Key Benefits

Prevent

- Identify vulnerabilities across the environment to prioritize patching
- Detect misconfigured or problematic security controls that could be exploited
- Closely inspect high-risk pathways to valuable assets or data with annual pen testing
- Improve employee vigilance with security training delivered in frequent, bite-sized modules

Respond

- Detect and respond to threats 24/7 across environment
- Track end-to-end activity of threat actors
- Utilize telemetry and correlate events from many popular security tools

Recover

- Rapidly respond if a serious incident or breach occurs
- Restore operations as highly skilled, certified Dell cybersecurity experts collaborate with your IT team

Dell Managed Detection and Response Pro Plus

Fully managed, 360° SecOps solution across endpoints, network and cloud

Taking on critical security operations challenges

Many IT organizations have adopted threat monitoring and detection to keep pace with the continually increasing volume and variety of threats.

While threat monitoring and detection provide vital coverage, it's best to handle fixable gaps up front, before threat actors have a chance to exploit them. IT teams can prevent much malicious activity by proactively addressing software vulnerabilities, misconfigured security controls and employee carelessness.

Knowledgeable security professionals know to patch vulnerabilities, but for most IT organizations it's impossible to patch them all. In 2021, more than 1,500 new vulnerabilities were reported each month.[1] To keep the patching load manageable, customers must prioritize the vulnerabilities that present the greatest risk.

It's equally daunting to try to validate all of your security controls, such as email gateways or web application firewalls. With hundreds of controls and complex configurations, IT security teams are hard-pressed to confirm that security controls are blocking unauthorized activity.

Additionally, organizations need employees to recognize when threat actors are trying to gain login credentials, confidential data or other sensitive information. One study found that 83 percent of responding organizations experienced a successful email-based phishing attack in 2021.[2]

Managed Detection and Response Pro Plus

Dell Technologies security experts closely examined these key SecOps concerns to design a new 360° security operations service: Managed Detection and Response Pro Plus.

MDR Pro Plus is a fully-managed SecOps solution in which top security experts utilize cutting-edge tools to prevent threats, detect and contain attack attempts quickly, and help to recover and restore your environment in the event of a breach. MDR Pro Plus helps you continually strengthen your organization's security posture.

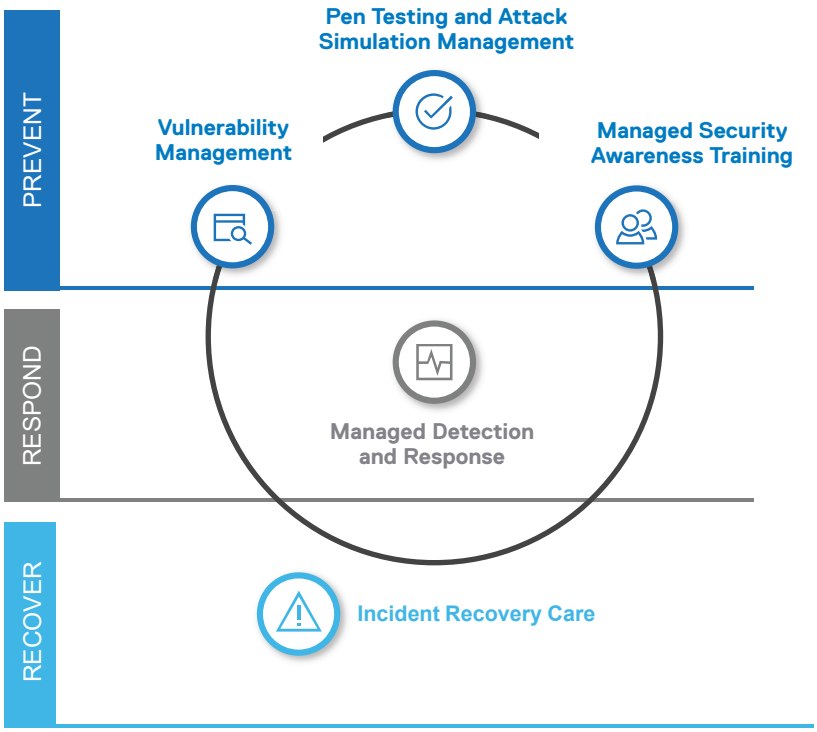
Seal openings in software and security controls

Vulnerability Management scans your environment monthly for vulnerabilities and employs machine learning to prioritize those most likely to be exploited and have a major impact. The prioritized list helps your IT team focus on the highest value vulnerabilities.

Just as threat actors know to look for unpatched vulnerabilities, they search for misconfigured or out-of-date security controls – so IT organizations need to find and address them first. **Pen Testing and Attack Simulation Management** features monthly automated breach and attack simulations (BAS) and annual penetration testing.

BAS detects faulty security controls on devices and software in your IT environment. Pen testing complements BAS by attempting to reach a specific goal, such as a high-value system. Skilled pen testers emulate threat actor techniques, including pivoting and adapting techniques to reach the target.

Dell runs vulnerability scans and BAS simulations against continuously updated databases to help you make sure patching and security controls stay up to date.



Help employees stay vigilant

A common model for security awareness training is an annual, multi-hour training session. Employees often do not retain this information as it can become a "check the box" exercise. In the event they are subjected to a social engineering tactic or an email with a malicious link, they may not react with sufficient caution.

Managed Security Awareness Training delivers bite-sized security training throughout the year, keeping employees actively engaged with customized learning paths and making security top of mind. Learning paths are created based on employee role, threat exposure level and progress.

Quickly detect and contain attack attempts

Dell MDR Pro Plus boasts 24/7 **Managed Detection and Response**. Skilled analysts monitor your environment and investigate threats using an advanced XDR security analytics platform. Machine- and deep learning-driven analyses of telemetry and events provide analysts with rich information to retrace the attacker's path and activities. The Dell team then provides you with instructions to contain and resolve the threat.

Assess incidents or breaches swiftly and work with you to restore operations

Well-executed preventive security measures combined with advanced detection and response significantly reduce the number of serious security incidents or breaches. Even so, there may be times when an attack gets through.

MDR Pro Plus includes Incident Recovery Care for rapid response by certified cybersecurity experts who assess the situation and work with you to recover and restore your environment in the event of a breach. The Dell team's familiarity with your environment supports an efficient and thorough recovery process.

Elevate your security operations with Dell

MDR Pro Plus helps prevent malicious activity by regularly informing you of vulnerability gaps, misconfigured security controls and high-risk pathways to valuable assets. In addition, we provide concise, easy-to-retain security training for employees throughout the year.

Threat detection and response provides always-on monitoring and tracking of suspicious activity. With Incident Recovery Care, expert resources are ready to help you recover and restore your IT operations in the event of a potentially damaging breach.

MDR Pro Plus provides you with an intelligent 360° IT security operations solution – with services based on advanced technology, delivered by experts. All managed by Dell Technologies: a company that organizations of all sizes across the globe trust for innovative IT devices, infrastructure and services.

Learn more about Dell Managed Detection and Response Pro Plus

Contact a Dell Technologies expert

[1]Source: With 18,378 vulnerabilities reported in 2021, NIST records fifth straight year of record numbers, ZDNet December 8, 2021. https://www.zdnet.com/article/with-18376-vulnerabilities-found-in-2021-nist-reports-fifth-straight-year-of-record-numbers/

[2]Source: 2020 Phishing Attack Landscape Report [Greathorn]. Cybersecurity Insiders. (2020). Retrieved November 15, 2022, from https://www.cybersecurity-insiders.com/portfolio/2020-phishing-attack-landscape-report-greathorn/