DELL Technologies

Advance Cybersecurity and Resilience Maturity

Cybersecurity Maturity is a Strategic Lever for Every Modern Business

Today's cyber threat landscape is more dynamic and unforgiving than ever, with AI-driven attacks increasing in frequency, speed, and sophistication. Organizations can no longer rely on patchwork defenses or incremental updates.

As a business leader, you need to operate as if a breach is inevitable, if not imminent. At Dell Technologies, we help customers increase their security maturity, the level of confidence they have operating the business in the face of cyber risk. We do this by advancing a comprehensive, layered cybersecurity and resilience approach built around three crucial practice areas.

Companies must have capabilities to:

- **Reduce their attack surface**
- **Detect and respond to cyber threats**
- **Recover from cyberattacks**

Effective cybersecurity starts by honestly assessing your current security posture and maturity. That clarity lets you prioritize the right improvements and invest in a more secure tomorrow.

Reduce the Attack Surface

An organization’s attack surface is dynamic and rapidly evolving, with AI introducing novel attack vectors. Together with remote work and legacy systems, they widen the attack surface, creating more entry points for threat actors. This makes reducing the attack surface a strategic necessity to reduce risk, meet compliance obligations, protect organizational resilience, and build baseline confidence.

Advance Cybersecurity and Resilience Maturity

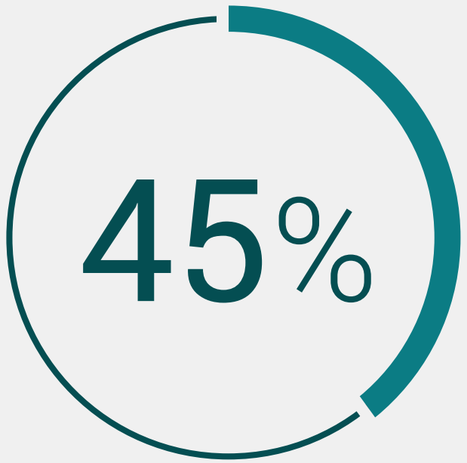
Reducing the attack surface helps you lower overall risk by minimizing entry points that attackers can exploit. This strengthens your security maturity and streamlines compliance efforts. The result is stronger resilience, lower costs by avoiding incidents, and the ability to move faster, innovate more freely and enter new markets with confidence knowing security is built in from the start. It begins with adopting zero trust principles — never trust, always verify — and enforcing least privilege across users, devices, and applications.

At Dell Technologies, we embrace a "secure-by-design" mentality. Cybersecurity is built into everything we do, starting with our secure global supply chain and extending to built-in protections in our core products. These protections begin at the hardware level to help ensure devices start up and run only trusted software. We align our solutions with zero trust principles, helping you eliminate vulnerabilities before attackers can exploit them. Our world's most secure commercial AI PCs [1], for example, provide foundational defenses for the modern workspace.

Reducing the attack surface raises your security maturity by eliminating uncertainty – fewer unknowns, fewer entry points, and fewer surprises.

Key Customer Outcomes:

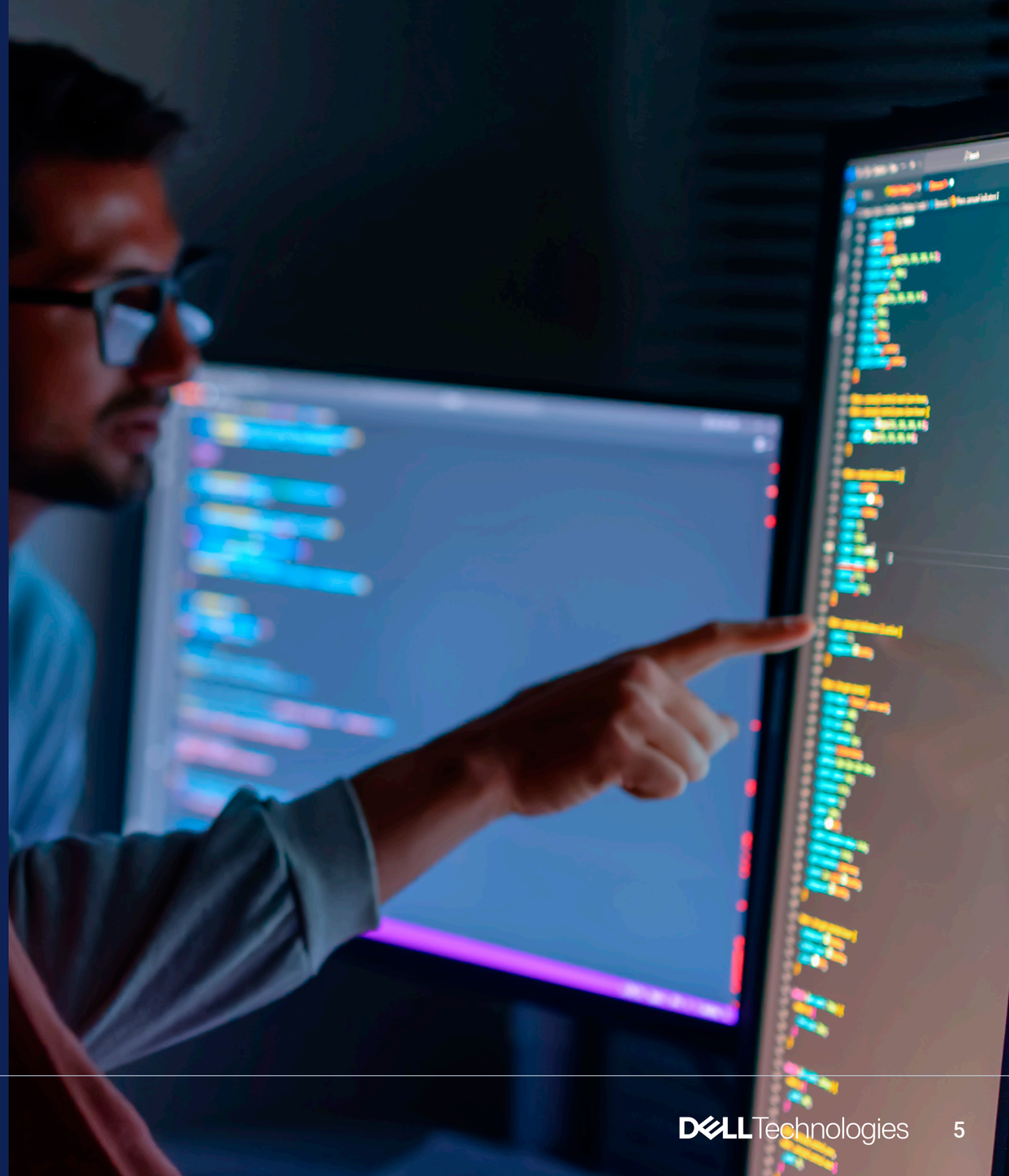
- **Minimizing Vulnerabilities:** By proactively hardening endpoints, infrastructure, and applications, you can dramatically reduce opportunities for attackers.
- **Simplified Security Management:** Fewer exposed assets mean fewer controls to manage, leading to a more streamlined and efficient security posture.
- **Stronger Foundation for Innovation:** With trusted endpoints and protected data, you can adopt new technologies like AI and edge computing with greater confidence.



Organizations that focus on reducing their attack surface achieve a 45% reduction in cyber-breach risk when managing external exposures.[2]

Detect and Respond to Cyber Threats

In the arena of cyber security, speed and intelligence go hand in hand. Effective detection and response allow you to identify and contain threats quickly, reducing dwell time and limiting the damage of an attack. The result is lower costs, less downtime, and greater operational confidence that your business can operate securely even when under constant threat.



Advance Cybersecurity and Resilience Maturity

However, many organizations struggle with limited visibility across hybrid environments and an overwhelming volume of alerts. Attackers now dwell inside networks for an average of 11 days before discovery. To counter this, you need real-time visibility across endpoints, networks, and systems through continuous monitoring, threat intelligence, and automation.

The right security partners provide specialized expertise in threat intelligence and incident response. Dell combines advanced analytics, AI/ML driven threat detection, and 24x7 managed services with a secure hardware foundation to identify and contain threats before they cause disruption. Optional services like our Managed Detection and Response (MDR) provide security expertise to expand visibility and quickly respond to and mitigate threats.

Strong detection and response capabilities increase your security maturity by shortening dwell time and giving teams confidence they can act decisively when threats emerge.

Key Customer Outcomes:

- **Faster Detection & Shorter Dwell Time:** Managed detection and response (MDR) can reduce mean time to detect and respond by 25-49%, reducing the likelihood of an attack becoming more serious.
- **Reduced Operational Burden:** Partnering with experts for proactive threat-hunting and continuous monitoring shifts the burden from internal teams, freeing them for strategic work.
- **Improved Resilience:** Mature detection and response capabilities lead to fewer security incidents and help avoid higher breach-related costs.

$4.44M

The average cost of a data breach hit $4.44M in 2025.[3]

Recover from a Cyberattack

When the worst-case scenario occurs, the primary goal is to return to normal operations as quickly as possible with minimal disruption. Recovering from a cyberattack ensures you can restore clean data and systems quickly, reducing reputational damage and giving you confidence that your recovery is reliable and free from reinfection.

Advance Cybersecurity and Resilience Maturity

Even though you build the strongest defenses possible, you must plan as though an attack is inevitable. Having a complete recovery plan and capabilities in place is crucial. This includes maintaining clean, immutable backups of critical data in an isolated recovery vault and using cleanroom environments to validate that restored systems are free from malware before bringing them back online.

Dell builds recovery capabilities into our product offerings – and getting businesses back to operational is our first priority when incidents occur. Solutions like our PowerProtect Cyber Recovery Vault isolate and safeguard clean copies of critical data for rapid recovery, limiting loss and taking leverage away from ransomware attackers. This architecture helps you get critical workloads back online rapidly, so you can feel confident.

Recovery is often where the security maturity is truly tested – when confidence depends on how quickly and cleanly the business can return to normal operations.

Key Customer Outcomes:

- **Reduced Business Impact:** Organizations with a well-rehearsed incident response plan can reduce breach costs by approximately 61%.
- **Faster Resumption of Operations:** Prioritizing a quick return to business, not just threat removal, helps restore operations with minimal disruption and cost.
- **Improved Data Integrity:** Isolating critical data, using immutable copies, and validating integrity before a restore builds confidence in the recovery process.

of organizations admitted they'd struggle to recover from a cyberattack while meeting their service level agreements.[4]

Advance Cybersecurity and Resilience Maturity

Strengthen Your Security Maturity Through Strategic Partnerships

Experienced partners are essential to navigate today's fast-moving and complex cybersecurity landscape. Cyber threats are becoming more sophisticated and frequent, making it nearly impossible for a single organization to maintain the expertise, resources, and technology needed to stay ahead. By collaborating with security leaders like Dell, companies gain access to specialized skills, cutting-edge technologies, and a network of trusted partners. These partnerships provide the support and expertise required to detect, prevent, and respond to threats effectively, ensuring businesses stay protected in an ever-evolving digital environment.

With the right approach across these three practice areas, organizations increase their security maturity – building the confidence to operate, innovate, and grow despite constant cyber pressure. Dell unites trusted infrastructure, trusted workspace, advanced services, and a partner ecosystem to help your organization stay secure, adaptive, and resilient - ready for what's next.

Explore Security Solutions

DELL Technologies

Frequently Asked Questions

1. Why should cybersecurity be a top priority for my business?
Cybersecurity is more than just protection; it is the foundation that a business can innovate and grow while withstanding the dangerous cybersecurity landscape. Strong security posture isn't just about defense — it's about enablement. Companies with mature cybersecurity frameworks can move faster, innovate more freely, and enter new markets with confidence. They're better equipped to handle regulatory changes, customer demands, and competitive pressures.

2. How can we balance the need for strict security with the freedom to innovate?
You shouldn't have to choose between being secure and being innovative. We believe that robust security actually empowers innovation. When you have a "secure-by-design" foundation—where security is built into your devices, infrastructure, and data from the start—your teams can adopt new technologies like AI and edge computing with confidence.

3. Why is supply chain security so critical?
Real security begins long before the power button is pressed. As your digital footprint grows, so does your exposure — and trust becomes your first line of defense. Every link in the supply chain must be protected, because a single compromised component can undermine even the most advanced software. That's why we build security from the ground up, safeguarding every step from production to deployment. From the factory floor to your front door, your technology arrives trusted, verified, and built to perform with confidence.

4. How does Dell help us recover after a cyberattack?
Minimizing downtime and disruption is critical when incidents occur. Preparation is key. Our PowerProtect Cyber Recovery Vault isolates a clean, immutable copy of your most critical data, safely separated from your primary environment. In the event of an incident, you can restore operations swiftly and confidently without compromise, and without paying a ransom.
Dell provides a variety of products and services designed to help you implement a comprehensive recovery strategy. It ranges from consulting services to create a recovery and training plan to data protection capabilities that can keep critical data safe. Dell takes a people and technology centric approach, ensuring that both employees and technology work together to help you recover quickly.

5. Can Dell assist with real-time threat detection?
Absolutely. Speed is everything when it comes to stopping a cyber threat. We combine built-in security features with advanced services like Managed Detection and Response (MDR) to monitor your environment 24/7. By using AI/ML-driven insights and human expertise, we help you spot anomalies and potential threats instantly, allowing you to respond and contain issues before they impact your business.

Sources

[1] Based on Dell internal analysis, October 2024 (Intel) and March 2025 (AMD). Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some features. Intel-based PCs validated by Principled Technologies, July 2025 Anatomy of a Trusted Device Infographic

[2] Forrester Consulting, "The Total Economic Impact™ of BitSight: Cost Savings and Business Benefits Enabled by BitSight," October 2024.

[3] IBM and Ponemon Institute, "Cost of a Data Breach Report 2025: The AI Oversight Gap," 2025.

[4] Dell Technologies, "Advance Cybersecurity Maturity: Technology Infrastructure is the Heartbeat of Every Modern Business," February 2025.

About Dell Technologies

Dell Technologies (NYSE: DELL) 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 AI era.

Learn more at Dell.com