AHEAD

Elements of a Strong Security Advisory Program

Enhancing Your Business's Cyber Resilience with AHEAD's Comprehensive Security Services

You hear it nonstop, but it never makes it less true: it's becoming more difficult to defend against evolving cyberthreats. As your enterprise adopts emerging technologies like AI and IoT, your technical footprint expands your attack surface. And not only that – malicious actors are adopting AI, too. The methods to exploit vulnerabilities, execute ransomware attacks, and attempt phishing campaigns are more sophisticated than ever before.

At the same time, many enterprises are struggling to modernize their existing security processes due to talent shortages, an overwhelming security tools market, and the increasing burden of technical debt. This presents both known and unknown risk to a business's operations and sensitive data. And how can you defend against what you don't yet know is a threat?

Enter the need for a security advisory partner that can help you not only identify all the vulnerabilities in your environment, but streamline remediation.

Read on to learn more about the security challenges enterprises will face in 2025, the need for a comprehensive security strategy, and the elements of a strong security advisory program.

Enterprise Security Challenges in 2025

Here are some of the major security challenges enterprises will face in the coming year:

A rapidly evolving threat landscape means enterprises are struggling to keep pace with the latest tactics and attack vectors. Malicious actors are increasingly using AI and other sophisticated methods to target the systems and data of enterprises across all industries.

The accumulation of technical debt limits the ability for some enterprises to adopt modern infrastructure and systems. In turn, this technical debt leads to security debt from outdated programming languages, flawed architectures, and a lack of ongoing support. An overreliance on legacy systems and processes leaves many organizations vulnerable to emerging threats – in these complex, outdated system, the weakest points provide attackers the ability to exploit the rest, even if the rest is more secure.

Increasing complexity from AI, multi-cloud, and IoT and the subsequent greater data volume and sprawl is introducing new security risks. Data sprawl makes it harder to identify sensitive data and protect it from breaches and ransomware attacks. Many organizations with smaller IT departments struggling to keep pace with these new technologies are also seeing an increase in shadow IT from their employees, as users start finding solutions that make their jobs easier, regardless of official policies.

Limited cross-domain expertise across data centers, cloud platforms, networks, and other areas makes it challenging to implement comprehensive security strategies. A fragmented security program can leave gaps and introduce weaknesses that malicious actors could exploit.

Broader cybersecurity talent shortages are preventing enterprises from building experienced teams to modernize their security operations and address new threats. It's also challenging for many enterprises to find experts in the legacy technologies they still rely on, so older systems may lack adequate security patches and upgrades.

A fragmented tool-heavy market is making it difficult to choose the right security solutions to implement unified processes and gain visibility across domains. This can result in a complex and fragmented security landscape with overlapping functionalities, inefficient resource utilization, increased maintenance costs, and potential security gaps. Some organizations might find themselves underutilizing their existing technologies as well. With different and overlapping toolsets, the question to ask might not be "What do we need to buy?" but rather, "How can we better use the tools we already have?"

Compliance frameworks requiring isolated recovery environments are becoming harder to adhere to without the right tools and talent. Stringent recovery capabilities like cyber vaults and air gapped environments are difficult for some organizations to implement.

Complex cyber insurance policies. Cyber insurance can be a lifeline for organizations, but there are plenty of horror stories about cyber insurance claims that don't get paid out due to poor implementation of an IRE. A security advisory partner can help navigate those policies and make sure you're properly prepared.

Board requirements for ransomware defense are growing as more organizations become victims of ransomware attacks. Safeguarding critical data and ensuring business continuity in the event of a ransomware attack can be complicated and costly.

SECURITY STRATEGY:

The Importance of Multi-Domain Considerations

Creating and implementing a comprehensive security strategy requires consideration of the following domains:

Data Centers

Today's data centers need robust access controls, advanced threat detection, and disaster recovery planning to ensure business continuity and mitigate the risk of cyber attacks.

Networks

As networks become more dynamic, adopting a zero trust architecture, macro/micro segmentation, and endpoint detect and response will be crucial to minimize the risk of unauthorized access, data breaches, and lateral movement of threats. AHEAD advocates for a "never trust, always verify" mindset, where every user, device, and network component is treated as potentially untrusted. This approach assumes that threats exist both outside and inside the network perimeter and aims to minimize the potential damage by restricting access and continuously verifying trustworthiness.

Cloud Platforms

The cloud requires secure configurations, continuous monitoring with a SIEM, workload protection, and other security measures to prevent breaches and maintain compliance with industry standards.

Data & AI

The widespread adoption of AI means there's an increased need to protect sensitive data and safely operationalize models. Robust security measures need to be integrated into MLOps pipelines and data management processes to ensure model safety and compliance with data privacy laws.

DevOps & Developer Platforms

Software Development Lifecycle (SDLC) consulting is meant for more than helping your dev teams adopt agile methodologies or platform engineering. It can help you identify potential security risks and issues in your development or platform engineering processes. For example, automated security measures can be integrated directly into internal platforms to prevent developers from inadvertently violating security protocols or compliance standards. These guardrails can mitigate security risks without impacting developer workloads.

Workflow Automation

Gaps in IT Service Management (ITSM) security can increase your overall attack footprint, especially in a remote workforce. Many organizations face a skills gap and a lack of platform governance that prevents them from seeing full benefits and ROI for their ITSM platform. A consulting partner can specialize in platform optimizations that increase the reliability of your platform and keep your IT service operations secure.

Observability & Automation

Organizations should consider ways to integrate automation and observability across all domains and environments. Many security teams have already started adopting operational observability practices to better understand system behavior from a security perspective. This newer approach called security observability enables security teams to analyze a wide range of data to streamline incident response, threat modeling, vulnerability management, and other security processes.

It should also be noted that each of these domains comes with their own set of compliance requirements. These compliance requirements, in turn, are a key piece of informing your greater security strategy. Defining compliance requirements in these domains depends upon your industry, organization size, and complexity, especially as it pertains to as hybrid frameworks, control mapping, and bringing automation to your control environment to reduce operational burdens.

It's all a hugely complicated matrix that a strong security advisory partner can help manage.

Elements of a Strong Security Advisory Program

An effective cyber advisory program requires in-depth assessments to identify potential vulnerabilities and compliance violations across all domains. The cybersecurity program should also include a plan to remediate potential vulnerabilities and address security and compliance gaps.

Gap and Risk Assessments

These assessments offer a means to define your target state of security maturity and inform your security strategy moving forward. They should evaluate your current security posture against industry standards like PCI, CMMC, or HIPAA, and larger security frameworks like NIST, ISO, and CISA. This can help you identify weaknesses within your existing security program, see if any third-party vendors pose a particular risk to your environments, and consider areas for improvement to guide your future security strategy. Gap assessments can also save you trouble down the line with cyber insurance in the event of a successful attack, since some insurers might find you liable or deny you a claim if your environments weren't meeting standards in the first place.

Penetration Testing

Penetration testing involves simulating real world attacks using a skilled red team to discover exploitable weaknesses. A good penetration tester might assess your defenses by escalating privileges and accessing backups to simulate a ransomware incident, try to access or exfiltrate sensitive business data, or see how long they can evade detection while gaining initial access and then persisting within your key systems. You can also conduct vulnerability research on individual applications, such as web or mobile apps or even AI models. AHEAD pen testers utilize the same playbook as your attackers to keep the simulation as realistic as possible, then provide comprehensive, actionable insights to address vulnerabilities before they are exploited by malicious actors.

Vulnerability Management

While gap assessments and penetration testing are useful to do periodically, it's also important to continuously manage vulnerabilities. Automatically scanning for vulnerabilities across all environments and prioritizing security fixes based on risk is crucial for mitigating risk. Just as crucial is staying on top of intel for the latest threats in your industry.

Remediation

Enterprises should develop a clear plan to address weaknesses and compliance issues discovered from gap assessments and penetration testing. A strong security posture requires targeted remediation of vulnerabilities that pose the most significant risk to utilize security resources most efficiently. But even with a strong roadmap for remediation and further security program development, with the security talent shortage – as of late 2024, over 650,000 cybersecurity positions in the US are unfilled – it can be difficult to effectively remediate your systems without help from a strong partner.

Why AHEAD for Security Advisory?

AHEAD is an enterprise solutions provider with deep experience in cybersecurity. We have a diverse team of security professionals that can provide the multi-domain expertise and additional capacity you need to enhance your security capabilities.

The AHEAD Cyber Advisory program offers a flexible pool of hours where you can customize your consultancy program to not only address gaps in your security posture, but help remediate them – and fast. Our experts can perform a gap assessment to examine the current state of your security program, build a maturity roadmap, and help you implement security and compliance best practices. We also have a team to perform network and physical penetration tests that simulate real world attacks and help inform a strategic roadmap, and offer ongoing vulnerability management with recurring environment scans, monthly updates on your progress and strategy, and additional guidance on the evolving threat landscape.

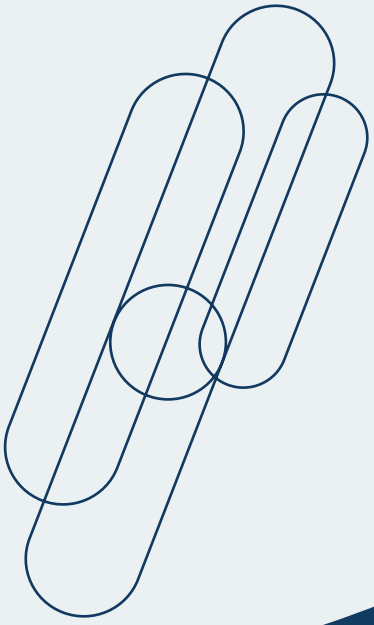
hatch
Powered by AHEAD

Our Security Accelerate Teams are a flexible extension of your teams that can scale up and down depending on your specific needs. You'll have access to 500+ highly qualified and specialized resources who can proactively work to remediate issues based on assessments and penetration test findings. And we can also help reduce the lost productivity of lengthy procurement times through our tight industry partnerships and complete visibility into the supply chain via the Hatch™ platform.

Through regular meetings and checkpoints, our teams get to know the ins and outs of your business to provide the best security strategies. AHEAD team members seek to form lasting relationships with your teams and are deeply invested in seeing you succeed.

Are you ready to consider a security advisory program to enhance the resilience of your organization?

Contact AHEAD to learn more about how we can help you enhance your cyber resilience.



AHEAD

Combining cloud-native capabilities in software and data engineering with an unparalleled track record of modernizing infrastructure, we're uniquely positioned to help accelerate the promise of digital transformation.

Visit us at ahead.com.

National Hubs

CHICAGO
444 W. Lake Street
Suite 3000
Chicago, IL 60606

NEW YORK
500 Fifth Avenue
Suite 1500
New York, NY 10110

ATLANTA
1117 Perimeter Center
W406
Atlanta, GA 30338

SAN FRANCISCO
2000 Crow Canyon Place
Suite 250
San Ramon, CA 94583