Cyber Trends Report

7 cybersecurity trends for 2026

SHI | stratascale CYBERSECURITY DIVISION OF SHI | CYBERSECURITY DIVE

Custom content for SHI from Studio by Informa TechTarget

Every few years, cybersecurity seems to hit an inflection point when all the old playbooks have to be rewritten. **2026 promises to be one of those years.**

AI is accelerating innovation, but its adoption is also expanding the attack surface, exacerbating identity sprawl, increasing data exposure risks, and pushing development teams to double down on secure tools and processes. Geopolitical tensions are driving more nation-state level threat activity, with these sophisticated attackers now targeting a growing number of commercial entities alongside the public sector and critical services. At the same time, economic uncertainty is raising questions about revenue projections and future budgets.

CISOs and security teams must continue to mature their programs and practices. Supply chain risks keep growing as attackers leverage widely-used software to try to gain a foothold in thousands of environments at once. And the time window between a vulnerability's initial public disclosure and its first exploitation has shrunk from days to hours, driving a need for faster event triage, more accurate investigation, and accelerated response. But figuring out how to achieve this isn't easy. It's hard to know which tools work best, or which vendors' claims accurately map to current needs. The cybersecurity marketplace is as crowded and complex as it has ever been, even as the largest companies make high-profile acquisitions in their efforts to win the "unified platform" game.

Navigating what's on the horizon

In this report, experts from SHI will outline cybersecurity trends for 2026. These are senior security leaders with decades of experience consulting with organizations across industries and developing roadmaps for Fortune 1000 companies. With backgrounds as practitioners, researchers, engineers and technical advisors, they bring hands-on experience as well as strategic acumen to every one of their engagements. Combined, they work with hundreds of companies every year.

This report will take a look at where our industry is right now, so that we can better predict where it's likely to be heading. We'll especially focus on how AI is transforming cybersecurity — and how forward-thinking leaders can build and mature their security programs for an AI-first world.

With the right strategy, robust security doesn't have to slow down business innovation. And embracing AI doesn't need to mean accepting more risk. But balancing these objectives requires forethought and continuous planning. SHI experts can provide guidance and support from a solution's inception through operationalizing it in production.

When everything becomes AI-driven

Since the launch of ChatGPT in November 2022, generative AI has taken the world by storm. This technology continues to see rapid adoption in enterprise environments, even while debates rage about how quickly implementers can realize ROI on new generative AI solutions.[1] In 2026, the momentum that started with generative AI will keep building, but early adopters are already looking for the next rising trend.

At present, the focus is on AI agents. While generative AI creates content in response to user prompts, agentic AI can autonomously execute complex, goal-oriented workflows with little to no human intervention. Agentic AI systems comprise intelligent agents that can reason, plan, and act independently, completing entire business processes on their own. Agentic AI adoption is currently proceeding at breakneck speed. Analysts forecast that the market for agentic AI systems will grow 175% each year for the next half decade, placing it among the fastest-growing market segments in the history of enterprise technology.[2]

For cybersecurity leaders and practitioners, the AI boom is both an opportunity and a concern. On the one hand, threat actors are weaponizing AI to make their attacks faster, more scalable, and harder to detect. On the other, AI promises to revolutionize security operations (SecOps), turning reactive, event-driven processes into highly efficient, proactive, automated defenses. To further complicate matters, AI systems themselves are becoming a top attack target, with model theft, training data poisoning, and prompt injection attacks all increasing dramatically over the past year.[3]

175%

Analysts forecast that the market for agentic AI systems will grow 175% each year for the next half decade, placing it among the fastest-growing market segments in the history of enterprise technology.[2]

Regardless of their feelings about AI — excitement, trepidation, ambivalence — security stakeholders cannot afford to ignore this technology's impact on their industry. But this isn't always clear-cut.

Organizations should consider the impact of AI in their planning. Building a team with expertise across IT operations functions to support AI initiatives can mitigate many of this technology's risks. This team should include core members from compliance, risk, cyber infrastructure, and application development, and it should be empowered to set cross-organizational standards. Creating a reference architecture for AI applications helps ensure consistency in adoption while business leaders build out broader AI policies.

No. 01

Doubling down on NHI security

Identity is the next cybersecurity frontier

Analysts, leaders, and practitioners widely recognize that the rapid proliferation of AI agents is challenging security teams' ability to govern and control non-human identities (NHIs). As the recent acquisition of CyberArk by Palo Alto Networks makes clear, major industry players see an enormous market opportunity in the emerging category of security for agentic AI.[4]

> Ephemeral identities and those associated with AI agents are directly contributing to the expansion of the attack surface and introducing new risks. We expect organizations will move to acquire tools to give them visibility into how these identities are being leveraged, what access they have, and whether or not they've been tampered with. The concept of just-in-time access can go a long way in this space.

Brad Bowers,
Field Chief Information Security Officer – Global, SHI

Nonetheless, the underlying challenge that agentic AI adoption magnifies — and casts a spotlight on — is not new. For years, NHIs (including bots, service accounts, virtual machines, API keys, and OAuth tokens) have outnumbered human identities in most enterprises. Even conservative estimates put the ratio at roughly 17,000 NHIs for every 1,000 employees.[5] AI agents merely spawn additional NHIs, often with broad and persistent access to sensitive data and applications across multiple systems.

Today's most commonly deployed identity security solutions, such as Identity and Access Management (IAM), Identity Governance and Administration (IGA) and Privileged Access Management (PAM) generally lack the ability to discover — or maintain full visibility into — NHIs across the organization. New vendors are emerging with solutions that promise to govern all aspects of the rapidly-expanding NHI ecosystem, while established players in the identity security space are attempting to apply technologies they've already built to the NHI problem. This market will likely see further growth in 2026.

Boosting NHI security

When it comes to securing NHIs, the challenge is clear: We already know what identity security best practices are for people (multi-factor and passwordless authentication, just-in-time access, etc.), but how can we extend these policies and protections to software? To strengthen your organization's ability to govern and manage NHIs:

01

Take an architectural approach to NHI security. This means embedding security controls and mechanisms to enforce policies directly into the foundational fabric of your security and IT infrastructure, including cloud workloads, application frameworks, network underlays, and DevOps pipelines. Your organization will need to establish its own definition of "NHI" since there are many types and forms of these "identities." Ensure you have appropriate tooling (or integrated solutions) to identify, understand, and prioritize NHI security issues.

02

Leverage automation wherever possible in NHI lifecycle management. Automating NHI provisioning, credentialing, and decommissioning helps eliminate "orphan" machine identities and ensures that permissions will be revoked whenever they're no longer needed.

03

Robust NHI governance may require integrating multiple solutions. Identity security platforms that can enforce policy-based access controls, limit credential lifespans, and unify the management of human and non-human identities cannot always discover and catalog all NHIs within an environment. For full-lifecycle NHI governance, organizations may need to integrate existing secrets management, IGA, PAM, and cloud identity and entitlements management (CIEM) solutions with specialized NHI discovery and management platforms.

No. 02

Futureproofing data protection

> The core question in data governance is: "Who should have access to which data?" Policies should be set based on your answers to that question.
>
> AI doesn't change this. AI systems are just doing what they were designed to do — gather all the information that's relevant to your prompt, ask for more, get smarter, and feed you the results. With strong governance in place, access rules should seamlessly carry over to AI engines, so that people are still granted only the access they should have.

David O'Leary, Senior Director of Cybersecurity – Financial Services, SHI

AI's role in data security: A double-edged sword

Protecting sensitive, confidential, and regulated data continues to be a top priority for organizations of all sizes. Like many aspects of cybersecurity, data protection is being made both easier and more difficult by widespread AI adoption. It's become all too common for AI agents and generative AI systems to expose data that they shouldn't be able to access. Recent research indicates that the number of data security incidents related to generative AI more than doubled in the first few months of 2025, now accounting for nearly 15% of sensitive data exposures.[6]

This isn't something new, but instead an example of AI adoption drawing attention to pre-existing issues with data governance. Organizations that had not built out a set of robust, least privilege-based access controls for their protected and sensitive data are finding that tools like Microsoft Copilot significantly increase the risk that information will be made available to unauthorized individuals.

If AI adoption complicates data protection by opening new avenues for data exposure, it also has the potential to simplify it by automating the discovery and classification of sensitive data. AI-powered solutions can map all the data in use within the organization with minimal manual effort, identifying which employees have access to protected information. AI enables contextual understanding, so that data security teams gain a much more nuanced view of the data flows within and across their organizations.

DLP to DSPM

Data loss prevention (DLP) — a technology designed to stop unauthorized data exfiltration or leakage by enforcing static policies and blocking or alerting on data movements that appear risky, based on pattern matching — is still widely deployed. Market analysts report, however, that the category of Data Security Posture Management (DSPM) is growing much more quickly than DLP, especially for new deployments.[7]

DSPM supports automated data discovery and classification across hybrid and multi-cloud environments. Many solutions also conduct real-time risk assessments, and some provide a foundation for automated remediation of data security risks. The movement to enhance data security capabilities and combine DLP functionality with DSPM capabilities stems at least in part from a growing need to gain better visibility into data — at rest and in motion — and access permissions across increasingly complex technology ecosystems. DLP and DSPM can both play a role in a mature data security architecture. DLP needs to be applied across all environments, including within Microsoft Purview, within secure access service edge (SASE) and secure service edge (SSE) deployments, and within email security gateways.

A recipe for successful data protection

The following four best practices support robust data security:

01 **Implement policy-based controls to ensure that only employees whose jobs require it have access to restricted data.**

02 **Use encryption or obfuscation to protect sensitive data both at rest and in transit. DLP and/or DSPM tools can help you identify the data that should be encrypted.**

03 **Adopt an architectural approach, where data discovery, protection, and exfiltration prevention capabilities are integrated across the entire organization, improving visibility and supporting consistent policy enforcement.**

04 **Implement continuous monitoring capabilities, including logging, analytics, and real-time alerting on anomalous activities.**

Where AI can help in data protection:

Data discovery:
AI tools can identify sensitive information located across the organization's repositories, including in cloud warehouses, on-premises databases, object storage, and file stores.

Data classification:
AI and ML models can perform contextual analyses to automatically sort data into categories such as personally identifiable information (PII), patient health information (PHI), financial data, and intellectual property, and then apply tags or labels.

Data risk analysis:
Models can assign risk scores to data based on traits like sensitivity, exposure, and typical access patterns. AI solutions can also monitor for security policy violations and compliance risks.

No. 03

Spotlight on supply chain security

Ongoing supply chain risks

No modern application could exist without relying on other software. A software supply chain is the entire catalog of components, tools, and services used to develop, build, and deliver production applications. This supply chain includes everything from open-source libraries and repositories to vendor packages, CI/CD pipelines, third-party distribution channels, and runtime environments. Other parts of the software supply chain that are sometimes overlooked include firmware for appliances and computing devices. Firmware security concerns are currently on the rise.

Threat actors have long targeted supply chains, but these attacks have significantly increased in scale and impact over the past year, continuing to set new records.[8] Their targets span verticals from FinTech to SaaS and beyond, including a recent high-profile breach affecting more than 600,000 network security devices.[9]

Managing software supply chain risks should be considered alongside software asset management and hardware lifecycle management. These practices can help stakeholders keep track of vulnerabilities as the organization acquires new assets and decommissions old ones.

AI ups the ante

As is the case for many other aspects of cybersecurity, AI is transforming software supply chain risks. As organizations race to build and deploy new AI applications, there's danger in moving too quickly and without adequate guardrails. Many AI systems depend on upstream open-source libraries, pre-trained models, and external datasets, all of which can be compromised or poisoned.

New open-source collaboration and code-sharing platforms — like Hugging Face, which is focused on natural language processing (NLP) and ML models — have become prominent almost overnight. These platforms are widely used to source datasets, models, and full applications, making them highly attractive attack targets. Even a minor AI supply chain compromise can quickly propagate across organizations or entire industries because of the interconnected nature of these tools. This is both a software supply chain concern as well as an application development concern. Teams from both areas of the business should share responsibility for managing these risks.

Strategies for strengthening supply chain security

Organizations are already familiar with most best practices for safeguarding software supply chains. There aren't significant differences for the AI era, even if the risks are more pronounced.

01

Vet vendors with care.
Limit suppliers to those that have undergone thorough review. Document all supplier relationships and ensure that your vendors can comply with your organization's security standards.

02

Include security requirements in contracts.
Require vendors to meet specific, clearly-outlined expectations when it comes to their data and security practices, as well as service-level agreements (SLAs) for incident notification and collaborative response.

03

Emphasize traceability.
Maintain a real-time software bill of materials (SBOM) for all applications built or running in your environment. This inventory should include dependencies, libraries, versions, and upstream sources, making it easier to identify and remediate vulnerabilities upon disclosure.

04

Perform ongoing monitoring.
Continuously monitor the security posture of all third-party vendors and software, leveraging automated tools and an industry-standard, risk-based framework.

05

Extend these principles into the physical realm.
It isn't only software that can be compromised. Source hardware only from OEMs and reputable, authorized distributors. Ensure that your suppliers maintain end-to-end chain-of-custody records, and inspect all hardware and packaging upon arrival. Leverage firmware validation tools to ensure that devices load only authorized, unmodified code at startup.

No. 04

Continuing the drive for platformization

The crowded cybersecurity marketplace

If AI has sped up software development, it also has the potential to accelerate the launch of new product companies. This trend is apparently being realized in the cybersecurity space, where early stage and pre-seed momentum remains high.[10] Based on promising innovations in AI, cloud, and data security, new companies continue to be born, joining a market that was already crowded and noisy.

It's estimated that there are more than 4,500 vendors in the ecosystem, spanning market segments ranging from email and identity security to threat intelligence and forensics, and well beyond.[11] Of course, an entirely accurate count is impossible to make, since company launches and failures — along with acquisitions — happen on a daily basis.

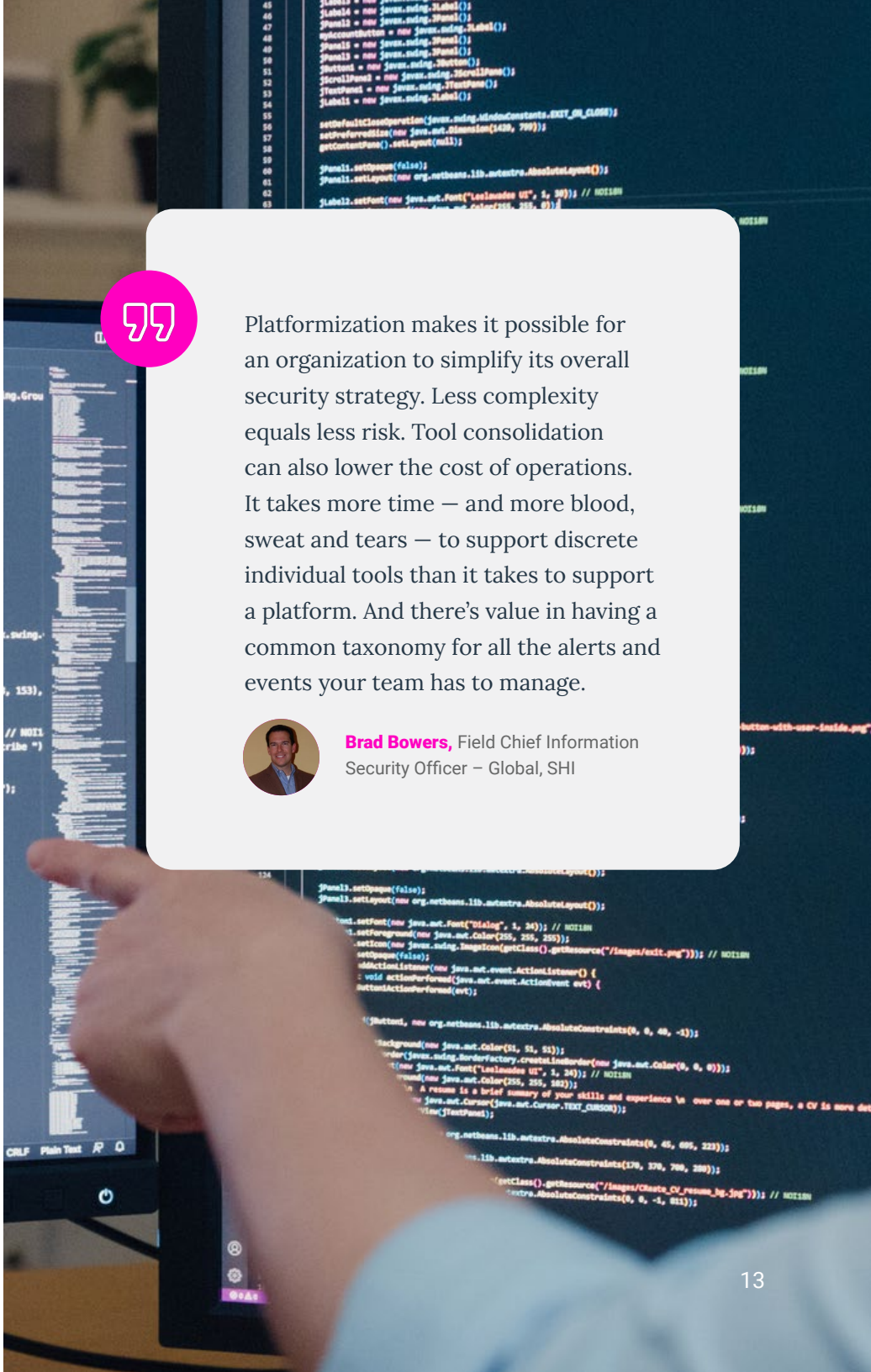
For most of the past two decades, "best-of-breed" — selecting a different specialized point solution to address each specific security need — was considered a procurement best practice. Adding another point solution to solve each new cybersecurity challenge or counter every emerging threat inevitably led to complex tool stacks that were difficult to integrate and operate, and costly to maintain. Today, growing numbers of organizations are adopting the holistic platform approach, where multiple tools and capabilities are consolidated into a single vendor's unified solution.

Vendor consolidation gathers steam

Currently, about 65% of the total cybersecurity market belongs to only seven companies, each with a market capitalization of over $10 billion.[12] In response to growing demand for platformization — and to enhance capabilities to respond to more complex threats — this handful of companies has been buying up smaller and younger competitors at a record pace. 2025 was one of the most active years in history for cybersecurity acquisitions, with deal volumes on pace to exceed 2024's by 10%.[13]

Among the biggest blockbuster deals of the year were Google's acquisition of cloud and AI security company Wiz for $32 billion and Palo Alto Networks' purchase of identity security company CyberArk for $25 billion.

So many acquisitions have taken place over the past five years, that it's now possible for individual platform vendors to deliver something close to "best-of-breed" in a single solution. As this trend has gathered momentum, growing numbers of large enterprises — and organizations with advanced security maturity — have adopted the single-platform approach in the hopes of simplifying cybersecurity operations.



> Platformization makes it possible for an organization to simplify its overall security strategy. Less complexity equals less risk. Tool consolidation can also lower the cost of operations. It takes more time — and more blood, sweat and tears — to support discrete individual tools than it takes to support a platform. And there's value in having a common taxonomy for all the alerts and events your team has to manage.

Brad Bowers, Field Chief Information Security Officer – Global, SHI

Navigating the current market landscape

Consolidating on a single cybersecurity vendor's platform can have both benefits and drawbacks. The one-platform approach may improve visibility and efficiency while reducing complexity and costs. But being dependent on just one vendor can also create risk, leaving customers vulnerable if that vendor experiences an outage or breach. It can also limit flexibility if an organization wants to integrate solutions from other providers in the future.

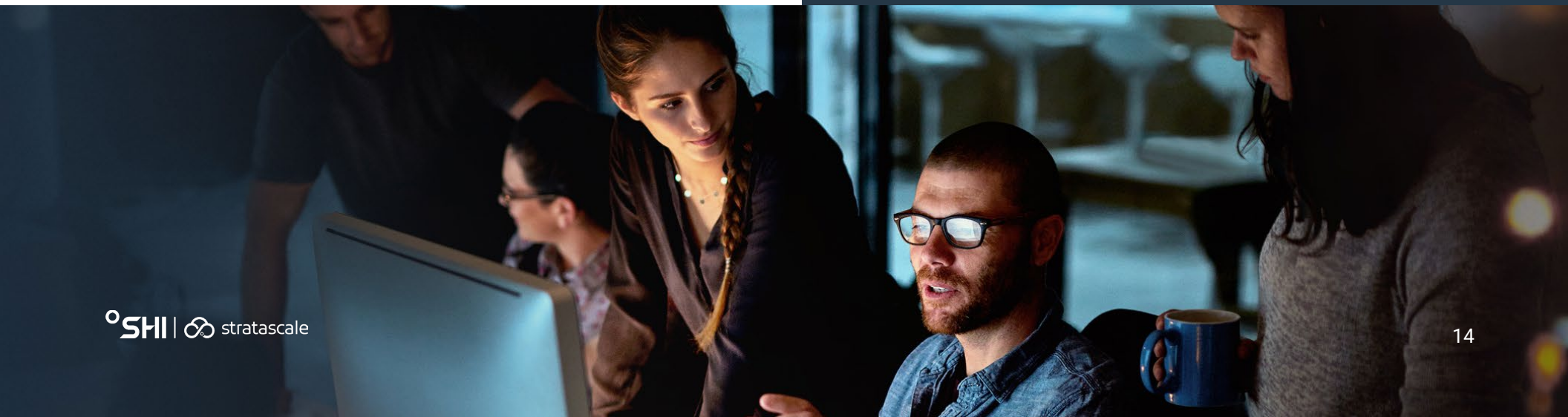
Although growing numbers of organizations are pursuing platformization, not everyone stands to gain from adopting this approach. Being able to meet complex operational, governance, and compliance requirements within a single solution demands a significant level of cybersecurity maturity. And even among organizations with highly mature SecOps programs, not all will find the single-vendor approach to be a good cultural fit.

Point solutions vs. unified Platform: Key questions to ask

If you're evaluating these two approaches to determine which is the better fit for your organization, ask yourself the following questions:

1. Which point solutions do you currently have?
2. How much are you paying for them?
3. How does this compare with platform pricing?
4. What kinds of workflows do you have in place to support those solutions?
5. How extensive are the process changes you'll need to make to onboard the new platform?

Cost optimization tools are available to help you evaluate the financial aspects of tool rationalization, but your team's preferences and flexibility should also be a consideration.



No. 05

Quantum readiness

Preparing for the arrival of quantum computing

Technology's advance is relentless, with the broad availability of quantum computers — which will be able to solve complex problems much faster than today's fastest supercomputers — now on the horizon. Experts differ in their forecasts of when systems capable of breaking today's cryptographic protections will become available, but nearly all agree that they're coming.[14]

Even though general-purpose quantum computing is unlikely to arrive in the next few years, threat actors are already harvesting and storing encrypted traffic with the goal of decrypting it once a cryptographically relevant quantum computer (CRQC) becomes available. For this reason, federal agencies such as NIST and CISA are urging all organizations to begin preparing immediately by creating a quantum-readiness roadmap.[15] Other sector-specific authorities, including the Financial Services Information Sharing and Analysis Center (FS-ISAC) explicitly call for organizations to begin upgrading their infrastructure and launching post-quantum pilot projects now, so that they will be ready to implement quantum-safe algorithms before transition deadlines.[16]

What is quantum readiness?

All organizations must be prepared to migrate away from today's cryptographic practices to quantum-safe data protection before quantum computing becomes broadly available. This requires technical, architectural, and governance changes, so that encryption, certificates, and key management systems can be upgraded without disruption. It's often referred to as encryption agility (or "crypto-agility"), since it means readying systems to swap encryption algorithms quickly as standards evolve.

Developing a quantum readiness plan

01

Start with an inventory and risk map.
Identify all the places in your environment where cryptography is currently used, including TLS certificates, public key infrastructure (PKI), databases, backups, and code signing, and determine which would be most vulnerable to direct attacks or “harvest now, decrypt later” risks.

02

Begin building quantum readiness into your architecture.
Re-design infrastructure (including key and certificate management systems) so that algorithms and keys can be changed without full re-platforming. Treat quantum readiness as a long-term architectural requirement, not a one-off project.

03

Embed quantum readiness into policies and governance.
Ensure that crypto-agility is included in your procurement standards, vendor qualification processes, and hardware lifecycle management procedures, so that you can avoid accumulating a new form of technical debt by adding systems that can’t easily be adapted for post-quantum computing (PQC) later.

> Right now, the biggest push in quantum readiness is certificate lifecycle management. Regulators want organizations to be able to rotate their certificates much more often, as well as increase the strength of their cyphers. We don’t really know when today’s cyphers will be broken, but it’s like an arms race. Getting ahead means being able to change out certificates without impacting your environment. The longer you wait, the more risk you’ll face.

Philip Armbrust,
Senior Director of Presales Engineering, SHI

Automation: The key to crypto-agility

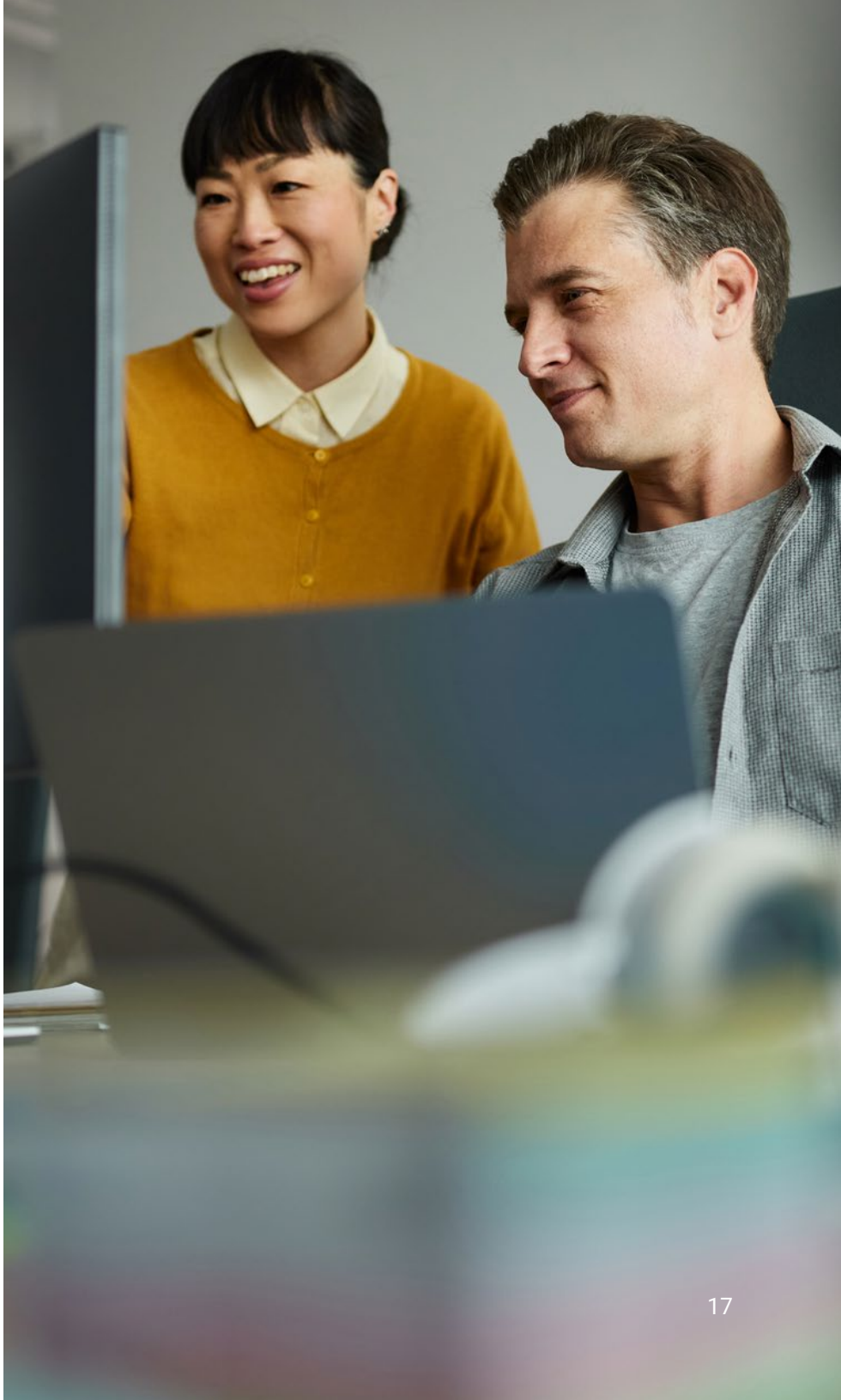
Building quantum readiness across a large and complex environment isn't easy, but it's a place where automation can really help. By leveraging automation, organizations can change keys and algorithms far more quickly — and with less disruption — than if they were doing this manually.

Automation makes it easier to:

- **Figure out where cryptography lives.** Organizations may have thousands if not millions of certificates and keys across clouds, on-premises infrastructures, devices and third-party applications Automated discovery makes it possible to create a living inventory of cryptographic assets — one that stays up-to-date even as the environment changes.

- **Rotate certificates at scale.** Manual key and certificate management is slow and error-prone. Automating lifecycle management enables teams to roll out new algorithms quickly, so that vulnerable, outdated, or noncompliant certificates can be replaced in a timely manner.

- **Enforce policies and guardrails.** Automation and orchestration make it possible to translate policies into effective controls by, for instance, scanning for noncompliant certificates, auto-remediating misconfigurations, and blocking deployments that violate standards before they go live.



No. 06

Transforming security operations

Reimagining SecOps for the AI era

The idea that threat actors are using AI, so defenders must adopt it if they are to keep pace has become an often-repeated truism among cybersecurity vendors. There's truth to it, of course. Recent research indicates that the average time between a vulnerability's disclosure and its exploitation has fallen from weeks to days and, in some cases, hours.[17] Attack volumes are up, and when data breaches happen, exfiltration is occurring three times faster than it did just four years ago.[18]

Still, cybersecurity vendors are quick to jump on the "AI-powered" bandwagon, and not all solutions live up to the hype. AI washing — where companies overstate or misrepresent how much AI their solutions actually use — is prevalent in the industry, leading organizations to adopt tools that increase costs without meaningfully improving outcomes. Avoiding this danger requires attending carefully to the measurable value that new solutions can deliver.

AI has enormous potential to help organizations solve the "too much telemetry" problem. On the one hand, collecting more data on what's going on in the environment can — in theory — improve visibility and detections. On the other, leaving all that data for human analysts to sort through will lead to frustration and burnout, not faster mean time-to-detection (MTTD) or mean time-to-response (MTTR). Applying AI to speed up and improve the accuracy of event triage is essential across today's security landscape.

> Every organization should be continuously looking to see where they can apply AI within their SecOps workflows right now. Solutions that can triage telemetry closer to the edge and provide rich data more effectively for analysts will allow for quicker mean time-to-remediation.

David O'Leary, Senior Director of Cybersecurity – Financial Services, SHI

> The fully autonomous SOC remains in the future, but growing numbers of organizations will be adding AI-driven incident response workflows in 2026.

Brad Bowers, Field Chief Information Security Officer – Global, SHI

Will AI replace human Tier 1 and Tier 2 SOC analysts?

Not anytime soon, according to experts.[19] AI agents do have the potential to take over many routine tasks in event triage. They can enrich alerts with context, making investigation easier. They can reduce the volume of false positive alerts that human analysts have to wade through. And they can empower junior analysts to conduct thorough investigations using simple, natural-language queries. But they require oversight, and are by no means a full replacement for human expertise and tribal knowledge.

Talent gaps have long been a problem in cybersecurity operations. They still are. Recent research shows that there's a global cybersecurity workforce shortage of more than 4.7 million employees, with 67% of leaders saying that their organizations are short-staffed.[20] Applied in the right places, AI does have the potential to fill in some of these gaps.

Moving beyond SIEM?

Many large organizations are re-evaluating the role that security information and event management (SIEM) platforms are playing within their SOC. SIEM technology has been complex and unwieldy for years now, and vendors continue to present their solutions as better alternatives.

Today, AI can enable more decisions to be made autonomously and closer to the edge. Instead of putting all the organization's telemetry into a single centralized repository, AI can make determinations at the endpoint that malicious — or unwanted — activity is taking place, accelerating response and making it more precise.

Key strategies for navigating AI transformation in security operations

01

Start with clear use cases driven by real needs.
Don't adopt AI just because of vendor claims or pressure from executive leadership. Instead, identify specific pain points within SecOps workflows that AI can address: alert fatigue, slow investigations, ineffective manual event triage, etc.

02

Evaluate every tool according to the most important metrics: MTTD/MTTR.
If the solution doesn't make you faster at detecting and responding to threats in everyday operations, it's not adding value.

03

Build an AI-augmented SOC where AI complements human expertise.
Let AI handle repetitive, data-intensive tasks while human analysts focus on complex investigations, oversight and tradeoff-based decision-making. Response can be automated where risk is well understood, but most SecOps workflows need a human in the loop.

04

Make governance and shadow AI control a priority.
Adhere to secure AI adoption frameworks that specify who can deploy AI tools in security workflows, which data sources can be used, what access controls will be placed around the models, and how AI actions and recommendations will be reviewed and audited.

No. 07

Building resilience with proactive security

Outpacing tomorrow's threats

Cyber risk mitigation starts with time-tested best practices: robust cyber hygiene, infusing security awareness into organizational culture through discussion and ongoing training, and investing in people and processes focused on risk management — not just technologies. Proactive security goes a step beyond this. It involves a practice of constantly probing your defenses, identifying weaknesses, and patching vulnerabilities. Offensive cybersecurity capabilities make it possible to get and stay ahead of adversaries.

The foundation of a proactive security posture involves a set of practices — penetration testing, red teaming, and adversary emulation — that enable you to see your environment through an attacker's eyes. With this information, you can find and fix weaknesses before they get exploited. These practices also support real-world risk prioritization, giving leaders a map of their highest-impact vulnerabilities and an understanding of where to direct budget and engineering effort to maximize ROI.

> True resilience is not just about being prepared to recover from cyberattacks. It's about actively anticipating, testing and disrupting threats before they impact the business. In today's threat landscape, resilience is built through continuous, adversary-focused validation and rapid adaptation, not just planning and recovery.

Quentin Rhoads-Herrera,
Vice President of Security Services, Stratascale

Becoming able to anticipate and prepare for future threats involves several core capabilities:

- **Penetration testing.** Structured assessments of your network, applications and cloud ecosystem — along with other aspects of IT — give you valuable insights that automated scans miss. The testing should combine advanced custom tooling with dedicated exploit research to stress-test your environment.

- **Red teaming and advanced threat operations (ATO).** These longer-running, goal-oriented exercises mimic the ways a real threat actor might target your environment. Campaigns might include phishing or social engineering, privilege escalation, lateral movement, and even data exfiltration to pinpoint your weaknesses and test the limits of your defense.

- **Continuous threat exposure management (CTEM).** Named as a category by Gartner in 2022 , CTEM is a structured approach to protecting the organization's entire attack surface — including unknown assets and shadow IT.[21] CTEM combines asset discovery (using automation to map the entire attack surface and ensure up-to-date visibility across all of it), vulnerability management, and continuous targeted testing. CTEM's goal is to meaningfully reduce business risk by prioritizing the exposures that are most likely to be exploited, and executing this as an ongoing process.

Key takeaways

Cybersecurity has long been a cat-and-mouse game, where every strategic advance by defenders is met with an evolution of attack tactics. That basic structure won't change anytime soon, but the pace of transformation keeps picking up. To be successful in building proactive resilience in 2026 — and beyond — security stakeholders will need to plan and prepare, but they'll also need to think creatively. Tomorrow's cybersecurity leaders will embrace innovations like automation and AI when building their tool stacks, but they'll also use skills like communication and collaboration to build cross-organizational alignment.

Here are our top five takeaways from this year's report:

1. **Identity is now the primary security perimeter, and governing NHIs is mission critical.** AI agents, machine identities, and other NHIs are proliferating rapidly, and traditional IAM, IGA and PAM can't keep up. Organizations will need to adopt an architectural approach to NHI security, integrating innovative NHI-focused solutions into their existing identity security stacks.

2. **Data protection is shifting from static controls to continuous posture management.** Generative AI has widened previously-existing gaps in data governance, but it can also help by automating data discovery and classification. Enforcing least-privilege, just-in-time, policy-based controls will be essential for ensuring that AI agents (and employees) can see only the data they should.

3. **Software supply chain visibility is much needed.** The proliferation of AI applications that rely on open-source models, datasets, and code libraries is expanding software supply chain risk. By adhering to familiar third-party risk management best practices, organizations can decrease the harm that will come to them in case of upstream compromise.

4. **Platformization can simplify security, but only when it's a good fit.** Many larger enterprises are now trading complex collections of point solutions for unified platforms that promise better integration, visibility, and cost control. To actually realize these benefits, though, an organization needs to have achieved the right level of security maturity — and built the right culture.

5. **AI-augmented security operations and proactive resilience will define the next generation of security leaders.** The near-term future of security operations is not the fully autonomous SOC, but instead an AI-enabled one, where AI and automation improve human productivity — and reduce alert fatigue — to decrease MTTD/MTTR. Along with zero trust adoption and a proactive mindset, this model of security operations will position organizations for resilience in the face of next-generation cyber threats.

Find clarity in cybersecurity with SHI and Stratascale

No two organizations are the same — so it's no surprise that each organization's cybersecurity infrastructure, processes, and procedures should differ, too.

SHI and Stratascale invest in developing a deep understanding of not only the key trends in cybersecurity, best practices, and compliance and regulatory drivers, but also in how we can map solutions to your unique cybersecurity challenges.

What sets us apart?

We're vendor-neutral and solution-agnostic, with experts who have decades of experience. As a trusted partner and advisor, we're capable of big-scale thinking and small-scale attention to detail.

All of our field CISOs come from industry backgrounds, utilizing deep understanding and experience to bring you value. Our security specialists also work with a wide range of organizations and security partners, which gives us a unique 360-degree view of the global cybersecurity landscape and of industry needs by vertical.

SHI's strong partnerships with OEMs ensure your cybersecurity infrastructure is designed, built, and maintained in line with the current and future needs of your organization.

SHI and Stratascale help you achieve crucial efficiencies across:

- Application and data-centric security
- Artificial intelligence
- Cloud and data center security
- Digital risk mitigation
- Endpoint security
- Governance, risk, and compliance
- Identity and access management
- Program strategy and operations
- Security operations
- Threat and vulnerability management
- Zero trust

SHI International Corp. is a transformational technology solutions provider serving the needs of more than 17,000 corporate, enterprise, public sector, and academic customer organizations around the world. It helps companies achieve business goals through the use of technologies ranging from software licensing and end user computing devices to innovative cloud and edge solutions. With over 7,000 employees worldwide, SHI is the largest Minority and Woman Owned Business Enterprise (MWBE) in the U.S.

Stratascale, SHI's cybersecurity division, was founded in 2020 to help enterprise leaders solve their most pressing security challenges and increase business resiliency through continuous security. From enterprise security architecture to vulnerability management, Stratascale's services strategically integrate to form robust solutions that solve complex, multi-domain problems and set the stage for modern security operations.

Learn more

Recent Partner of the Year awards and other accolades:

Crowdstrike, 2024 Global Solution Provider of the Year

Crowdstrike, 2024 Public Sector Partner of the Year — Americas

Crowdstrike, 2024 Solution Provider Partner of the Year — Americas

Cloudflare, 2025 AMER Partner of the Year

Cloudflare, 2025 Global Partner of the Year

Cisco, U.S. 2025 Commercial Software & Services Partner of the Year, East

Cohesity, 2025 Partner of the Year Award

KnowBe4, 2025 National Partner of the Year Award

Quest, 2025 Solution Provider of the Year

Rapid7, 2025 North America Partner of the Year

Rapid7, 2025 Cloud Partner of the Year

Rapid7, 2025 VM Partner of the Year

SentinelOne, 2025 Partner of the Year, North America

Tanium, 2025 Global Growth Partner of the Year

Tenable, 2025 Public Sector Partner of the Year

TrendMicro, 2025 U.S. Enterprise Partner of the Year

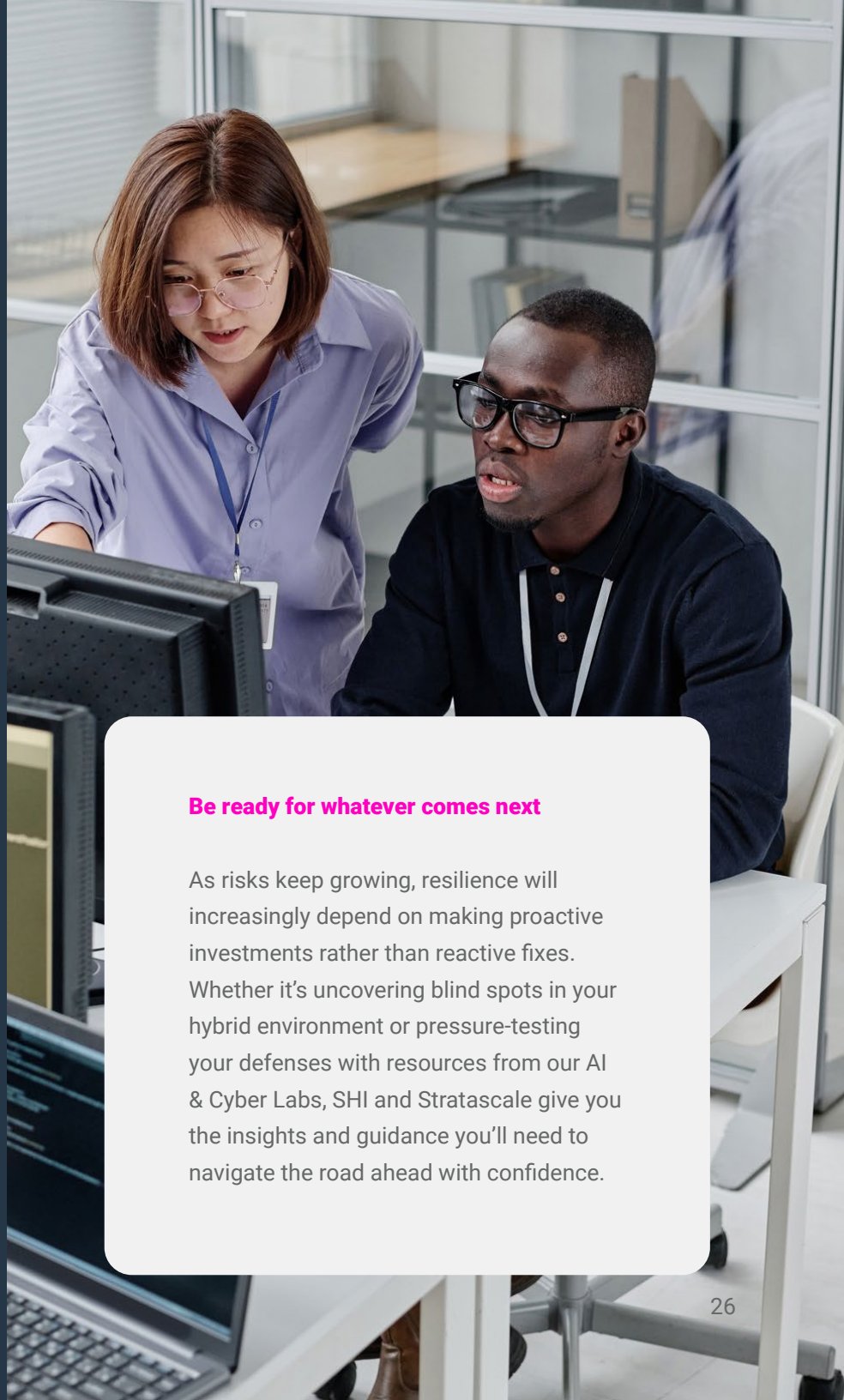
Vertiv, 2025 North American Partner of the Year

Axonius, 2024 Emerging Partner of the Year

Broadcom (Symantec), 2024 Cybersecurity Marketing Excellence Award

CyberArk, 2024 DM Partner of the Year

Palo Alto Networks, 2024 North America Cortex Partner of the Year



Be ready for whatever comes next

As risks keep growing, resilience will increasingly depend on making proactive investments rather than reactive fixes. Whether it's uncovering blind spots in your hybrid environment or pressure-testing your defenses with resources from our AI & Cyber Labs, SHI and Stratascale give you the insights and guidance you'll need to navigate the road ahead with confidence.

Resources

1. MIT Nanda, The GenAI Divide: State of AI in Business 2025, 2025, Available at: https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf
2. Omdia, "New Omdia analysis shows Agentic AI outpacing growth rates of traditional generative AI," September 2025, Available at: https://omdia.tech.informa.com/pr/2025/sep/new-omdia-analysis-shows-agentic-ai-outpacing-growth-rates-of-traditional-generative-ai
3. Cisco, 2025 Cisco Cybersecurity Readiness Index, 2025, Available at: https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/2025/documents/2025_Cisco_Cybersecurity_Readiness_Index.pdf
4. Omdia, "Palo Alto Networks buys CyberArk with a view to securing agentic AI," September 2025, Available at: https://omdia.tech.informa.com/om138027/palo-alto-networks-buys-cyberark-with-a-view-to-securing-agentic-ai
5. Veza, 2026 State of Identity & Access Report, 2025, Available at: https://veza.com/resources/stateofaccess/
6. Palo Alto Networks, The State of Generative AI 2025, 2025, Available at: https://www.paloaltonetworks.com/resources/research/state-of-genai-2025
7. Omdia Universe, Data Security Posture Management (DSPM), 2025, 2025, Available at: https://omdia.tech.informa.com/om138114/omdia-universe-data-security-posture-management-dspm-2025
8. Industrial Cyber, "Software supply chain attacks surge, as ransomware groups escalate and industrial sectors face more exposure," September 2025, Available at: https://industrialcyber.co/reports/software-supply-chain-attacks-surge-as-ransomware-groups-escalate-and-industrial-sectors-face-more-exposure/
9. Cybersecurity Dive, "F5 supply chain hack endangers more than 600,000 internet-connected devices," October 2025, Available at: https://www.cybersecuritydive.com/news/f5-supply-chain-hack-internet-connected-devices-stats/803108/
10. Return on Security, State of the Cybersecurity Market 2024, January 2025, Available at: https://www.returnonsecurity.com/p/the-state-of-the-cybersecurity-market-in-2024
11. Software Analyst Cyber Research, "Cybersecurity $10B Giants: Insights into Cyber's Largest Public Companies," October 2024, Available at: https://softwareanalyst.substack.com/p/cybersecurity-10b-giants-insights
12. Omdia, "Security Operations Market Tracker," Last Updated January 2026, Available at: https://omdia.tech.informa.com/collections/afccy008/security-operations-market-tracker
13. Kroll Advisory, Cybersecurity Sector Update—Fall 2025, November 2025, Available at: https://www.kroll.com/en/reports/m-and-a/cybersecurity-sector-ma-industry-insights-fall-2025
14. Centre for International Governance Innovation (CIGI), "'Q Day' Is Coming: Is the World Prepared?," November 2024, Available at: https://www.cigionline.org/articles/q-day-is-coming-is-the-world-prepared/
15. United States National Security Agency, Press Release: Post-Quantum Cryptography: CISA, NIST and NSA Recommend How to Prepare Now," August 2023, Available at: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/
16. ABA Banking Journal, "FS-ISAC urges financial sector to adopt timeline for implementing quantum computing defenses," September 2025, Available at: https://bankingjournal.aba.com/2025/09/fs-isac-urges-financial-sector-to-adopt-timeline-for-implementing-quantum-computing-defenses/
17. The Hacker News, "159 CVEs Exploited in Q1 2025—28.3% Within 24 Hours of Disclosure," April 2025, Available at: https://thehackernews.com/2025/04/159-cves-exploited-in-q1-2025-283.html
18. Unit 42, Global Incident Response Report 2025, 2025, Available at: https://www.paloaltonetworks.com/engage/unit42-2025-global-incident-response-report
19. Cybersecurity Dive, "How AI agents could revolutionize the SOC—with human help," June 2025, Available at: https://www.cybersecuritydive.com/news/artificial-intelligence-ai-agents-security-operations-center-gartner/750370/
20. ISC2, ISC2 Cybersecurity Workforce Study: Global Cybersecurity Workforce Prepares for an AI-Driven World, 2024, Available at: https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf
21. Gartner Insights, "How to Manage Cybersecurity Threats, Not Episodes," August 2023, Available at: https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes

Studio
by informa techtarget

Expert led.
Impact driven.

Studio is Informa TechTarget's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

Learn more