Futurum®

DELL Technologies

Fortifying the Enterprise: Modern Strategies for Cybersecurity and Resilience

SEPTEMBER 2025

Introduction

Cyber threats today move at a pace, and with a level of sophistication, never seen before. With the assistance of AI, the "barrier to entry" for cybercrime has never been lower for malicious actors. As a result, security operations teams can no longer rely on static defense strategies. According to Futurum's 1H25 Cybersecurity Decision Maker research, addressing new and more sophisticated threats has become the single most pressing challenge impacting risk management and security operations buyers.

Against this backdrop, the urgency to build and maintain robust cybersecurity and resilience is at its peak. No matter how threats shift and morph, the essential building blocks for protecting enterprise assets will continue to remain consistent: reducing the attack surface, enabling rapid and accurate threat detection and response, and ensuring swift, validated recovery in the event of a cyberattack – all built on the foundation of a secure supply chain. This asset explores best practices to meet these interconnected goals.

Reduce the Attack Surface

Today's typical organization has to contend with a sprawling attack surface with a slew of new identity, software, and system vulnerabilities that are very difficult to defend against. This expanding attack surface is fueled by:

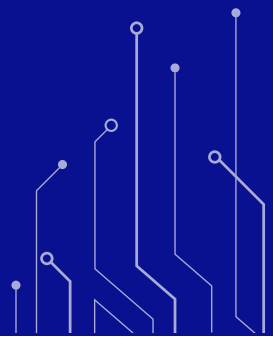
- The explosion of endpoint devices that lack consistent, enterprise-grade security controls.
- The proliferation of SaaS applications and third-party integrations, each introducing new vectors for attack.
- The rise of non-human identities, including bots and AI agents, which must be managed and secured like human users but at machine scale.

This complexity brings more vulnerabilities, and greater challenges identifying, prioritizing, and remediating them. Organizations can follow the following best practices to combat this challenge:

- **Start with Supply Chain Security:** A secure supply chain underpins enterprise security and resilience. This means rigorous vetting of vendors, securing software development lifecycles, and validating the integrity of hardware and firmware on arrival.
- **System and Device Hardening:** Enforcing secure configurations, including disabling unnecessary services, enforcing strong passwords, and ensuring all endpoints follow hardened baselines, reduces the exploitable "surface area."
- **Zero Trust Architecture:** While Zero Trust is not a compliance requirement for all organizations, access control principles of "never trust, always verify" via micro-segmentation, robust identity and access management (IAM), and enforcing least privilege access is a best practice for all. Multi-factor authentication (MFA), role-based access controls, single sign-on (SSO), and advanced session management are also important.
- **Application-Level Defenses:** Secure coding practices, regular code reviews, and automated tools such as web application firewalls (WAFs) are important to minimize vulnerabilities at the application layer.
- **Continuous Vulnerability Management:** Regular patching and updates are crucial, as is ongoing vulnerability scanning and penetration testing to detect new weaknesses.
- **Intelligent Threat Prevention:** Using machine learning/AI-driven analytics to proactively identify and flag potential vulnerabilities before they become breaches.

As digital estates grow, the ability to reduce the attack surface requires a secure foundation, zero trust access principles, and the ability to uncover and address critical vulnerabilities. Dell Technologies offers a number of key capabilities in this area:

- Dell's Secured Component Verification (SCV) ensures components are authentic and tamper-free.
- Secure credential storage security via secure BIOS, robust patch management, and configuration controls.
- IAM, including the ability to apply policies of least privilege access and capabilities for multi-factor authentication (MFA), role-based access control (RBAC), SSO, dual authentication, and password and session management.
- Penetration testing and end-to-end vulnerability management to strengthen ongoing defenses.



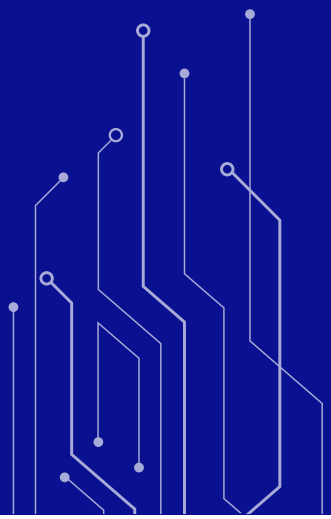
Threat Detection and Response

Even the strongest defenses cannot stop every attempted intrusion. As attackers accelerate their own innovation, the ability to swiftly, accurately, and effectively detect and respond to threats has become critical to maintaining business continuity and protecting sensitive data. In fact, in Futurum's 1H25 Cybersecurity Decision Maker IQ research, data loss and system/operational downtime were cited as the most severe consequences of breaches in the past year, and enhancing threat detection and risk management capabilities ranked as the top two priorities among risk and security leaders.

Best practices for this practice area include the following:

- Continuous Monitoring: Real-time surveillance of networks, endpoints, and cloud environments, including data center infrastructure, for vulnerabilities and malicious activities via intrusion detection systems (IDS), log analysis, and advanced analytics. The backup environment is an important piece of this equation, as protection infrastructure is very often targeted first.
- Layered Detection: Augmentation scanning for known attack signatures with behavioral analytics and ML-driven anomaly detection. These advanced methods can identify previously unknown, "zero-day" threats by spotting deviations from baseline behavior.
- Timely and Accurate Alert Escalation: Today's Security Operations Centers (SOCs) must transform mountains of raw logs into actionable intelligence – prioritizing and escalating the vulnerabilities and attacks with the greatest potential business impact.
- Automated Remediation: Where possible, automate responses to contain and remediate the most critical vulnerabilities.
- Timely Incident Triage and Investigation: When a threat is confirmed, teams must have clear plans and tools to isolate affected systems, disable compromised accounts, and conduct rapid triage, in order to reduce dwell time, prevent lateral movement, and resume critical business operations as quickly as possible. This includes the ability to:
    - Quickly and effectively isolate affected systems and disable compromised accounts in order to prevent further damage
    - Automate as many remedial as possible, using AI when possible.
    - Conduct forensic analysis to understand the attack, the scope of compromise, and gather evidence for legal and compliance purposes
    - Consider Managed Detection and Response (MDR) services; given the strain on internal teams, offloading detection, threat hunting, and rapid response to experienced partners can be a force multiplier.

Dell's storage platforms bring embedded threat detection and monitoring, including built-in detection of anomalous activity and live BIOS scanning, to ensure that malicious changes are flagged at the firmware and system levels. Integrations with strategic partners such as CrowdStrike, Microsoft, and SecureWorks extend these capabilities with real-time threat intelligence, advanced threat hunting, and rich context for investigations. For organizations needing expert support, Dell's own MDR services offer 24x7 attention, bringing together human analysts and automation for faster, more effective responses.



Rapid Recovery

Modern cyber resilience must emphasize not just prevention, but also the ability to recover quickly and with confidence when incidents do occur, given the precedence of maximizing business continuity. A practiced and validated strategy for recovering impacted data and systems is a vital part of cyber resilience. As attackers innovate, it is equally important that security teams can learn from successful incidents, in order to strengthen their future defenses.

Key best practices for minimizing business disruption include:

- Automated, Validated Restoration: The ability to rapidly restore, utilizing automation when possible. This includes restoring systems to a clean, secure state, and recovering compromised data from clean backups. This includes protecting data with isolated, immutable storage to reduce the risk of ransomware propagating into backup sets, and clean room approaches to insulate recovery environments.

- Practiced Incident Response Plans: Regularly test and validate incident response strategies to ensure that business service level agreements (SLAs) for recovery point objectives and recovery time objectives (RPOs and RTOs) can be met under real-world conditions.

For its part, Dell offers a number of capabilities to ensure and validate rapid, clean recoveries:

- Dell storage platforms, including PowerStore and PowerMax, when combined with IndexEngines CyberSense, which validates clean data for backup, and Dell's minimum viable clean room capability allow organizations to quickly and surgically recover clean data from pre-attack snapshots, validated as uncompromised.

- Specifically, CyberSense complements core Dell capabilities by using machine learning-based analytics to scrutinize backup file changes and metadata for the subtle signals of ransomware and corruption that might escape traditional signature-based monitoring and detection. This provides a "last line of defense," ensuring that backup environments are clean and recoverable.

- Automated system recovery (ASM), BIOS image capture, and proactive MDR for backup capabilities support rapid, orchestrated response to attacks.

- Dell's Unified Data Services (UDS) systems, including integrations with MDR partners such as CrowdStrike and Microsoft, exemplify this "security is a team sport" philosophy, allowing organizations to scale expertise and adapt to evolving threats.

- Dell complements its production storage platforms, including PowerStore and PowerMax, with IndexEngines CyberSense, which validates clean data for recovery, with Dell its PowerProtect Cyber Recovery and minimum viable clean room capability. This combination allows organizations to quickly and surgically recover clean data from pre-attack snapshots, validated as uncompromised.

- Dell Incident Response and Recovery (IRR) services support initial forensics and eradication as well as full recovery of infrastructure and business applications.

A successful security strategy blends resilient technology, clear processes, ongoing training, and a willingness to draw from external expertise as needed. Dell's IRR and MDR services address this requirement, extending human expertise and providing organizations with hands-on support when it matters most. Additionally, Dell works strategically with a broad ecosystem of third-party cybersecurity technology partners, spanning areas such as identity security, threat detection, and compliance. This partner network enables Dell to deliver integrated, end-to-end security solutions that can be tailored to diverse customer environments and needs.

Addressing the Human Element: Overburdened SecOps Teams

Effective threat prevention, detection, and recovery requires coordination among IT and security teams as well as third-party experts. A robust toolchain of best-of-breed but strategically integrated technologies, coupled with regular testing and validation, is critical to shifting enterprises from hoping from the best, to preventing cutting-edge attacks and being ready to preserve business continuity in the event of a breach.

A key challenge is that SecOps teams alike are stretched thin, often operating under immense pressure that leads to fatigue, burnout, and ultimately, increased risk of misconfigurations, missed alerts, and slow response times. At the same time, there is a persistent shortage of skilled cybersecurity professionals, and especially for seasoned incident responders, further exacerbating operational challenges. Experienced defenders become valuable and are aggressively recruited by other organizations, leading to high turnover and a loss of institutional knowledge. These factors create strong incentives to engage with trusted cybersecurity service providers for blue-team expertise, forensic analysis, and ongoing prevention support.

Conclusion

Modern enterprises face an escalating arms race between powerful cyber adversaries and the teams tasked with defending against them. While the tools and tactics of attackers continue to evolve, the three strategic pillars of cyber resilience remain constant: minimizing the attack surface, detecting and responding to threats rapidly, and ensuring swift recovery. Yet, true resilience is not simply a matter of deploying the newest tool or technology. It demands a balanced strategy that integrates best-in-class solutions and addresses the critical shortage of skilled defenders by leveraging service partners where gaps arise. Automation and intelligence (including AI-driven analytics) play an increasingly important supporting role, helping organizations do more with less and keep pace with adversaries. Organizations that invest in these integrated defense, detection, and recovery strategies, supported by strong partnerships and a secure supply chain, will be best positioned to confront whatever threats the future brings.

Important Information About This Report

AUTHORS

Krista Case
Research Director, Cybersecurity | The Futurum Group

PUBLISHER

Futurum Research

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DELL Technologies

ABOUT DELL TECHNOLOGIES

Dell Technologies provides enterprise IT infrastructure solutions across servers, storage, networking, and services. Its storage platforms are designed to support a range of workloads with an emphasis on performance, scalability, and data protection. The company also incorporates cyberresilience capabilities into its offerings, including features for data immutability, recovery, and threat detection. These elements are positioned to help organizations strengthen data security and maintain operational continuity in the face of potential disruptions.

Futurum®

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

Futurum®
CONTACT INFORMATION: The Futurum Group LLC | futurumgroup.com | (833) 722-5337