

A woman with dark hair, wearing a blue and white patterned jacket, is looking upwards and to the right. The background is a dark blue digital space filled with blurred lines of code and colorful bokeh light effects. Two curved lines, one solid yellow and one dashed green, sweep across the upper half of the image. The Deloitte logo is in the top left corner.

Deloitte.

Together makes progress

Reimagine the modern
cybersecurity organization
through AI

The cyber imperative: Building for the future	02
Evolving compliance and security risk	04
Security organizations need to secure AI systems and reimagine how cyber runs	05
Across cyber capabilities, work can be refactored and reimaged	06
Leadership for the AI era	07
AI-driven attacks call for new AI countermeasures	08
Early adopters are prioritizing use cases that deliver measurable impact	09
Having a blueprint establishes a North Star to help organizations reimagine the cyber function	10
Blueprint for integrated AI security	11
Transformation example using NIST framework	12
Elevating cyber-AI maturity: A call for coordinated action	13

The cyber imperative: *Building* for the future

As the digital economy accelerates into the era of artificial intelligence (AI)-driven innovation, the traditional boundaries of cybersecurity are being redrawn. Cyber leaders now face a convergence of challenges: AI-powered adversaries; rapid shifts in compliance expectations; quantum-fueled uncertainty; and pressure to enable fast, low-friction business transformation. For the chief information security officer (CISO) and IT executive, the question is no longer only “How do we protect our assets?” but also “How do we architect trust, resilience, and competitive advantage at the speed of agentic AI?” This transformation is unfolding amid an ever-changing legal and risk landscape that organizations need to continuously navigate. At the same time, the cyber technologies CISOs depend on are increasingly AI-enabled—expanding supply chain and third-party risks across vendor dependencies, embedded model behavior, and upstream data and update pipelines. Resilience expectations are rising accordingly.

To move from experimentation to measurable outcomes, CISOs and IT leaders need a clear cyber-AI blueprint grounded in early-adopter lessons; actionable frameworks; and the realities of operating in a volatile, high-velocity threat environment. Enterprises need more than a vision of an AI-powered security organization—they need a pragmatic roadmap spanning workforce, technology, operating model, and governance.



"When foundation
models fail, ***organizations***
are challenged to recover."

Naresh Persaud,
Principal & AI Transformation Leader,
Deloitte & Touche LLP

Evolving compliance and security risk

The compliance and security risk environment is rapidly evolving

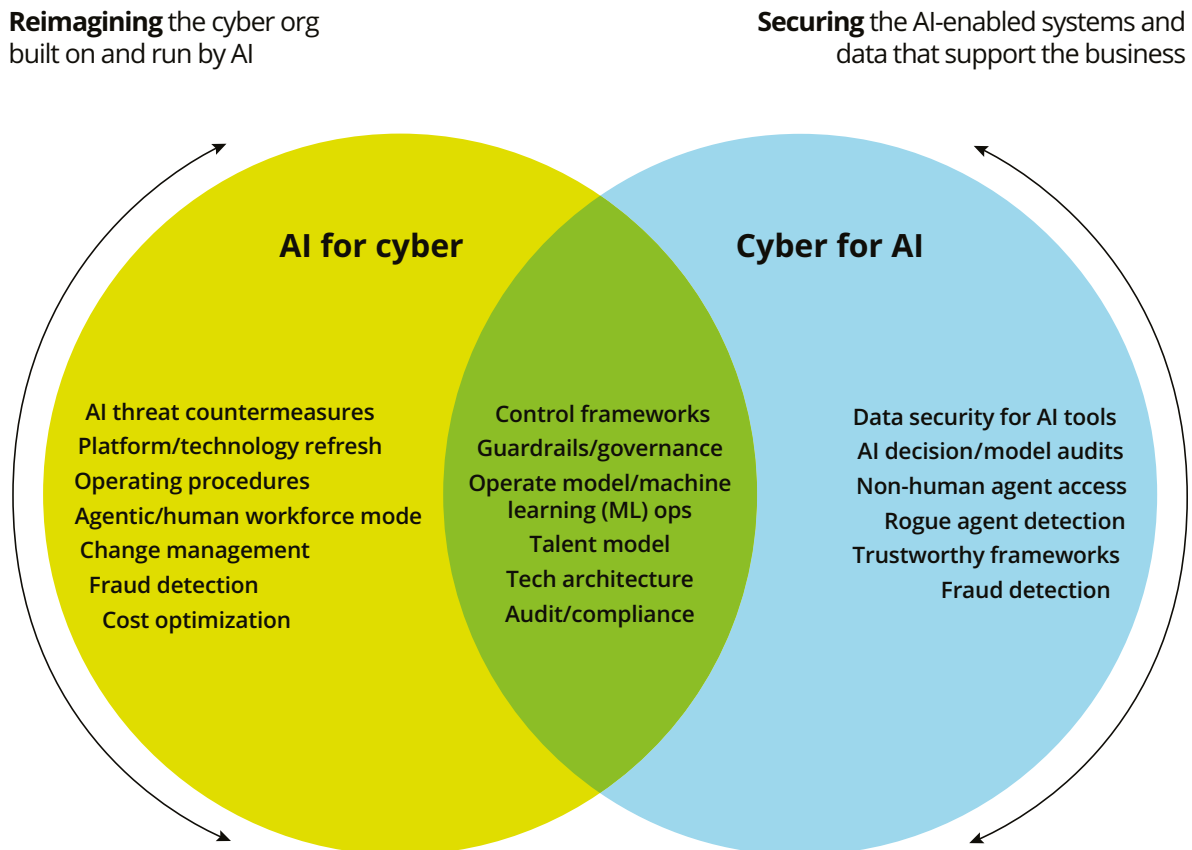
due to the convergence of several technology trends. These include zero trust design, AI-driven applications, advanced AI threats, and quantum computing. In response, many organizations are transitioning away from traditional perimeter-based security, adopting zero trust services to enable continuous verification and least-privilege access. AI is accelerating business innovation, but it also introduces new vectors of risk, particularly as advanced AI-powered threats emerge that are capable of evading conventional security controls. Meanwhile, quantum technologies threaten to disrupt current encryption methods, prompting enterprises to prepare for quantum-safe protocols. Together, these trends create the opportunity to reimagine how modern cyber organizations function.

When the entire business depends on the AI and intellectual property (IP) at the core, protecting it is everything. Organizations should seek to implement integrated governance models, guardrails, and trust frameworks to enable AI.

Security organizations need to secure AI systems and reimagine how cyber runs

Addressing these technology opportunities and risks involves a dual approach: “AI for cyber” focuses on embedding AI into the security organization to modernize threat detection, enable dynamic workforces, and drive operational change; while “Cyber for AI” helps ensure AI-enabled systems and data are secure, controlled, and aligned with governance frameworks. Scaling this dual approach requires lots of data, system integration, guardrails, and controls to enable outputs that are trustworthy.

Figure 1. Scaling AI requires lots of data, system integration, guardrails, and controls to enable outputs that are trustworthy across cyber capabilities, so work can be refactored and reimaged



Across cyber capabilities, work can be refactored and reimagined

The nature of cyber work is being fundamentally redefined. With AI now enhancing or transforming more than 50% of essential activities, organizations are moving beyond automating routine tasks to reimagining how core security functions operate, driving measurable improvements in speed, accuracy, and impact.

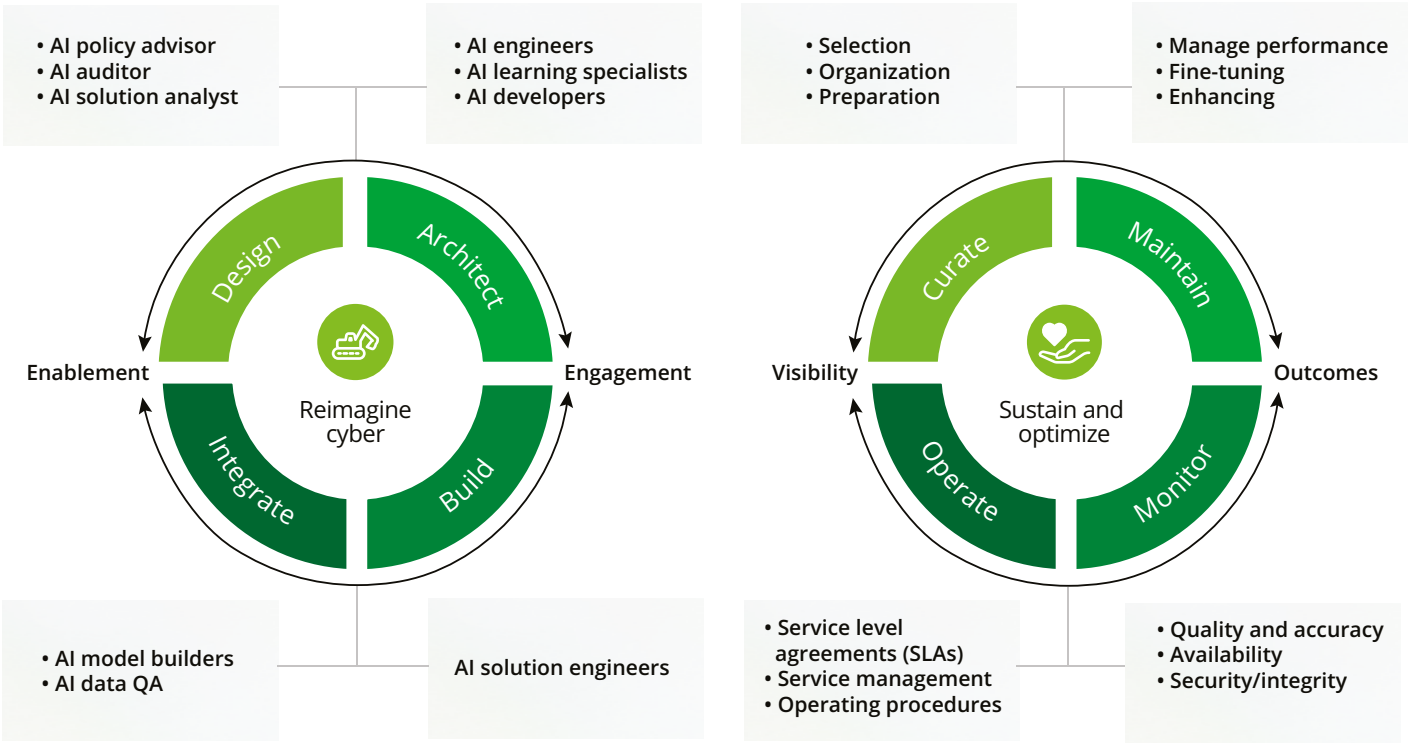


Leadership for the AI era

As cyberattackers are increasingly leveraging advanced AI techniques to amplify threats, organizations are adopting AI-driven security processes—shifting from static controls to adaptive, proactive defenses that integrate human expertise and AI capabilities for greater agility and resilience.

This transformation relies on a clear framework: designing, building, integrating, and continuously optimizing security operations with the optimal mix of strategic planning and specialized talent. By blending AI with human oversight and focusing on ongoing improvement, organizations can reduce fatigue, improve resilience, and deliver sustained value across their cyber landscape.

Figure 2. Organizations need a blueprint to combine agentic AI and GenAI with physical full-time equivalents (FTEs) to create results



AI-driven attacks call for new AI countermeasures

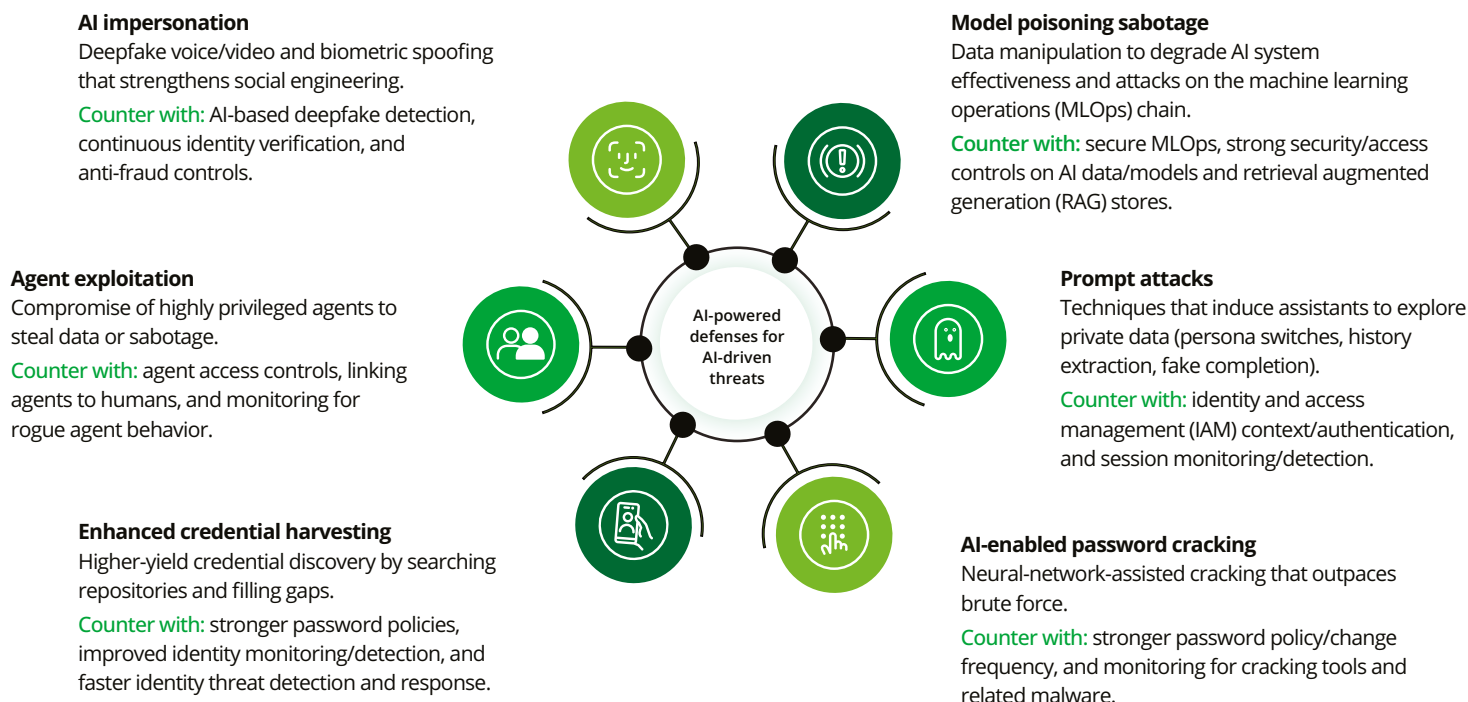
AI is driving a fundamental redesign of security processes that were originally built for slower, more predictable threat environments. As AI amplifies both attack sophistication and speed, security processes need to evolve from static, rule-based workflows to adaptive, intelligence-led systems.

Ultimately, this is a shift from isolated controls to coordinated, AI-enabled resilience. As attackers compress timelines and scale operations, defenders need a phased path that starts with visibility and hygiene (assets, exposures, privileged access), extends governance and monitoring across AI/machine learning (ML) models and supporting infrastructure, and then operationalizes AI-driven detection and response to reduce dwell time and disruption. Done well, this becomes an enterprise capability—not just a security operations center (SOC) upgrade—requiring alignment across stakeholders and a deliberate maturity journey from reactive pilots to integrated, continuously learning defenses.

“The landscape of threats will continue to evolve by learning from past attacks and using this input to drive future success.”

**Linda Walsh, Managing Director,
Deloitte & Touche LLP**

Figure 3. AI driven attacks call for new strategies and tactics leveraging AI countermeasures

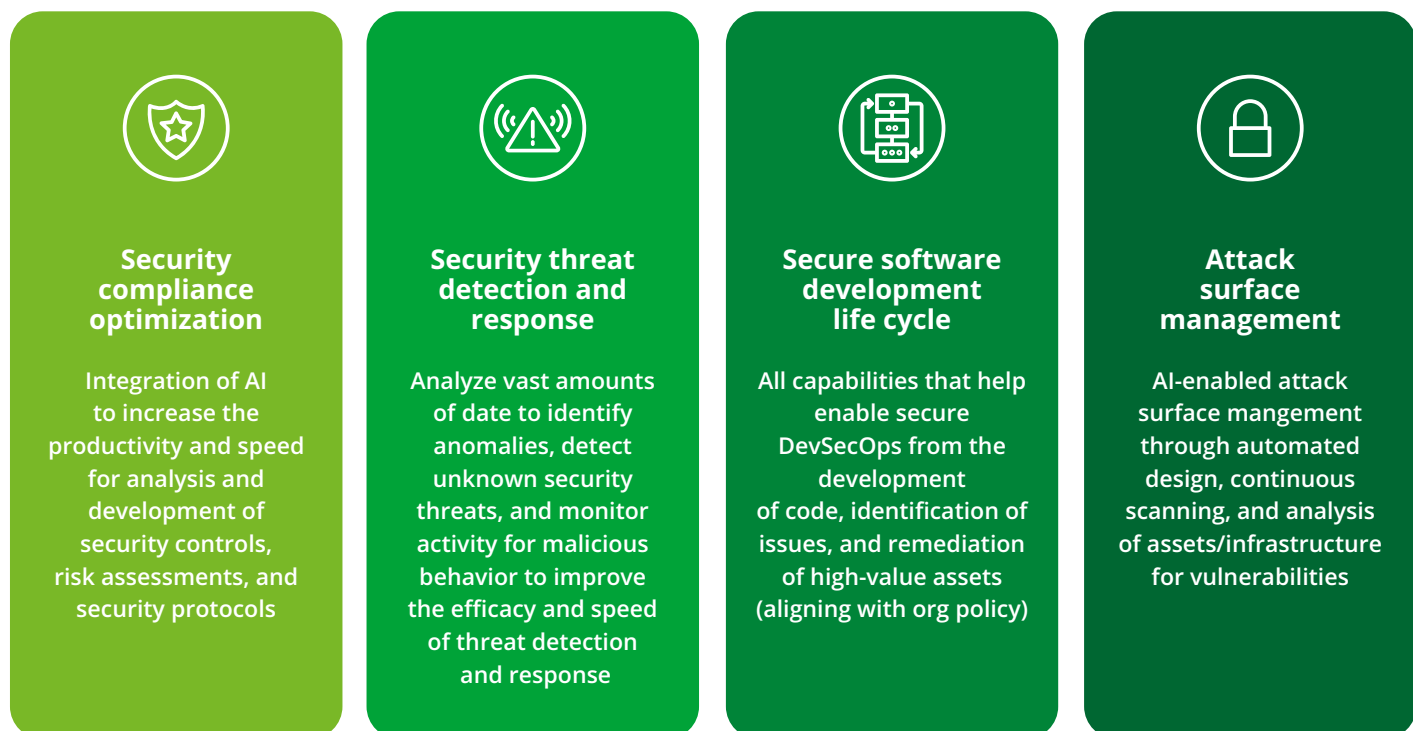


Early adopters are prioritizing use cases that deliver measurable impact

Rather than pursuing broad transformation up front, many organizations are focusing on targeted applications where AI can reduce risk, cost, and operational burden in the near term. The use cases can address common pain points faced by security teams including alert fatigue, fragmented tooling, and manual analysis.

By applying AI to priority areas, organizations can process large volumes of security data more efficiently, improve response times, and achieve greater consistency. These early investments also establish the data, processes, and operating foundations required to scale more advanced AI-enabled security capabilities.

Figure 4. Definitions for cyber priorities bolstered by AI



Having a blueprint establishes a North Star to help organizations reimagine the cyber function

Successfully scaling AI-enabled security requires more than technology adoption—it requires a clear organizational blueprint. Without this foundation, AI risks becoming another layer of complexity rather than a source of simplification and value.

The blueprint helps enable organizations to adopt AI in a structured, sustainable way. A well-defined blueprint helps translate AI potential into repeatable outcomes while maintaining control, trust, and regulatory confidence.

Figure 5. A blueprint establishes a North Star to help businesses reimagine the cyber organization

Workforce design	Agentic AI patterns and capabilities combined with human interaction	• Skills and roles • AI inclusion approach	• Change management • Training and enablement
Technology architecture	Aligning the capabilities needed to deliver on business outcomes	• Technology choices • Selection and comparison	• Roadmap • Timeline and plan
Operating model	Establishing the operating processes, practices, responsibilities, and cost optimization	• Operational assessment • Technology enablement	• Operating procedures • Organization structure
Governance model	Business case, roles, and responsibilities to drive the execution	• Governance structure • Business alignment	• Agent operations • AI framework

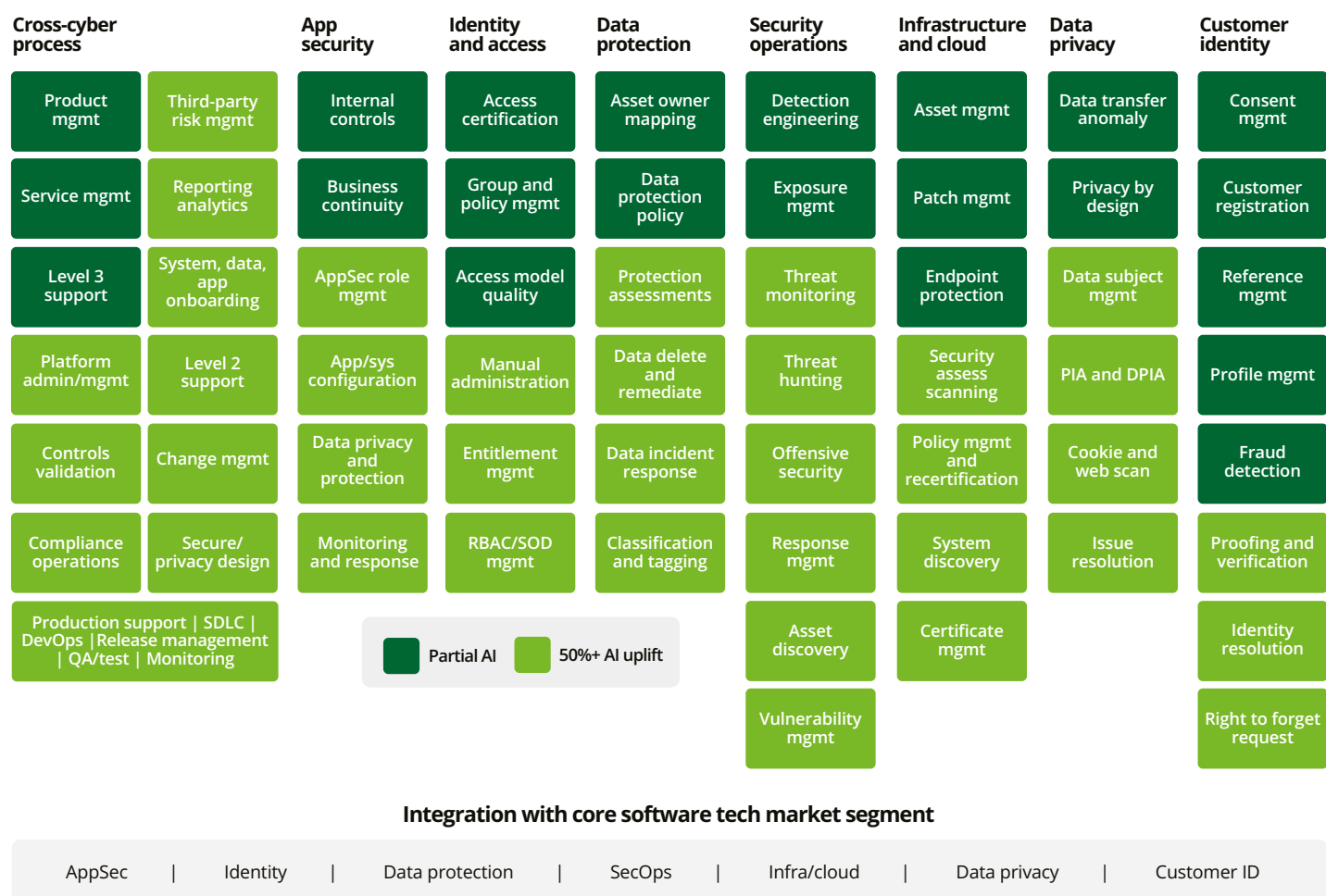
Blueprint for integrated AI security

An effective blueprint for modern cyber strategy begins by breaking down the old siloed model. Instead of treating security as a patchwork of tools and teams, organizations should reimagine it as an interconnected, AI-driven fabric. Many are still burdened by fragmented controls and manual processes, which slow response and create hidden risks.

Embedding AI across security domains spanning applications, identities, cloud, data, and operations fosters active collaboration between people, processes, and technology. AI-driven automation and analytics enable earlier detection, faster coordinated response, and smarter enforcement. For example, anomalous activity flagged in identity management can instantly inform access controls across cloud applications, while intelligent triage dramatically reduces alert fatigue.

This integrated framework is about more than technology—it is foundational to business growth, agility, and trust. A true AI-enabled security blueprint unifies core processes, supports rapid digital scale, and empowers teams to shift from firefighting to strategic oversight. In doing so, organizations move security from a reactive cost center to a proactive enabler of innovation and resilience.

Figure 6. The blueprint: By refactoring the silos of cyber, organizations can simplify and enable AI in the security processes

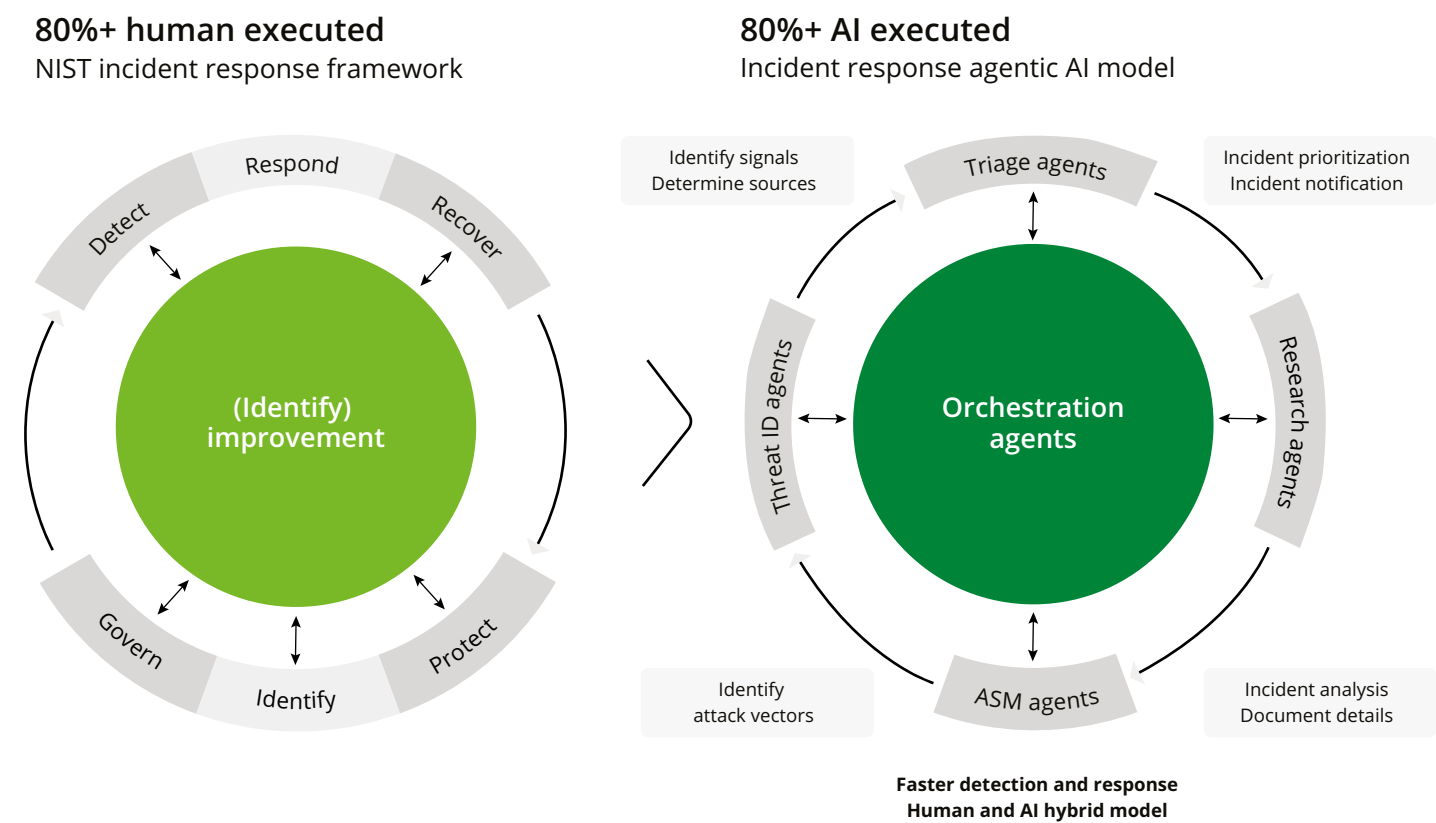


Acronyms are used throughout this figure for readability. Please refer to the Acronym glossary in the appendix for full definitions.

Transformation example using NIST framework

Let's look at a concrete example of this transformation in action. Using the familiar National Institute of Standards and Technology (NIST)¹ Incident Response Framework, we can see the dramatic shift. The agentic AI model can result in faster detection and response times and creates a true human-AI hybrid model in which fatigue is reduced, quality is improved, and human talent is leveraged for the most critical tasks.

Figure 7



Elevating cyber-AI maturity: A call for coordinated action

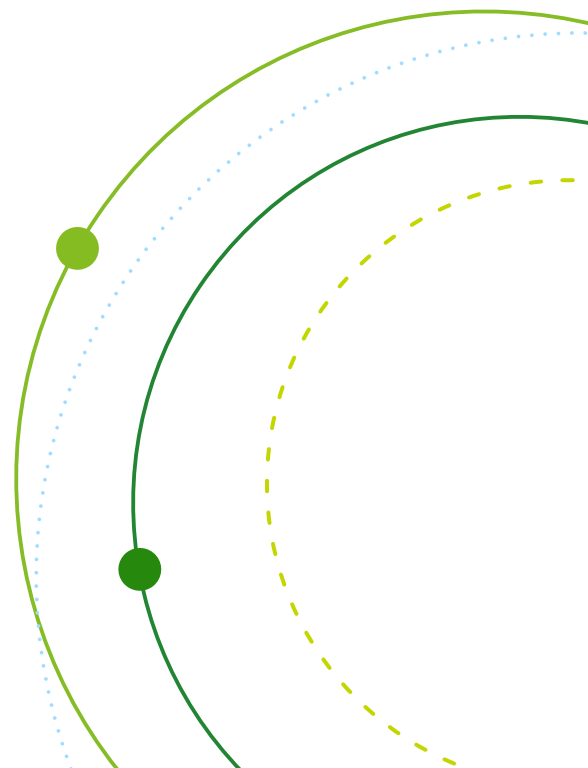
The journey toward an AI-powered cybersecurity function is deliberate; it requires a structured roadmap, organizational alignment, and a commitment to ongoing maturity. With a clear blueprint, organizations can assess their current posture and identify pragmatic steps to advance AI capabilities in security.

Success depends not only on piloting new technologies, but also on aligning cybersecurity with a broad set of enterprise stakeholders and embedding AI-driven practices across the business. The path starts with targeted pilots and policy development, then scales through the integration of AI and cyber strategies into operations, risk governance, and business objectives.

As organizations make this shift, those that act boldly and collaboratively, connecting cyber efforts to enterprise transformation and embracing innovation, may be better positioned to turn cybersecurity into a catalyst for digital trust and sustainable growth. Now is the time to move beyond incremental change and harness the power of integrated, intelligent security to lead in a dynamic risk landscape.

Explore more:

[Reach out to learn how Deloitte can help you design, build, and operate future-ready solutions.](#)



Appendix

admin: administration
AI: artificial intelligence
App: application
AppSec: application security
CASB: cloud access security broker
Cloud: cloud (computing)
DevOps: development and operations
DLP: data loss prevention
DNS: domain name system
DPIA: data protection impact assessment
DSR: data subject request
ID: identifier/identity (context here: customer ID = customer identifier)
Infra: infrastructure
MFA: multi-factor authentication
mgmt: management
PIA: privacy impact assessment
QA: quality assurance
RBAC: role-based access control
ROPA: records of processing activities
SDLC: software development life cycle
SecOps: security operations
SOD: segregation of duties
SSO: single sign-on
Sys: system
WAF: web application firewall

End note:

1. National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework (CSF) 2.0, February 26, 2024.



This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2026 Deloitte Development LLC. All rights reserved.