DELL Technologies

Advance your cybersecurity and Zero Trust maturity.

Don’t let security risks stifle innovation.

Today’s rapidly evolving threats, especially with the rise of GenAI, create new and unexpected challenges for even the most seasoned cybersecurity specialists. Learn how partnering with experienced security professionals can help you avoid cyber attacks, maintain robust security practices and accelerate ideas to innovation.

Cyber threats are like ants at a picnic

You take care of one. Then, another is right behind it.

In an increasingly interconnected world, where organizations rely heavily on digital infrastructures and data has become a far-reaching commodity, it's best to assume that a sophisticated attacker has already breached your IT environment.

The good news is that there are experienced partners that specialize in the intersection of technology and cybersecurity.

Dell Technologies brings innovative solutions and valuable expertise that may not be available in-house to help you navigate the ever-evolving threat landscape.

- Hardware and software security
- Insights into emerging risks
- Understanding of advanced attack techniques
- AIOps to meet fast-moving threats
- New security strategies and best practices

Build layers of defense that continuously advance security practices and embrace a Zero Trust approach.

Dell Technologies is a cybersecurity partner that provides comprehensive professional services, hardware and software solutions and a robust partner ecosystem that limits the opportunity for attack, identifies and minimizes vulnerabilities, and helps you quickly restore business operations.

Reduce the attack surface →

Detect and respond to cyber threats →

Recover from a cyber attack →

Edge **Core** **Multicloud**

Professional Services

Business / Technology Partner Ecosystem **Secure Supply Chain**

DELL Technologies

Reduce the attack surface

Raise your defenses and make yourself a smaller target by reducing the avenues cyber criminals love to exploit.

To strengthen your security posture, you need to identify and minimize vulnerabilities and entry points that can compromise applications, systems or networks across various domains, including edge, core and cloud.

IDENTIFY points of vulnerability

- Software vulnerabilities
- Misconfigurations
- Weak authentication mechanisms
- Unpatched systems
- Excessive user privileges
- Open network ports
- Poor physical security

IMPLEMENT preventative measures

- Work with secure suppliers
- Apply comprehensive network segmentation
- Isolate critical data
- Enforce strict access controls
- Update and patch systems and applications
- Identify and address vulnerabilities using AI, regular assessments and testing

Embrace Zero Trust principles

A Zero Trust architecture means your organization doesn't automatically trust anything inside or outside its perimeters. Instead, everything trying to connect to your systems is verified before granting access. It's a model that incorporates **7 interrelated pillars** that advances cybersecurity maturity.

1. User trust
2. Device trust
3. Data trust
4. Application and workload
5. Network and environment
6. Visibility and analytics
7. Automation and orchestration

DELL Technologies

Reduce the attack surface

Identify the weak points that undermine your systems before trouble comes knocking.

Cybersecurity is not a one-time task but an ongoing process. Regular assessments, penetration and vulnerability testing and audits, with the help of an experienced security services partner, can help identify and fill the gaps to reduce risk.

Secure Supply Chain Practices	Security begins earlier than you think. Establish a trusted foundation using devices and infrastructure designed, manufactured and delivered using a secure supply chain, secure development lifecycle and rigorous threat modeling.
Built-in Security	Work with devices and infrastructure featuring built-in, hardware-based security designed to catch and repel attacks before they do damage.
Regular Patching and Updates	Address known vulnerabilities and minimize the risk of exploitation by keeping applications, firmware and operating systems up to date with the latest security patches.
Least Privilege	Limit user and system accounts to have the minimum access rights necessary to perform their tasks. This approach restricts the potential impact of an attacker gaining unauthorized access.
Network Segmentation	Isolate critical assets to limit network access by using modern network segmentation for critical data and business groups and applications. This contains an attack by preventing lateral movement.
Application Security	Implement secure coding practices, conduct regular security testing and code reviews, and use Web Application Firewalls (WAFs) to help protect against common application-level attacks and reduce the attack surface of web applications.
Professional Services and Partnerships	Collaborate with cybersecurity service providers and form partnerships with business and technology partners to bring in expertise and solutions that might not be available in-house.
User Education and Awareness	Train employees and users to recognize and report potential security threats, phishing attempts and social engineering tactics to minimize the risks that exploit human vulnerabilities.

DELL Technologies

Detect and respond to cyber threats

Like dial-up internet, old school security practices are too slow and ineffective in today's demanding environment.

To combat sophisticated cyber threats, you need better security tricks up your sleeve, such as AI and ML built into applications and methodologies that identify and respond to what's known and unknown.

Implement powerful intrusion detection and prevention systems

Leverage AI and ML for anomaly detection

Establish real-time monitoring of network traffic and user behavior

Increase resilience by partnering with experienced professional services to gain specialized expertise.

As an experienced technology partner, Dell Technologies can help you establish proactive incident response and recovery protocols that outline roles and responsibilities and ensure seamless communication and coordination between constituents.

Enhance your ability to proactively detect and respond to cyber threats by using advanced:

- Threat intelligence
- Incident response
- Security Information and Event Management
- Endpoint protections
- Behavioral analytics

Facilitate an efficient, swift recovery and minimize data loss with:

- A well-defined incident response plan and collaboration
- Regular backups of critical data and systems
- Secure off-site storage solutions and data encryption

DELL Technologies

Detect and respond to cyber threats

Stay vigilant and take action swiftly.

Detecting and responding to cyber threats means staying alert and planning for the worst-case scenario. Establish a response and recovery plan that is continually updated and routinely practiced so that your whole organization knows how to reduce the effects of an attack. It's an ongoing and iterative process that requires a combination of technology, skilled personnel, well-defined processes and team collaboration.

Continuous Monitoring

Security tools such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), log analysis and threat intelligence help identify signs of unauthorized access, intrusions, malware infections and data breaches.

Threat Detection

Take advantage of AI and ML to analyze data to identify patterns, anomalies and Indicators of Compromise (IoCs) that may point to a threat. This includes recognizing known attack signatures and identifying deviating behavior.

Alerting and Notification

Provide early warnings to prompt investigation and response. Bubble alerts and notifications to the surface for swift action with integrated security. Feed device-level telemetry above the OS to help speed threat detection and unleash security personnel or a Security Operations Center (SOC) when potential threats or incidents are detected.

Incident Response

Initiate a response plan to investigate and mitigate confirmed security incidents. This involves containing the impact, identifying the root cause and implementing necessary actions to restore systems and prevent further damage.

Forensic Analysis

Conduct detailed analysis of incidents to understand the attack methodology, determine the extent of the breach, identify affected systems or data and gather evidence to find and address security weaknesses.

Remediation and Recovery

Take steps to remediate vulnerabilities, patch systems, remove malware and implement enhanced security measures to prevent similar incidents. Restore affected systems and data to their normal state to complete the recovery process.

DELL Technologies

Recover from cyber attacks

Put the pedal to the metal and get your business back in the fast lane.

Cyber resilience is necessary in today's data-driven world and expected by customers and partners alike. To be successful, it requires multiple layers of protection to ensure that critical data is safeguarded and isolated so that it can be quickly recovered with confidence following an attack. Assess your cyber resiliency ›

Take action to mitigate the damage caused by a cyber attack

Rebuild compromised or disrupted services and devices

Analyze the incident to prevent future attacks

Meet business SLAs and return operations to normal

Create a comprehensive cybersecurity strategy so your organization can recover effectively and efficiently.

Recovering from a cyber attack requires a coordinated effort involving IT teams, cybersecurity professionals, management, and, at times, external experts. The key to recovery is to get systems and operations back to normal quickly while learning from the incident to reduce disruption and downtime, restore services and data integrity, minimize financial and reputational impacts and strengthen cybersecurity to prevent similar attacks in the future.

- Assess the impact of an attack on business operations
- Prioritize critical services
- Deploy data protection systems
- Communicate about any incident and recovery progress
- Develop a plan and practice, practice, practice to ensure continuity

DELL Technologies

Recover from cyber attacks

Get back on the dance floor by reviving systems, networks and data after an incident.

Achieving a cyber resiliency strategy incorporates people, processes and technology into a holistic framework that protects your entire organization.

Incident Containment

The first step is to isolate and contain the cyber attack's impact. This involves disconnecting affected systems from the network, disabling compromised accounts and implementing measures to prevent further spread or damage.

System or Device Restoration

Once an incident is contained, affected systems and networks are restored to a clean and secure state. This may involve rebuilding compromised systems, reinstalling software, and applying security patches and updates. Automation and self-healing can play a significant role in getting back to operational.

Data Recovery

Data that may have been compromised, encrypted or deleted during the attack must be recovered. This can involve restoring data from backups or employing specialized data recovery techniques to regain lost or encrypted files.

Forensic Analysis

After an attack, it's crucial to understand how the breach happened, what vulnerabilities were exploited and the steps to prevent similar attacks. Systems like Security Information and Event Management (SIEM) and capabilities like off-host BIOS comparisons provide useful insights.

Incident Response Evaluation

After recovery, it's essential to evaluate the incident response process and identify areas for improvement. Lessons learned from the attack can be used to enhance security practices, update incident response plans and provide better protection against future incidents.

Professional Services and Partnerships

Cybersecurity service providers and technology partners bring valuable expertise and resources to help your organization recover. They can assist with tasks such as forensic analysis, identifying the breach's occurrence and recommending measures to prevent future incidents.

DELL Technologies

Extend cybersecurity to edge and cloud environments

As networks spread from the core to the edge to the cloud, environments have become a crucial point of vulnerability.

As you advance cybersecurity maturity, you should ensure that ZT principles cover edge and cloud to ensure rigorous access controls, continuous authentication and comprehensive visibility and control over network traffic. As threat landscapes evolve, it's wise to deploy AI capabilities as a first line of defense. In addition, a strategy is only complete if your core network and cloud environments have security measures, such as network segmentation, encryption and continuous monitoring.

Cybersecurity Professional Services can help you take a holistic approach.

Connecting various security solutions can be a challenge. Collaborating with professional services specializing in edge, core and cloud security gives you the expertise to put in place effective measures that protect your organization from all angles.

Edge

Establish multiple layers of security at the edge, in the network and within hardware and software.

Core

Align your infrastructure to Zero Trust principles using AI, ML and automation.

Multicloud

Protect any workload in any environment, including public cloud, containers and cloud native workloads.

DELL Technologies

GenAI: A double-edged sword for cybersecurity

The next generation in AI is speeding us toward new risks but also improved security.

As the next phase in AI, GenAI encompasses systems that can understand, learn, adapt and implement knowledge across an array of tasks.

On the one hand, it promises improved threat detection and response, predictive capabilities and operational efficiency. On the other, it brings new challenges that require evolving cybersecurity strategies that address risks through robust security measures, continuous monitoring, regular updates and patching and an ever-evolving approach to data privacy and ethics.

Securing GenAI Applications

While GenAI offers substantial security benefits, its functionality can be used maliciously if not appropriately secured.

- Ensure data privacy and integrity.
- Mitigate adversarial attacks designed to deceive AI systems that cause malfunction.
- Detect and respond to system misuse from malicious AI.
- Auditing and mitigating ethical issues and biases.
- Implementing strong access controls for AI systems.
- Securely protect and recover large language models (LLM).

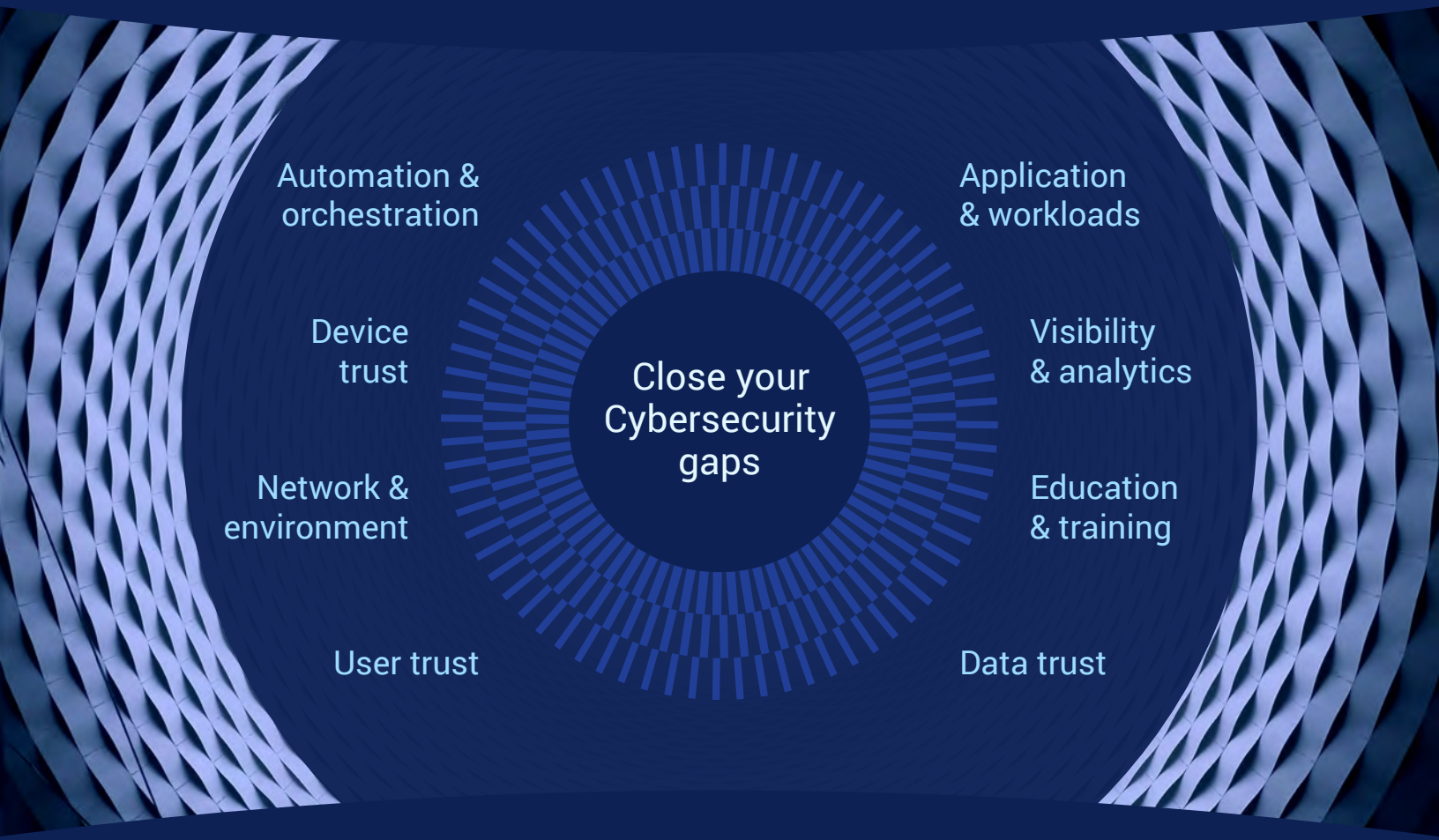
Securing Organizations with GenAI

GenAI has become a crucial ally in cybersecurity, opening novel avenues to protect organizations.

- Improve efficacy of threat detection and response.
- Predict future threats or identify potential vulnerabilities.
- Automate threat detection and provide efficiency.
- Forensic analysis to quickly identify patterns, anomalies and indicators of compromise.
- Personalized security awareness training.
- Scale security operations with faster access to richer insights.

Modern cybersecurity should be intelligent, scalable and automated

Dell Technologies can help you establish comprehensive security that protects against evolving cyber threats. As technology advances, our approach to cybersecurity stays a step ahead, harnessing the power of AI and ML to safeguard your digital infrastructures and maintain trust in the digital realm. No matter where you are on your cybersecurity journey, we'll work with you to go beyond simply protecting your organization with steps that keep you agile and resilient.



DELL Technologies

Dell.com/SecuritySolutions
Request a callback
Chat with a security advisor
Call 1-800-433-2393