoring, third-party access governance, data center and cloud provider risk management, and ecosystem resilience.
- As it stands today, AI systems and tools are the most likely assets for tech organizations to fall in the vulnerability zone.
- Eighty-three percent of tech respondents believe quantum-enabled cyber threats become a real risk within the next five years. While select tech companies indicate they are prepared, now is the time to start having board and CISO-level discussions.

Vulnerability zone



AI systems and tools

1. AI API gateways and access keys
2. AI model training workflows
3. Customer-facing AI features
4. Retrieval systems that connect AI models to internal data sources

Cloud assets

5. Backup and disaster recovery storage
6. Cloud accounts, subscriptions and organizational structures
7. Cloud storage and managed databases
8. Container platforms and serverless services

Data assets

9. AI training and evaluation datasets
10. Customer data stored within products
11. Product plans, intellectual property and contracts
12. Source code and software release artifacts

Ecosystems

13. Certificate authorities and external trust providers
14. Cloud, SaaS and data center providers
15. Customer-managed or hybrid deployments
16. Hardware and appliance partners

Network infrastructure

17. Core network services such as DNS and time synchronization
18. Internal network segmentation controls
19. Network connections to partners and subsidiaries
20. Secure remote access platforms

Non-AI digital assets

21. Customer support platforms
22. Licensing, usage tracking and billing systems
23. Public and private APIs and developer portals
24. Source code repositories and internal documentation systems

Physical assets

25. Corporate offices and engineering labs
26. Hardware used for cryptographic key protection
27. Media storage and secure disposal systems
28. On-premises servers and co-location equipment

Asset in vulnerability zone

Sector impact

Telecommunications

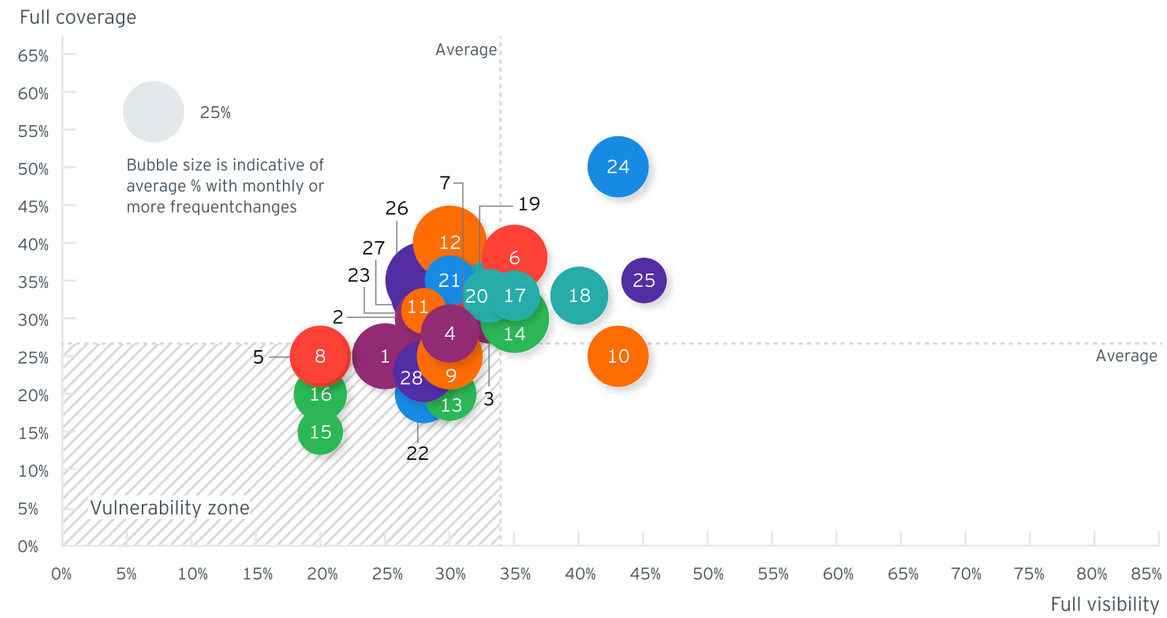
Telecommunications organizations are managing cybersecurity risk across large, connected networks, customer-facing applications and supplier ecosystems.

That exposure is becoming more important as frontier AI lowers the effort needed to find and exploit weaknesses, while state-backed actors continue to target communications infrastructure for espionage and potential disruption. For telecom companies, this raises the value of strong visibility not only across core network assets but also across customer channels and third-party relationships, because weaknesses in those environments can give attackers a starting point for lateral movement that is difficult to detect and slow to contain.

Key sector insights from the study

- Thirty-two percent of assets in the Telecommunications sector fall into the vulnerability zone.
- Respondents have the strongest visibility and coverage over assets most central to network operations, including cell sites, towers, radios and antennas, and public and private APIs. On the other hand, ecosystem assets are most likely to fall into the vulnerability zone.
- Many customer-facing assets face cybersecurity issues, with only 28% of respondents saying they had full visibility over web and mobile account applications, and only 20% saying they had full cybersecurity coverage over them.
- Customer modems and routers are also a concern, with only 28% of respondents saying they had full visibility over them, and only 35% saying they had full cybersecurity coverage over them.

Vulnerability zone



AI systems and tools

1. **Churn prediction and customer personalization models**
2. Fraud detection systems for subscriptions and SIM usage
3. Predictive maintenance systems for physical infrastructure
4. Revenue assurance and billing anomaly detection systems

Cloud assets

5. **Centralized network and usage data platforms**
6. Key and certificate storage systems
7. Private cloud platforms running network services
8. **Public cloud services supporting analytics and applications**

Data assets

9. **Authentication keys and signaling credentials**
10. Customer support recordings and transcripts
11. Network configuration and routing data
12. Subscriber identity and account data

Ecosystems

13. **Cloud, SaaS, and data center providers**
14. Content delivery and streaming partners
15. **Device manufacturers and retail partners**
16. **Payment, identity, and fraud service providers**

Network infrastructure

17. Backbone and internet transit networks
18. Core network systems for voice and data services
19. Radio access network components
20. Signaling and interconnection networks

Non-AI digital assets

21. Customer billing, charging, and payment platforms
22. **Customer web and mobile account applications**
23. Operations and billing support systems
24. Public and private APIs

OT and physical assets

25. Cell sites, towers, radios, and antennas
26. Customer premises equipment such as modems and routers
27. Fiber networks and cable infrastructure
28. **SIM and eSIM provisioning equipment**

Asset in vulnerability zone

Sector impact

Wealth & Asset Management

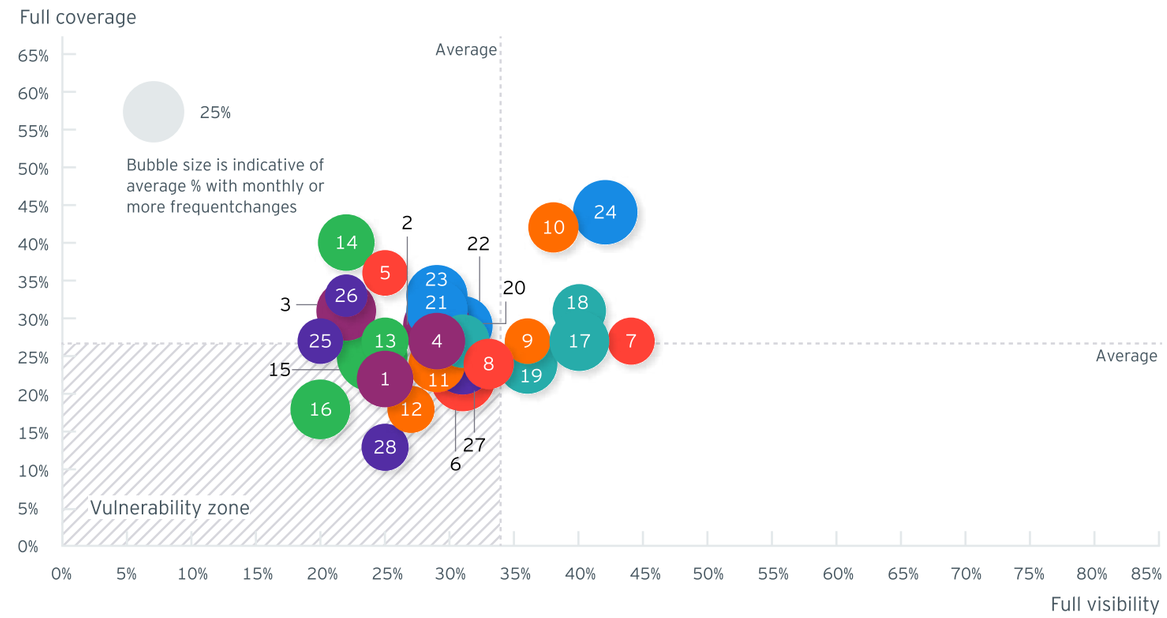
The Wealth & Asset Management operating model depends heavily on external providers across cloud, SaaS, research, market data and outsourced back-office services.

As AI expands into client service and internal workflows, the challenge shifts toward understanding a broad service ecosystem that may have access to sensitive data or connected processes, especially because faster vulnerability discovery can shorten the path from a weak external provider to lateral movement into core workflows and client-facing services.

Key sector insights from the study

- Thirty-two percent of assets in the Wealth & Asset Management sector fall into the vulnerability zone.
- A notable concern sits in ecosystems, with fewer than a quarter of respondents saying they had visibility over cloud, SaaS and data center providers, research providers, or outsourced back-office providers. This could become more significant where those providers have network access or support critical workflows.

Vulnerability zone



AI systems and tools

1. Advisor copilots; research summarization; meeting note assistants
2. AI for portfolio optimization and rebalancing
3. MLOps: model registries; shared feature stores across desks/teams
4. RAG over research & client correspondence (MNPI leakage risk)

Cloud assets

5. CI/CD pipelines for quant and client-facing code
6. Cloud compute platforms for services and APIs
7. Cloud data lakes and warehouses for analytics
8. Cloud storage buckets for reports and statements

Data assets

9. Communications archives for regulatory retention
10. Credentials and secrets for brokers and data vendors
11. Holdings, transactions, and client statements
12. Material non-public information and restricted lists

Ecosystems

13. Cloud, SaaS, and data center providers
14. Outsourced middle and back office providers
15. Prime brokers, executing brokers, and trading venues
16. Research providers and alternative data suppliers

Network infrastructure

17. Client portal perimeter controls such as WAF and DDoS
18. Low-latency trading networks and market connectivity
19. Network segmentation between research, trading, and operations
20. Remote access for advisors and secure jump hosts

Non-AI digital assets

21. Order and execution management systems
22. Portfolio accounting and performance reporting systems
23. Public and private APIs
24. Trading platforms and algorithmic trading engines

OT and physical assets

25. Local NAS/team shared storage devices (often unmanaged)
26. Mobile devices used by relationship managers
27. Secure rooms and hardware used for key protection
28. Thin clients and virtual desktop endpoints

Asset in vulnerability zone

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2026 EYGM Limited.
All Rights Reserved.

SCORE 112326-26-GBL
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/cybersecurity

Authors

Richard Watson
EY Global Consulting Cybersecurity Leader

Richard Bergman
EY Global Cybersecurity Transformation Leader

Piotr Ciepiela, Maez De Guzman, Ganesh Devarajan, Scott McCowan, AnnMarie Pino, William Reid, and Joe Morecroft contributed to this article.