Gartner

Gartner Insights

2026 Planning Guide for Cybersecurity

William Dupre, Anthony Carpino, Greg Harris, Steve Santos, Mike Huskey, Kevin Schmidt, Odie Adesina, Alex Tytarenko, Richard Bartley, Dennis Xu, Nahim Fazal, Patrick Hevesi, Eric Grenier, Matthew Brisse

2026 Planning Guide for Cybersecurity

13 October 2025 - ID G00832314 - 65 min read
By: William Dupre, Anthony Carpino, Greg Harris, Steve Santos, Mike Huskey, Kevin Schmidt, Odie Adesina, Alex Tytarenko, Richard Bartley, Dennis Xu, Nahim Fazal, Patrick Hevesi, Eric Grenier, Matthew Brisse
Initiatives: Security Technology and Infrastructure for Technical Professionals; Deliver IT and Business Value Through Enterprise Architecture; Meet Daily Cybersecurity Needs

> Political upheaval and AI disruption are impacting the risk landscape for organizations worldwide. Cybersecurity technical professionals must understand the major cybersecurity trends to effectively plan for cybersecurity initiatives in 2026.

Overview

Key Findings

- Geopolitical tensions and regulatory uncertainty are creating a more volatile and unpredictable risk landscape for chief information security officers (CISOs) and their teams. Protecting data, applications, and corporate resources in such an environment is not just a challenge, but an escalating struggle. The ever-changing cybersecurity vendor landscape only exacerbates the problem.
- Organizations are focusing too much on sophisticated attacks and not enough on basic cybersecurity hygiene and incident response practices. This oversight leaves them exposed to ransomware and account takeover risks.
- Disruption from organizationwide adoption of AI continues to put pressure on cybersecurity teams. Lenient organizations may suffer from AI-native risks, such as sensitive data loss through insecure prompts and use of harmful or biased output. By contrast, a strict approach can stifle AI innovation.
- Managing the various aspects of an incident continues to overwhelm incident responders. This situation exposes organizations to employee turnover, fatigue, overlooked events, and a lack of overall institutional resilience.

Recommendations

- Adapt cybersecurity to respond to geopolitical and technology risks by adopting cybersecurity architectures that increase organizational resilience. These include security by design, zero trust and cybersecurity mesh patterns.
- Include attack surface reduction approaches as part of a new defense-in-depth strategy. Execution will involve implementing hardening baselines and continuous threat exposure management (CTEM).
- Improve application security practices by prioritizing software supply chain security and implementing secure-by-design principles for all application development, including AI products.
- Implement security controls for AI consumption across the organization. Provide end-user training and technical controls, such as security service edge (SSE) and specialized AI protections, to prevent sensitive data leakage to unauthorized AI SaaS applications.
- Implement AI security operations center (SOC) agents to minimize risks from missed threat identification and to increase SOC automation and task efficiency.

Cybersecurity Trends

Geopolitical challenges continue to provide a backdrop for global cybersecurity risk, with kinetic conflicts, cyberattacks, and policy uncertainty affecting organizations directly and indirectly through third parties. According to the 2025 Gartner Agenda Poll for Chief Information Security Officers (CISOs), 60% of CISOs see macroeconomic volatility and uncertainty as a challenge to meeting strategic objectives over the next six months. [1]

Cybersecurity teams are also addressing disruptions and potential opportunities resulting from the proliferation of artificial intelligence (AI) capabilities. The technical upheaval caused by the extensive use of these technologies, which are increasingly employed by attackers and misused by internal staff, exposes organizations to various forms of risk. However, the same technologies also proffer enormous opportunities for organizations, including cybersecurity teams. Gartner's Agenda Poll also found that 48% of CISOs have little to no confidence in their organization's ability to establish AI risk and value metrics. [1]

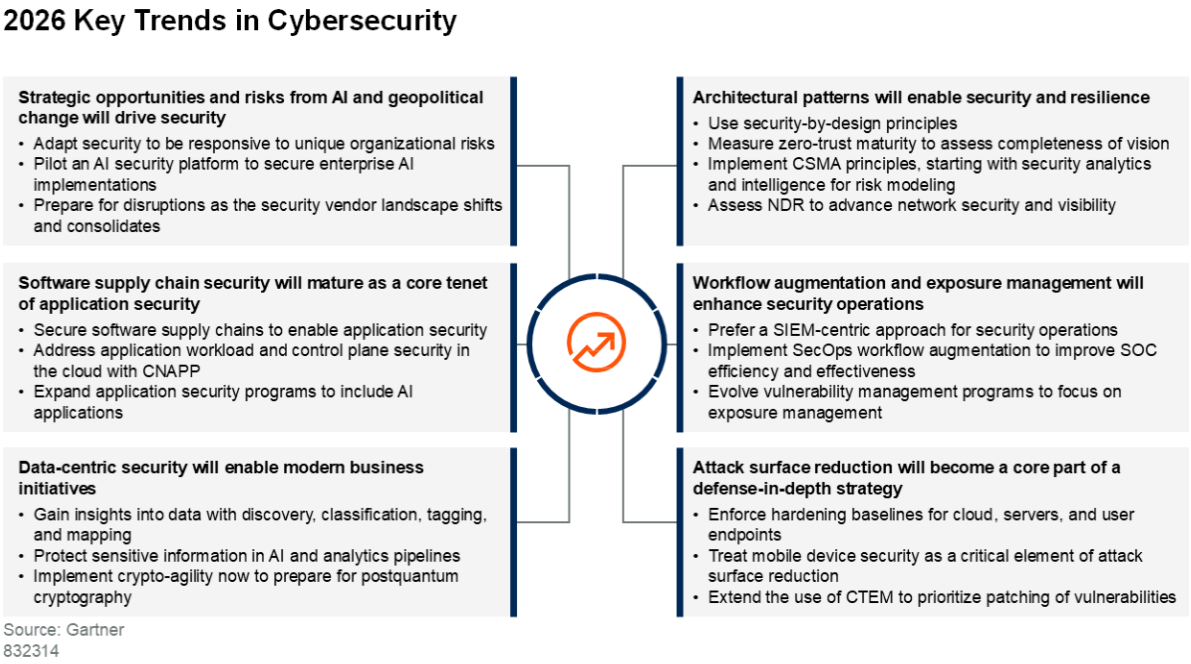
In summary, strategic concerns impacting cybersecurity include:

- Technical security strategy lacking architectural approaches that enable organizational resilience

- Risks to applications and data not being addressed holistically
- Emerging cybersecurity concerns around AI technology consumption and development of AI applications, including agentic capabilities
- Organizational resilience plans that don't include exposure management (EM) and SecOps augmentation capabilities

In light of these concerns, Figure 1 lists Gartner's six key cybersecurity trends for 2026, along with associated planning considerations for organizations.

Figure 1: 2026 Key Trends in Cybersecurity



The planning considerations for 2026 cover a range of cybersecurity controls within each trend. There are considerations for controls ranging from basic hygiene and monitoring to highly advanced capabilities. Some of last year's recommendations have evolved to provide a steady foundation for advancing maturity.

Gartner provides a maturity assessment to evaluate the capabilities of a cybersecurity program, determine where improvements will add business value, and develop a roadmap to ensure that an organization balances cyber risk against business outcomes. (See IT Score for Security and Risk Management for details.)

This Planning Guide focuses on the current key challenges in cybersecurity. The subsequent sections expand on the trends identified in Figure 1. The relative importance of each trend, and its related planning considerations, will depend on an organization's current maturity in digital business and IT, as well as its security posture.

As noted above, the six key cybersecurity trends that require focus in 2026 are (click links to jump to sections):

- Strategic opportunities and risks from AI and geopolitical change will drive security.
- Architectural patterns will enable security and resilience.
- Software supply chain security will mature as a core tenet of application security.
- Workflow augmentation and exposure management will enhance security operations .
- Data-centric security will enable modern business initiatives.
- Attack surface reduction will become a core part of defense-in-depth strategy.

Strategic Opportunities and Risks From AI and Geopolitical Change Will Drive Security

Back to top

An organization's security technology program is driven by internal and external influences. Internal influences include budget challenges, technical debt, and transformation demands. External ones include geopolitics, regulations, and vendor consolidation concerns. AI technology usage is increasing risk, and without effective governance and security controls, it will have damaging unforeseen impacts on organizations.

Open warfare, trade disputes, nationalism, and their human and economic impacts will continue to add to cybersecurity challenges. Policy uncertainty has the potential to impact cybersecurity programs, both regionally and globally (where it may become impossible to implement cybersecurity successfully with common tools).

Organizations may be the direct target of a cyberattack or become collateral damage in a more widespread attack. Geopolitical cybersecurity risks may manifest as supply chain impacts, because partners and trusted third parties may be affected. Cybersecurity attacks may take the form of direct malware attacks, attacks on cloud infrastructure, and attacks on system integrity and availability — such as distributed denial of service (DDoS) attacks, ransomware, and data theft or loss.

As geopolitical uncertainty continues and AI usage expands the technological attack surface, cybersecurity teams must become the trusted partner that helps their organizations navigate the coming increase in cyber risk.

The hype and potential of AI technologies are having a substantial impact on strategic business planning as organizations scramble to understand and identify how AI can benefit them. Cybersecurity technical professionals want to leverage the benefits of AI, but they have not really accounted for the risks posed by these technologies. Cybersecurity governance is necessary to temper expectations and to limit users' ability to expose corporate data. AI-enhanced tools must be verified and secured before they are used to support organizational goals.

Given this trend, organizations should focus their 2026 cybersecurity efforts on the following activities (click links to jump to sections):

- Adapt security to be responsive to unique organizational risks.
- Pilot an AI security platform to secure enterprise AI implementations.
- Prepare for disruptions as the security vendor landscape shifts and consolidates.

Planning Considerations

Adapt Security to Be Responsive to Unique Organizational Risks

Back to top | Back to planning considerations list

Organizations, even if not directly targeted, can be impacted by a host of geopolitical risks. For example, organizations using offshore sourcing models for application development or incident response services must factor in risks to the wider supply chain. Increased geopolitical tension will result in a continuously changing threat landscape, with targeted and disruptive attacks becoming more likely. Organizations must not only prepare and audit their own cyber resilience plans, but also do the same for every part of their supply chain. Many geopolitical risks impact organizations via their physical and software supply chains.

Significant cybersecurity challenges from geopolitical risks include:

- System availability risk due to isolated and focused operations in specific geographies
- Reduced business agility due to manual processes creating a lack of responsiveness to the increasing pace of change
- Increased supply chain threats (both physical and software) proving to be sources of cybersecurity risk
- Incident response mechanisms lacking robustness to handle the diversity of geopolitical risk events
- Data fragmentation and increased nationalistic tendencies creating onerous legal, regulatory, and bureaucratic challenges
- Inability to track relevant threats due to the complexity of geopolitical risk
- Lack of visibility into diverse and global services and systems, leading to potential blind spots ripe for exploitation
- Insufficient or out-of-date resilience plans that are unable to address relevant geopolitical challenges

Figure 2 illustrates approaches to being more resilient to geopolitical risks.

Figure 2: Resilience to Geopolitical Events

Related Research

- How to Manage Concentration Risk in Public Cloud Services
- How Recent Geopolitical Risks Will Impact Cloud Contracts and Costs
- Technical Brief: How to Plan and Execute an Emergency EPP Migration
- Cloud Security Requires Refined Incident Response Strategies
- The Israel-Iran Conflict: Risks to Assess

Pilot an AI Security Platform to Secure Enterprise AI Implementations

Back to top | Back to planning considerations list

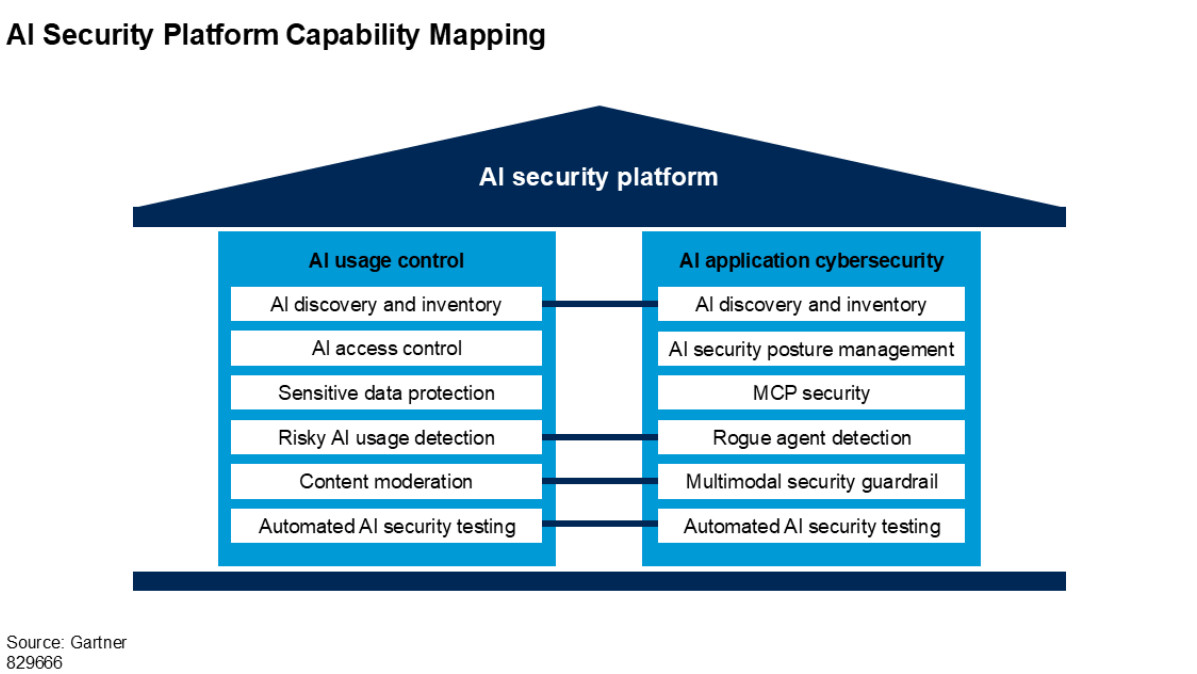
AI's rapid rise has introduced a number of native security risks that have led to concerns about employee usage of third-party services and considerable AI project delays. To address these issues, cybersecurity teams must explore AI security platforms (AISPs).

AISPs have emerged as a critical solution to defend against AI-native security risks. As shown in Figure 3, such platforms typically focus on two pillars: AI usage control (AIUC) and AI application protection (AIAP). AIUC secures third-party AI usage, while AIAP protects custom-built AI applications. A large number of vendors are emerging in this space with products to help reduce AI-native security risks.

AIUC is a technology to discover the use of third-party AI and enforce the security policies of an organization. Capabilities include discovery and categorization of third-party AI consumed as a service, installed within applications, or embedded within applications. AIUC defines and enforces usage policies, inspects content for sensitive data, assesses risk, and raises alerts on anomalies.

AIAP provides visibility into custom-built AI applications, scans downloaded models to identify malicious artifacts, and provides input and output guardrails to protect custom-built AI applications from AI-native threats. These solutions can also perform automated security testing to ensure custom-built AI applications are resilient against prompt injection attacks that could lead to undesired output or rogue actions by AI agents. AIAP can also trace communications between an AI agent's internal components and external entities to identify when high-risk actions are being taken (see Figure 3).

Figure 3: AI Security Platform Capability Mapping



Source: Gartner
829666

Gartner

Related Research

- Top Strategic Technology Trends for 2026: AI Security Platforms
- Use an AI Security Platform to Launch Your AI Security Strategy
- AI Security Platforms Are Core to Cybersecurity Revenue Growth Strategy

- Top 5 Microsoft 365 Copilot Security Risks and Mitigation Controls
- Generative AI Adoption: Top Security Threats, Risks and Mitigations

Prepare for Disruptions as the Security Vendor Landscape Shifts and Consolidates

Back to top | Back to planning considerations list

Vendor landscape disruption caused by consolidation and megaplatforming efforts is impacting how organizations are choosing and implementing cybersecurity tools. In certain areas of the security vendor landscape, this consolidation makes sense. It builds toward integrated sets of tools to provide a wider and greater set of capabilities, such as cloud-native application protection platforms (CNAPPs) and secure access service edge (SASE). Meta-architectural approaches, such as cybersecurity mesh architecture (CSMA), are evolving to actively seek out consolidation and integration of all security tooling. However, this strategy can backfire when vendors attempt to create an unrealistic all-in-one solution by adding all sorts of peripheral capabilities aimed at attracting clients in difficult and competitive markets.

Organizations need to plan for procurement, support, and license changes as vendor consolidation continues. Partnerships will change and will require a rethinking of current catalogs and toolsets. As the trend continues, organizations should plan for the risks of vendor concentration and the resiliency impacts from single points of failure. Other actions to consider include:

- Prioritizing organizational outcomes and capabilities by defining clear requirements, focusing on cybersecurity needs, and not getting distracted by market churn
- Assessing whether current vendor relationships can meet future needs by working with existing vendors to understand their product/platform roadmap and vision
- Evaluating where a best-of-breed approach is justified and where a converged solution, with some threshold of effective tool components, is sufficient

Related Research

- How to Manage Concentration Risk in Public Cloud Services
- Technical Brief: How to Plan and Execute an Emergency EPP Migration

Architectural Patterns Will Enable Security and Resilience

Back to top

Security and resilience are not mutually exclusive. Modern deployment patterns, such as cloud deployments, enable organizations to achieve both objectives across a complex and evolving environment. However, these environments are dynamic and ever-changing, so cybersecurity teams must be able to identify gaps resulting from new IT strategies, such as AI development, deployment, and enablement. Also, overlapping and misconfigured security controls create operational downtime risk and a false sense of security if left unattended.

It is increasingly difficult to overlay the right controls across these heterogenous and changing environments — no one-size-fits-all solution exists. A range of options are possible, including niche tools, broad cybersecurity platforms, and native provider security, each claiming to offer protection for various potentially overlapping areas of control. However, this strategy can backfire when vendors attempt to create an unrealistic all-in-one solution by adding all sorts of peripheral capabilities aimed at attracting clients in difficult and competitive markets.

Cyber resilience: *The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.* [2]

Actionable, objective insights

Position your IT organization for success. Explore these additional, complementary resources and tools for security leaders and their teams:

Guide

Cloud Security: Understand, Mitigate and Manage Risk Types

Achieve reliable, secure and efficient protection for all your cloud-based needs.

Download Now

Insights

Cybersecurity Management for Technical Professionals

Access action plans for the key trends for cybersecurity architects.

Learn More

Webinar

Strengthen Zero Trust Data Strategies for Enhanced Protection

Embrace strategies that strengthen data security in today's digital landscape.

Watch Now

Tool

Gartner Cybersecurity Controls Assessment

Measure the maturity of controls implementation against leading frameworks and standards.

Learn More

Already a client?
Get access to even more resources in your client portal. Log In

Connect with us

Get actionable, objective business and technology insights that drive smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Technical Professionals
gartner.com/en/gartner-for-technical-professionals

Stay connected to the latest insights

Attend a Gartner conference
View Conference

Gartner®