DELL Technologies

Advance Your Cybersecurity and Zero Trust Maturity

Don’t let security risks stifle your innovation

Know where your cybersecurity stands

Know where it needs to get to

In today's complex and rapidly evolving threat landscape, organizations often face resource and knowledge limitations when it comes to maintaining robust cybersecurity practices. Advancing cybersecurity and zero trust maturity is essential to combat evolving cyber threats to keep your environment safe while not stifling innovation.

Use these checklists to assess the current state of your cybersecurity maturity. Knowing your organization's strengths and vulnerabilities enables you to take the right next steps in advancing your cybersecurity maturity.

Contents

Learn more

Learn more about advancing your cybersecurity and zero trust maturity

Checklist:

Reduce the attack surface

The attack surface refers to all the possible points or areas in an environment that can be targeted or exploited by a cyber attacker. These points can include software vulnerabilities, misconfigurations, weak authentication mechanisms, unpatched systems, excessive user privileges, open network ports, poor physical security and more. These questions can help determine how you can minimize vulnerabilities and entry points that a malicious actor can compromise.

Yes	No	
☐	☐	Does your organization perform regular assessments, penetration testing or breach attack simulations to identify vulnerabilities and weaknesses in systems and networks, allowing for timely remediation and improvement?
☐	☐	Does your organization perform regular security training for your employees?
☐	☐	Does your organization utilize Multifactor Authentication (MFA) and Roles Based Access Controls (RBAC)?
☐	☐	Has your organization implemented network segmentation to isolate critical assets and limit access between different parts of your network?
☐	☐	Is your organization implementing secure coding practices, conducting regular security testing and code reviews, and using web application firewalls (WAFs) to help protect against common application-level attacks and reduce the attack surface of web applications?
☐	☐	Does your organization choose IT suppliers who can attest to the processes and procedures to secure their supply chain?
☐	☐	Is your organization implementing zero trust principles to replace traditional perimeter-based security?
☐	☐	Does your organization leverage the principle of least privilege to limit users and system accounts to only have the minimum access rights necessary to perform their tasks?
☐	☐	Does your organization regularly patch your systems and software?
☐	☐	Do your organization's security tools utilize AI/ML capabilities to help proactively identify vulnerabilities?

Checklist:

Detect and respond to threats

Detecting and responding to cyber threats is an essential component of any security strategy. It involves monitoring and analyzing network traffic, system logs, and other areas as well as security data to identify signs of unauthorized access, intrusions, malware infections, data breaches, or other cyber threats. These questions can help determine how your organization proactively identifies and actively addresses potential security incidents and malicious activities within a computer network, system, or organization.

Yes	No	
☐	☐	Does your organization continuously monitor network and system activities using security tools and technologies Extended Detection and Response (XDR), intrusion detection systems (IDS), intrusion prevention systems (IPS), SIEM and log analysis?
☐	☐	Does your organization analyze collected data to identify patterns, anomalies, and indicators of compromise (IoCs) and/or indicators of attack (IOA) that may indicate a potential cyber threat?
☐	☐	Has your organization deployed the latest visibility and monitoring tools to quickly detect and alert on potential?
☐	☐	Does your organization monitor network traffic for unusual patterns or suspicious activity that may indicate a cyberattack in progress?
☐	☐	Has your organization implemented any AI/ML tools to help detect cyber threats through real-time analysis of unusual data patterns or behaviors?
☐	☐	Has your organization considered implementing a next generation SIEM solution to better manage security alerts and begin the correlation of security event data from across the IT ecosystem?
☐	☐	Does your organization practice vulnerability testing and management to prioritize and address existing vulnerabilities, as well as efficiently respond to new vulnerabilities?
☐	☐	Does your organization have an incident response plan in place to investigate and mitigate confirmed security incidents?
☐	☐	Does your organization incorporate Security Orchestration, Automation and Response (SOAR) tools to speed incident response actions that can help reduce the spread of a cyberattack?
☐	☐	Does your organization's incident response plan account for containment policies, communication plans, compliance requirements, forensic analysis and recovery process?

Checklist:

Recover from a cyberattack

Recovering from a cyberattack is the process of restoring affected systems, networks, and data to a secure and operational state after a security incident. It involves taking action to mitigate the damage caused by the attack, rebuilding compromised or disrupted services and devices, analyzing the incident to prevent future attacks and returning the organization's operations back to normal. These questions can help determine if your organization is effectively recovering from cyberattacks.

Yes	No	
☐	☐	Has your organization implemented any incident containment measures to isolate and contain a cyberattack?
☐	☐	Does your organization have processes in place for system and/or device restoration after an incident is contained?
☐	☐	Does your organization utilize data isolation, immutability or a cyber vault when protecting your data?
☐	☐	Has your organization established procedures to cleanly recover data in the event of compromised, encrypted or deleted data?
☐	☐	Does your organization utilize AI/ML technologies to help automate or expedite recovery from a cyberattack?
☐	☐	Does your organization continually evaluate the incident and identify areas for improvement after an attack and recovery?
☐	☐	Has your organization conducted a forensic analysis to understand the attack methodology, determine the extent of the breach, identify affected systems and data and gather evidence to help make you more secure and pursue legal or disciplinary actions?
☐	☐	Does your organization know to notify relevant parties, such as customers, partners, and vendors, about a cyberattack and any potential impact on their data or operations?
☐	☐	Does your organization practice your recovery strategies multiple times per year to gain confidence in restoring your business and meet your SLAs?
☐	☐	Does your organization collaborate with service provides to assist with your organization's recovery?

Advance cybersecurity and zero trust maturity

It is vital for IT organizations to plan for the worst-case scenario when it comes to cybersecurity and have multiple layers of defense. In the ever-evolving threat landscape of cybersecurity, it is crucial to continuously advance security practices and embrace zero trust principles. This encompasses:

Reduce the attack surface

Minimize the vulnerabilities and entry points that can be exploited to compromise the environment.

Detect and respond to cyber threats

Actively identify and address potential security incidents and malicious activities.

Recover from cyberattacks

Restore the organization to a previous, known secure and operational state after a security incident.

By leveraging the expertise of professional services and collaborating with trusted business partners, Dell can help organizations establish a comprehensive security posture that protects against evolving cyber threats. As technology continues to advance, so must our approach to cybersecurity to safeguard our digital infrastructure and maintain trust in the digital realm.

DELL Technologies

About Dell Technologies

Dell Technologies helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

Learn more at www.dell.com/securitysolutions