Overall we score your organization as:

Vulnerable

Based on your responses, when it comes to shrinking your attack surface, your organization is rated as:

Exposed

Based on your responses, when it comes to detecting and responding to threats, your organization is rated as:

Vulnerable

Based on your responses, when it comes to recovering from attacks, your organization is rated as:

Prepared

Your Customized Cybersecurity and Resilience Assessment Results

Overview

Thanks for taking the Dell Technologies Cybersecurity and Resilience self-assessment, powered by Enterprise Strategy Group. The goal of this assessment is twofold:

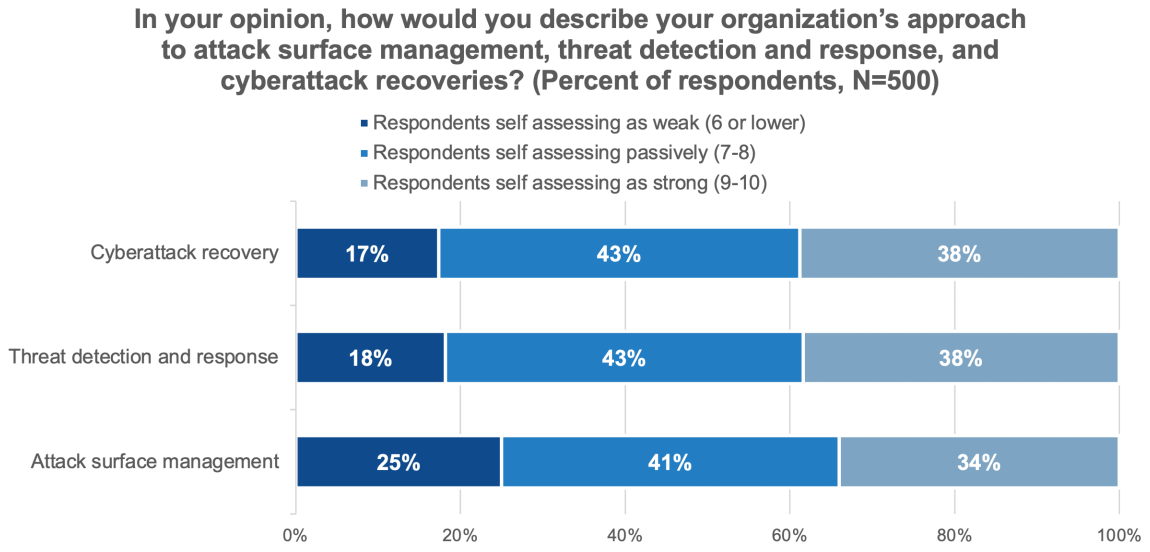
- Understand how effective your current cybersecurity strategies are in protecting and defending your organization from cyberattacks.
- Provide actionable guidance on where to focus to improve both individual strategies and your overall cybersecurity program outcomes.

To accomplish this, the tool assesses your organization's cyber security maturity across three key security practice areas: attack surface reduction, threat detection and response, and the completeness of your recovery capabilities.

Enterprise Strategy Group research shows that 89% of organizations are leaning in to reducing the attack surface. This same research revealed that on average, attack surface management is ranked lower than both threat detection and response or cyberattack recovery strategies.

When asked to rate their capabilities from 1 (basic) to 10 (leading edge), 25% of respondents said attack surface management at their organization was a 6 or lower vs. 18% of respondents when considering threat detection and response and 17% of respondents when considering cyberattack recovery capabilities.

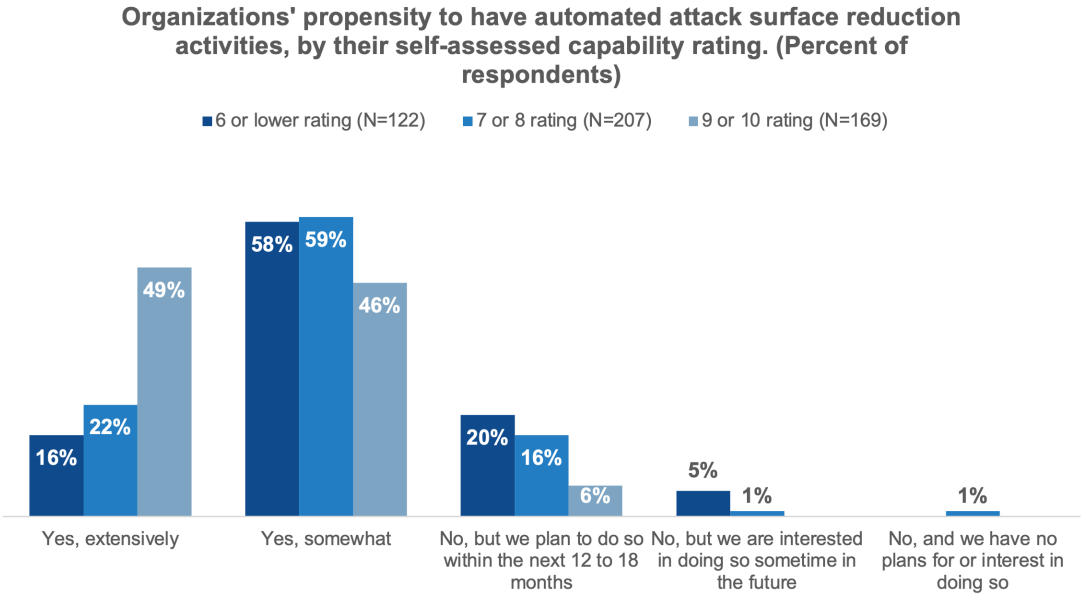
Figure 1. Your Peers' Self-assessment of Their Cybersecurity Maturity



Source: Enterprise Strategy Group, now part of Omdia

Notably, those reporting the best attack surface management capabilities are also investing more aggressively in automation, (49% vs. 16%).

Figure 2. How Automation Helps Organizations Reduce Their Attack Surface



Source: Enterprise Strategy Group, now part of Omdia

Based on your responses to the assessment across each of these areas, we categorize your organization as **Vulnerable**. This is the **Middle** tier of preparedness in this assessment. The following pages detail why your organization received this rating and include recommendations for your organization to consider. Also included in this report is information about how Dell can help your organization with cybersecurity and resilience.

Section 1: Reduce the Attack Surface

Proactive security strategies are crucial to keeping up with the accelerating pace and growth of the threat landscape. Proactive strategies limit the opportunity for adversaries to gain access to identities, devices, infrastructure and other critical IT assets. Some of the more common proactive activities include ensuring the strategy is aligned with business and IT needs, hardware and software supply chain risk management, risk/exposure/vulnerability management, network segmentation, privileged access management, and ensuring security controls across the estate are active and properly configured.

Your Rating: Considering just your answers in this practice area, you have obtained a rating of: **Exposed**.

Your organization has some serious gaps in proactive security measures. Without these activities, your security team is likely overwhelmed with reactive activities. Some alerts go untouched. Some investigations remain incomplete, and vulnerable assets continue to provide entry points for adversaries.

Recommendations to Reduce Your Attack Surface

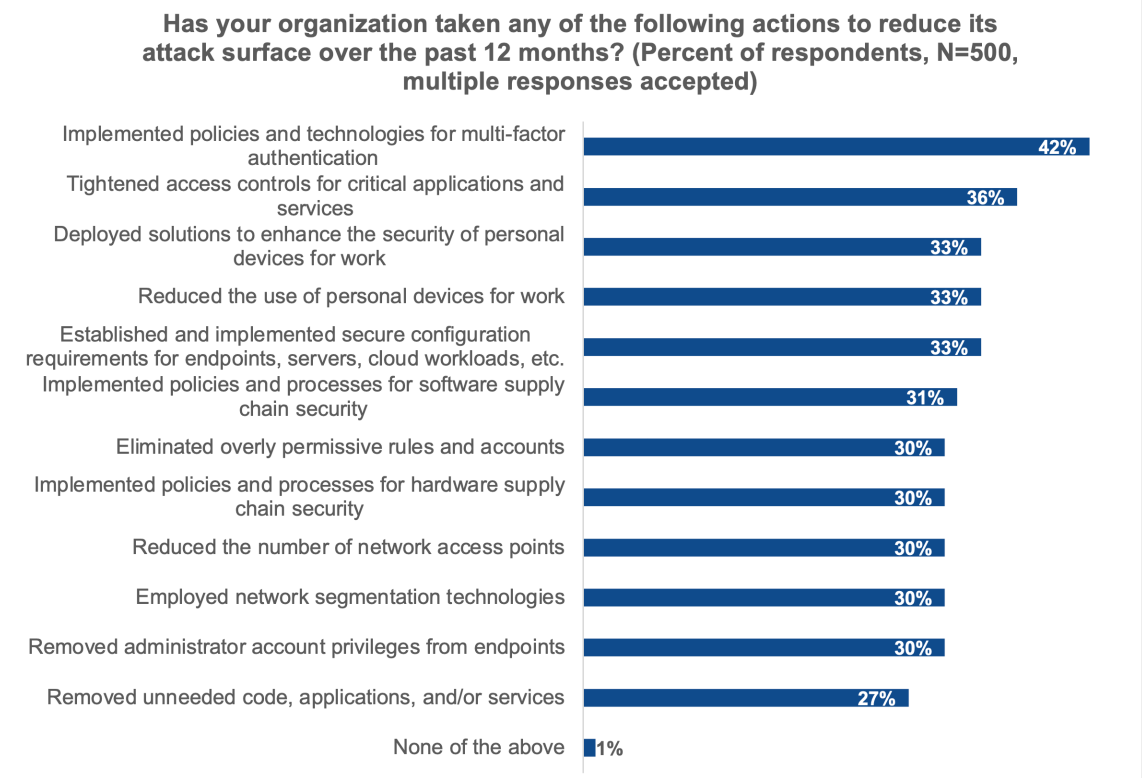
1. Implementing multifactor authentication (MFA) is a worthwhile endeavor as it adds protection beyond easily compromised passwords. Unlike single-factor authentication, MFA combines something you know (password) with something you have (mobile device) or something you are (biometric), creating multiple security layers that attackers must breach. This approach can effectively prevent credential theft, password spraying, and account takeovers, as stolen passwords alone become useless without the second verification factor.
    - You did not report this has been an area of focus for your organization over the past year and that suggests reviewing your environment for gaps in coverage would be a worthwhile exercise.

2. Many organizations have found they need to focus on tightening access controls for critical apps and services. Accounts with overly permissive access rights need to be tightened to a small number of administrators. For example, executives are often given a high degree of access even though they rarely need it. Given these individuals are frequently targeted by attackers, assigning them privileged accounts drives significant risk. Another dynamic at play is that users are increasingly working from a variety of locations, on non-corporate devices, and leveraging an array of approved and non-approved cloud services. Broadly tightening user access is key given this combination of risk factors.
    - You did not report this has been an area of focus for your organization over the past year and that suggests auditing your environment for overly permissive access policies to critical systems is an initiative you should likely engage in.

3. Many of your peers have deployed security solutions to cover employees' personal devices or even restricted the use of these devices for work because these unmanaged personal devices introduce numerous threat vectors including inconsistent security configurations, mixed personal/work usage, and potential unauthorized access by family members. Implementing mobile device management solutions or restricting personal device usage for work creates security boundaries that prevent these personal devices from becoming unprotected entry points into an organization's interconnected digital environment.
    - You did not report that this has been an area of focus for your organization over the past year and that suggests revisiting the risk vs. benefit profile of allowing personal devices to be used for work is warranted.

4. Establishing secure policies spanning both identities and configurations for endpoints is critical. A single stolen credential or misconfigured endpoint can lead to critical compromise, regardless of where workloads and data reside. The rapid pace of change in IT environments, including sprawling cloud adoption and privileged account proliferation, often outpaces security implementations, making standardized identity security policies and secure endpoint configurations a crucial defense mechanism that helps organizations maintain control over their expanding digital footprint.
    - You did not report this has been an area of focus for your organization over the past year and that suggests a greater focus on proactive security configurations and hygiene would help your organization keep its attack surface manageable.

Figure 3. What Your Peers Are Doing To Reduce Their Attack Surface



Source: Enterprise Strategy Group, now part of Omdia

How Dell Can Help You Reduce Your Attack Surface

- **Dell's Secure Design Lifecycle** mitigates the risk of product vulnerabilities. Our supply chain controls mitigate the risk of product tampering from sourcing through to delivery. For added assurance, Dell cryptographically validates components from factory to deployment with Secured Component Verification, ensuring shipped hardware hasn't been tampered with—mitigating the risk of supply chain-based backdoors.

- All of our infrastructure solutions are built from the ground up with security in mind with the ability to continuously verify the integrity of systems. Our solutions, such as PCs, Servers, Networking, Storage and Cyber Resilience are built to activate **zero trust principles** and include capabilities such as **MFA, RBAC and BIOS-level visibility** to ensure the right people have access to the right information.

- Every Dell PC includes a **Trusted Platform Module** for secure credential storage, attestation, and verified boot. This ensures only trusted OS and firmware loads, helping to negate bootkits and cryptographically secure assets on the device.

Section 2: Detecting and Responding to Attacks

The second practice aera of the assessment focuses on reactive threat detection and response strategies and activities—that is, the technologies and processes in place at your organization to detect and respond to a cyberattack or ransomware-related incident, limiting its impact.

Your Rating: Considering just this practice area, based on your answers in this area, you have obtained a rating of: **Vulnerable**

Your organization is making progress but still has work to do. Consider investing in coverage assessments to identify visibility gaps, especially in rapidly changing areas, such as cloud workloads, infrastructure to support new, critical digital services, and AI infrastructure and AI-enabled devices.

Recommendations to Improve Detection and Response to Attacks

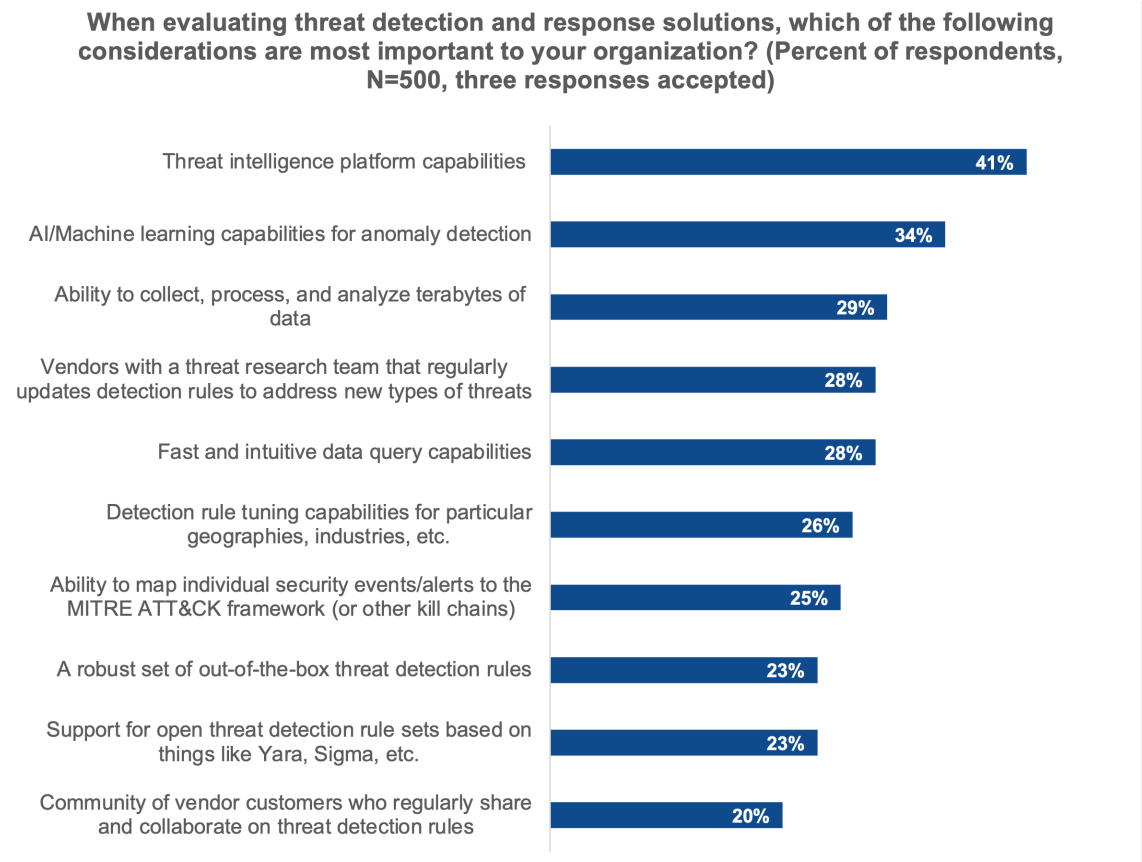
1. As the complexity of the threat landscape continues to increase, attackers commonly leverage multiple attack vectors to compromise and breach organizations. Siloed, point security solutions often provide rich monitoring capabilities, but can also overwhelm SecOps teams with extreme alert volumes, and can challenge security analysts in aggregating, correlating, and analyzing disparate signals to identify true threats. Investing in tools consolidation initiatives, together with scalable security data management and analytics capabilities can help simplify and improve overall SecOps throughput.
    - You did not report this has been an area of focus for your organization over the past year and that suggests reviewing your environment for gaps in coverage would be a worthwhile exercise.

2. Data security is becoming increasingly more relevant in the AI-era. Data loss prevention (DLP), data security posture management (DSPM), data integrity, and file access monitoring can all improve detection of ransomware and AI attacks. While these security strategies are not new, their importance has increased. Consider assessing your capabilities here through internal or third-party assessments to identify gaps and your attack surface expands.
    - You did not report this has been an area of focus for your organization over the past year and that suggests reviewing your environment for gaps in coverage would be a worthwhile exercise.

3. As adversaries increase the use of AI-enabled attack strategies, it is becoming increasingly important to strengthen threat intelligence capabilities, AI-driven anomaly detection capabilities, and the scalability of the security data layer. While you might have investments in some of these areas to date, consider further attention to these areas to strengthen your security outcomes moving forward.
    - You reported this has been an area of focus for your organization which puts your organization in good company.

4. Enterprise Strategy Group research also shows that organizations who struggle most with reactive security activities, often overwhelmed by alerts and extended mean-time-to-respond times, align with a lack of proactive security strategies. For many, offloading reactive detection and response security operations to a third party has enabled internal resources to refocus on proactive security strategies, ultimately resulting in stronger posture and fewer successful attacks.

Figure 4. What Your Peers Prioritize in Threat Detection and Response Solutions



Source: Enterprise Strategy Group, now part of Omdia

How Dell Can Help You Detect and Respond to Threats

- **Secure PCs & Servers:** The number of end users who are working remotely and, on the go, has increased exponentially. With breaches now happening both above and below the OS, you need intelligent solutions that prevent, detect, and respond to threats wherever they occur. Dell PCs and servers are built securely and continuously monitor for firmware and BIOS tampering, unauthorized configuration changes, and hardware-level anomalies, surfacing alerts for investigation. Dell-unique PC telemetry from "below-the-OS" tamper detections (e.g., Indicators of Attack) help enrich partner software for improved threat detection and response.

- **AI-Powered Anomaly Detection:** Integrated into Dell storage (PowerStore, PowerMax, PowerScale), Cyber Resilience (PowerProtect) and endpoints for early identification of unusual file or access patterns, supplementing signature-based threat monitoring.

- **Attack Simulation Management & Pen Testing Services:** Dell offers automated breach and attack simulations as well as human-driven penetration testing—validating that controls work when confronted with evolving attack techniques.

- **Managed Detection & Response (MDR):** 24x7 security operations from Dell (with software from Secureworks, CrowdStrike, or Microsoft) provide always-on expertise, threat hunting, and rapid alerts—across endpoints, network, cloud, and data protection environments.

Section 3: Recovering From Attacks

While detection and response are critical to quickly detecting something amiss, having a recovery strategy in place is equally important, including rehearsed incident response plans and reliable backup strategies. The third and final practice area of the assessment therefore focuses on completeness of recovery preparedness and capability. That is, the technologies and processes in place at your organization that recover all your data and enable the resumption of normal operations in order to resume normal operations as quickly as possible.

Your Rating: We asked how much of your data you believe you would be able to recover in the event of an attack. Considering just this practice areas, based on your answers in this area, you have obtained a rating of: **Prepared**

Data sets are digital business assets and must be protected as prized possessions. Your business literally is the data. Your ability to recover all systems, data, and applications after a cyber event is critical to enable the resumption of business operations. Not only does it limit your business risk, Enterprise Strategy Group research shows it also mitigates costs associated with direct revenue loss and reputational loss. Your high confidence in your cyber-recovery capabilities is great news for your organization. Your answers also indicate you have a well-rehearsed recovery plan which is regularly tested and validated.

Recommendations to Improve Recovery

1. Your ability to recover systems and data is predicated on your ability to ensure the integrity and availability of data at the time of recovery from a cyber event. Modern attack tactics associated with ransomware are increasingly tampering with data recovery mechanisms and assets, further challenging traditional data protection strategies. Enterprise Strategy Group research shows organizations should, and are, investing in multiple storage mechanisms and processes to mitigate this risk. The use of air-gapped backup solutions, together with regular recovery testing and backup integrity testing are all recommended.
    - You reported this has been an area of focus for your organization which puts your organization in good company.

2. In addition to the integrity of your data, your ability to rapidly and confidently execute your recovery processes is critical to minimizing the impact of a successful cyberattack. Keeping incident response and recovery (IRR) plans current and complete requires regular assessment and updates but also requires exercises to rehearse all aspects of the IRR process, including people, trusted third parties and technologies. Best practices show at least quarterly updates to plans, and at least as frequent rehearsals.
    - You reported this has been an area of focus for your organization which puts your organization in good company.

3. Enterprise Strategy Group's research consistently shows that cybersecurity is an area of technology in which skill sets are lacking. Having the right staff and skills in place is an advantage that can help your organization better defend itself and recover from cyberattacks.
    - It is a great sign that your organization has the people and skills needed to recover from destructive cyberattacks today, but the importance of continuing to invest in your teams and their skills should continue to be a priority.

How Dell Can Help You Recover from a Cyberattack

Dell Services

- **Incident Response and Recovery** is a global team of experts ready at a moment's notice for assistance in rebuilding, restoring, and redeploying vendor agnostic infrastructure, data and applications.
- **Security & Resilience Advisory Services** provide expert advice and solution integration to reduce business downtime, regardless of its origin with automated resilience solutions.

Dell Storage

- **Snapshots on Dell storage** can be configured as immutable (read-only), meaning once they're created, they cannot be modified or deleted, even by privileged administrators. This prevents attackers from erasing or corrupting recovery points if they've compromised admin credentials.
- **PowerProtect Cyber Recovery** creates isolated recovery environments disconnected (air-gapped) from the main network, preventing attackers from accessing vital recovery data. Technologies include policy-driven retention, automation for recovery, and scanning tools to validate data and ensure it's malware-free before restoring.

PowerEdge

- Through **Dell SafeBIOS, PowerEdge servers** continually verify the integrity of server firmware both at boot and runtime. If tampering is detected, SafeBIOS can automatically restore firmware to a trusted version, blocking attackers from persisting at the firmware level. This "self-healing" capability, also termed Automated System Recovery (ASR), allows servers to recover corrupted firmware, operating systems, and critical workloads rapidly—helping IT teams get systems back online with minimal downtime.

Dell PCs

- **Rapid OS and Application Recovery:** Many Dell PCs include recovery partitions or automated OS restore tools, allowing users to revert systems to factory or IT-approved settings. If malware or ransomware disrupt the operating system, these built-in utilities let organizations quickly roll back to a clean state with minimal downtime. Additionally, partner software enables self-healing of critical endpoints and applications.
- **Endpoint Management & Remote Remediation:** Dell PCs can be managed by centralized endpoint management solutions (like Dell Client Command Suite and third-party end user management platforms), enabling IT teams to remotely isolate, sanitize, and restore compromised endpoints at scale. Integration with Dell's cyber recovery framework ensures coordinated restoration and forensic analysis across all business endpoints.

Conclusion

Dell Technologies strives to build a secure, connected world. We work tirelessly to keep your devices, network, data, organization, and customers' safety top-of-mind—with cybersecurity and resilience engineered end-to-end into all our products, solutions, and services. From a secure supply chain to intrinsic security built into all of our solutions, we help you create and maintain a secure and resilient organization even as new threats emerge. Our global team of services experts are ready to help improve your cybersecurity and resilience maturity. Based upon your assessment and current score we have made prioritized recommendations to help improve your resilience. **Our Security and Trust Center** provides easy access to additional resources and solutions to help you quickly find answers to your consumer and enterprise security questions.

From the endpoint, to the core, to the cloud—our industry experts offer strategic guidance and proven practical capabilities to help you protect your business and preserve your reputation from cyberthreats. Learn more about **Dell's security solutions**.

[1]All data cited in this report originates from Enterprise Strategy Group custom research commissioned by Dell, "Assessing Organizations' Security Journeys," January 2024.

About Enterprise Strategy Group

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content support enterprise technology buying and selling. | www.esg-global.com | contact@esg-global.com