SHI

8 cybersecurity trends for 2025: Navigate the evolving threat landscape

SHI's experts guide the way with key insights about what lies ahead

2025

Table of contents

The threat landscape is complex and ever-changing.

And with so many disparate sources offering cyber predictions and insights, how can you filter through the noise to focus on the most critical trends?

In this ebook, SHI's experts break down the top eight cybersecurity trends to look for in 2025 and provide guidance for integrating security practices into your cybersecurity strategies and programs. This report helps zero in on where the industry is heading, so you can better support your cybersecurity initiatives and improve your security posture as you navigate the evolving threat landscape.

The importance of staying ahead in *cybersecurity*

Before you can solve what's next, let's examine the current state. Converging artificial intelligence (AI) technologies and platform consolidation are rapidly transforming the cybersecurity industry. The breakneck pace is fundamentally shifting program strategies, as attackers and cybersecurity defenders must find new ways to operate and innovate.

New and increasingly sophisticated threats persist as well, causing disruption at each encounter. While you must continue implementing traditional security measures, it's essential to develop a proactive and adaptive approach to security programs. A strong cybersecurity strategy is more crucial than ever for maintaining business continuity, protecting customer trust, and ensuring regulatory compliance.

> Staying ahead in cybersecurity is not merely about defense; it's about enabling growth, innovation, and continuous program improvement.

It's time to reimagine how you operate your cybersecurity programs and focus on deliberate approaches to modernize and unify siloed cyber systems and teams. As threats become more complex in 2025, organizations must adopt forward-thinking strategies, leveraging advanced technologies while continuing to align security initiatives with business goals.

1 AI and its impact on cyber programs

Preparing your *security program*

As generative AI technologies become more prevalent, they present both opportunities for productivity and challenges for organizations to implement securely. It is not surprising that this technology is and will continue to be a critical element in cybersecurity programs. However, there are mixed thoughts on where and how to take advantage of this rising tech.

AI's ability to process and analyze vast amounts of data can enhance decision-making and operational efficiency. Yet, it also raises significant security and data privacy concerns, as these systems often require access to sensitive personal and organizational data and may transport components of this data outside of a controlled IT environment.

A key challenge for security leaders in 2025 is implementing a secure foundation with proper controls and policies to support AI business goals.

Consider at least three different prospective focus areas:

Data privacy and security
Establish guidelines and procedures for handling data, implement strong access controls, and monitor and audit data access, safeguarding sensitive information with identity and access management (IAM).

Applied AI for cybersecurity
Focus on telemetry and improvement within security operations (SecOps) programs.

AI application development
Apply controls to support the appropriate business usage of each AI application while securing the app itself, its data elements, and identity-related access.

In the context of generative AI, IAM is crucial for ensuring data privacy and security. As users and AI systems access and process sensitive information, robust IAM solutions ensure only authorized users have access to specific data and functionalities. By integrating effective IAM strategies with AI systems, organizations can minimize unauthorized access risks and enhance data protection, thereby maintaining compliance with privacy regulations and building trust with stakeholders.

Regulatory *considerations*

The rise of AI has prompted new regulatory frameworks focused on data protection and privacy. Laws such as the European Union's (EU) General Data Protection Regulation (GDPR) and emerging AI-specific guidelines require organizations to be transparent about data usage and to implement robust privacy safeguards.

Organizations must stay informed about these evolving regulations to ensure compliance. This includes conducting regular audits, implementing privacy impact assessments, and ensuring AI systems adhere to principles of data minimization and user consent.

Best practices for secure *AI integration*

To navigate the complexities of AI and data privacy, stay ahead by adopting the following best practices:

Data governance frameworks

Establish and enforce comprehensive data governance policies that define how data is collected, processed, and stored. These frameworks should include guidelines for AI system usage and data protection measures. Data security posture management (DSPM) is a programmatic component that can support this journey aligned with a data-centric program.

Privacy by design

Integrate privacy considerations into the design and development of AI systems from the outset. This approach ensures privacy is a foundational element of AI solutions, rather than an afterthought.

Secure application development

Modernize current development lifecycles to support large language models (LLM), retrieval-augmented generation (RAG), and other key components. Look for enclave technologies that incorporate all components of the AI application to provide integrated security controls.

Robust encryption and anonymization

Employ strong encryption techniques and anonymize data wherever possible. These measures help protect sensitive information from unauthorized access and reduce the risk of data breaches.

Continuous monitoring and auditing

Implement ongoing monitoring of AI systems to detect and address potential privacy issues. Regular audits can help ensure compliance with regulatory requirements and internal policies. Reevaluate red team technologies and incorporate technologies like STRIDE GTP for threat modeling and advanced red teaming scenarios.

6

Employee training and awareness
Educate employees about the importance of data privacy and the specific challenges associated with AI. Training should emphasize the organization's data protection policies and the role of employees in safeguarding information.

7

Identity strategy
Identify and manage overprivileged accounts, focus on non-human identity, and enforce and strengthen authentication. Consider robust user verification methods, like passwordless access.

By adopting these best practices, your organization can harness the power of AI while safeguarding data privacy, ensuring compliance, and maintaining trust with customers and stakeholders.

2 Outcome-driven metrics

> The number one ingredient needed to make your metrics worthwhile, regardless of your industry or function, is data — correlated, normalized, CORRECT data. Axonius provides exceptional infrastructure visibility by collecting and correlating data derived directly from your assets, giving you the most accurate base for understanding your environment. With the hard work of data quality done, deriving reflective, actionable metrics is a relatively small lift.
>
> Metrics ideally tell the story of, "How are we doing?" and the answers to that question are how Axonius determines not just the degree of their success, but how they direct their resources to improve continuously. Without good data, it is impossible to accurately tell the story of your security posture, the efficacy of your security or operational processes, or how close you are to reaching your business goals. Axonius takes the hard work of asset management out of the equation so teams can focus on how to best develop your metrics.
>
> *- Liz Morton, Axonius Field CISO*

AXONIUS

Aligning cybersecurity with *business goals*

Organizations are increasingly focusing on outcome-driven metrics to quantify the effectiveness of security investments, such as mean time to identification (MTTI) and mean time to remediation (MTTR). This trend reflects a shift from traditional, activity-based metrics to those that directly correlate with business outcomes.

The goal is to provide clarity to stakeholders by demonstrating how cybersecurity initiatives align with and support broader organizational goals.

Outcome-driven metrics are designed to translate technical security measures into business-relevant outcomes, such as time to value (TTV). For instance, rather than simply reporting the number of attacks blocked, organizations are now measuring the impact of these efforts on business system resiliency, risk reduction, and financial performance.

Business value and *ROI*

The adoption of outcome-driven metrics provides significant business value by enabling organizations to:

Communicate risk effectively: By aligning cybersecurity metrics with business objectives, CISOs can articulate risk in terms that resonate with executive leadership and boards of directors. This alignment facilitates informed decision-making and resource prioritization.

Demonstrate ROI: Organizations can better validate the return on investment (ROI) of cybersecurity initiatives by linking security efforts to tangible business benefits, such as reduced downtime, improved customer trust, and enhanced regulatory compliance.

Enhance strategic planning: With clear, outcome-focused metrics, organizations can more effectively plan and allocate resources for future cybersecurity initiatives, ensuring alignment with strategic business goals.

Implementation *strategies*

To successfully execute outcome-driven metrics, we recommend the following strategies:

1

Identify key business objectives

Outline your core objectives and determine how cybersecurity can support these goals. This alignment will guide the selection of relevant metrics.

2

Develop relevant metrics

Create metrics that reflect cybersecurity's impact on business outcomes. Examples include measuring the periodic cost of security incidents (labor, impact, etc.) over time, which can demonstrate the impact of deployed controls, breakouts of security effort and the activities driving these processes, and operational efficiency gains following security enhancements.

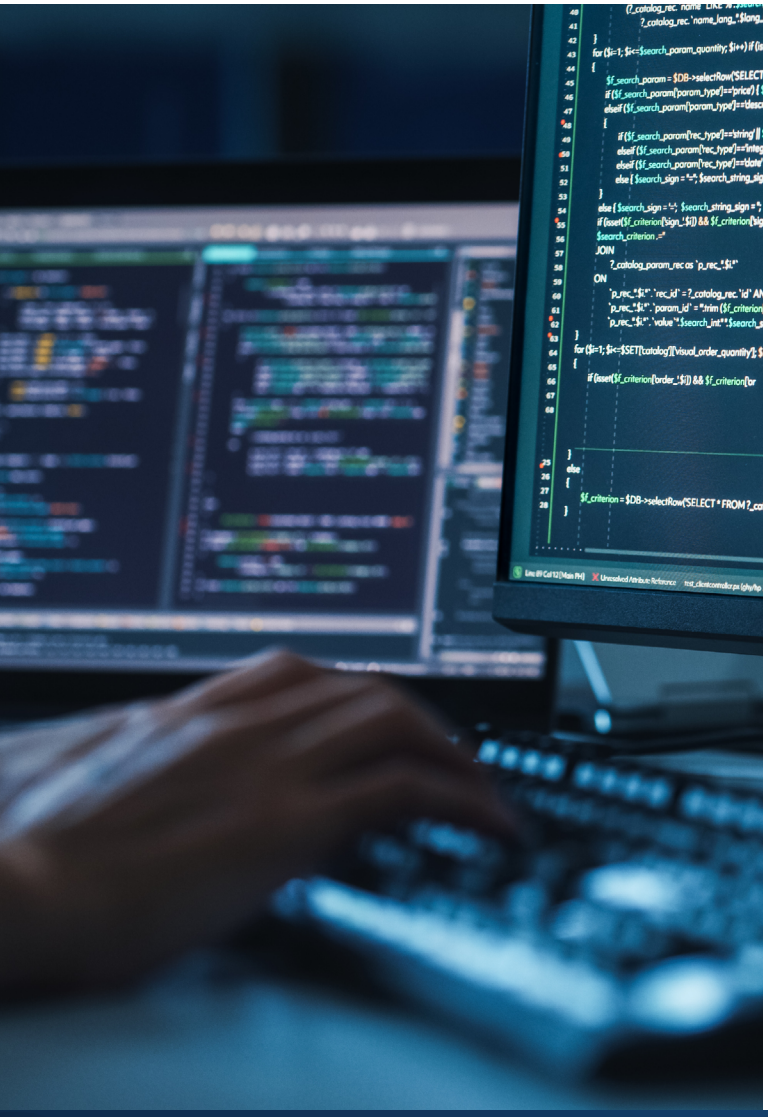
3

Leverage technology and automation
Utilize advanced analytics and automation tools to collect, analyze, and report on security metrics in real time. Modern security posture management tools can aid in this process by ingesting information from many diverse systems, which helps ensure accurate, timely, and actionable data.

4

Foster a collaborative culture
Encourage collaboration between cybersecurity teams and other business units to ensure security initiatives align with business needs and metrics reflect cross-functional contributions. Interactions should be programmatic as well as ad hoc to ensure a communication cadence between groups.

By adopting outcome-driven metrics, you can enhance your cybersecurity posture while simultaneously driving business growth and innovation. This approach not only strengthens security but also positions cybersecurity as a strategic enabler within your organization.



3 Cyber resiliency

Defining and building *cyber resiliency*

As cyber threats grow in sophistication and frequency, building resiliency is crucial for maintaining business operations and protecting critical assets.

Cyber resiliency refers to an organization's ability to anticipate, withstand, recover from, and adapt to cyberattacks and disruptions. It involves a holistic approach that integrates cybersecurity practices into every aspect of the business recovery and continuance strategies. This strategy requires subject matter expert (SME) technologists from all IT operations (ITOps) disciplines to build and support a sustainable practice.

Current challenges and *solutions*

While the concept of cyber resiliency is not new, recent high-profile incidents have underscored its importance. Many organizations struggle with legacy systems, fragmented security solutions, inadequate response plans, and growing dependencies on third-party suppliers and sprawling application ecosystems. These challenges can hinder the ability to respond effectively to attacks and maintain cyber resiliency.

To address these issues, organizations should focus on:

Comprehensive risk assessment
Regularly evaluate potential vulnerabilities and threats to prioritize security investments effectively.

Robust incident response plans
Establish and regularly update incident response plans to ensure quick and efficient recovery from cyber incidents.

Integrated security architecture
Develop a cohesive security architecture that aligns with business operations and supports seamless communication and integrated telemetry across departments.

A well-built resiliency team
Made up of SMEs from cyber, infrastructure, and applications teams, this core team is responsible for planning for and prioritizing business continuity as disruption occurs. Additionally, they focus on technologies and architecture to avoid downtime.

Future *directions*

As the cybersecurity landscape evolves, so too must your strategies for building cyber resiliency. Key future directions include:

Adopting a zero-trust model
Implement a zero-trust architecture that continuously verifies users and devices, minimizing the risk of unauthorized access.

Leveraging advanced analytics
Use AI and machine learning to enhance threat detection and response capabilities, enabling proactive defense against emerging threats.

By focusing on these areas, your organization can enhance your cyber resiliency, ensuring you are prepared to face the challenges of an increasingly complex threat landscape. This proactive approach not only safeguards business operations but also supports long-term growth and innovation.

4 Platform consolidation

Benefits of *platformization*

Platform consolidation involves integrating multiple security tools and solutions into a unified platform. This approach offers several benefits, including reduced complexity, improved efficiency, and cost reinvestment. By streamlining security operations, organizations can enhance visibility, improve incident response times, and simplify management.

Consolidation also facilitates better data integration, allowing for more comprehensive threat analysis and decision-making. This holistic view of security operations enables organizations to respond more effectively to emerging threats.

Platform consolidation isn't always simple, though. Some organizations fear switching off a tool with no visibility, while others are trapped under existing contracts that soak up budget and prevent more fleet-footed moves.

Risks of *single vendor reliance*

Consolidation also presents risks, particularly when organizations rely heavily on a single vendor. This dependency can lead to vulnerabilities if a critical component fails or if the vendor experiences a security breach. Additionally, it may limit flexibility, making it challenging to adopt innovative solutions from other providers.

To mitigate these risks, we recommend adopting strategies that include best-in-class tools from multiple vendors, ensuring you maintain resilience and adaptability.

> To defeat modern adversaries, cyber defenders must adopt a platform approach that delivers the speed and agility necessary to match the velocity of today's attacks. Relying on outdated point solutions creates gaps that adversaries readily exploit.
>
> A unified platform closes these gaps and enables defenders to anticipate and disrupt threats before they can cause harm, shifting the balance of power in favor of security teams.
>
> *- David Hampton, CrowdStrike VP Horizon*

CROWDSTRIKE

Market trends and *predictions*

The trend toward platform consolidation is expected to continue as organizations seek to optimize security operations. Major vendors are expanding their offerings to provide comprehensive security platforms, integrating endpoint protection, network security, and cloud security solutions.

Looking ahead, we anticipate increased collaboration between vendors, resulting in more integrated solutions that address a broader range of security needs. Stay informed about these developments to make strategic decisions that align with your business objectives.

By strategically embracing platform consolidation, you can enhance your security posture, reduce operational complexity, and achieve better alignment with your overall business goals.

5 Supply chain security

Understanding supply chain *risks*

Supply chain security and the ability to validate third-party code have become critical concerns as organizations increasingly rely on interconnected networks of suppliers and partners. Cyber threats targeting supply chains can disrupt operations, compromise sensitive data, and damage reputations. Recent incidents have underscored the vulnerability of supply chains to attacks, highlighting the need for robust security measures.

Recent incidents and *lessons learned*

High-profile supply chain attacks, such as those targeting software and hardware providers, have demonstrated the cascading effects of vulnerabilities. These incidents reveal the importance of visibility into the entire supply chain, including third-party suppliers and subcontractors. Comprehensive risk assessments and continuous monitoring of supply chain partners are critical to protect your sensitive information.

Strategies for mitigating *risks*

By implementing the following strategies, your organization can help strengthen supply chain security, reduce the risk of disruptions, and enhance your overall cyber resilience.

1. **Thorough vendor assessment**
   Conduct rigorous evaluations of suppliers' security practices and ensure they comply with your security standards.

2. **Continuous monitoring**
   Establish processes for monitoring supplier activities and vulnerabilities on an ongoing basis. This includes using tools that provide real-time insights into supply chain risks.

3. **Contractual security requirements**
   Include specific security clauses in contracts with suppliers, outlining expectations and responsibilities for protecting data and systems.

4. **Collaboration and information sharing**
   Foster collaboration with industry peers and participate in information-sharing initiatives to stay informed about emerging threats and best practices.

5. **Incident response planning**
   Develop and regularly update supply chain incident response plans to address potential breaches quickly and effectively.

6 Cyber physical systems

Emergence of *cyber physical systems*

Cyber physical systems (CPS) integrate computing, networking, and physical processes, playing a crucial role in sectors like manufacturing, healthcare, and critical infrastructure. As these systems become more prevalent, they introduce new security challenges due to their interconnected nature and potential impact on physical operations.

Security challenges and *solutions*

The integration of physical and digital components in CPS increases the attack surface, making them vulnerable to cyber threats that can lead to physical consequences. Common challenges include outdated security protocols, lack of visibility, and insufficient patch management.

To address these challenges, organizations should:

Implement robust security frameworks
Adopt comprehensive security frameworks that encompass both IT and operational technology (OT) environments.

Enhance visibility and monitoring
Deploy advanced monitoring tools to gain real-time insights into CPS operations and detect anomalies quickly.

Reduce the attack surface
Implement network segmentation strategies to minimize the impact CPS systems can have on other business systems.

Regularly update and patch systems
Ensure all components are regularly updated and patched to protect against known vulnerabilities.

Industry *applications*

Cyber physical systems are transforming a wide range of industries by enhancing efficiency and enabling new capabilities. In manufacturing, CPS improves productivity by facilitating automation and real-time data analysis. In healthcare, these systems support advanced diagnostic tools and patient monitoring, while in energy, they enable smart grid technologies.

As CPS continues to evolve, organizations must prioritize security to protect both digital and physical assets. By implementing strategic security measures, you can fully leverage the transformational benefits of CPS while mitigating associated risks.

> To drive proper visibility in cyber physical environments, customers should operationalize asset and vulnerability management alongside anomaly detection. In modern organizations, CPS assets are no longer siloed or air-gapped; it's crucial to understand and monitor their interactions with traditional IT devices and systems. Understanding the relationships and associated risks between IT assets, identities, and CPS devices is key to a robust exposure management strategy.
>
> A holistic exposure management strategy is essential because CPS devices are often difficult or impossible to patch. This approach helps asset owners identify, expose, and close attack paths, strengthening their security posture even when CPS devices cannot be updated.
>
> *- Jeff Rotberg,*
> *Tenable Global Strategic Partners Director OT*

7 Legislative and regulatory changes

Overview of *new regulations*

Governments worldwide continue to introduce new regulations aimed at enhancing data protection and privacy. These regulations are designed to address the complexities of today's ITOps environments and encourage stronger cyber defenses in the face of ever-increasing threats.

Impact on *businesses*

New regulations — including the EU's AI Act and Digital Operational Resilience Act (DORA), the U.S. Securities and Exchange Commission's Regulation S-P, and recent GDPR updates — impose stricter requirements on data handling and privacy, as well as incident reporting and response. These should be at the heart of a mature cyber program, yet many organizations have gaps.

Organizations should focus on the benefits of avoiding substantial fines, reputational damage, and cyber breaches. Compliance with legal regulations involves implementing robust cyber program measures, conducting regular audits, maintaining transparency, and adopting continuous automated validation capabilities.

Compliance *strategies*

To navigate these regulatory changes, organizations should adopt the following strategies:

1. **Stay informed**
   Keep abreast of the latest regulatory developments and understand their implications for your industry.

2. **Conduct regular audits**
   Perform regular compliance audits to identify gaps and ensure adherence to regulatory standards.

3. **Implement strong data governance**
   Establish comprehensive data governance frameworks that align with regulatory requirements and best practices.

4. **Engage legal and compliance experts**
   Consult with legal and compliance experts to interpret regulations and develop tailored compliance strategies.

5. **Enhance employee training**
   Educate employees about the importance of regulatory requirements and data protection to foster a culture of instinctive compliance.

By proactively addressing regulatory changes, your organization can not only achieve compliance but also enhance your overall cybersecurity posture and build trust with customers and stakeholders.

8 Incident response and recovery

Evolving incident response *strategies*

As AI-powered cyber threats become more sophisticated, organizations must adapt their incident response strategies to ensure quick and effective recovery. Traditional response methods are no longer sufficient to handle the complexities of modern cyberattacks. Successful organizations are now focusing on integrated, agile approaches that encompass both digital and physical domains.

Integration with *cyber resliency*

Incident response is a critical component of broader cyber resiliency efforts. By aligning response plans with resiliency strategies, organizations can minimize downtime and mitigate the impact of attacks. This involves establishing clear protocols for detection, containment, eradication, and recovery, ensuring a coordinated response across all departments.

> Incident response teams need to be thinking about 'closing the doors' as much as they think about 'detecting the bad guys.' As an industry, we should be investing in trustworthy solutions that tell us what to fix, and autonomously apply all the necessary changes.
>
> *- Stephanie Aceves, Tanium Sr. Director, Product Management*

TANIUM

Future *challenges*

The future of incident response will be shaped by several key challenges:

Dispersed data environments
As data becomes more decentralized, organizations must develop response plans that address cloud, on-premises, and hybrid environments.

Resource constraints
Many organizations face staffing and resource deficiencies, necessitating the use of automation and AI to enhance response capabilities. But these types of responses can lead to increased false positives and negatives.

To overcome these challenges, organizations should invest in advanced incident response technologies, conduct regular simulations and drills, and foster collaboration between IT, security, and business units. By doing so, you can ensure a robust and agile response to cyber incidents, safeguarding your operations and reputation.

Key takeaways for strategic cybersecurity

As we navigate the complexities of 2025, cybersecurity remains pivotal. The trends explored in this guide — ranging from outcome-driven metrics to emerging technologies — highlight the dynamic nature of the threat landscape and the innovative solutions reshaping the industry.

Your organization must adopt a proactive approach, integrating cybersecurity into every aspect of your operations. By understanding and leveraging these trends, you'll enhance security posture, protect critical assets, and drive sustainable growth.

Here are our key takeaways for your 2025 strategy and beyond:

Align security with business goals
Use outcome-driven metrics to demonstrate the value of cybersecurity investments in terms that resonate with business leaders.

Embrace innovation
Integrate AI, machine learning, and other emerging technologies to enhance threat detection and response capabilities.

Enhance resiliency
Develop comprehensive strategies to help ensure operational continuity and rapid incident recovery.

Stay compliant
Monitor regulatory changes and implement robust data governance to maintain compliance and protect stakeholder trust.

By implementing these strategies, your organization can not only defend against current threats but also anticipate and prepare for future challenges. Cybersecurity is not just about protection — it's a strategic enabler that supports innovation and business success.

Find clarity in cybersecurity *with SHI*

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

SHI invests in developing a deep understanding of not only the key trends in cybersecurity, best practices, 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 helps 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

Solve what's next in your *cybersecurity plan*

As the threat landscape evolves, we can help you best prepare for what lies ahead. From identifying hidden vulnerabilities in your current environment to unlocking potential in our state-of-the-art AI and Cyber Labs, SHI delivers the valuable insights, choices, and control you need to progress your cybersecurity strategy.

Sign up for your complimentary *Security Posture Review* (SPR) today and receive:

- A comprehensive assessment of your organization's current security maturity level.
- An in-depth analysis and prioritization of prevalent threats to your organization.
- Tailored recommendations for strengthening your overall security.

Request your SPR and connect with an *SHI cybersecurity expert*.

Think of SHI as *your personal technology concierge*. We connect your team with the IT solutions and services you need to support your organizational growth and employee experience.

Whether you're building a modern hybrid workplace, defending against an evolving threat landscape, making the cloud work harder for you, or searching for ways to optimize your software portfolio, our friendly 6,000-person team is ready to solve what's next for your organization.

Our in-house data center integration, device configuration, and deployment and license advisory services, plus our top-tier status with vendors and flexible financing make life simpler for IT decision makers.

Execute your IT vision with stress-free, scalable solutions you – and your people – will love.

SHI is proud to be the largest Minority/Woman Owned Business Enterprise (MWBE) in the United States.

Tailored IT services for *maximum value*

Maximize your technology investments with our premier IT services. SHI's expert teams help you with strategic technology selection, seamless deployment, and ongoing management, all designed for your unique business needs.

Managed services
Optimize costs and workloads with our cloud-managed services

Training and adoption
Drive technology adoption and propel your organization forward

Integration services
Build and integrate end-to-end IT infrastructure at scale

Customer Innovation Center
Make evidence-based decisions with expert support from SHI Labs

Leasing and financing
Accelerate your digital transformation with flexible financing services

SHI at a *glance*

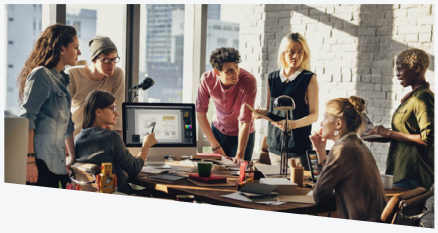
WBENC WOMEN'S BUSINESS ENTERPRISE NATIONAL COUNCIL

NMSDC National Minority Supplier Development Council

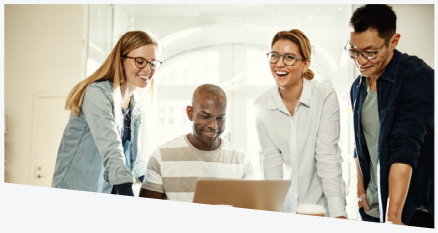
SILVER | Top 15% ecovadis Sustainability Rating DEC 2024

THE CHANNEL CO. CRN MSP 500 2024

Making connections
We connect your team with the scalable IT solutions and services you need to securely support your organizational growth and employee experience.



Beyond the contract
We have contracts and SLAs with our customers, of course. But we also emphasize going the extra mile to deliver exceptional value and ensure true success for your organization.



Sweating the small stuff
We help you focus on what's most important by handling distractions. From managing long-tail vendors to arranging logistics to managing IT assets, we've got your back.

Friendly, knowledgeable, and well-connected — *we're ready when you are*.