The Fight for Cyber Resilience

Solutions Guide

The Fight for Cyber Resilience

- A global cybersecurity talent shortage means that IT leaders often have little choice but to do business with third-party service partners.[3]
- $1.5 trillion to $2 trillion total cybersecurity market opportunity for cybersecurity technology and service providers — about 10 times the current vended market.[3]
- Security was the top technology sold by 59% of partners, the top skill set that 38% of partners are hiring for, and the top-ranked issue of importance over the last two years.[4]
- 90% of security is delivered through partner-led channels.[4]
- By 2027, 75% of employees will acquire, modify, or create technology outside IT's visibility — up from 41% in 2022.[5]
- Just 29% have high confidence that they have a robust mechanism to test their environments against the most current threat vectors.[6]
- Only 31% of organizations have high confidence that their tools can continuously adjust to new configurations to identify new threats and vulnerabilities.[6]
- Just 32.7% of organizations have high confidence they can investigate every incident.[6]
- Only 34% of organizations have high confidence they can autonomously stop threats in real time.[6]

The Fight for Cyber Resilience

Pervasive Cyberattacks

We're living in an increasingly connected world. The number of devices and things continues to grow exponentially, connecting where we live, work and play. Network perimeters continue to dissolve as more and more of us work remotely. Cloud services continue to proliferate and emerging technologies, such as artificial intelligence (AI), are bringing more unknowns than knowns, forcing us to consider difficult questions.

While this modern, hyperconnected world brings never-before-considered conveniences, it also brings the likelihood of a cyberattack. You only need to run down a list of recent cyberattacks to understand just how pervasive they are:[1]

- **March 15, 2024 –** A French government department, responsible for registering and assisting unemployed people, became the victim of a "mega" data breach that compromised the information of up to 43 million citizens.
- **March 13, 2024 –** Hackers targeted over 15,000 U.S. users of the Roku TV streaming platform to buy unauthorized subscriptions between 2003 and 2024 — and likely used logins/passwords leaked from previous hacks at third-party services.
- **March 11, 2024 –** The Cybersecurity Infrastructure Security Agency (CISA) was hacked, forcing it to take two key computer systems offline — including one that enables federal, state, and local officials to share security assessment tools.
- **March 8, 2024 –** Swiss authorities found that 65,000 government documents holding classified information and sensitive personal data were leaked following a ransomware attack last year on one of its IT vendors.
- **March 4, 2024 –** Casino Del Sol in Tucson, Arizona, confirmed that an unauthorized party accessed their IT network, bringing some hotel, dining and gaming operations to a standstill.

These are only some of the attacks that make the headlines. It's likely that someone in your circle has also been the victim of a cyberattack — or that you yourself have received a "Dear Customer" letter with an offer of free credit monitoring services. Clearly, the more connected we become, the more we're susceptible to an attack.

Key Issues Impacting Cyber Resiliency

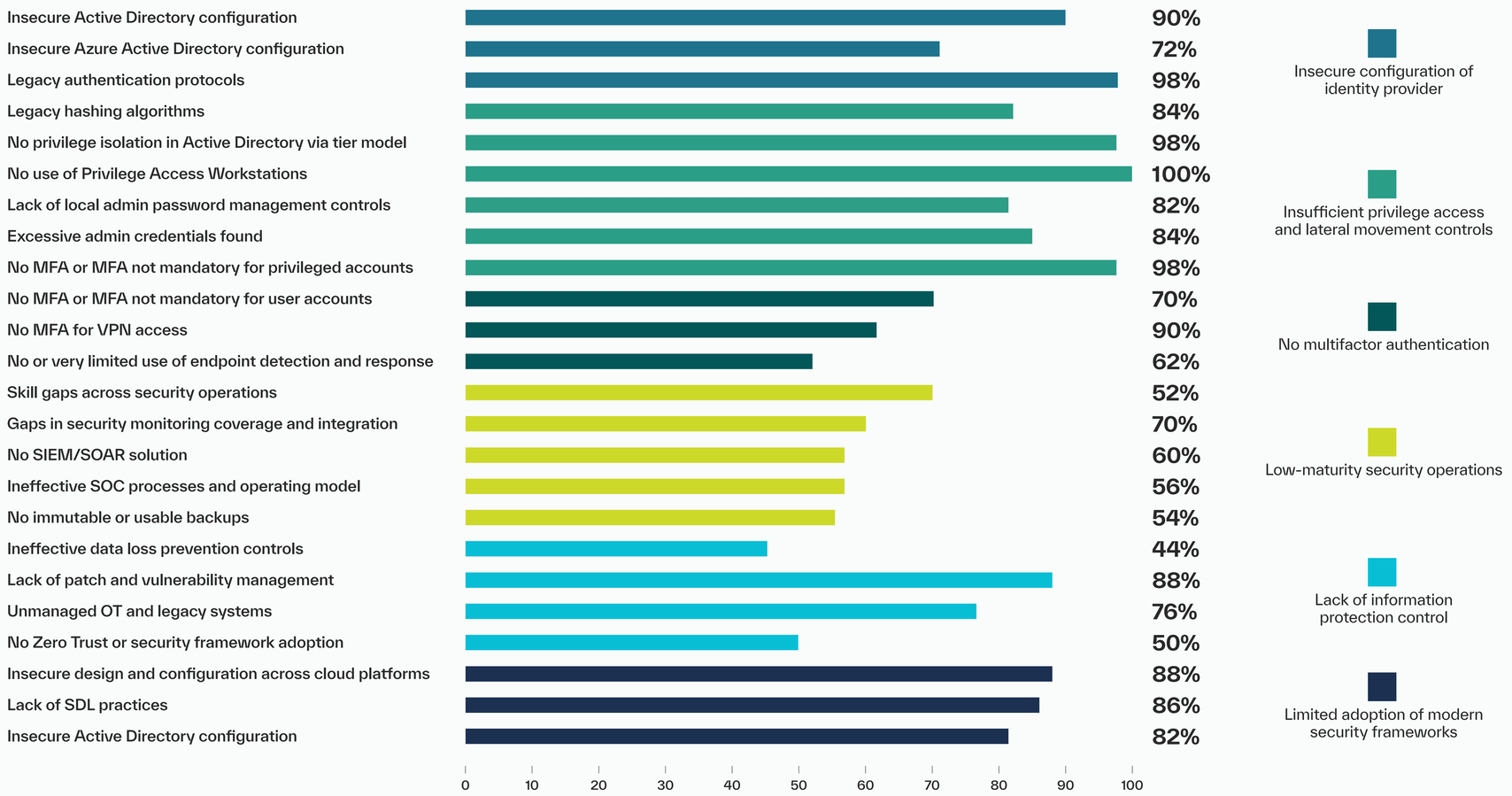
Cyber Resilience Defined

- A global cybersecurity talent shortage means that IT leaders often have little choice but to do business with third-party service partners.[3]
- $1.5 trillion to $2 trillion total cybersecurity market opportunity for cybersecurity technology and service providers — about 10 times the current vended market.[3]
- Security was the top technology sold by 59% of partners, the top skill set that 38% of partners are hiring for, and the top-ranked issue of importance over the last two years.[4]
- 90% of security is delivered through partner-led channels.[4]
- By 2027, 75% of employees will acquire, modify, or create technology outside IT's visibility — up from 41% in 2022.[5]
- Just 29% have high confidence that they have a robust mechanism to test their environments against the most current threat vectors.[6]
- Only 31% of organizations have high confidence that their tools can continuously adjust to new configurations to identify new threats and vulnerabilities.[6]
- Just 32.7% of organizations have high confidence they can investigate every incident.[6]
- Only 34% of organizations have high confidence they can autonomously stop threats in real time.[6]

The Fight for Cyber Resilience

Pervasive Cyberattacks

Key Issues Impacting Cyber Resiliency



Source: "Microsoft Digital Defense Report 2022," Microsoft.com.

- A global cybersecurity talent shortage means that IT leaders often have little choice but to do business with third-party service partners.[3]
- $1.5 trillion to $2 trillion total cybersecurity market opportunity for cybersecurity technology and service providers — about 10 times the current vended market.[3]
- Security was the top technology sold by 59% of partners, the top skill set that 38% of partners are hiring for, and the top-ranked issue of importance over the last two years.[4]
- 90% of security is delivered through partner-led channels.[4]
- By 2027, 75% of employees will acquire, modify, or create technology outside IT's visibility — up from 41% in 2022.[5]
- Just 29% have high confidence that they have a robust mechanism to test their environments against the most current threat vectors.[6]
- Only 31% of organizations have high confidence that their tools can continuously adjust to new configurations to identify new threats and vulnerabilities.[6]
- Just 32.7% of organizations have high confidence they can investigate every incident.[6]
- Only 34% of organizations have high confidence they can autonomously stop threats in real time.[6]

Cyber Resilience Defined

The Fight for Cyber Resilience

Pervasive Cyberattacks

Key Issues Impacting Cyber Resiliency

Cyber Resilience Defined

Unfortunately, "perfect protection" against an attack is impossible. No individual, organization or government has the necessary resources to ensure that they'll never get hacked. Instead, we must strive for "cyber resiliency" or what the National Institute of Standards and Technology (NIST) defines as:

> *The ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.*[2]

To be clear, cyber resilience is not the same as cybersecurity. Cybersecurity complements cyber resilience with technologies and processes to protect systems, networks, data and IT infrastructure from threats. Effective cybersecurity reduces the risk of cyberattacks and protects resources and assets from loss, theft or damage.

Cyber resilience, on the other hand, combines cybersecurity and operational resilience to help organizations to consistently anticipate, withstand, recover, and adapt to cyberattacks. This includes threats and attacks from cybercriminals and malicious insiders, as well as catastrophic system failures due to misconfigurations and accidental deletions. Cyber resilience can be applied to both external and internal threats.

The Value of Cyber Resilience

Given that "perfect protection" is pretty much a pipe dream, one of the best ways to help your customer as their managed service provider (MSP) or their managed security service provider (MSSP) is to change their culture from "if we're attacked" to "when we're attacked."

Helping them assess their risk and then building a plan that presumes an attack is imminent ensures that they'll have the tool set to quickly identify, respond and recover from a cyberattack when it occurs — and makes it possible for business operations to continue even in the face of a potential disruption. That is the basis of cyber resilience.

- A global cybersecurity talent shortage means that IT leaders often have little choice but to do business with third-party service partners.[3]
- $1.5 trillion to $2 trillion total cybersecurity market opportunity for cybersecurity technology and service providers — about 10 times the current vended market.[3]
- Security was the top technology sold by 59% of partners, the top skill set that 38% of partners are hiring for, and the top-ranked issue of importance over the last two years.[4]
- 90% of security is delivered through partner-led channels.[4]
- By 2027, 75% of employees will acquire, modify, or create technology outside IT's visibility — up from 41% in 2022.[5]
- Just 29% have high confidence that they have a robust mechanism to test their environments against the most current threat vectors.[6]
- Only 31% of organizations have high confidence that their tools can continuously adjust to new configurations to identify new threats and vulnerabilities.[6]
- Just 32.7% of organizations have high confidence they can investigate every incident.[6]
- Only 34% of organizations have high confidence they can autonomously stop threats in real time.[6]

Steps for Planning Cyber Resilience: Perform a Risk Assessment

Undertaking Risk Assessment

Consider these solutions

Steps for Planning Cyber Resilience: Perform a Risk Assessment

Undertaking Risk Assessment

A cyber resilience plan is built on a solid assessment of the risks your customer's organization is most likely to experience. These can include threats from those within the organization, as well as external threats like data breaches and ransomware attacks.

Regularly undertaking cybersecurity risk assessments is akin to periodically checking the locks and the security system in your home. Is your safety and security at risk? Can intruders "outsmart" your security controls and invade your privacy? Will law enforcement arrive in time to prevent entry?

The same concept holds true for assessing the risks and locking down the digital assets in your customer's organization to seal the gaps and protect against threats.

For your convenience, TD SYNNEX offers a comprehensive suite of top-tier complimentary and billable cybersecurity assessments that you can seamlessly offer to your customers. Complimentary assessments include:[7]

- Infrastructure Security Maturity Assessment
- Cloud Governance Security Maturity Assessment
- General Security Assessment
- Cloud Security Assessment
- Healthcare Security Assessment
- Education Security Assessment
- Vulnerability Assessment

Billable assessments include (you'll find more detail in the Opportunities for MSPs and MSSPs section):[7]

- **Vulnerability Assessment –** Uncovers, prioritizes and recommends action for discovered vulnerabilities.
- **Penetration Test –** Thoroughly evaluates the resilience of your customer's IT infrastructure and provides recommendations.
- **Risk Assessment –** Methodically scrutinizes your customer's cybersecurity capabilities and controls.
- **Compliance Assessment –** Ensures your services stay on the right side of applicable regulatory mandates and cybersecurity practices are up to date.
- **Incident Response Assessments –** Examines your customer's response capabilities to formulate an incident response plan.
- **Zero Trust Assessment –** Dissects your customer's security maturity using zero-trust principles and architectures.

Start by using one of the complimentary assessments in your initial interactions with customers. That can open the door to new opportunities, while serving to deepen your relationship as a trusted advisor.

Identify Assets

But before performing any sort of cybersecurity risk assessment, it's important to understand what assets your customer has, who is responsible for each one and how critical they are to their organization. Assets can include physical assets such as buildings, equipment as well as infrastructure, and intangible assets such as data, intellectual property and reputation.

An asset inventory prioritizes which assets are mission- and business-critical and, therefore, more valuable and susceptible to risk — as well as lower priority assets that require less attention and investment. Taking an asset-based risk assessment approach will be helpful when it comes to developing a risk management plan for your customer.

> *"Cybersecurity assessments are not just about evaluating your current state but highlight the importance of forging a path to a more secure, resilient, and compliant future."*[7]

Only 38%

said they have

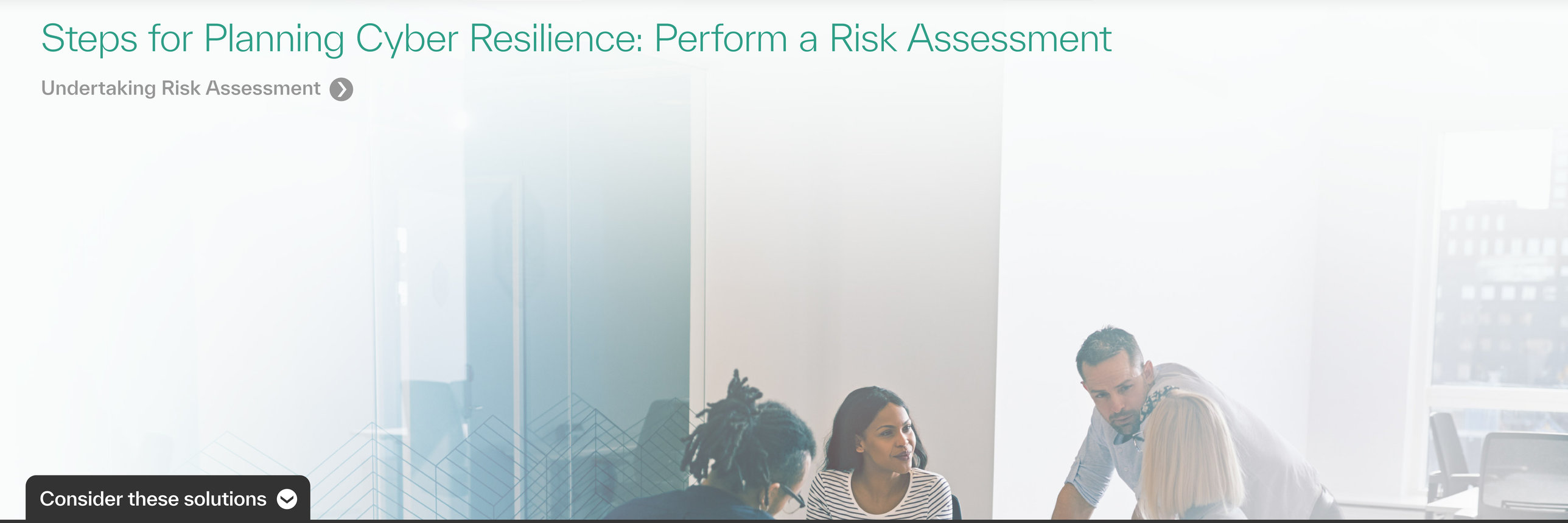
high confidence in having good oversight

over all assets and where they sit within an environment.[6]

Consider these solutions

Steps for Planning Cyber Resilience: Perform a Risk Assessment

Undertaking Risk Assessment



Consider these solutions

ActZero

- **MDR Service With Incident Response Retainer -** Included at no extra cost, ActZero's Incident Response Retainer quickly identifies, isolates and mitigates threats to eliminate adversaries' traces and facilitates rapid recovery to minimize disruption, enhancing overall cyber resilience.

DigiCert

- **DigiCert® Software Trust Manager –** Protects software integrity across the software supply chain, reducing risk of code compromise, enforcing corporate and regulatory policy, performing vulnerability/threats/malware scans, and delivering granular key usage and access controls for code signing.
- **DigiCert® IoT Device Trust Manager –** Addresses the needs of developers, manufacturers, and operators with a simple, scalable IoT security platform for device identity, integrity, and control, delivering time-to-market acceleration, operational security improvements, and full ecosystem enablement.

HP Inc.

- **Predictive PC Analytics and Fleet Security –** The fleet security dashboard will help you gain visibility into overall security of your device fleet so you can identify threats and noncompliant devices and act before they lead to security risks.

Symantec

- **Symantec SMART AI –** Leverages SymantecAI™ for maximum cybersecurity and cyber resilience for SMBs — with Symantec SMART Security and SMART Security Premium and cloud-based Symantec SMART ZTNA and SMART Cloud DLP to identify, respond, and recover from security incidents.

Steps for Planning Cyber Resilience: Develop a Strategy

- Cyber Resillence Strategy
- Establish Objectives
- Allocate Resources
- Create Policies and Procedures

Consider these solutions

Steps for Planning Cyber Resilience: Develop a Strategy

Cyber Resillence Strategy

A cyber resilience strategy helps your customer to prepare for, respond to, and quickly recover from cyberattacks and continue business operations with minimal disruption to workflow and processes.

It starts with a realistic assessment of the potential risks the organization faces, including internal threats and external risks, such as data breaches and ransomware attacks. Planning how to handle a range of risks is not just a best practice, it's a business imperative. While cyber resilience differs from business resilience, greater cyber resilience will increase overall business resilience.

NIST lays out four goals that can be used to help your customer build their cyber resiliency strategy[8]:

1. **Anticipate –** Maintain a state of informed preparedness for adversity.
2. **Withstand –** Continue essential mission or business functions despite adversity.
3. **Recover –** Restore mission or business functions during and after adversity.
4. **Adapt –** Modify mission or business functions and/or supporting capabilities in response to predicted changes in the technical, operational, or threat environments.

In other words, cyber resiliency isn't just the ability to anticipate or withstand a threat. Your customer must improve resiliency by recovering from the threat and then modifying processes, practices, and technologies to better anticipate and withstand the next threat.

Establish Objectives

Allocate Resources

Create Policies and Procedures

Consider these solutions

Steps for Planning Cyber Resilience: Develop a Strategy

Cyber Resillence Strategy

Establish Objectives

NIST has also established cyber resiliency objectives that they describe as "specific statements of what a system is intended to achieve in its operational environment and throughout its life cycle to meet stakeholder needs for mission assurance and resilient security.[8]"

Objective	Description	Discussion
Prevent/Avoid	Preclude the successful execution of an attack or the realization of adverse conditions.	This objective relates to an organization's preferences for different risk response approaches. Risk avoidance or threat avoidance is one possible risk response approach and is feasible under restricted circumstances. Preventing a threat event from occurring is another possible risk response, similarly feasible under restricted circumstances.
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity.	This objective is driven by the recognition that adversity will occur. It specifically relates to an organization's contingency planning, continuity of operations plan (COOP), training, exercises, and incident response and recovery plans for critical systems and infrastructures.
Continue	Maximize the duration and viability of essential mission or business functions during adversity.	This objective specifically relates to essential functions. Its assessment is aligned with the definition of performance parameters, analysis of functional dependencies, and identification of critical assets. Note that shared services and common infrastructures, while not identified as essential per se, may be necessary to essential functions and, thus, related to this objective.
Constrain	Limit damage from adversity.	This objective specifically applies to critical or high-value assets — those cyber assets that contain or process sensitive information, are mission-essential, or provide infrastructure services to mission-essential capabilities.
Reconstitute	Restore as much mission or business functionality as possible after adversity.	This objective relates to essential functions, critical assets, and the services and infrastructures on which they depend. A key aspect of achieving this objective is ensuring that recovery, restoration, or reconstitution efforts result in trustworthy resources. This objective is not predicated on analysis of the source of adversity (e.g., attribution) and can be achieved even without detection of adversity via ongoing efforts to ensure the timely and correct availability of resources.
Understand	Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity.	This objective supports the achievement of all other objectives, most notably Prepare, Reconstitute, Transform, and Re-Architect. An organization's plans for continuous diagnostics and mitigation (CDM), infrastructure services, and other services support this objective. The detection of anomalies, particularly suspicious or unexpected events or conditions, also supports achieving this objective. However, this objective includes understanding resource dependencies and status independent of detection. This objective also relates to an organization's use of forensics and cyberthreat intelligence information sharing.
Transform	Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively.	This objective specifically applies to workflows for essential functions, supporting processes, and incident response and recovery plans for critical assets and essential functions. Tactical modifications are usually procedural or configuration-related; longer-term modifications can involve restructuring operational processes or governance responsibilities while leaving the underlying technical architecture intact.
Re-Architect	Modify architectures to handle adversity and address environmental changes more effectively.	This objective specifically applies to system architectures and mission architectures, which include the technical architecture of the system-of-systems supporting a mission or business function. In addition, this objective applies to architectures for critical infrastructures and services, which often support multiple essential functions.

Source: "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," NIST Special Publication 800-160, Volume 2 Revision 1, 12/2021.

Because every organization is different, these constructs can serve as a guide to help your customer and their stakeholders tailor and prioritize their goals and objectives in support of their business needs.

Allocate Resources

Create Policies and Procedures

Consider these solutions

Steps for Planning Cyber Resilience: Develop a Strategy

Cyber Resillence Strategy

Establish Objectives

Allocate Resources

Cyber resilience requires significant investments in budgets and people. Lack of resources (or poorly allocated resources) unduly raises the threat risk.

That's why a key part of cyber resiliency is ensuring that your customer not only has the necessary resources, but also that those resources — typically hardware, software, and staffing — are appropriately funded. This is critical because it ensures that your customer has the right resources to effectively Anticipate, Withstand, Recover, and Adapt to threats.

It starts with educating your customer's executive team and/or board of directors about acceptable levels of risk and getting their buy-in. Regularly meet with them to discuss what the security team did to reduce risk and how security projects tie into the organization's overall goals. Regularly review and refine your customer's strategy to ensure their resources are being used efficiently and recommend reallocation when they're not.

Create Policies and Procedures

Consider these solutions

Steps for Planning Cyber Resilience: Develop a Strategy

Cyber Resillence Strategy

Establish Objectives

Allocate Resources

Create Policies and Procedures

For processes and technology to be an effective part of a cyber resilience program, governance is required. Recommendations to support governance for the people, processes, and solutions used to support cyber resilience include:

- Board-level commitment and involvement
- Governance structure and processes
- Risk management program
- External certifications and validation
- Internal audits

What makes cyber resilience complicated — continuous change — also drives its success. Changes to the threat landscape, attack surface, people, technology, and systems all need to be rolled into cyber resilience programs as changes occur. This evolution ensures that an organization is optimally prepared to address whatever cyber incidents occur with as little disruption as possible.

Consider these solutions

Steps for Planning Cyber Resilience: Develop a Strategy

Cyber Resillence Strategy

Establish Objectives

Allocate Resources

Create Policies and Procedures

Consider these solutions

ActZero

- **MDR Service With End-to-End Coverage-** Guarantees cyber resilience and better block rate by gathering all data and incorporating industry-leading EDR technologies and AI/ML capabilities, for a comprehensive, fully-managed solution safeguarding mobile, cloud, identity and email accounts.
- **MDR Service With 24/7 SOC -** Our round-the-clock service delivers rapid, automated responses — filtering out noise and focusing on critical alerts — while our AI technology boosts 25x SOC efficiency compared to competitors for proactive threat mitigation and cyber resilience.
- **MDR Service With 24/7 SOC -**Included at no extra cost, ActZero's Incident Response Retainer quickly identifies, isolates, and mitigates threats to eliminate adversaries' traces and facilitates rapid recovery to minimize disruption, enhancing overall cyber resilience.

DigiCert

- **DigiCert® Trust Lifecycle Manager –** For CA-agnostic certificate management and PKI services, this solution centralizes visibility and control over certificates, reduces risk from certificate expiration or human error, automates operations, and enables fast adaptation to changing cybersecurity standards.
- **DigiCert® Software Trust Manager –** Protects software integrity across the software supply chain, reducing risk of code compromise, enforcing corporate and regulatory policy, performing vulnerability/threats/malware scans, and delivering granular key usage and access controls for code signing.
- **DigiCert® IoT Device Trust Manager –** Addresses the needs of developers, manufacturers, and operators with a simple, scalable IoT security platform for device identity, integrity, and control, delivering time-to-market acceleration, operational security improvements, and full ecosystem enablement.

HP Inc.

- **PC Endpoint Security Protection –** Intelligent threat defense that uses deep-learning AI to find and neutralize malware and isolating it before it can attack.
- **The World's Most Secure and Manageable PC and Printer –** With hardware-enforced security, this is the world's first self-healing security solution that leverages built-in hardware for automatic recoveries.
- **Predictive PC Analytics and Fleet Security –** The fleet security dashboard will help you gain visibility into overall security of your device fleet so you can identify threats and noncompliant devices and act before they lead to security risks.

Symantec

- **Symantec SMART Security –** Leads the way in cybersecurity and cyber resilience for businesses and organizations — including Symantec Endpoint Security Complete and Symantec Email Security Cloud for industry-leading endpoint protection, advanced email security, and greater ROI.
- **Symantec SMART Security Premium –** Builds on the power of Symantec SMART Security (Symantec Endpoint Security Complete + Symantec Email Security.cloud) with the added force of Symantec SMART Web Protection, Symantec SMART Encryption, and Symantec SMART Multifactor/MFA.
- **Symantec SMART AI –** Leverages SymantecAI™ for maximum cybersecurity and cyber resilience for SMBs — with Symantec SMART Security and SMART Security Premium AND cloud-based Symantec SMART ZTNA and SMART Cloud DLP to identify, respond, and recover from security incidents.

Veritas

- **Veritas Alta™ Data Protection –** Enjoy data protection and cyber resilience for enterprise cloud workloads with AI-powered automation, flexible recovery options, cloud-native storage technology, and elastic infrastructure for reduced costs and carbon footprint.
- **Veritas Alta™ Recovery Vault –** Provides secure-by-default, cloud-based data vaulting, enabling quick and confident data recovery for ensuring the cyber resilience and continuity of your critical operations.
- **Veritas Alta™ SaaS Protection –** Protect the full range of data stored across SaaS platforms to ensure that data is quickly and easily recoverable in the event of unplanned deletion or a ransomware attack.

Steps for Planning Cyber Resilience: Implement

Implement Security Controls

Deliver Training and Awareness Programs

Perform Incident Response Planning

Consider these solutions

Steps for Planning Cyber Resilience: Implement

Implement Security Controls

A few organizations still struggle to adopt critical security controls (and now, best practices), due in part to their high cost, complex deployment or lack of concern. Even if they do make the investment, these organizations view it as "checking the box" rather than as something that adds strategic value.

Yet, more and more, these controls are becoming must-haves to help mitigate risk and improve overall cybersecurity and resilience. And they are becoming mere minimums just to get cyber insurance. Without them, your customer may be hit with a double whammy of "at risk" and "uninsurable."

These are the security controls that all organizations should have at a minimum for cyber resilience:

- Multifactor authentication (MFA) for remote access and privileged or admin access
- Email filtering and web security
- Secured, encrypted and tested backups
- Privileged access management (PAM)
- Endpoint detection and response (EDR)
- Patch management/vulnerability management

Deliver Training and Awareness Programs

Perform Incident Response Planning

> *Mistakes are made at ALL levels and across ALL departments due to insufficient cyber risk awareness training, distraction, burnout or even complacency. Some of the worst breaches occur from a simple lack of knowledge.*[10]

Consider these solutions

Steps for Planning Cyber Resilience: Implement

Implement Security Controls

Deliver Training and Awareness Programs

They don't mean to do it. There's something about that email that just demands that it be opened. And so, in an instant, an employee unwittingly starts a chain of events that will be hard to come back from.

Educating employees about cyber risks and best practices and developing a culture of cybersecurity awareness is essential to a cyber resilience program.

Ongoing training and awareness helps employees stay on top of emerging threats and techniques and create a security-conscious work environment. In addition to comprehensive cybersecurity training, awareness programs can include regular newsletters, security bulletins, posters and other resources that continually highlight cybersecurity best practices and recent threats.

By continuing an ongoing dialogue about cybersecurity, employees can stay informed and develop a strong security mindset.

Perform Incident Response Planning

> *"Mistakes are made at ALL levels and across ALL departments due to insufficient cyber risk awareness training, distraction, burnout or even complacency. Some of the worst breaches occur from a simple lack of knowledge."*[10]

Consider these solutions

Steps for Planning Cyber Resilience: Implement

Implement Security Controls

Deliver Training and Awareness Programs

Perform Incident Response Planning

Incident Response (IR) planning is crucial, but it isn't just a rote exercise when an incident occurs. It's an integrated step-by-step plan that enables your customer to quickly respond to threats that includes a mechanism for testing and refining to align with evolving threats.

The NIST incident response framework includes:[9]

- **Preparation and prevention –** Compile a list of IT assets and identify which ones are critical or hold sensitive data. Set up monitoring so there's a baseline of normal activity. Determine which types of security events should be investigated and create detailed response steps for common types of incidents.
- **Detection and analysis –** Collect data (from IT systems, security tools, publicly available information and internal/external resources) and identify data showing that an attack has happened or is happening now and signs that an incident may happen in the future. Analyze the data by comparing baseline activity for the affected systems, correlating related events and seeing if/how they deviate from normal behavior.
- **Containment, eradication and recovery –** The containment strategy depends on potential damage, the need to keep critical services available and the duration of the solution. The goal is to stop the attack before it overwhelms resources or causes damage. It's also important to identify the attacking host and validate its IP address. After the incident has been successfully contained, eradicate all elements of the incident from the environment. Then, restore systems and recover normal operations as quickly as possible, taking steps to ensure the same assets are not attacked again.
- **Post-incident activity –** Key to the NIST incident response methodology is learning from the incident at hand to improve the process going forward. Undertake an investigation and document your answers. Use your findings to improve the process and refine your IR policy, plan and procedures.

> *"Mistakes are made at ALL levels and across ALL departments due to insufficient cyber risk awareness training, distraction, burnout or even complacency. Some of the worst breaches occur from a simple lack of knowledge."*[10]

Consider these solutions

Steps for Planning Cyber Resilience: Implement

Implement Security Controls

Deliver Training and Awareness Programs

Perform Incident Response Planning

Consider these solutions

ActZero

- **MDR Service With End-to-End Coverage -** Guarantees cyber resilience and better block rate by gathering all data and incorporating industry-leading EDR technologies and AI/ML capabilities, for a comprehensive, fully-managed solution safeguarding mobile, cloud, identity and email accounts.

DigiCert

- **DigiCert® Trust Lifecycle Manager –** For CA-agnostic certificate management and PKI services, this solution centralizes visibility and control over certificates, reduces risk from certificate expiration or human error, automates operations, and enables fast adaptation to changing cybersecurity standards.
- **DigiCert® Software Trust Manager –** Protects software integrity across the software supply chain, reducing risk of code compromise, enforcing corporate and regulatory policy, performing vulnerability/threats/malware scans, and delivering granular key usage and access controls for code signing.
- **DigiCert® IoT Device Trust Manager –** Addresses the needs of developers, manufacturers, and operators with a simple, scalable IoT security platform for device identity, integrity, and control, delivering time-to-market acceleration, operational security improvements, and full ecosystem enablement.

HP Inc.

- **PC Endpoint Security Protection –** Intelligent threat defense that uses deep-learning AI to find and neutralize malware and isolating it before it can attack.
- **The World's Most Secure and Manageable PC and Printer –** With hardware-enforced security, this is the world's first self-healing security solution that leverages built-in hardware for automatic recoveries.
- **Predictive PC Analytics and Fleet Security –** The fleet security dashboard will help you gain visibility into overall security of your device fleet so you can identify threats and noncompliant devices and act before they lead to security risks.

Symantec

- **Symantec SMART Security –** Leads the way in cybersecurity and cyber resilience for businesses and organizations — including Symantec Endpoint Security Complete and Symantec Email Security Cloud for industry-leading endpoint protection, advanced email security, and greater ROI.
- **Symantec SMART Security Premium –** Builds on the power of Symantec SMART Security (Symantec Endpoint Security Complete + Symantec Email Security.cloud) with the added force of Symantec SMART Web Protection, Symantec SMART Encryption, and Symantec SMART Multifactor/MFA.
- **Symantec SMART AI –** Leverages SymantecAI™ for maximum cybersecurity and cyber resilience for SMBs — with Symantec SMART Security and SMART Security Premium AND cloud-based Symantec SMART ZTNA and SMART Cloud DLP to identify, respond, and recover from security incidents.

Steps for Planning Cyber Resilience: Testing and Evaluation

Undertake Routine Security Audits

Perform Penetration Testing

Undergo Tabletop Exercises

Consider this solution

Steps for Planning Cyber Resilience: Testing and Evaluation

Undertake Routine Security Audits

As cyber threats continue to evolve, routine security audits—vital to shoring up your customer's defenses and ensuring the resilience of their environment—must evolve along with them. Here are four ways that AI powers routine security audits:[1]

- **Enhanced threat intelligence and analysis –** Analyze vast datasets and identify patterns, providing an unparalleled level of threat intelligence that allows auditors to delve deeper into potential risks.
- **Predictive analytics for proactive –** Give auditors the foresight needed to anticipate and proactively address potential vulnerabilities. By learning from historical data and predicting future threats, auditors can fortify defenses before new risks materialize, transforming the auditing process from reactive to proactive.
- **Efficiency through automation and optimization –** Streamline mundane tasks, such as data analysis and routine checks, allowing auditors to focus their expertise on critical decision-making. This not only enhances efficiency but also ensures a more thorough and nuanced evaluation of security measures.
- **Dynamic adaptation to evolving cyber threats –** AI-driven audits evolve in real time, learning from emerging threats and adjusting methodologies accordingly. This adaptability is crucial in an environment where the only constant is change, enabling auditors to stay ahead of the curve.

Perform Penetration Testing

Undergo Tabletop Exercises

Consider this solution

Steps for Planning Cyber Resilience: Testing and Evaluation

Undertake Routine Security Audits

Perform Penetration Testing

With AI, the ability to automate repetitive and time-consuming penetration testing tasks has increased substantially. AI-powered pen testing can simulate hacking attacks on systems to uncover vulnerabilities and threats that might be exploited by real-world hackers.

For example, machine learning machine-learning can quickly cull large data sets to identify patterns or anomalies for significantly faster detection of vulnerabilities and misconfigurations. This kind of automation enables pen testers to focus on more complex vulnerabilities that require more critical and nuanced human thought.

In addition, automation allows pen testing to be conducted more efficiently and comprehensively, so you can shore up your customer's defenses in less time.

Just 34%

feel that pen testing/red teaming can provide them with **actionable insights** on where and how to harden defenses.[6]

Undergo Tabletop Exercises

Consider this solution

Steps for Planning Cyber Resilience: Testing and Evaluation

Undertake Routine Security Audits

Perform Penetration Testing

Undergo Tabletop Exercises

Cybersecurity leaders often use tabletop exercises to improve threat preparedness and response capabilities. These exercises simulate real-world incidents in a controlled environment, which enables your customer to test their IR, evaluate team coordination and identify vulnerabilities.

But AI and machine learning (ML) technologies can now model and simulate adversarial behaviors, both known and unknown. By analyzing historical attack data, threat intelligence and patterns, these technologies can generate realistic adversary profiles.

Tabletop exercises can then include a range of adversarial behaviors, for more real-world exercises. Algorithms can analyze historical data from previous incidents and help identify patterns and trends. With this data, your customer can predict and anticipate future threats, vulnerabilities or attack vectors. And predictive analytics helps security teams proactively enhance their defensive skills.[10]

Consider this solution

Steps for Planning Cyber Resilience: Testing and Evaluation

Undertake Routine Security Audits

Perform Penetration Testing

Undergo Tabletop Exercises

Consider this solution

DigiCert

- **DigiCert® Software Trust Manager –** Protects software integrity across the software supply chain, reducing risk of code compromise, enforcing corporate and regulatory policy, performing vulnerability/threats/malware scans, and delivering granular key usage and access controls for code signing.

Leveraging AI for Cyber Resilience: AI in Threat Detection

Today's organizations can combine AI/ML with automation to strengthen their cyber resilience. It helps you detect and prevent cyberattacks by recognizing suspicious behavior patterns, such as identifying network vulnerabilities before cyber criminals gain access.

Machine-Learning

Traditional antivirus and malware detection tools use signatures or indicators of compromise to identify and detect previously known threats. But how do you detect unknown threats?

Machine learning augments traditional signature-based methods of threat detection to quickly detect new threats in the wild. It automates manual work, especially in processes where high levels of accuracy are needed—such as instantaneously discerning the differences between benign and malicious threats—and responding with machine-level speed. The goal is to maximize true positive detections while minimizing false positives. Though machine learning models can better detect unknown threats with a high degree of accuracy, it doesn't take the place of human expertise and interpretation.

Behavioral Analysis

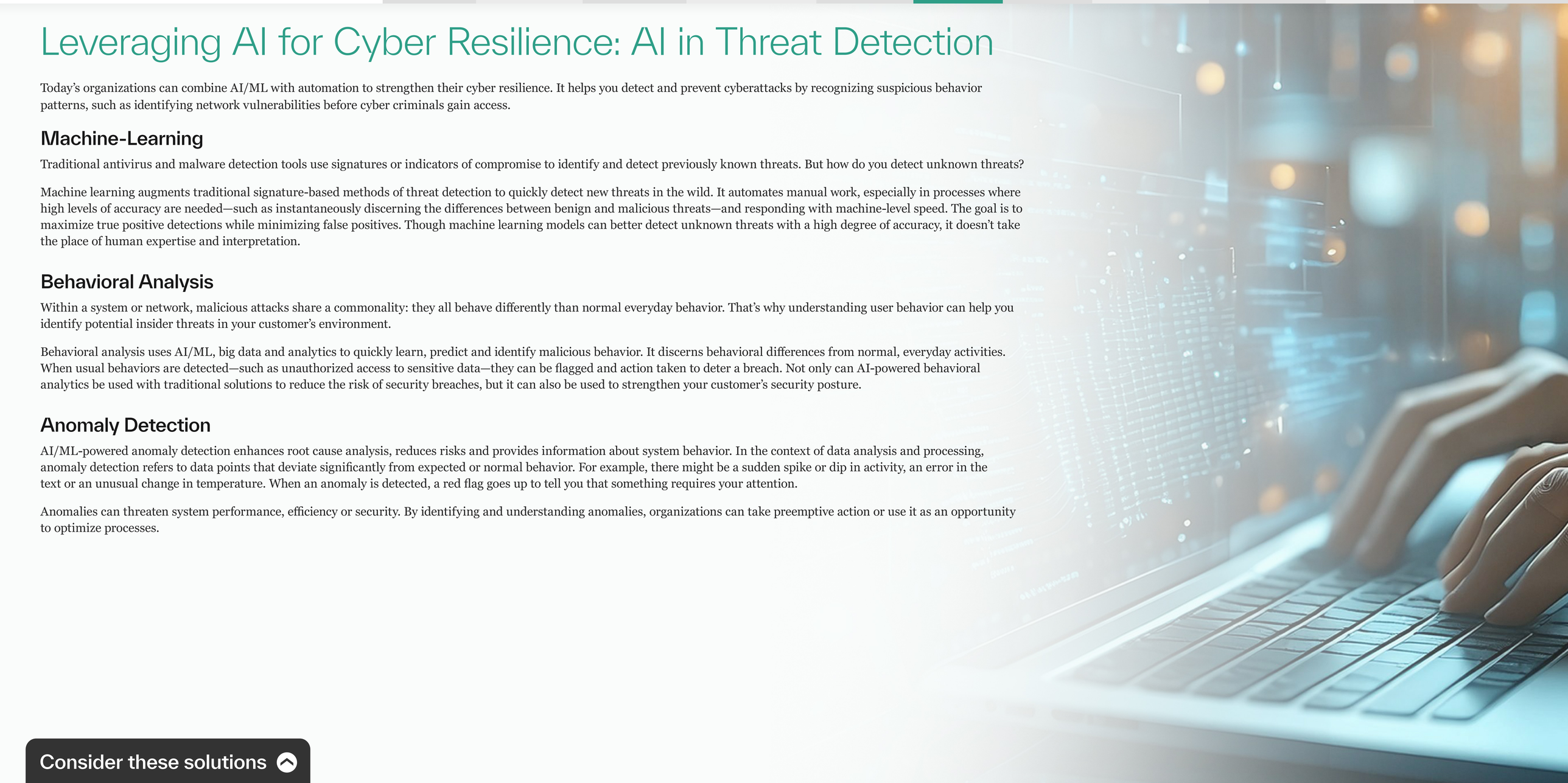
Within a system or network, malicious attacks share a commonality: they all behave differently than normal everyday behavior. That's why understanding user behavior can help you identify potential insider threats in your customer's environment.

Behavioral analysis uses AI/ML, big data and analytics to quickly learn, predict and identify malicious behavior. It discerns behavioral differences from normal, everyday activities. When usual behaviors are detected—such as unauthorized access to sensitive data—they can be flagged and action taken to deter a breach. Not only can AI-powered behavioral analytics be used with traditional solutions to reduce the risk of security breaches, but it can also be used to strengthen your customer's security posture.

Anomaly Detection

AI/ML-powered anomaly detection enhances root cause analysis, reduces risks and provides information about system behavior. In the context of data analysis and processing, anomaly detection refers to data points that deviate significantly from expected or normal behavior. For example, there might be a sudden spike or dip in activity, an error in the text or an unusual change in temperature. When an anomaly is detected, a red flag goes up to tell you that something requires your attention.

Anomalies can threaten system performance, efficiency or security. By identifying and understanding anomalies, organizations can take preemptive action or use it as an opportunity to optimize processes.



Leveraging AI for Cyber Resilience: AI in Threat Detection

Today's organizations can combine AI/ML with automation to strengthen their cyber resilience. It helps you detect and prevent cyberattacks by recognizing suspicious behavior patterns, such as identifying network vulnerabilities before cyber criminals gain access.

Machine-Learning

Traditional antivirus and malware detection tools use signatures or indicators of compromise to identify and detect previously known threats. But how do you detect unknown threats?

Machine learning augments traditional signature-based methods of threat detection to quickly detect new threats in the wild. It automates manual work, especially in processes where high levels of accuracy are needed—such as instantaneously discerning the differences between benign and malicious threats—and responding with machine-level speed. The goal is to maximize true positive detections while minimizing false positives. Though machine learning models can better detect unknown threats with a high degree of accuracy, it doesn't take the place of human expertise and interpretation.

Behavioral Analysis

Within a system or network, malicious attacks share a commonality: they all behave differently than normal everyday behavior. That's why understanding user behavior can help you identify potential insider threats in your customer's environment.

Behavioral analysis uses AI/ML, big data and analytics to quickly learn, predict and identify malicious behavior. It discerns behavioral differences from normal, everyday activities. When usual behaviors are detected—such as unauthorized access to sensitive data—they can be flagged and action taken to deter a breach. Not only can AI-powered behavioral analytics be used with traditional solutions to reduce the risk of security breaches, but it can also be used to strengthen your customer's security posture.

Anomaly Detection

AI/ML-powered anomaly detection enhances root cause analysis, reduces risks and provides information about system behavior. In the context of data analysis and processing, anomaly detection refers to data points that deviate significantly from expected or normal behavior. For example, there might be a sudden spike or dip in activity, an error in the text or an unusual change in temperature. When an anomaly is detected, a red flag goes up to tell you that something requires your attention.

Anomalies can threaten system performance, efficiency or security. By identifying and understanding anomalies, organizations can take preemptive action or use it as an opportunity to optimize processes.

Consider these solutions

HP Inc.

- **PC Endpoint Security Protection –** Intelligent threat defense that uses deep-learning AI to find and neutralize malware and isolating it before it can attack.
- **Predictive PC Analytics and Fleet Security –** The fleet security dashboard will help you gain visibility into overall security of your device fleet so you can identify threats and noncompliant devices and act before they lead to security risks.

Symantec

- **Symantec SMART AI –** Leverages SymantecAI™ for maximum cybersecurity and cyber resilience for SMBs — with Symantec SMART Security and SMART Security Premium AND cloud-based Symantec SMART ZTNA and SMART Cloud DLP to identify, respond, and recover from security incidents.

Veritas

- **Veritas Alta™ Data Protection –** Enjoy data protection and cyber resilience for enterprise cloud workloads with AI-powered automation, flexible recovery options, cloud-native storage technology, and elastic infrastructure for reduced costs and carbon footprint.

Leveraging AI for Cyber Resilience: AI in Incident Response

AI offers an important ability to "separate the wheat from the chaff" by quickly breaking down and triaging hundreds of alerts coming in at once. It can then automate responses for routine alerts and prioritize critical alerts for immediate action. Again, AI does not replace human expertise. A successful incident response program understands that analysts bring significant skills to bear on interpretation, including understanding context and thinking critically and ethically and can marry those skills with AI's capabilities for a comprehensive incident response (IR) strategy.

Automated Incident Triage

As an incident is detected, AI can automatically classify it based on severity and prioritize it using historical and predefined data. With automated incident triage, critical incidents receive immediate attention, enabling faster resolution and minimizing downtime, while lower priority incidents can be put in a queue for automated resolution. Not only can AI reduce the number of false-positive alerts, it also minimizes the impact on business operations.

Response Orchestration

IR orchestration empowers teams by giving them the processes and tools they need to act quickly, effectively and correctly when a security incident arises. AI uses historical data and past remediation actions to provide recommendations for fast and effective remediation. It analyzes current and previously resolved incident data and suggests specific steps to take—such as isolating compromised systems, applying patches, updating security configurations or deploying additional security controls—based on proven best practices.

AI can also help your customer to prevent future incidents. It analyzes incident data to identify security vulnerabilities, misconfigurations or gaps and provides guidance on enhancing defenses, such as implementing intrusion detection and prevention systems, tightening access controls, updating security policies or conducting security awareness training.

Using AI, your customer can distill massive data sets into actionable insights that can be used to quickly mitigate incidents in the present, while preventing future incidents.

Predictive Analysis

When an incident occurs, fast response is required—whether that's routing it to a queue for an automated response or alert a human for a more nuanced response. But it would be beneficial to get ahead of and block potential incidents before they become issues. That is the premise of predictive analytics.

AI uses machine learning algorithms to analyze historical data and spot patterns and vulnerabilities in order to predict future incidents. Properly configured Predictive AI can automatically monitor, categorize and alert teams to potential threats. This approach gives your customer time to harden security policies and mitigate future attacks by putting preventative measures in place.

Leveraging AI for Cyber Resilience: AI in Incident Response

AI offers an important ability to "separate the wheat from the chaff" by quickly breaking down and triaging hundreds of alerts coming in at once. It can then automate responses for routine alerts and prioritize critical alerts for immediate action. Again, AI does not replace human expertise. A successful incident response program understands that analysts bring significant skills to bear on interpretation, including understanding context and thinking critically and ethically and can marry those skills with AI's capabilities for a comprehensive incident response (IR) strategy.

Automated Incident Triage

As an incident is detected, AI can automatically classify it based on severity and prioritize it using historical and predefined data. With automated incident triage, critical incidents receive immediate attention, enabling faster resolution and minimizing downtime, while lower priority incidents can be put in a queue for automated resolution. Not only can AI reduce the number of false-positive alerts, it also minimizes the impact on business operations.

Response Orchestration

IR orchestration empowers teams by giving them the processes and tools they need to act quickly, effectively and correctly when a security incident arises. AI uses historical data and past remediation actions to provide recommendations for fast and effective remediation. It analyzes current and previously resolved incident data and suggests specific steps to take—such as isolating compromised systems, applying patches, updating security configurations or deploying additional security controls—based on proven best practices.

AI can also help your customer to prevent future incidents. It analyzes incident data to identify security vulnerabilities, misconfigurations or gaps and provides guidance on enhancing defenses, such as implementing intrusion detection and prevention systems, tightening access controls, updating security policies or conducting security awareness training.

Using AI, your customer can distill massive data sets into actionable insights that can be used to quickly mitigate incidents in the present, while preventing future incidents.

Predictive Analysis

When an incident occurs, fast response is required—whether that's routing it to a queue for an automated response or alert a human for a more nuanced response. But it would be beneficial to get ahead of and block potential incidents before they become issues. That is the premise of predictive analytics.

AI uses machine learning algorithms to analyze historical data and spot patterns and vulnerabilities in order to predict future incidents. Properly configured Predictive AI can automatically monitor, categorize and alert teams to potential threats. This approach gives your customer time to harden security policies and mitigate future attacks by putting preventative measures in place.

Consider these solutions

ActZero

- **MDR Service with Incident Response Retainer –** Included at no extra cost, ActZero's Incident Response Retainer quickly identifies, isolates and mitigates threats to eliminate adversaries' traces and facilitates rapid recovery to minimize disruption, enhancing overall cyber resilience.

HP Inc.

- **The World's Most Secure and Manageable PC and Printer –** With hardware-enforced security, this is the world's first self-healing security solution that leverages built-in hardware for automatic recoveries.

Symantec

- **Symantec SMART AI –** Leverages SymantecAI™ for maximum cybersecurity and cyber resilience for SMBs—with Symantec SMART Security and SMART Security Premium AND cloud-based Symantec SMART ZTNA and SMART Cloud DLP to identify, respond and recover from security incidents.

Veritas

- **Veritas Alta™ Data Protection –** Enjoy data protection and cyber resilience for enterprise cloud workloads with AI-powered automation, flexible recovery options, cloud-native storage technology, and elastic infrastructure for reduced costs and carbon footprint.
- **Veritas Alta™ Recovery Vault –** Provides secure-by-default, cloud-based data vaulting, enabling quick and confident data recovery for ensuring the cyber resilience and continuity of your critical operations.
- **Veritas Alta™ SaaS Protection –** Protect the full range of data stored across SaaS platforms to ensure that data is quickly and easily recoverable in the event of unplanned deletion or a ransomware attack.

Leveraging AI for Cyber Resilience: AI in Vulnerability Management

While attackers are using new technologies (like AI) to launch sophisticated attacks and evade detection, they are also going back to their old playbook. With greater contextual intelligence about which common vulnerabilities and exposures (CVEs) are most vulnerable, bad actors can easily weaponize legacy CVEs in organizations with lax patch management practices.

Automated Patching

AI-powered patch management removes the herculean effort of manual patching to automate and streamline the patch management process. Systems are automatically scanned to detect missing patches and testing is done before deployment. Patches can be automatically distributed and applied to targeted devices.

In addition, automated patching tools can typically identify patching needs and allow you to create and maintain an automated patching schedule that aligns with your customer's policies.

Not only does automated patching boost network security, but it's also significantly faster and more efficient, making it much easier to stay up to date with patches.

Vulnerability Scanning

The main purpose of a vulnerability scanner is to probe your systems' defenses and gather useful information about vulnerabilities—such as outdated or non-patched software, misconfigurations, coding flaws, etc.—that could be exploited.

With AI/ML, these data analyses can be performed in real time, enabling vulnerabilities to be prioritized far more quickly and efficiently than any human can prioritize them. AI-powered vulnerability scanning tools are also better at predicting risk factors that are usually indicators of more complex attack vectors, such as phishing or user-related weaknesses.

Once the scanning is complete, you'll receive a detailed report on problem areas that may be used to gain unauthorized access to your customer's systems, steal sensitive information, or disrupt business operations. This report can then be used to remediate serious weaknesses and/or increase the level of security before there are issues.

Finally, since cyberthreats are continually evolving, monitoring and detecting threats with AI-powered vulnerability scanning is typically an ongoing process.

Prioritizing Risk

How can security teams more efficiently manage and prioritize vulnerabilities?

AI helps teams to intelligently analyze vulnerabilities based on factors, such as severity, exploitability and potential business impact. This approach not only enables security teams to focus on the most critical issues, but it also maximizes the effectiveness of remediation efforts.

The team can develop a risk-based remediation plan focusing on high-risk vulnerabilities, while continuously monitoring and retesting for more effective vulnerability management.

> *"Old versions of applications which are unsupported remain in active use on millions of commercial devices. As a result, organizations are at risk of carrying vulnerabilities that will not be patched.[13]"*

> *"While some of these adversaries use advanced tools and techniques, most take advantage of unpatched vulnerabilities, poor cyber hygiene or the failure of organizations to implement critical technologies……[14]"*

Leveraging AI for Cyber Resilience: AI in Vulnerability Management

While attackers are using new technologies (like AI) to launch sophisticated attacks and evade detection, they are also going back to their old playbook. With greater contextual intelligence about which common vulnerabilities and exposures (CVEs) are most vulnerable, bad actors can easily weaponize legacy CVEs in organizations with lax patch management practices.

Automated Patching

AI-powered patch management removes the herculean effort of manual patching to automate and streamline the patch management process. Systems are automatically scanned to detect missing patches and testing is done before deployment. Patches can be automatically distributed and applied to targeted devices.

In addition, automated patching tools can typically identify patching needs and allow you to create and maintain an automated patching schedule that aligns with your customer's policies.

Not only does automated patching boost network security, but it's also significantly faster and more efficient, making it much easier to stay up to date with patches.

Vulnerability Scanning

The main purpose of a vulnerability scanner is to probe your systems' defenses and gather useful information about vulnerabilities—such as outdated or non-patched software, misconfigurations, coding flaws, etc.—that could be exploited.

With AI/ML, these data analyses can be performed in real time, enabling vulnerabilities to be prioritized far more quickly and efficiently than any human can prioritize them. AI-powered vulnerability scanning tools are also better at predicting risk factors that are usually indicators of more complex attack vectors, such as phishing or user-related weaknesses.

Once the scanning is complete, you'll receive a detailed report on problem areas that may be used to gain unauthorized access to your customer's systems, steal sensitive information, or disrupt business operations. This report can then be used to remediate serious weaknesses and/or increase the level of security before there are issues.

Finally, since cyberthreats are continually evolving, monitoring and detecting threats with AI-powered vulnerability scanning is typically an ongoing process.

Prioritizing Risk

How can security teams more efficiently manage and prioritize vulnerabilities?

AI helps teams to intelligently analyze vulnerabilities based on factors, such as severity, exploitability and potential business impact. This approach not only enables security teams to focus on the most critical issues, but it also maximizes the effectiveness of remediation efforts.

The team can develop a risk-based remediation plan focusing on high-risk vulnerabilities, while continuously monitoring and retesting for more effective vulnerability management.

> *"Old versions of applications which are unsupported remain in active use on millions of commercial devices. As a result, organizations are at risk of carrying vulnerabilities that will not be patched.*[13]

> *"While some of these adversaries use advanced tools and techniques, most take advantage of unpatched vulnerabilities, poor cyber hygiene or the failure of organizations to implement critical technologies……*[14]

Consider these solutions

HP Inc.

- **Predictive PC Analytics and Fleet Security –** The fleet security dashboard will help you gain visibility into overall security of your device fleet so you can identify threats and noncompliant devices and act before they lead to security risks.

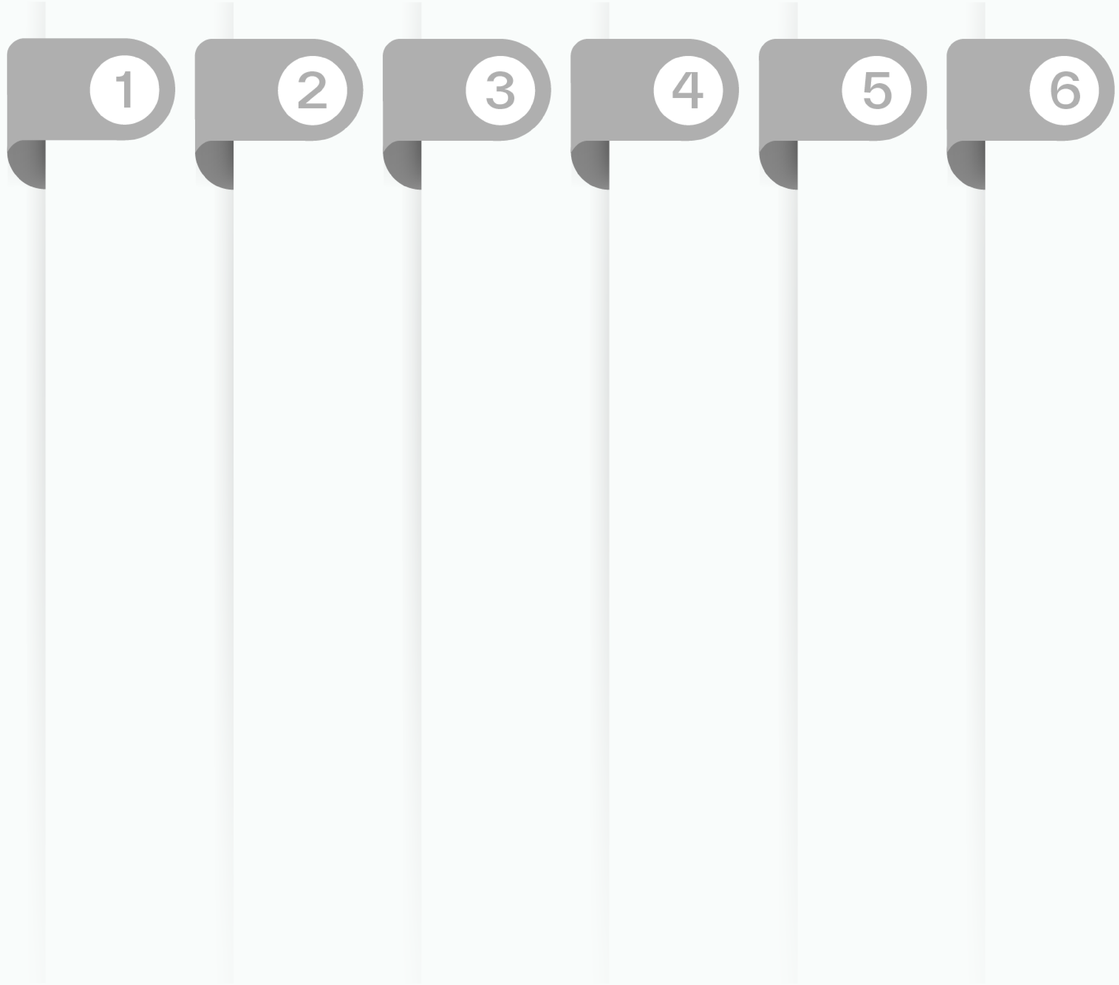
Symantec

- **Symantec SMART AI –** Leverages SymantecAI™ for maximum cybersecurity and cyber resilience for SMBs — with Symantec SMART Security and SMART Security Premium AND cloud-based Symantec SMART ZTNA and SMART Cloud DLP to identify, respond, and recover from security incidents.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments.

Is your customer ready to take their first steps? Start by offering these services:



Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments.

Is your customer ready to take their first steps? Start by offering these services:

1 Build a Zero-Trust Roadmap

Success starts with a comprehensive zero-trust roadmap that outlines the activities needed to implement your customer zero-trust strategy. This strategy document will provide a clear view of the deliverables, budget, and business outcomes expected.

- Determine a framework, whether it's the NIST or CISA framework or a framework from Gartner, Forrester, or others. TD SYNNEX can help you select the right vendors to craft a zero-trust vision.
- Recruit business and IT stakeholders—from IT operators to enterprise architects to business unit leaders to C-suite executives—who can help build your customer's zero-trust roadmap and evangelize the need for new or shifting investments or significant cultural and organizational change.
- Identify interdependencies between the zero-trust implementation and other IT and business projects.

2 3 4 5 6

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments.

Is your customer ready to take their first steps? Start by offering these services:

1 2 3 4 5 6

2 Refine the Business Continuity Plan

Every organization today should have a business continuity plan that outlines what happens when (not if) they're attacked. The next step is to help them adopt or periodically stress-test and refine their business continuity plan.

Then, put together an up-to-date inventory of systems and their criticality to make it easy to prioritize actions in case there's a threat or attack. Create playbooks, conduct tabletop exercises, and test backups for critical assets.

The more you can help them prepare, the better off they'll be in the event of a cyberattack or other disaster.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments.

Is your customer ready to take their first steps? Start by offering these services:

1 2

3 Assess Their Environment

4 5 6

Next, help your customer understand their unique risks by identifying vulnerabilities in their environment and providing recommendations. Take advantage of these assessments:

- **Security Maturity Assessment –** Get a complimentary 45-minute assessment of your customer's security practices and controls and provide a graded report with a customized action plan to improve their security posture.
- **Penetration Testing –** Show them how bad actors exploit their systems to access and disclose sensitive data, and how to best prioritize vulnerabilities for remediation.
- **Vulnerability Assessments –** Point out the pathways that attackers use to exploit their systems and provide a complete financial risk analysis with ways to re-allocate limited resources to ensure they're protected.
- **Additional Assessments –** Access additional assessment capabilities, including Security Risk Assessments, Physical Security Assessments, Physical Penetration Testing, GDPR Assessments, and many others.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments.

Is your customer ready to take their first steps? Start by offering these services:

1 2 3

4 Offer Comprehensive Services

5 6

Help customers focus on their core business by leveraging our advanced managed and other security services.

- **Incident Response Services –** Comprehensive Incident Response (IR) services—including Plan Development, Readiness Review, and Emergency Response—ensure they have the right capabilities to respond to and recover from threats.
- **Compliance Services –** Governance and compliance readiness services for HIPAA, HITRUST, PCI-DSS, NIST 801-171, ISO 27001, NERC-CIP, SOC 1and2, GDPR, and others—ideal for businesses that face a high regulatory burden.
- **Implementation Services –** Services for new installations, integrations, patch services, configurations, and staff augmentations to help you design the best solution for them.
  - **SOC-as-a-Service –** Have a bench of cyber experts who can monitor, analyze, manage, and act on threats across your customer's business.
  - **Firewall Services –** Help your customer focus on their core business while you administer, monitor, and maintain their firewall infrastructure.
  - **ISAO Threat Feed –** Join a very large community of companies, local governments, and security professionals to collaborate, share intelligence, and participate in training and conferences and leverage competent collaborative analysis.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments.

Is your customer ready to take their first steps? Start by offering these services:

1 2 3 4

5 Engage through training and engagement experiences

6

Engage your customer's team with numerous training and engagement experiences for both new and advanced users.

Training

- **Foundational –** Develop the foundational cybersecurity skills needed to advance to the next level through the Cyber Essentials Series.
- **Accelerated –** Access over 50 cloud-based, instructor-led classroom learning courses to prepare for cybersecurity careers and train on a hyper-realistic network within a cloud-hosted cyber range using the tools your team uses every day.
- **Virtual –** Choose from an extensive set of courses for new cybersecurity team members or, for more advanced users, an upgraded training program that includes the entire course library, 200+ Virtual Lab Environments, a guided mentor, and industry certification practice tests.
- **Advanced threat training –** Learn how to contain threats, fix weaknesses, and use the latest threat hunting tools via online, gamified training using real-world simulations within a protected environment.

Engagement

- **Demos –** Test and engage with leading cybersecurity offerings to see how they work in real time.
- **Engagement –** Engage in an "up close and personal" live cyber experience to test the responses of your team and/or environment in a cyber range.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments.

Is your customer ready to take their first steps? Start by offering these services:

1 2 3 4 5

6 Sell and Build SASE and XDR into the Security Stack

According to Gartner, "by 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch, and edge access, up from 10% in 2020."[15] Security leaders will also want to consolidate their products/vendors, be more proactive in their response to threats, and drive greater efficiency—and they're increasingly turning to MSPs and MSSPs who truly understand their security challenges.

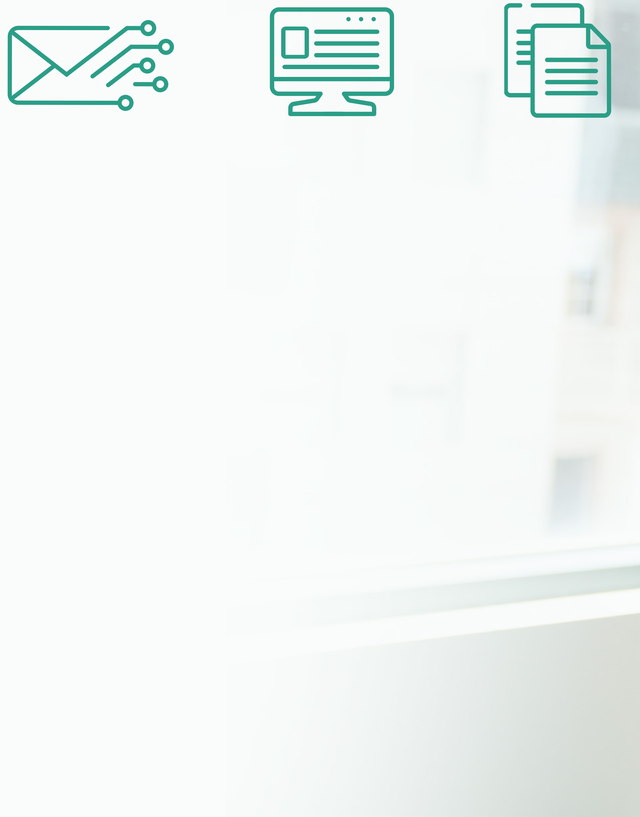
- Perform a gap analysis and establish a high-level SASE strategy and roadmap that's closely aligned with business goals and wider organizational strategic initiatives (such as cloud migration, cybersecurity policies, and IT strategy plans). Ensure the plan leverages the customer's existing assets and enables them to transition to a SASE model over time.
- Assess your client's current network and security environment, and the resources they have available, to determine which services they need, the processes to be used, what technologies will be deployed, and the training required.
- If your customer already has an SD-WAN, they may only need SSE capabilities. If they don't, determine whether they can benefit from SASE now or whether SSE can be an on-ramp for SASE.
- Evaluate the point solutions your customer has and any underutilized functionality, as well as the level of automation and integration between them, and consider a consolidation strategy anchored with XDR.
- Help your customer understand the synergistic value offered by XDR—for example, underlying data lake foundation with lower-cost and flexible data storage, functional orchestration and automation, and advanced security analytics—and not just in how you can pare down the number of solutions and/or vendors.
- Deliver XDR as a service to minimize maintenance for you and your customer.
- Cut time to sale by packaging up or bundling solutions you've already vetted—or provide a menu of pre-vetted vendor solutions from which to choose.

We're Here to Help

If your team is short on time, budget or expertise, we can help. We're backed by a team of dedicated security consultants with the expertise and resources to ensure that your customer's environment is secure. Our solutions and services, extensive portfolio, and industry expertise help address most critical cybersecurity needs.

Our sponsors are listed on the next page, along with contact information to reach a TD SYNNEX security professional.

Contact the Team



Thank You!

For more information on any one of these or other TD SYNNEX security solutions or services, please contact the security professionals below:

ActZero

To learn more about our service, read how AI is changing the cybersecurity game or reach out to ActZero@tdsynnex.com to see how organizations can leave the defense to us.

digicert®

To learn more, contact us at DigicertBD@tdsynnex.com .

hp

Reach out to your dedicated HP Inc. team at TD SYNNEX to learn more! For PC and Services, contact HPPSG@tdsynnex.com or for Print and Supplies, contact HPINC.PG2@tdsynnex.com.

Symantec™ by Broadcom

For more information about Symantec SMART AI, Symantec SMART Security Premium and Symantec SMART Security, contact sales specialists at BroadcomBD@tdsynnex.com.

VERITAS™

To learn more, visit www.tdsynnex.com/na/us/veritas/ or reach out to Veritas@tdsynnex.com.

References and Further Reading

1. Who's Hacked? Latest Data Breaches and Cyberattacks," CybersecurityVentures.com, retrieved 03/16/2024.
2. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-171 Revision 2, 02/2020.
3. "New Survey Reveals $2 Trillion Market Opportunity for Cybersecurity Technology and Service Providers," McKinsey.com, 10/27/2022.
4. "Direction of Technology 2023: TD SYNNEX Ecosystem Report," 2023.
5. "IT Road Map for Cybersecurity," Gartner.com, #2290572, 2023.
6. "Building the Case for a Virtuous Cycle in Cybersecurity," IDC.com, #EUR149649622, 01/2023.
7. TD SYNNEX. "Unlocking Cyber Resilience: A Deep Dive into Risk Assessments," LinkedIn, 2023, https://www.linkedin.com/pulse/unlocking-cyber-resilience-deep-dive-risk-assessments-tdsynnex-yeamc/?trk=organization_guest_main-feed-card_feed-article-content.
8. "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," NIST Special Publication 800-160, Volume 2 Revision 1, 12/2021.
9. "NIST Incident Response Plan: Process, Templates, and Examples," Cynet.com.
10. "The Human Firewall: Strengthening the Weakest Link in Cybersecurity," CyberDefenseMagazine.com, 12/12/2023.
11. DANIEL DANSO. "Leveraging AI in security audits," LinkedIn, 12/20/2023. https://www.linkedin.com/pulse/leveraging-ai-security-audits-daniel-danso-dthxf/
12. "Strengthening Cyber Defenses: A Guide to Enhancing Modern Tabletop Exercises," CyberLeadershipInstitute.org, 09/23/2024.
13. Microsoft Digital Defense Report 2022," Microsoft.com.
14. Jen Easterly, Director/CISA.
15. "2021 Strategic Roadmap for SASE Convergence," Gartner.com, 03/24/2021.