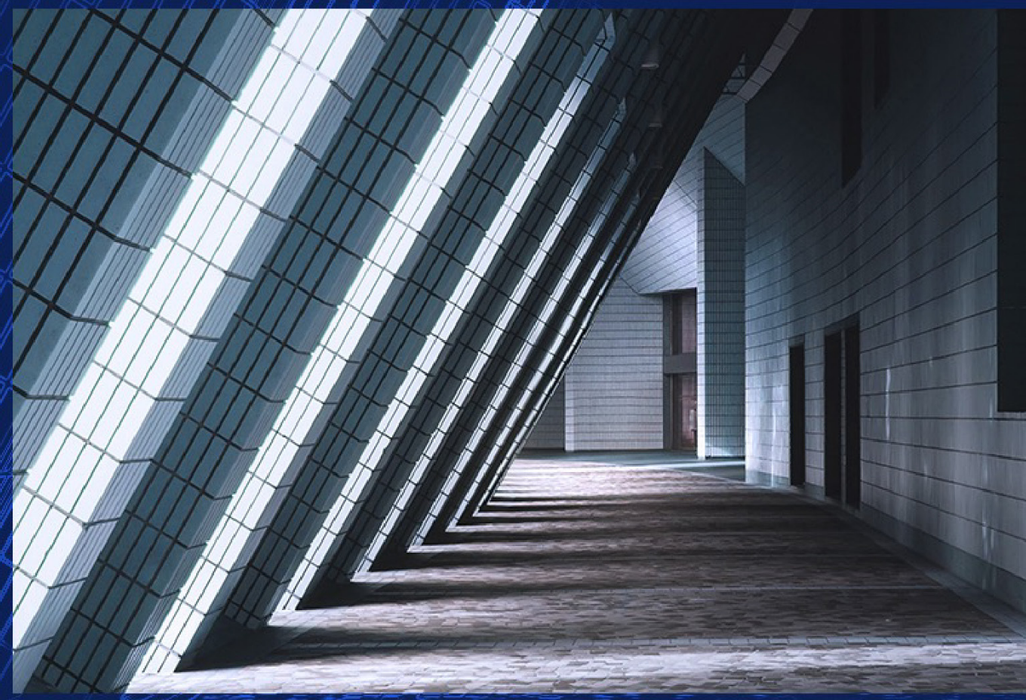
DELL Technologies



Advance Cybersecurity Maturity

Technology Infrastructure is the Heartbeat of Every Modern Business

Security and resilience are instrumental in keeping these vital organs pumping. However, many companies struggle to keep pace with evolving threats — in fact, our recent research indicates that 93% of organizations acknowledge their security strategies need improvement.

The question is no longer if your organization will face a cyber threat, but when and how. As a business leader, you need to operate as if a breach is inevitable, if not imminent. At the same time, you must ensure security risks don't stifle your organization's ability to innovate. Our research suggests that 79% of respondents struggle with balancing security and innovation.

Due to increasingly sophisticated cyber threats and the rapid proliferation of technologies like artificial intelligence (AI), a proactive security mindset is more essential than ever. The path forward consists of three important security focus areas. Companies must have robust capabilities to:

- **Reduce their attack surface;**
- **Detect and respond to cyber threats; and**
- **Recover from a cyber attack.**

Reduce the Attack Surface

An organization's attack surface is very dynamic and rapidly evolving. Over the past decade, the organization's attack surface has grown by approximately 1000%, reflecting the increasing security complexity of modern digital environments.

Each new technological advancement creates potential security gaps. Generative AI (GenAI), for example, introduces new risks around data exposure, result manipulation, sensitive information disclosure, prompt injection — and the list goes on. Security challenges extend beyond AI implementations, too. In fact, 67% of business leaders fear new innovations will increase their attack surface.

Reducing that attack surface requires a multi-layered approach. It starts with foundational practices like conducting thorough penetration testing and vulnerability assessments to identify and address potential security gaps that require immediate attention. Additional critical components include: comprehensive network segmentation, critical data isolation, enforcing strict access controls, and regularly updating and patching systems and applications.

Additionally, as cybersecurity is an ongoing process and not a finite activity, the initial penetration testing and vulnerability assessments must be conducted regularly, as both the organization and threat landscape are continually evolving.

At Dell Technologies, we embrace a "security built-in" mentality. This starts with our secure supply chain and includes zero trust principles such as identity access management through Multi-Factor Authentication (MFA), and Role-Based Access Control (RBAC), included in our core products. As an example of the power of these capabilities, Dell offers the most secure commercial AI PCs.

85%

of business leaders agree that their supply chain is critical to their security posture.

54% of organizations are implementing GenAI or plan to within the next 12 months.

56% of IT decision-makers (ITDMs) are concerned about GenAI risk.

32% of ITDMs believe GenAI has the potential to enhance security.

Detect & Respond to Cyber Threats

In the arena of cyber defense, speed and intelligence go hand in hand. Companies must work to actively identify and address potential security incidents and malicious activities in the earliest stages of a breach.

To this end, threat detection technologies powered by AI and machine learning algorithms are a foundational requirement. These systems monitor network traffic, data patterns, and user behavior in real time, using AI to pinpoint possible security threats.

The right security partners can also provide specialized expertise in threat intelligence and incident response. At Dell, we build security directly into our PCs and infrastructure products. Optional services like Managed Detection and Response (MDR) help identify and respond to threats.

80%

of organizations admit they could improve their cyber threat detection and response capabilities.

Recover From a Cyberattack

When the worst-case scenario occurs, the primary goal should be a return to the normal state as quickly as possible with minimal disruption. However, in our recent survey, 64% of organizations admitted they'd struggle to recover from a cyberattack while meeting their service level agreements (SLAs).

Even though you must build the strongest defenses possible, you must plan as though an attack is inevitable. Therefore, having a recovery plan and capabilities in place is crucial. This includes maintaining secure backups of critical data and systems, along with immutable, isolated, and/or secure off-site storage utilizing encryption. It also involves establishing clear incident response protocols that outline all parties' roles and responsibilities from the moment an attack occurs, and identifying channels for seamless coordination among internal teams and partners. Finally, it requires regularly testing recovery procedures, including simulating various attack scenarios to ensure readiness.

Dell builds recovery capabilities into our product offerings — and getting businesses back to normal is our first priority when incidents occur. Solutions like our PowerEdge servers with automated system recovery (ASR), PowerStore and PowerMax systems with advanced snapshotting capability to immutable storage, and the PowerProtect Cyber Recovery Vault help ensure your most mission-critical data remains intact.

65%

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

Strengthen Your Security Posture Through Strategic Partnerships

Cybersecurity and resilience maturity is an ongoing journey that requires constant vigilance and evolution. By maintaining a strong security and resilience posture, organizations can significantly reduce their risk exposure, minimize financial losses, improve operational efficiency, and build greater trust with their customers.

Experienced partners can help you navigate this fast-moving landscape. By collaborating with security leaders like Dell, companies benefit from specialized skills and knowledge that may not be available in-house — including insights into emerging risks, advanced attack techniques, and the very latest security strategies and best practices.

With the right approach to reducing attack surfaces, detecting and responding to threats, and recovering from incidents, organizations can build the resilience needed to thrive in today's digital age — and innovate to meet tomorrow's challenges with peace of mind.

Learn more about Dell's security solutions.

DELL Technologies

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

All data points in this eBook come from a Dell Technologies survey of 750 business and IT decision makers across US, UK, DE, FR and JP, all segments, Feb 2025. Full findings here.