
accenture
State of Cybersecurity Resilience 2025
Elevate your cybersecurity to fit an AI-driven world

Authors

Paolo Dal Cin
Global Lead
Accenture Security

With over 27,000 professionals under his leadership, Paolo heads Accenture Security globally. He has 25+ years of experience in cybersecurity, business resilience and complex international cybersecurity projects.

Daniel Kendzior
Global Data and AI Lead
Accenture Security

Daniel specializes in cybersecurity strategy and architecture, working with C-suites and boards to guide them through executing large-scale information security transformations as well as managing evolving enterprise risks.

Yusof Seedat
Global Research Lead
Accenture Security

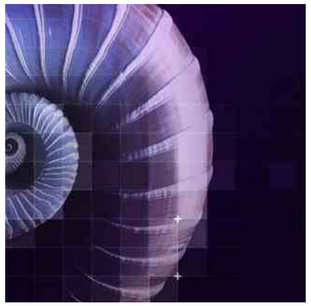
Yusof leads cybersecurity research with a focus on shaping data-driven thought leadership to help guide strategic decision making and market positioning for organizations globally.

AI is moving faster than security—most organizations don’t even realize how exposed they are.

Just **36%** of technology leaders say generative AI is outpacing their security,

yet **90%** lack the maturity to defend against modern, AI-driven threats.

Contents



Executive summary

Cyber threats are evolving faster than enterprise defenses can adapt—and generative AI is widening the gap.

With unprecedented speed and scale, AI is enabling attackers to bypass legacy systems and overwhelm security teams. Traditional defenses are no longer sufficient. Our *State of Cybersecurity 2025* research shows just 36% of technology leaders acknowledge that AI is outpacing their security capabilities—yet a staggering 90% of companies lack the maturity to counter today's AI-enabled threats.

This is not merely a technical issue; it is a strategic risk. The cyber threat landscape is being reshaped not only by technology, but by geopolitics. Heightened global tensions, changing trade dynamics and shifting regulations are compounding cyber exposure. As companies respond by adjusting supply chains and data strategies, many are unknowingly introducing new cyber risks—especially when security assessment, compliance and risk protocols fail to keep pace.

We surveyed 2,286 security and technology executives—80% CISOs, 20% CIOs—from $1 billion-plus enterprises across 24 industries and 17 countries. Their insights offer a sobering view of the current state of cybersecurity—and a clear call to action for what must come next (see "About the research" on page 39 for more on the security posture maturity methodology).

Our research reveals that 77% of organizations lack the foundational data and AI security practices needed to safeguard critical models, data pipelines and cloud infrastructure[1]. These are not just vulnerabilities—they are systemic blind spots that leave enterprises fundamentally unprepared to defend against modern, AI-driven threats.

While AI adoption races ahead, security is playing catch-up. Speed and innovation continue to eclipse safety, with less than half (42%) of organizations striking a balance between AI development and security investment[2]. Just 28% of organizations embed security into transformation initiatives from the outset—forcing many to scramble to retrofit defenses later, often under duress[3]. This reactive approach places growing pressure on already stretched security teams.

Only 34%

of organizations have a mature cyber strategy. Fewer still—just 13%—possess the advanced cyber capabilities needed to defend against modern, AI-driven threats.

The challenge is compounded by a persistent talent shortage: 83% of executives cite workforce limitations as a major barrier to sustaining a secure posture[4].

Drawing on rigorous research, our work with leading organizations and in-depth interviews with security executives worldwide, we assess the scope of organizations' rapidly evolving cybersecurity challenges in this report. Our analysis identifies three security maturity zones that most companies need to address across two dimensions: *cyber strategy maturity*—how effectively organizations design and implement cyber risk strategies—and *cyber capability*—the technical depth required to build cyber resilience and secure increasingly complex, cyber-physical systems.

The findings are sobering. Only 34% of organizations have a mature cyber strategy. Fewer still—just 13%—possess the advanced cyber capabilities needed to defend against modern, AI-driven threats[5]. The vast majority remain exposed, underprepared and at risk of falling behind as AI-powered threats accelerate.

But there's a path to safety, a high ground we call the Reinvention-Ready Zone. Only 10% of companies have reached this level[6]. These companies demonstrate maturity in both strategy and capability with a proactive, adaptive and resilient security posture that continuously evolves to counter emerging threats. The payoff? Compared to those in the most vulnerable zone, which we refer to as the Exposed Zone, this group of companies are 69% less likely to be hit by an advanced attack such as AI-powered cyberattack[7]. They also see 1.6 times higher returns on their AI investments and reduce technical debt by 1.7 times—fueling faster, more secure innovation[8]. These companies report building stronger customer trust, 1.6 times more than those in the Exposed zone, a critical factor in sustaining long-term business success[9].

Our economic modeling of security outcomes reveals that a 10% increase in security investment, strategically directed toward Reinvention-Ready Zone practices, can enable organizations to detect, contain and remediate cyber threats 14% faster[10].

We recommend four decisive actions for companies to achieve Reinvention-Ready Zone status. These actions not only protect AI investments but also leverage AI to enhance cybersecurity defenses and resilience.

01 Develop and deploy a fit-for-purpose security governance framework and operating model accounting for the realities of an AI-disrupted world.

Establish clear accountability and align AI security with regulatory and business objectives. With 72% of organizations reporting increased cyber threats and 63% citing an evolving threat landscape as their biggest challenge[11], AI security cannot remain fragmented or siloed—it must be embedded into governance structures and elevated to a board-level priority to ensure sustained investment and leadership buy-in.

02 Design the digital core to be generative AI-secure from the outset.

AI must be developed, deployed and operated with security integrated at every stage, yet only 37% of organizations assess AI security before deployment, despite 66% recognizing AI's transformative impact on cybersecurity in the coming year[12].

03 Maintain resilient AI systems with secure foundations and proactive threat management.

Emerging AI-based cyberattacks—including AI worms like Morris II—can embed malicious prompts into AI models, allowing attackers to hijack AI systems and compromise sensitive data. Without continuous monitoring, independent third-party testing of AI models and solutions, robust third-party risk management and AI-specific threat intelligence, organizations will remain vulnerable to data poisoning, model manipulation and adversarial AI attacks.

04 Reinvent cybersecurity with generative AI to scale security capabilities, strengthen cyber defenses and detect threats earlier.

With an estimated 4.8 million cybersecurity positions unfilled worldwide[13], AI presents an opportunity to bridge the cybersecurity talent gap by amplifying security professionals. AI-powered security solutions analyze massive datasets, detect anomalies and help predict attacks earlier than traditional methods. Our research shows that 71% of security analyst tasks can be amplified using generative AI, significantly improving efficiency, reducing detection time and enabling faster remediation of cyber threats[14].

The message is clear: act now.

Organizations that bake security into their AI-powered transformations will not only survive but thrive, gaining a crucial competitive edge, cementing customer loyalty and building unshakable resilience. Ascending to the Reinvention-Ready Zone—where robust security is deeply embedded in both strategy and capability—requires focused effort, strategic investment and leadership from the top down. This report provides the essential roadmap, empowering organizations to close the cybersecurity maturity gap and confidently navigate the future of AI-driven innovation.

Cyber threats are escalating

Cyber threats that have dominated the landscape over the last few years have not only persisted but have intensified, becoming more sophisticated, relentless and rapid.

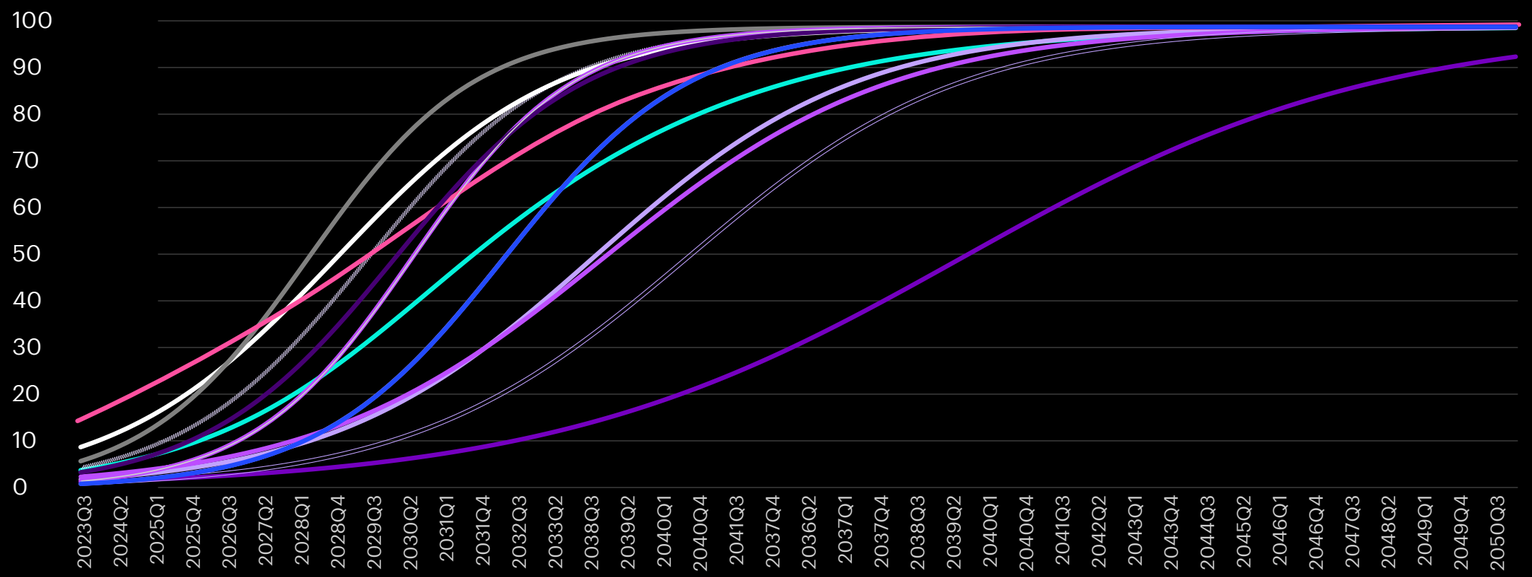
Executives recognize this escalating risk; 72% report a rise in cyber threats. The top 5 risks they rank as most concerning are ransomware, cyber-enabled fraud, supply chain attacks, malicious insiders and disinformation[15]. These threats are growing in complexity, exploiting security gaps and placing immense pressure on organizations to strengthen their defenses before they become victim to attacks. In the third quarter of 2024 alone, organizations faced an average of 1,876 cyberattacks, reflecting a 75% year-over-year increase[16]. This increase is more than a trend. It shows that attackers are using advanced technologies to target weaknesses faster than organizations can protect them.

Current geopolitical tensions are accelerating this risk further. Tariffs, trade restrictions and international instability are forcing organizations to reconfigure global supply chains—changes that often happen without fully accounting for cybersecurity impacts. Each adjustment introduces new third-party vendors, alters data access practices and potentially shifts regulatory obligations, increasing exposure to both known and emerging threats. Cybercriminals exploit these moments of operational change, using them as cover to target weak links, especially where security posture assessments and threat intelligence have not kept pace.

The AI revolution is escalating this challenge. The rise of generative AI is reshaping industries, unlocking unprecedented efficiency and innovation. However, it is also amplifying cyber risks in ways that many organizations are unprepared for.

Figure 1: Estimated AI adoption

Our economic analysis projects 80% industry-wide growth in AI adoption over the next decade.



	Education	Professional Services	Information (includes Data, Systems, Software)	Financial Services	Wholesale Trade	Health	Total	Construction	Retail	Manufacturing	Accommodation	Transportation
In 5 years, AI adoption will reach:	64.3%	54.6%	48.6%	47.1%	33.6%	40.1%	30%	16.9%	15.3%	14.2%	8.3%	5.1%
AI adoption will reach 50% by:	2027Q4	2028Q2	2029Q1	2029Q2	2029Q4	2029Q3	2031Q1	2031Q3	2033Q3	2033Q2	2035Q1	2040Q2

Accenture's Pulse of Change Index—based on key business indicators—measures change across six areas: Technology, Talent, Economic, Geopolitical, Climate and Consumer & Social. It shows that technology change rose by 37% in 2024 compared to 2023. This is mostly because of the fast growth of generative AI applications. Executives are recognizing its value; 83% acknowledge greater business potential for generative AI based on their past years' experience, and 86% plan to increase AI investments in 2025[17]. This momentum signals an accelerating shift—AI adoption is not just expanding but becoming a cornerstone of business strategy. Our economic analysis projects even stronger industry-wide growth over the next decade (Figure 1).

Only 20%

of organizations express confidence in their ability to secure their generative AI models against cyber risks.

Despite its promise, security risks tied to AI adoption are becoming more evident. Over half of technology leaders express concern over the rise in cyber threats due to widespread AI accessibility. One in three executives report AI is amplifying existing attack vectors, making detection significantly more challenging while also being directly leveraged in cyberattacks[18]. One such example is Morris II, an AI worm developed by researchers from Cornell Tech, the Israel Institute of Technology and Intuit. The worm tricks models like ChatGPT and Gemini into generating malicious prompts, which can then be used to extract sensitive data from emails and even send spam through compromised AI assistants.

Morris II is particularly concerning because it demonstrates how adversarial self-replicating prompts can embed themselves into text and image files, manipulating AI systems without human intervention[19]. This raises alarm over the ability of attackers to hijack AI models and use them for persistent cyber threats.

Deepfake technology in particular presents an acute and growing challenge. AI-generated forgeries can convincingly mimic voices, videos and text, making it nearly impossible to distinguish real from fake. These threats extend beyond cybersecurity, jeopardizing operational integrity and amplifying risk across the entire institution. A sophisticated scam using AI-generated voice technology impersonated Italy's Defence Minister Guido Crosetto to defraud high-profile business figures, including Giorgio Armani and members of the Beretta and Menarini families. Scammers, posing as Crosetto and his staff, made phone calls requesting around €1 million to be wired to a Hong Kong bank account, claiming the funds were needed to rescue kidnapped Italian journalists.

One entrepreneur transferred a large sum after speaking with a fake "General Giovanni Montalbano," believing he was assisting a government operation. The fraud was uncovered when a businessman contacted Crosetto to verify the request, prompting the minister to alert authorities and publicly warn others[20]. This attack highlights how AI-generated deepfakes are becoming an increasingly effective tool for cyber-enabled fraud, enabling large-scale financial deception that bypasses traditional security measures.

Concerns over AI-driven vulnerabilities extend even further—50% of executives worry that large language models (LLMs) expose sensitive data, and 57% fear that threat actors could manipulate training data to compromise AI model integrity. Despite these growing threats, only 20% of organizations express confidence in their ability to secure their generative AI models against cyber risks, underscoring the urgent need for stronger AI security measures[21].

The Security Maturity Gap: Most organizations lack the strategy and capabilities to withstand modern threats

Our research reveals a sobering truth: a minority (36%) of tech leaders admit generative AI's rapid rollout is outpacing their ability to integrate security measures[22]; yet 90% lack the security maturity needed to combat modern threats[23].

Additionally many organizations lack the foundational elements necessary to improve their security posture. For instance, 84% struggle to develop and operationalize cyber risk strategies that align with their transformation goals[24].

Furthermore, 92% of organizations struggle with essential resilience-building efforts, such as pressure-testing defenses, understanding emerging threats and establishing rapid response mechanisms. Even implementing Zero Trust, a fundamental security framework, poses a significant challenge for 88% of organizations. This vulnerability extends to the physical world, with 80% unable to effectively protect their cyber-physical systems[25].

A concerning 77% of organizations lag in adopting essential Data & AI security practices[26]. Only 22% have implemented clear policies and training for generative AI use, and a handful maintain a comprehensive inventory of AI systems, crucial for managing supply chain risks. Additionally, data protection remains inadequate—only 25% of organizations fully leverage encryption methods and access controls to safeguard sensitive information in transit, at rest and during processing[27].

Security gaps extend into cloud infrastructure as well. Despite AI's reliance on cloud-based processing, 83% of organizations have not established a secure cloud foundation with integrated monitoring, detection and response capabilities[28].

Only 10%

of organizations occupy the coveted Reinvention-Ready Zone, demonstrating both robust security capabilities and integrated cyber strategy.

To better understand security readiness, we've identified three distinct security posture maturity zones (Figure 2. Also see "About the research" for methodology details), assessed across two critical dimensions: cyber strategy—the ability to design and execute risk strategies—and cyber capability—the technical proficiency to apply Zero Trust, enhance resilience and secure cyber-physical systems at scale.

The results are stark. Only 10% occupy the coveted Reinvention-Ready Zone, demonstrating both robust security capabilities and integrated cyber strategy.

Around 27% fall into the Progressing Zone—showing cybersecurity strong on strategy but lacking in implementation (24%) or strong on protection but lacking strategic alignment (3%). And the vast majority, a worrying 63%, languish in the Exposed Zone, lacking both strategy and capability, making them prime targets for cyber threats. Looking at the strategy and capability dimensions separately, 34% of organizations demonstrate a strong cyber strategy through intensified practices, and just 13% possess the robust protection and resilience needed to truly weather the storm[29].

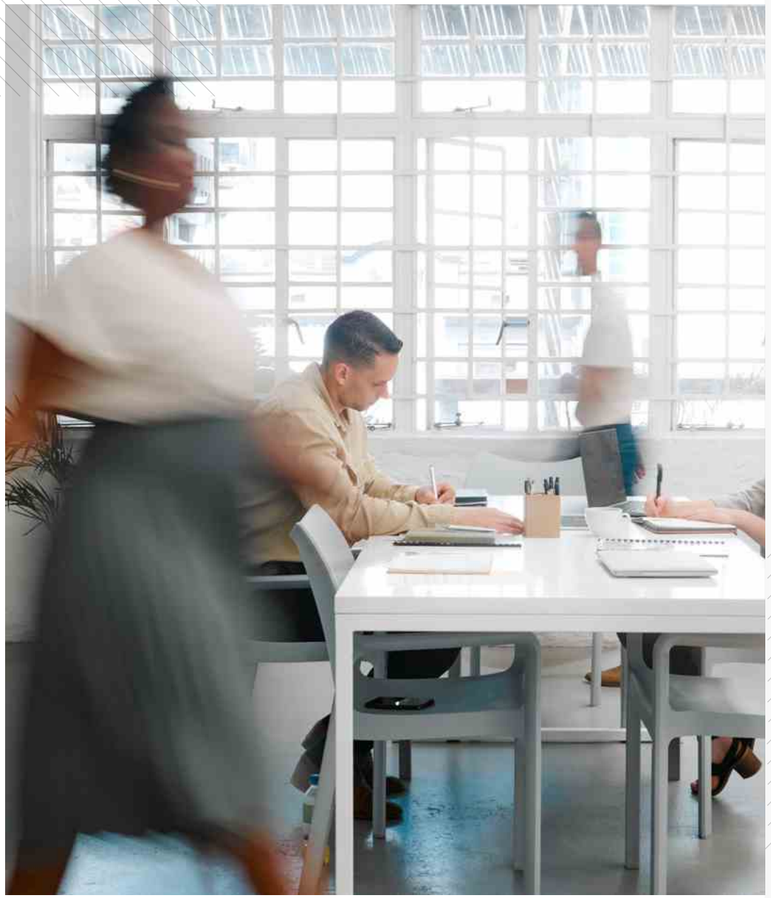
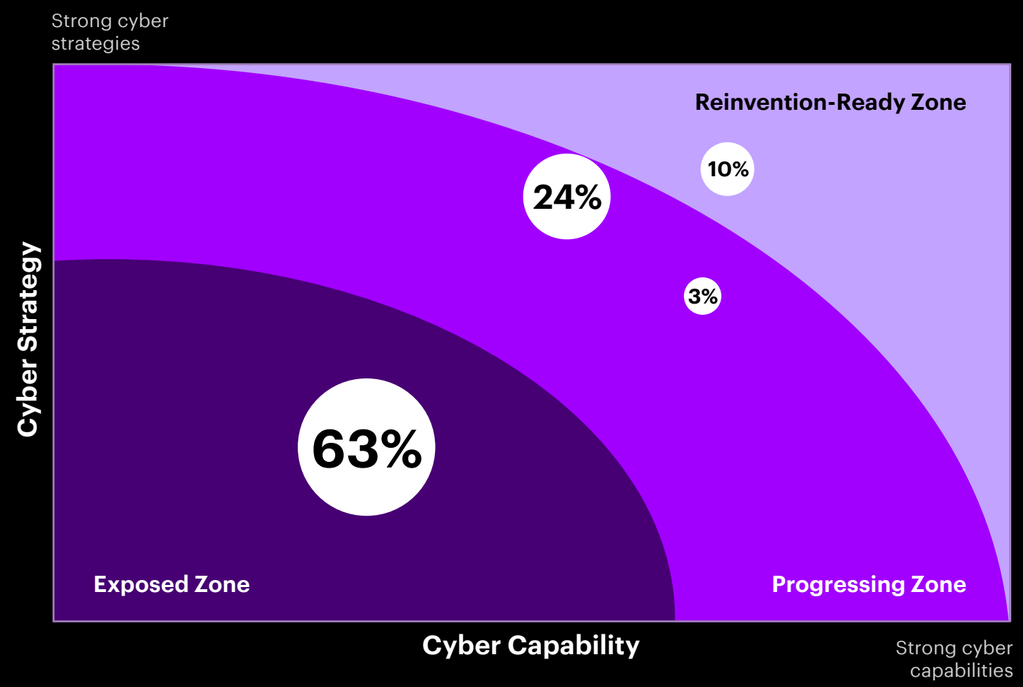


Figure 2: Security Posture Maturity:
Moving from Exposed to Reinvention-Ready Zone
Only 10% of companies achieve both strong security and strategy, while 34% focus on strategy and just 13% have true cyber resilience.



Reinvention-Ready Zone

Organizations in this zone lead in cybersecurity, mastering cyber protection, resilience and cyber-physical security while designing and operationalizing risk strategies to secure transformations and build customer trust. Their adaptive, resilient security posture continuously evolves to counter emerging threats.

Progressing Zone

Organizations in this zone show cybersecurity strengths but face challenges in either defining a strategic direction or implementing security defenses effectively. Some excel in technical defenses, i.e. they demonstrate strength in cyber protection, resilience and cyber-physical, but take a fragmented, reactive approach due to a lack of strategic vision. Others have a clear cybersecurity strategy but fall short in execution, limiting their ability to turn vision into impact. While they may be strong in either cyber protection or strategy, they lack the full capability to design and operationalize cyber risk strategies effectively.

Exposed Zone

The most vulnerable category, where organizations lack both a cohesive cyber strategy and the necessary capabilities, leaving them open to significant risk. They fall short in cyber protection, resilience and cyber-physical security and lack the ability to design and operationalize cyber risk strategies to secure transformations and build customer trust.

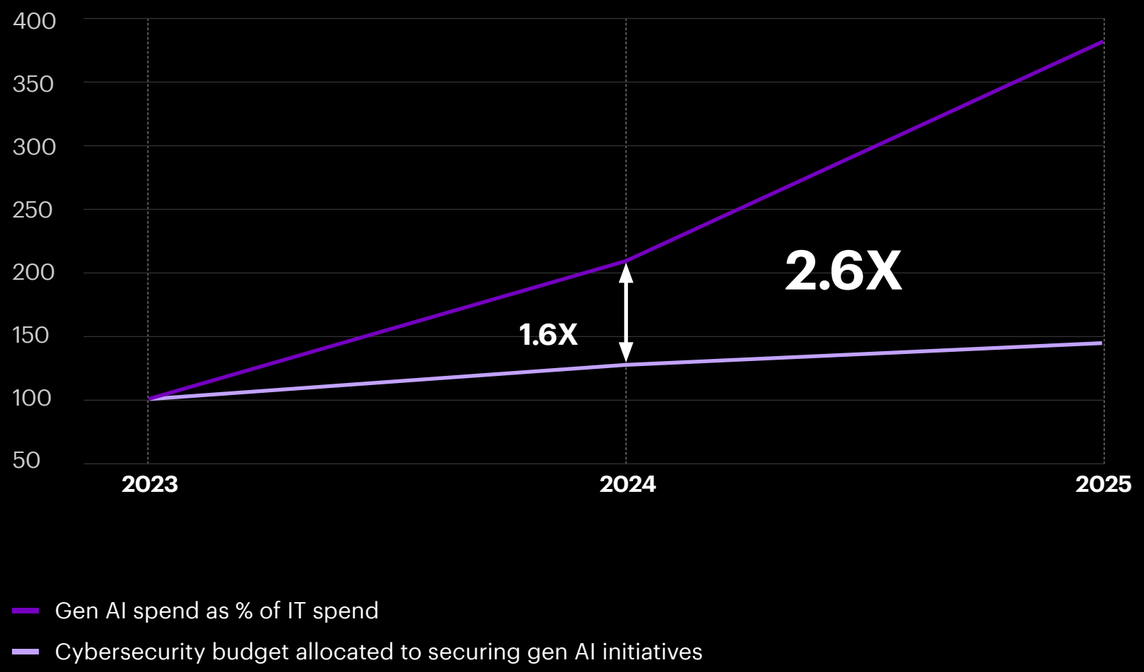
The race to AI adoption, coupled with talent shortages, is outpacing security

The rapid adoption of AI, coupled with a severe cybersecurity talent shortage, presents a significant security challenge. While awareness of AI-related risks is increasing, security measures are simply not keeping pace.

Organizations are prioritizing speed and innovation over security, often treating it as an afterthought in the race to integrate AI. This translates to a dangerous pattern: security controls are frequently omitted from initial planning phases, forcing teams into costly and inefficient retrofitting. Spending on generative AI initiatives is significantly outpacing investments in securing generative AI. From 2023 to 2024, spending on gen AI initiatives was 1.6 times higher than budgets that were allocated for security, and by 2025 this gap is expected to widen to 2.6 times (Figure 3). This growing disparity underscores the disconnect between innovation and protection. In essence, companies are building AI systems on insecure foundations, exposing themselves to a rapidly evolving threat landscape. This reactive approach is unsustainable, with only 28% of companies embedding security controls in all transformation initiatives from the start[30] and less than half (just 42%) are balancing their AI development with the essential security investments needed to protect those systems[31].

This challenge is further compounded by a critical cybersecurity talent shortage, with 83% of executives identifying it as a major obstacle to achieving a strong security posture[32].

Figure 3: Generative AI spend vs. security spend
Spending on generative AI initiatives is outpacing investments in securing generative AI.

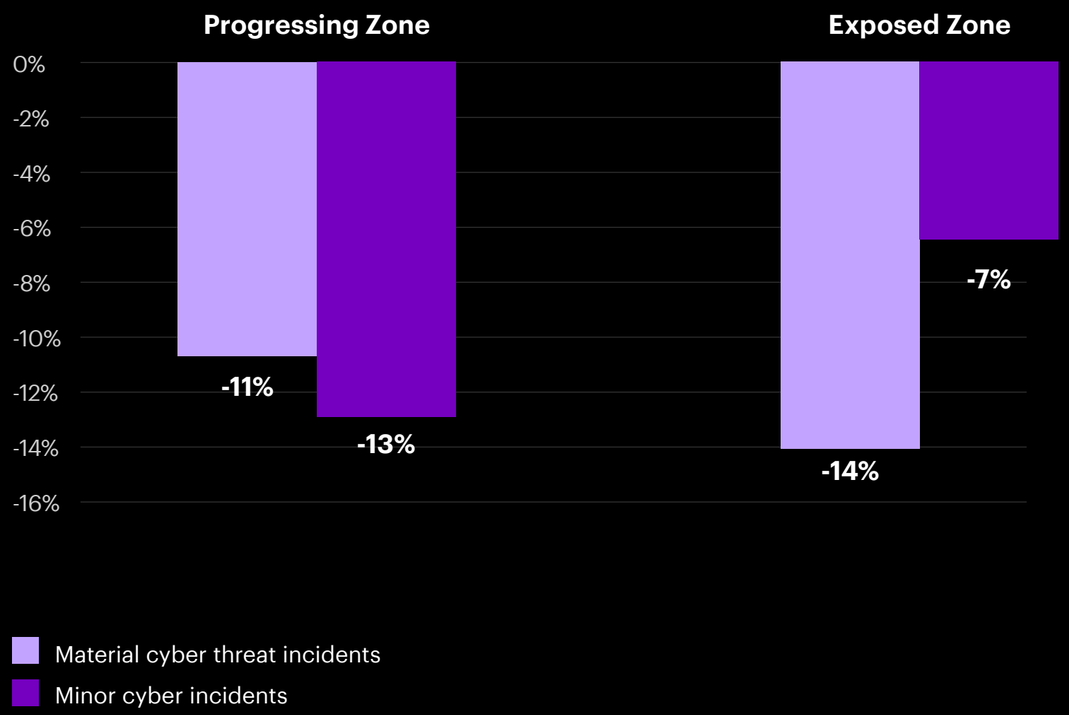


The Reinvention-Ready Zone advantage—where security fuels success

Companies in the Reinvention-Ready Zone demonstrate a significant advantage. Compared to those in the Exposed Zone, they are 69% less likely to experience advanced attacks such as AI-powered cyberattacks and have a 1.5 times higher success rate in blocking attacks. This translates to greater operational visibility, with Reinvention-Ready Zone companies achieving 1.3 times higher visibility across their IT and OT infrastructure[33].

The benefits of this zone extend beyond security, driving significant business value. These firms achieve 1.6 times higher ROI on their generative AI initiatives, demonstrating that embedding security from the start fuels both resilience and financial success.

Figure 4: Advantage of security investments
Increasing investments in security posture practices to reach the Reinvention-Ready Zone builds resilience, empowering companies to stay ahead of threats.



Furthermore, their robust security practices contribute to a 1.7 times reduction in technical debt, paving the way for more efficient and sustainable innovation. And perhaps most critically, strong cybersecurity builds trust. Reinvention-Ready Zone companies see a 1.6 times greater improvement in customer trust—a vital ingredient for long-term business success[34].

Progressing to this zone requires a commitment to enhancing security posture maturity. Our economic modeling underscores a compelling financial benefit: a 10% increase in security investment boosts an Exposed Zone firm's ability to detect, contain and remediate cyber threats by 14% (Figure 4)[35].

By prioritizing security alongside AI advancements, businesses can not only stay ahead of the ever-evolving threat landscape but also unlock the full, transformative potential of AI.

Four actions to strengthen AI security

The rise of AI, particularly generative AI, presents both opportunities and challenges for security. While AI can enhance security, it also introduces new risks and expands the attack surface. Companies must take four decisive actions to protect AI investments and leverage AI's defensive capabilities:

01 Develop and deploy a fit-for-purpose security governance framework and operating model accounting for the realities of an AI-disrupted world to establish clear accountability and align AI security with regulatory and business objectives.

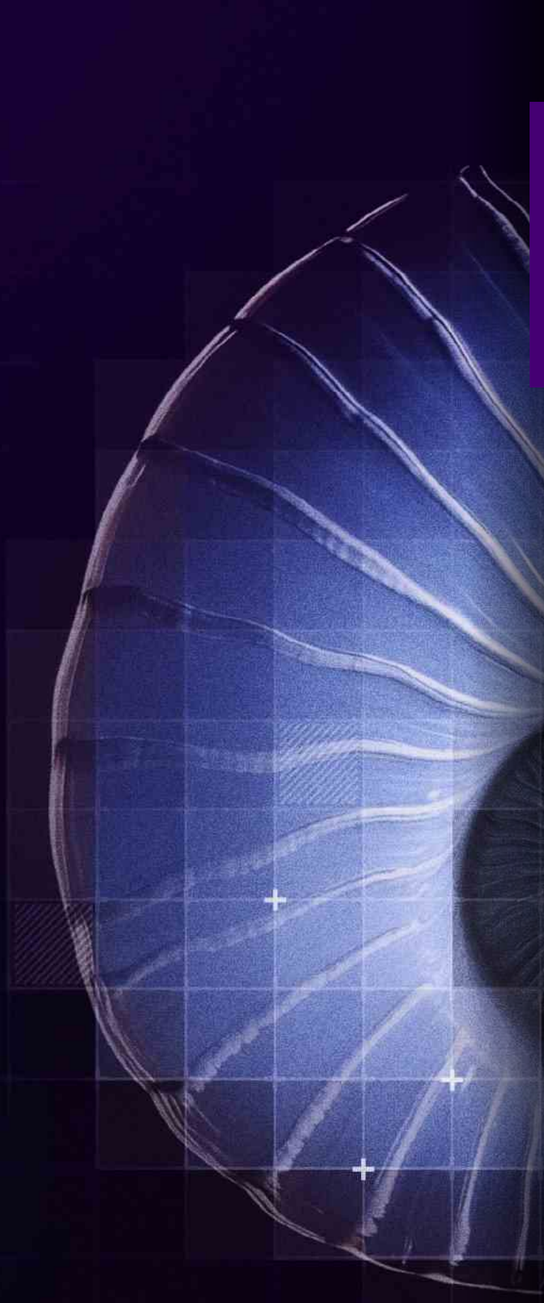
02 Design a digital core to be generative AI secure from the onset by embedding security into AI development, deployment and operational processes from the outset.

03 Maintain resilient AI systems with secure foundations that proactively address emerging threats, enhance detection capabilities, enable AI-model testing and improve response mechanisms.

04 Reinvent cybersecurity with generative AI by leveraging it to automate security processes, strengthen cyber defenses and detect threats sooner.

Built for protection

Developing and deploying fit-for-purpose security in an AI-disrupted world



Cyber threats are escalating, with 72% of organizations reporting an increase in attacks and 63% identifying the evolving threat landscape as their biggest challenge[36]. CISOs must move beyond reactive security as generative AI amplifies risks. Here are three actions resilient companies are taking now.

Make AI security a C-Suite priority with accountability and collaboration

AI security isn't just an IT issue; it's a business imperative that requires executive-level accountability. CISOs must work closely with the CEO, AI leadership and board to drive clear ownership of AI security and cyber resilience. Organizations in the Reinvention-Ready Zone lead the way, with 73% ensuring board-level cybersecurity accountability, embedding security into strategic decision-making[37]. Build a compelling business case for AI security by positioning it as an enabler of innovation, compliance and competitive advantage—not a constraint.

Foster collaboration across business and AI teams to ensure generative AI systems remain secure while navigating evolving risks and regulations.

Security teams must align with business objectives, while business leaders must recognize security as essential to success. Bridging this gap requires clear, jargon-free communication, showing how measures like multi-factor authentication and data encryption, for example, create safer, more transparent customer experiences. Security shouldn't be a hurdle—it should be a competitive advantage, integrated into marketing, customer interactions and brand trust.

Embed AI security into every strategic decision, from product launches to M&A, ensuring innovation doesn't introduce unmanageable risks. 85% of organizations in the Reinvention-Ready Zone align cybersecurity with business strategy and integrate security into digital transformation from the start—compared to just 45% in the Exposed Zone[38].

Establish shared security performance metrics early in product development and service delivery. Go beyond speed and functionality—measure how effectively security is incorporated by design, tracking the percentage of security requirements addressed in initial design phases, post-launch vulnerabilities and patch deployment times. Ensure executive leadership reviews AI security metrics alongside business KPIs, embedding risk considerations into strategic decision-making.

By making AI security a board-level priority, fostering collaboration and embedding security into strategic initiatives, organizations can turn AI security into a business enabler—driving resilience, trust and long-term success.

Build an adaptive AI risk and compliance framework

AI regulations are evolving at lightning speed, so organizations need a flexible, forward-looking approach to AI security. Establish an adaptive AI security framework that goes beyond merely meeting compliance requirements; it should continuously evolve to tackle emerging threats like adversarial attacks, data poisoning and model manipulation. Reinvention-Ready Zone organizations excel in this area, with 87% defining AI-specific policies for data security, privacy and access control, alongside clear governance and compliance controls[39].

Maintaining agility requires continuous learning. Regular AI risk management training enables teams to anticipate and respond to evolving threats. Assign clear oversight roles to prevent breaches, ethical issues and AI-specific risks, and regularly update Responsible AI practices based on lessons learned from real-world attacks, internal audits, regulatory feedback, and to address new challenges.

Finally, integrating AI risk assessments into procurement, vendor management and product development allows organizations to identify vulnerabilities early. A real-time, adaptive approach strengthens security while enabling innovation—ensuring resilience in an ever-changing regulatory and threat landscape.

To stay resilient in a fractured geopolitical environment, organizations should ensure their cybersecurity frameworks are flexible enough to account for changes in sourcing models, data flows and cross-border operations. This includes regularly assessing how shifting trade policies, tariffs and regional tensions affect regulatory obligations, data residency requirements and third-party exposure. For multi-country operations, the cybersecurity operating model should be reviewed and updated to reflect region-specific risks—ensuring security controls, reporting lines and compliance practices are responsive to local threats and political conditions.

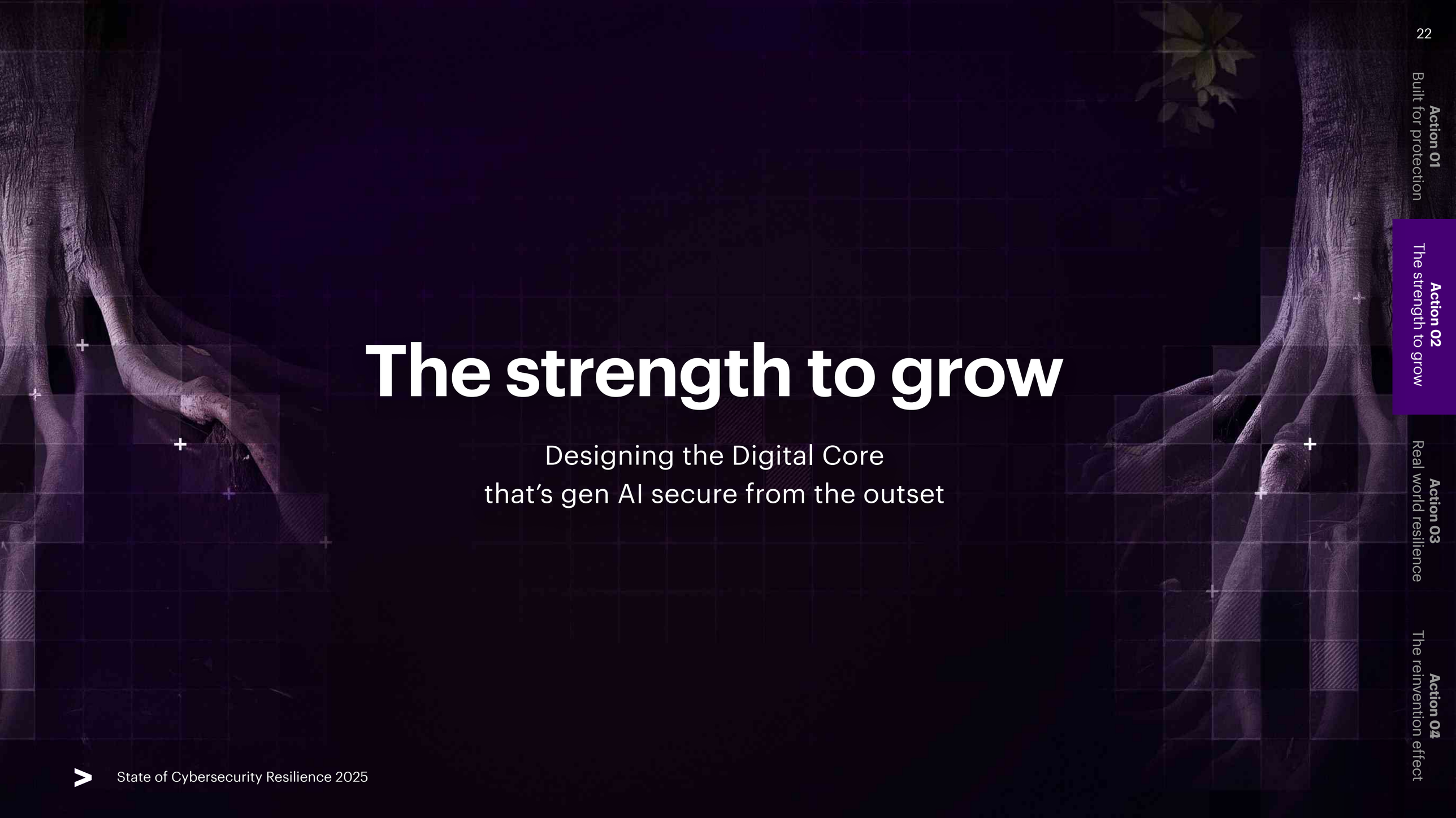
Strengthen human risk awareness to close the security gap

Technology alone won't secure AI—people remain the first line of defense. As deepfakes, AI-powered phishing and identity fraud become more sophisticated, social engineering attacks increasingly bypass traditional security controls. Reinvention-Ready Zone organizations recognize this, with 75% implementing structured AI-focused security awareness training, while those in the Exposed Zone leave employees vulnerable due to a lack of education programs[40].

Equip employees at all levels—from senior leadership to frontline staff—with the skills to recognize and respond to AI-driven threats. Tailor training to specific roles, ensuring executives, developers and frontline teams understand the AI risks most relevant to their responsibilities. Strengthen cyber readiness through AI-specific awareness programs, hands-on incident response drills and interactive training, such as phishing simulations. Promote cybersecurity certifications to deepen expertise and foster a security-conscious culture. Assess effectiveness by tracking AI phishing resilience, incident reporting rates and measurable behavioral improvements.

To future-proof AI security, strengthen AI talent pipelines by upskilling security teams and investing in AI-specific cybersecurity training. Establishing clear AI security policies and usage guidelines prevents misuse, unauthorized access and compliance failures—ensuring AI systems operate securely and responsibly.

By prioritizing AI awareness, training and talent development, organizations can reduce human risk, strengthen cyber resilience and turn employees into active defenders against AI-driven threats.



The strength to grow

Designing the Digital Core
that’s gen AI secure from the outset

While 66% of organizations recognize AI's impact on cybersecurity, only 37% have processes in place to assess AI tool security before deployment—a stark disconnect between awareness and action[41]. Securing the entire generative AI stack, from data and models to applications and access controls, is critical.

Traditional security alone is insufficient; AI-specific defenses are needed to prevent data exposure, model compromise and application vulnerabilities. True cyber resilience in an AI-driven world requires embedding advanced security controls into the digital core.

As Chapter 2 of our digital core research points out, in order to benefit from the advances of AI, organizations must move from traditional instruction-driven, predefined technology stacks to intention-based systems, powered by AI, with a cognitive architecture that mimics human-like thinking and learning. This is essential for an era characterized by deep generative AI integration, enabling machine operations and customization to meet specific industry needs[42].

Ensure secure-by-design cloud for AI

Cloud misconfigurations are one of the biggest risks to AI security, giving attackers an entry point to manipulate training data, extract sensitive information and compromise AI models. The best defense is embedding security from the start—not treating it as an afterthought. Establish dedicated and segmented Secure AI environments, which can facilitate prototyping and experimentation at speed under controlled conditions. The aim is to foster innovation while also ensuring critical information and processes are not impacted. These environments should complement the secure cloud strategies outlined below.

Adopt Infrastructure-as-Code (IaC) to ensure security is built into cloud environments by default, eliminating misconfigurations and reducing human error. Organizations in the Reinvention-Ready Zone are 3.3 times more likely to take this proactive approach, giving them a stronger security foundation[43].

Security should be integrated into cloud operations from the outset, embedding tools directly into DevSecOps workflows and cloud application teams. This enables automated threat detection, continuous monitoring and real-time policy enforcement, ensuring vulnerabilities are caught early—before they become serious threats.

Leverage cloud-native security tools to proactively detect and remediate misconfigurations. Pre-configured security policies, anomaly detection and automated compliance validation strengthen cloud security. AI is well placed to strengthen the rigor, coverage as well as velocity of secure cloud operation and should be employed across the cloud operating model. Reinvention-Ready Zone organizations already lead in this space, with 82% using cloud-native security tools compared to just 54% of their peers[44].

Finally, establish clear cloud access governance to enforce least-privilege access for AI models, data and cloud resources. Well-defined access models significantly reduce risk— Reinvention-Ready Zone organizations are 82% more likely to have these controls in place[45].

Cloud security must be an ongoing effort, embedded into every application and transformation project from day one. With a proactive, integrated approach, organizations can minimize risk, secure AI workloads and build resilience in an evolving cloud landscape.

Strengthen identity and access management (IAM) with centralized security and Zero Trust

As AI operations scale, traditional perimeter security is no longer enough. Organizations need a centralized, AI-driven IAM approach built on Zero Trust principles to ensure secure access across AI and cloud environments.

Implement a centralized IAM solution to streamline identity governance, ensuring consistent verification, controlled permissions and consistent access enforcement. Adopt a "never trust, always verify" mindset. Zero Trust eliminates implicit trust by enforcing strict access verification at every step. Reinvention-Ready Zone organizations are already leading in this area—twice as likely to have fully implemented Zero Trust compared to their peers.

Continuous authentication, strict segmentation and least-privilege access prevent unauthorized activity, while context-aware controls dynamically adjust permissions based on location, device status and user behavior. Ephemeral access further reduces risk by granting permissions only for the duration of a task—eliminating privilege creep.

Strengthen authentication with privileged account controls, continuous session monitoring and passwordless multi-factor authentication (MFA) using biometrics, hardware security keys or adaptive risk-based models. Reinvention-Ready Zone organizations are ahead, with 84% implementing advanced authentication measures to enhance security and improve user experience[46].

Secure AI data with robust governance, protection and monitoring

As AI becomes deeply integrated into business operations, data security and governance are no longer optional—they're mission-critical. Yet only 20% of organizations feel confident in securing their generative AI models[47]. Without strong safeguards, AI systems are vulnerable to data manipulation, exposure and regulatory non-compliance.

Start with a clear data classification framework. A remarkable 86% of Reinvention-Ready Zone organizations lead the way in properly labeling AI-related data, ensuring sensitive information is protected and security policies are enforced[48]. Categorizing data by sensitivity levels enables tighter access controls, compliance enforcement and prevention of unauthorized access to training and inference datasets.

Robust encryption and strict access controls should be applied across the AI data lifecycle—at rest, in transit and during processing. Reinvention-Ready Zone organizations are ahead, with 91% implementing end-to-end encryption and granular access policies, preventing cyber threats from compromising AI data[49].

Reduce privacy risks with anonymization techniques like synthetic data, masking and tokenization. AI models process vast amounts of personal and proprietary business data, making synthetic data a critical strategy for security and compliance. By replacing real-world data with synthetic equivalents, organizations train AI models without exposing sensitive information to breaches or adversarial manipulation.

Continuous monitoring is key to preventing unauthorized access and detecting unusual data usage before it escalates. AI models are prime targets for data poisoning attacks, where adversaries inject malicious data to corrupt AI outputs. Leverage real-time anomaly detection and behavioral analytics to identify suspicious activity, mitigate threats and ensure data integrity.

Finally, maintain a comprehensive inventory of AI systems, tools and integrations to improve governance and enhance supply chain risk management. Knowing where AI models are deployed, how data is used and where vulnerabilities exist allows for proactive security oversight and regulatory compliance.

By embedding strong governance, encryption, monitoring and privacy-enhancing techniques, organizations can secure AI-driven environments while maintaining trust and compliance.

Secure and future-proof applications

As organizations accelerate AI adoption and digital transformation, application security must evolve to address modern development risks. Securing applications begins with embedding security into the software development lifecycle (SDLC)—from initial design to deployment and continuous monitoring—ensuring AI-driven applications remain resilient against evolving cyber threats.

Threat modeling early in the design phase helps identify vulnerabilities before development begins, strengthening application defenses from the start. Organizations in the Reinvention-Ready Zone are 85% more likely to embed DevSecOps methodologies[50], integrating security testing into CI/CD pipelines to detect and remediate vulnerabilities before deployment. This includes static, dynamic and open-source security testing, as well as Software Bill of Materials (SBOM) generation to continuously assess proprietary and third-party components for risks.

Beyond secure coding, protecting sensitive credentials and access points is critical. Regularly scanning application code and source repositories helps prevent exposure of API keys, encryption certificates and other sensitive assets—common attack vectors that adversaries exploit to gain unauthorized access. Automating these scans and enforcing strict access controls significantly reduces security risks.

Emerging technologies such as serverless architectures, low-code/no-code platforms and generative AI-powered applications introduce new risks that traditional security frameworks may not fully address. Here too, organizations in the Reinvention-Ready Zone are ahead, with 88% implementing adaptive security programs to continuously assess and mitigate threats in evolving application environments[51].

By integrating security at every stage, enforcing automated risk detection and adapting to new technology risks, organizations can secure their applications, maintain compliance and future-proof AI-driven innovation against next-generation cyber threats.

Case Study

Safeguarding generative AI systems against critical threats

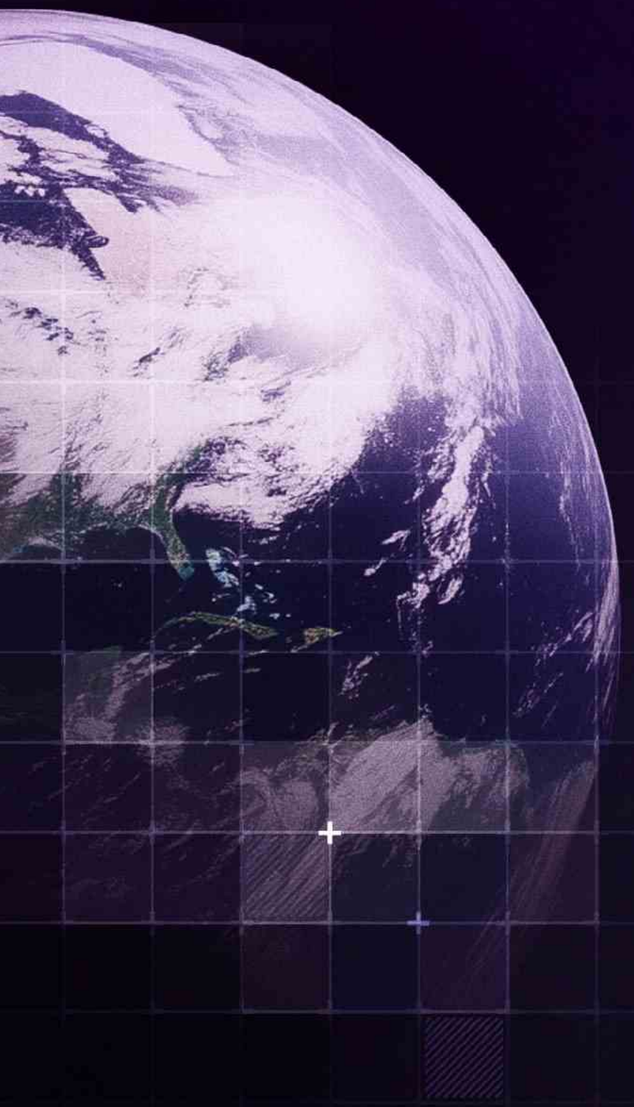
A leading platform company partnered with Accenture Security to assess risks tied to proprietary Large Language Models (LLMs) and new gen AI-powered products aimed at enhancing customer experience.

The company faced emerging threats—including prompt injection, training data leakage and lack of guardrails for user input and model output—highlighting the need for a stronger AI security framework.

A tailored approach aligned with business objectives and gen AI use cases was applied, which included close collaboration with product and security teams to understand architecture, identify model-level vulnerabilities and evaluate security across the application stack. Custom and open-source adversarial prompt libraries were used to simulate prompt attacks, data leakage and denial-of-service scenarios.

Beyond testing, the team conducted in-depth code reviews, infrastructure analysis, and risk mapping across the gen AI product landscape. Clear, actionable recommendations were provided to improve prompt design, enforce access controls and embed security testing into development workflows.

As a result, the company identified and remediated critical vulnerabilities, strengthened data privacy protections and reduced the risk of credential or sensitive data exposure. With stronger guardrails and a secure-by-design foundation, the company was able to launch new gen AI products with greater confidence.



Real world resilience

Maintaining AI systems with secure foundations and proactive threat management

As AI adoption accelerates, threat actors are leveraging adversarial AI techniques like data poisoning, model inversion and automated prompt injections.

To counter these evolving threats, organizations must establish strong security foundations and continuously monitor AI-specific risks. Yet only 17.5% fully leverage threat intelligence and industry data to prioritize security decisions, leaving many vulnerable to emerging AI-driven attacks[52].

Strengthen AI defenses with threat intelligence, continuous monitoring and proactive security testing

AI models aren't just another IT asset—they're a prime target for adversarial attacks, data poisoning and model manipulation. The key to staying ahead? Continuous monitoring, real-time threat intelligence and rigorous security testing.

Prioritize model observability, detection and continuous monitoring to secure AI systems in the cloud while ensuring responsible AI practices. This provides real-time visibility into AI systems, helping you spot unusual activity, prevent data corruption and detect adversarial threats before they escalate. Organizations in the Reinvention-Ready Zone are 80% more likely to have advanced AI monitoring in place, giving them a critical edge[53].

But monitoring alone isn't enough. AI security needs constant validation. Run tabletop exercises, red team simulations and real-world attack testing to stress-test defenses against model inversion, prompt injections and deepfake threats. Reinvention-Ready Zone organizations are nearly six times more likely to conduct these kinds of drills, ensuring they can quickly adapt to emerging attack tactics.

Security teams should also integrate AI threat modeling into risk assessments, refine detection models and build resilience against API abuse, model poisoning and integrity compromises. Engaging security, legal and engineering teams in structured drills enhances forensic readiness, improves incident coordination and strengthens containment strategies.

By combining threat intelligence with continuous validation, security teams can fine-tune detection models, strengthen response workflows and build AI-driven systems that are both resilient and secure.

Build AI incident response plans that actually work

AI-driven cyberattacks aren't a hypothetical threat—they're already happening. Yet, many organizations still lack a clear AI-specific incident response plan. Without one, security teams risk prolonged disruptions, financial losses and cascading impacts across suppliers, customers and business operations.

To avoid that chaos, develop an AI-focused Cybersecurity Incident Response Plan (CIRP) that outlines exactly how to contain, mitigate and recover from an AI-related breach. Map out AI-specific threat scenarios, from compromised training data to adversarial AI attacks, and bake them into existing playbooks.

AI incidents rarely happen in isolation. Extend your response plan beyond your own walls—involving suppliers, cloud providers and external AI vendors to ensure coordinated action. And don't wait for a real attack to test your plan. Run executive-level crisis simulations so leadership knows how to respond when it matters most.

Those in the Reinvention-Ready Zone have already figured this out—92% have incident response plans in place. It's not just about compliance; it's about making sure your AI security strategy holds up under real-world pressure[54].

Lock down AI supply chain risks before they become problems

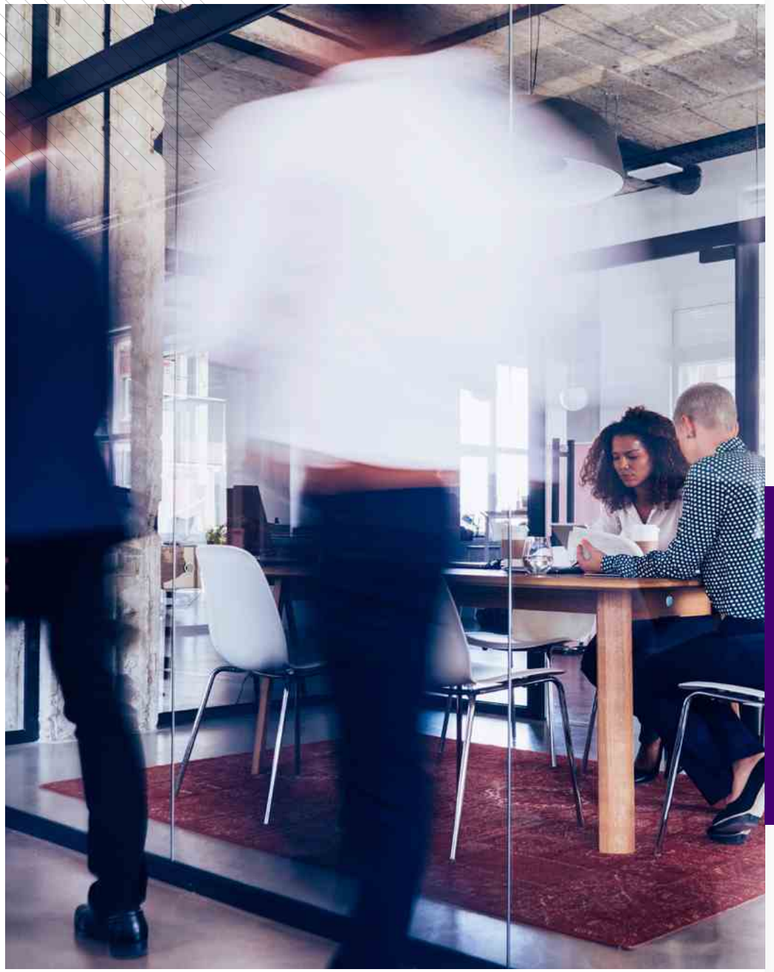
AI doesn't work in a vacuum. Your models rely on third-party vendors, pre-trained models and external AI services—which means your security is only as strong as your weakest link. Without clear supplier security standards, you're leaving the door open for model corruption, data leaks and compliance failures.

The best way to prevent this? Put vendors through the same rigorous security scrutiny as your internal systems. Require transparent AI security controls, enforce contractual security commitments and conduct independent security audits before onboarding any third-party AI provider.

Go deeper than surface-level compliance. Validate where your models are coming from, check data sources for bias or tampering and ensure pre-trained AI models undergo rigorous security testing before deployment. Organizations in the Reinvention-Ready Zone lead in this area, implementing real-time AI supply chain monitoring and automated risk scoring to flag vulnerabilities before they become crises.

To take it further, strengthen vendor lifecycle management with continuous security assessments, model performance validation and post-deployment monitoring. By embedding AI security into procurement and vendor management, you're not just protecting your own organization—you're ensuring every AI model in your ecosystem meets the highest security standards.

In response to trade-driven supply chain shifts, organizations must extend third-party risk assessments to include cybersecurity posture evaluations of newly onboarded suppliers. These reviews should include how data access methods may change, the introduction of new dependencies, and any vulnerabilities arising from the broader geopolitical environment. Threat intelligence should be used to anticipate country-specific risks and assess how political instability may increase the likelihood of cyber exploitation across the extended supplier network. These inputs should be baked into sourcing decisions, vendor contracts and dynamic monitoring mechanisms.



Case Study

Strengthening agentic AI security for a Brazilian healthcare company

A leading Brazilian healthcare company used agentic AI to eliminate the manual processing of patient exam requests by automating workflows through Optical Character Recognition (OCR) and Large Language Models (LLMs).

This allowed seamless data extraction and integration across cloud APIs, legacy databases, billing systems, and diagnostic devices. However, the expanded connectivity exposed the company to serious cyber risks, particularly data poisoning—where malicious actors manipulate training data to mislead the AI—and prompt injection, where hidden commands embedded in scanned images could hijack system behaviour.

To mitigate these risks, the company overhauled its AI security in three phases. First, through threat modelling, it mapped every interaction and identified vulnerabilities using the OWASP LLM Top 10 framework. Then, in the security testing phase, it ran adversarial simulations, including red team exercises,

to expose real-world exploits like a prompt in an image instructing the system to input false data. Finally, in the runtime protection phase, it enforced strict input validation, encrypted API calls, segmented systems, and implemented identity and access controls to prevent unauthorized manipulation. These measures not only reduced exposure to data poisoning, prompt injection, and shadow AI risks but also ensured safe, scalable deployment of AI agents while maintaining compliance and patient trust.

The reinvention effect

A new approach to cybersecurity
with generative AI

AI is reshaping cybersecurity by reducing manual workloads, enhancing threat detection and addressing a critical skills gap, with an estimated 4.8 million cybersecurity positions unfilled[55]. As threats grow more complex, organizations must strengthen security with fewer resources. Generative AI accelerates response times by processing vast data, uncovering risks and detecting threats faster than ever.

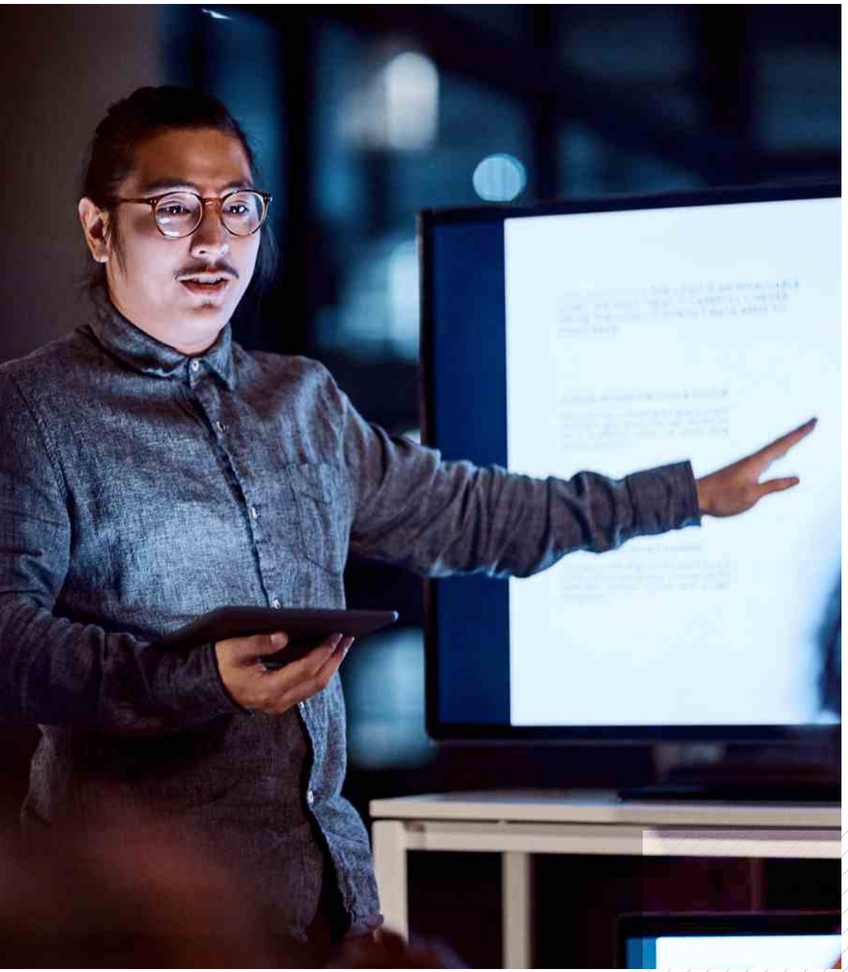
According to Accenture's research on generative AI's workforce impact, we found that generative AI can transform cybersecurity by automating and augmenting 71% of security analyst tasks, streamlining manual efforts and enhancing threat detection[56]. AI-powered solutions improve alert triage, prioritize incidents, detect anomalies, classify vulnerabilities, automate patching and optimize security configurations. However, attackers are also leveraging generative AI to scale cyber threats, making AI-driven defenses essential.

AI is also revolutionizing red-teaming and penetration testing. As regulations evolve, security teams must proactively defend against adversarial AI attacks, model poisoning and deepfakes. Here are three actions leading platforms and hyperscalers take to mitigate AI-driven risks.

Anticipate and automate threat response with AI

Cyber threats are evolving faster than ever, and security teams can't afford to play catch-up. AI-powered security tools provide the speed, accuracy and automation needed to identify threats early, reduce false positives and accelerate incident response.

Start with AI-powered threat modeling to simulate attack scenarios, predict vulnerabilities and assess AI-specific risks like adversarial attacks, data drift and model evasion. Leverage machine learning-based anomaly detection to continuously monitor for unusual behavior—spotting privilege escalations, suspicious API calls and attack patterns before they escalate.



AI-enhanced behavioral analytics also improves zero-day threat detection, adapting to evolving attack techniques faster than manual processes ever could. Organizations in the Reinvention-Ready Zone are already leading the way—83% use AI-powered analytics to accelerate alert correlation, automate threat investigations and generate more contextualized intelligence reports[57].

To stay ahead, embed AI-driven risk assessments into security workflows, train AI models on adversarial tactics and operationalize AI-driven risk scoring to dynamically prioritize and neutralize threats faster. With AI in your corner, your security team can shift from reacting to threats to proactively stopping them before they cause harm.

Use AI security agents for efficiency

Security teams are overwhelmed with alerts, manual processes and ever-growing cyber threats. AI-driven automation changes the game, streamlining security operations, reducing analyst workload and enabling faster, more precise responses.

Deploy generative AI-powered security assistants to handle time-consuming tasks like log analysis, threat summarization and incident documentation, allowing human analysts to focus on real threats instead of sifting through endless data. Implement AI-driven alert triage and case enrichment to correlate threat intelligence, prioritize alerts based on risk scoring and generate contextual incident reports—ensuring teams focus on what matters most.

Enhance SOC operations with generative AI-powered security assistants that analyze vast threat intelligence, deliver real-time risk assessments and automate incident triage. AI-driven task orchestration further optimizes efficiency by dynamically assigning incidents based on analyst expertise, workload distribution and past performance. Reinvention-Ready Zone organizations are already leveraging these capabilities to accelerate response times, enhance decision-making and bolster cyber resilience.

To maximize impact, embed AI automation across security platforms, leverage explainable AI for transparency and continuously validate AI-driven processes to ensure accuracy, trust and operational effectiveness. With AI streamlining security workflows, teams can operate faster, smarter and more effectively, staying ahead of evolving threats.

Fortify digital trust with AI-driven access intelligence

Traditional IAM cannot keep up with today's dynamic threats. AI-driven automation transforms identity security, ensuring the right people have access—while keeping bad actors out.

Implement AI-powered identity governance to monitor user behavior in real time, enforce risk-based access controls and detect anomalies before they escalate. AI-driven authentication—leveraging behavioral biometrics and contextual risk scoring—dynamically adjusts access levels based on real-time threats, eliminating friction while strengthening security.

Automate IAM lifecycle management to streamline provisioning, role-based access control (RBAC) and privileged access governance, reducing manual errors and ensuring compliance. Reinvention-Ready Zone organizations are already ahead—automating access reviews, detecting privilege escalations and enforcing Zero Trust policies to eliminate gaps in identity security.

To stay resilient, deploy AI-powered identity threat detection, enforce continuous authentication and automate access policies across hybrid and multi-cloud environments. With AI-driven IAM, security teams can enhance protection, reduce complexity and ensure seamless, secure access—without slowing down the business.

Start your journey

The Reinvention-Ready Zone is within reach—but it requires decisive action. By adopting a secure governance framework, building resilient AI systems, leveraging generative AI for security and embedding security into every stage of AI development, companies can close the security gap and confidently navigate an era of accelerating cyber threats.

The path forward is clear:

Security is not just a safeguard—it is a strategic enabler of innovation, trust and long-term success.

The CISO checklist

Designing and operationalizing cyber risk strategies

1. Is cybersecurity fully embedded into our business and AI transformation strategies from the outset, or is it still treated as bolt-on?
2. Do we have a clear governance framework with board-level accountability for AI and cybersecurity risks?
3. Are we proactively assessing and managing cyber risks related to AI adoption, including compliance with emerging regulations and ethical AI principles?
4. Do we have a cybersecurity training and awareness program that ensures employees, executives, and third parties understand and mitigate evolving AI-driven threats?
5. Have we integrated a cybersecurity technology evaluation capability to support secure-by-design decisions when major changes are made to our delivery or sourcing model?

Securing the digital core and supply chain

1. Have we implemented a Zero Trust architecture across cloud, data, identity and AI systems to mitigate unauthorized access and lateral movement?
2. Are our AI and data security controls aligned with regulatory requirements and industry best practices to prevent data breaches and model poisoning?
3. Do we have full visibility across IT and OT environments, ensuring real-time monitoring and detection of potential cyber-physical threats?
4. Do we have rapid supplier security assessments in place—supported by threat intelligence and geopolitical risk analysis—to evaluate exposure when operations or supply chains shift across regions?
5. Do we have real-time visibility into regulatory cybersecurity requirements when delivery models, technologies or third-party ecosystems change—enabled by a centralized regulatory intelligence capability?

Testing resilience and defending proactively

1. Are we conducting regular red-teaming, AI-driven attack simulations, and resilience stress tests to measure our ability to detect, respond and recover from cyberattacks?
2. Do we have clear playbooks for AI-related threats, including adversarial AI attacks, AI worms and deepfake based social engineering?
3. How do we leverage gen AI to enhance threat detection, automate security workflows and reduce incident response times?
4. Are we integrating gen AI-driven threat intelligence and predictive analytics to proactively identify and neutralize emerging cyber threats before they escalate?

About the research

Survey demographics

2286 Survey Respondents from companies with global revenues of >$1 billion
CISO: 1828 (80%)
CIO: 458 (20%)

Countries inclued: 17

US (458), Canada (79), Brazil (102), UK (236), Ireland (68), France (182), Germany (190), Italy (180), Spain (100), UAE (66), KSA (66), South Africa (50), Australia (128), Japan (166), India (89), Singapore (77), Thailand (49)

Industries included: 24

Banking (125), Insurance (130), Capital Markets (113), Automotive (50), Chemicals (100), Consumer Goods and Services (100), Retail (125), Telecommunications (125), Media (100), Oil & Gas (150), Healthcare Payers (50), Healthcare Providers (100), High Tech (100), Industrial (50), Life Sciences – BioPharma (142), Life Sciences – MedTech (76), Public Services (150), US Federal Services (50), Utilities (150), Software & Platforms (100), Transport (50), Aerospace & Defence (50), Travel & Hospitality (50), Natural resources (50)

Methodology for Security Posture Maturity and defining Security Zones

We assess security posture maturity across Strategy and Capability. Cyber Strategy focuses on designing and operationalizing risk frameworks to protect digital transformation and strengthen customer trust. Capability spans three key areas: Cyber Protection, which applies Zero Trust principles to secure the digital core; Cyber Resilience, which involves pressure-testing defenses, monitoring emerging threats and enabling rapid response and Cyber-Physical Security, which safeguards industrial control systems and connected products throughout their lifecycle.

Our cybersecurity maturity evaluation follows a structured four-phase methodology. First, we established a cybersecurity benchmark by defining key capabilities through AI-driven research, expert interviews and insights from high-performing organizations. Next, we developed the Security Posture Maturity Framework, incorporating 94 best practices across Strategy and Capability, covering Cyber Protection, Resilience and Cyber-Physical Security, and categorized companies into three maturity zones. We then analyzed 2,286 companies, assessing their adoption intensity of these practices and classifying them into the Reinvention-Ready Zone, Progressing Zone or Exposed Zone based on their strategic alignment and execution capabilities. To ensure a balanced assessment across industries, Cyber-Physical Security was weighted lower for asset-light sectors. Finally, we validated the framework through econometric modeling, demonstrating a strong association between high cybersecurity maturity and superior business and security performance.

References

[1,5,6,7,8,9,23,26,29,33,34] Accenture Research analysis based on State of Cybersecurity Data

[3,4,18,21,22,24,25,27,28,30,32,37,38,39,40,43,44,45,46,47,48,49,50,51,52,53,54,57] State of Cybersecurity Survey 2025 | Accenture

[10,35] Accenture Research economic modeling based on State of Cybersecurity data

[2,11,12,15,31,36,41] Global Cybersecurity Outlook 2025 | World Economic Forum

[13,55] 2024 Cybersecurity Workforce Study | ISC2 Research

[14,56] Accenture Research analysis

[16] A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide | Checkpoint Research

[17] Pulse of Change Survey | Accenture

[19] This AI malware worm can steal private data and send spam emails without you ever having to click | Euronews

[20] Italian Elite Targeted by Scammers Using AI Voice Impersonation | Bloomberg

[42] Building a reinvention-ready digital core | Accenture

Acknowledgments:

Research Project Lead: Manav Saxena

Cybersecurity SME: Periklis Papadopoulos

Research team:

Archana Doreraju, Arlene Lehman,
Gargi Chakrabarty, Katarzyna Furdzik,
Shachi Jain, Pankaj Kishnani,
Toms Bernhards Callahan, Emily Thornton

Marketing team:

Kamilla Giedrojc, Ewa Szkudlarek

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent- and innovation-led company with approximately 799,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology and leadership in cloud, data and AI with unmatched industry experience, functional expertise and global delivery capability. Our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Song, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients reinvent and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities.

Visit us at www.accenture.com

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data-science-led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value and deliver on the power of technology and human ingenuity. For more information, visit Accenture Research on www.accenture.com/research.