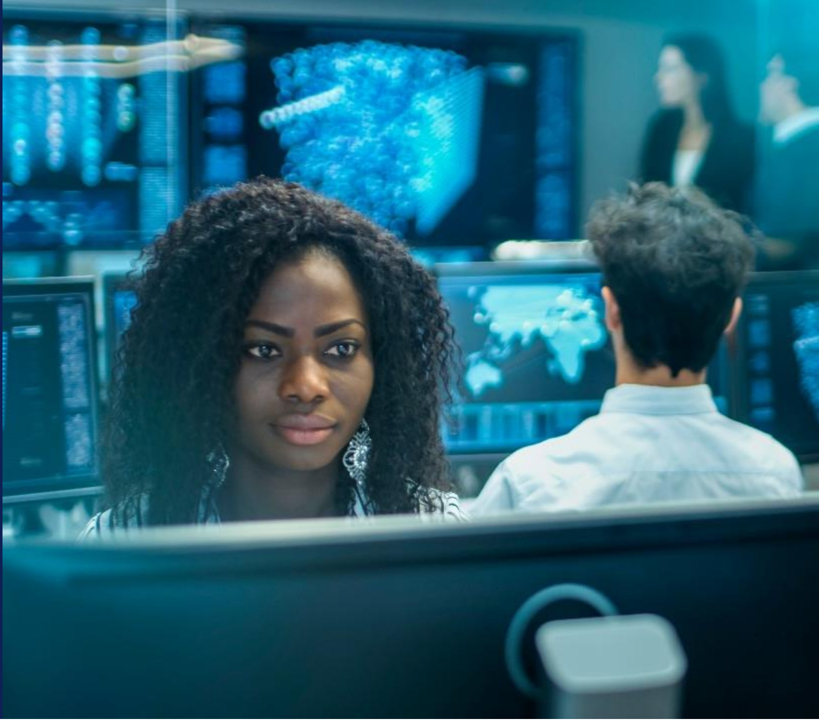
DELL Technologies

Security & Resiliency Services

Shift continuous threat detection and response to where attackers target first



Today's challenges

The need for threat detection and response for high value targets like IT infrastructure has never been more critical. However, achieving this presents significant manual integration burdens for security teams. One of the primary hurdles is based on how security visibility tools work. For endpoint, cloud and network, the default behavior for security teams is to install an agent to gain visibility with existing tools. Unfortunately, no such agents exist for data protection infrastructure. Instead, these systems typically provide log files to Security Incident and Event Management (SIEM) tools managed by the organization's security team. Not only do these tools generate a flood of alerts that are not prioritized, they add significant management burdens to already understaffed security teams[3]. Critical alerts can easily be missed. Terms like 'alert fatigue' have emerged to characterize their experiences of managing these tools. While logs may be used in a broader incident investigation, the deluge of alerts effectively leaves security teams looking for a needle of a clue amidst a haystack of alerts. There must be a better way!

Trends to consider

62 minutes for threats to spread from initial point of compromise[1]

67 percent paid ransom to recover data when backups are compromised[2]

Threat actors target backups and demand higher ransom amounts when those are compromised[2]

Extending proactive security coverage

Recognizing these challenges, we have expanded our Managed Detection and Response (MDR) service and it's 24x7 coverage to secure data protection environments and speed threat response. Our approach takes a services-driven approach to free organizations from the burdens of managing infrastructure security through two unique elements:

1. **New Advanced Threat Detection capabilities:** Expanding upon our partnership with CrowdStrike, we have jointly developed over 60 proprietary Indicators of Compromise (IOC) specifically for the data protection environment to better understand threat actor behavior and speed threat detection and response efforts. These IOCs have been mapped to the MITRE ATT&CK framework and prioritized by severity to provide actionable, high-quality forensics data to our security analysts.
2. **Collaborative SOC Model:** This model fosters close cooperation between Dell and your security teams to drive the common objective of improving your security posture. You retain all your existing SOC responsibilities and gain a trusted third party to enhance visibility and threat response in the data protection environment. This partnership ensures that security teams are not working in isolation but are supported by experts who can provide expertise, guidance and resources.

How does it work?

We start by ingesting telemetry from **Dell PowerProtect Data Domain** and **PowerProtect Data Manager** with our proprietary data connectors into CrowdStrike Next Generation SIEM which automates log correlation and is managed by our expert security analysts. We can also provide this capability for PowerProtect Data Domain irrespective of the data protection software, helping customers secure their multivendor data protection environments. When there is a detection, our analysts immediately begin an investigation, often working closely with our Incident Response and Recovery team to determine what they're seeing and if necessary, document a clear path to remediation. Your teams will be engaged with our analysts throughout this process to improve your response speed with effective and efficient remediation steps for your teams to action.

Extending MDR to cover data protection infrastructure and software enhances visibility, improves proactive threat detection, and fosters collaboration between your security teams and outside experts. This approach, supported by our deep industry partnerships, leverages advanced, prioritized IOCs to speed threat detection and response efforts. By addressing critical challenges in today's threat landscape, we empower customers to protect their most valuable assets and improve their cyber resilience.

This capability is included as part of our broader MDR service; therefore, we can easily extend coverage beyond data protection infrastructure to cover your entire IT ecosystem with continuous threat detection and response across endpoint, cloud and network.

Why Dell?

Building upon longstanding expertise in data protection, security, cyber recovery and resilience, Dell is leading cybersecurity innovation by improving threat response and reducing SecOps burdens in securing data protection infrastructure. We are proud to be recognized as **CrowdStrike's Global Partner of the Year** for the work we do together, and our engineering-level relationship has enabled several unique-to-Dell integrations between our products and services.

Explore additional Security & Resiliency Services

Security and Resiliency Advisory Services

Managed Detection and Response

Incident Response and Recovery

Cyber Recovery Services

[1] https://ir.crowdstrike.com/news-releases/news-release-details/2024-crowdstrike-global-threat-report-breakout-breach-under#, February 2024
[2] https://www.techrepublic.com/article/ransomware-attackers-target-backups, April 2024
[3] https://www.isaca.org/about-us/newsroom/press-releases/2023/new-isaca-research-59-percent-of-cybersecurity-teams-are-understaffed, Oct 2023

Explore Dell Security and Resiliency Services

Contact a Dell Technologies expert

Join the conversation with #DellTechnologies