Strengthen your security posture with Managed Detection and Response

Detect, investigate, and respond to advanced threats across your IT environment

Dell Managed Detection and Response

Combining Dell Technologies' security expertise and deep knowledge of IT environments with your choice of select industry-leading XDR security analytics platforms.

How secure is your business?

It's difficult for IT teams to keep pace with the growing volume of ever-evolving security threats. In 2022, there were 5.5 billion malware attacks globally, up 100 million from 2021.[1]

Fully protecting your organization requires quick detection and effective response to new threats across the environment. This is difficult due to point products and tools that fragment visibility, challenges in finding and retaining qualified security professionals, and IT teams that are already fully occupied with critical demands and daily operations.

Managed Threat Detection and Response

Dell Managed Detection and Response is a fully managed, end-to-end, 24/7 service that monitors, detects, investigates and responds to threats across the entire IT environment, helping organizations with 50 or more endpoints to quickly and significantly improve their security posture—while reducing the burden on IT.

The service leverages two key capabilities:

- The expertise of Dell Technologies security analysts, gained through years of experience helping organizations worldwide to better protect their business
- Industry-leading extended detection and response (XDR) security analytics platforms that incorporate AI-enabled analyses of telemetry and events from multiple attack vectors.

Key benefits:

- Unified detection and response across the entire ecosystem
- Continuously updated threat database keeps protection current
- Even the stealthiest threat actor tactics can be detected
- Comprehensive view of attacker's end-to-end activity
- A team of Dell Technologies security professionals whose expertise includes security, advanced infrastructure, cloud and more
- Expert help in implementing the cloud-native SaaS XDR
- Quick initiation of cyber incident response when a breach occurs
- Continuously align to the highest level of security compliance for service providers

Full-Service Solution

Dell Technologies security analysts assist with initial set up, monitoring, detection, remediation and response—all for one predictable price. They work closely with your IT team to understand the environment, advise on security posture improvements and help deploy the XDR software agent to endpoints.

Alerts are monitored and reviewed 24/7. If an alert merits investigation, analysts determine and perform the appropriate response. If a threat is malicious or requires your action, you are informed and, if necessary, provided with step-by-step instructions.

In the event of a security incident, Dell Technologies helps you initiate the process to get your business back up and running.

Choose your XDR platform

Your security and technology needs and preferences are unique. We give you the flexibility to choose from three industry-leading options: Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR or Microsoft Defender XDR so you can get an XDR platform that fits your needs.[2]

Key Features

Trusted Support

- Partner closely with you to understand your environment, resolve investigations and advise on security posture improvements
- 24/7 monitoring with your choice of select XDR platforms that incorporate AI-enabled analyses of telemetry and events from multiple attack vectors
- Expert advice for deploying and configuring the XDR platform

Threat Response and Security Configuration

- Utilizing XDR capabilities, the Dell SOC team will automate remediation or collaborate with you to address threats uncovered during monitoring
- Deliver detailed, easy-to-understand instructions to contain the threat even in complex situations
- Up to 40 hours of service-related security configuration included per quarter

24/7 Detection & Investigation

- Processes and alerts tailored to your organization's security environment and automated for efficient daily operations
- Proactive threat hunting specific to each customer's environment to discover new threats or variations of known threats that evade security systems
- Daily summary of less critical alerts enables the Dell SOC team to focus attention on critical alerts
- Quarterly reports on investigations, alert trends analytics and security posture guidance

Cyber Incident Response Initiation

- 40 hours of annual remote incident response assistance enables investigative activities to commence quickly
- Guidance from our certified security experts who have helped organizations of all sizes recover from severe security events

Start securing your environment today with Dell

With the average total cost of a ransomware breach reaching $5.13 million, 13 percent higher than in 2022, now is the time to learn more about whether Dell Managed Detection and Response is right for you.[3]

Contact your sales representative today.

1. Statista, Annual number of malware attacks worldwide from 2015 to 2022
2. Minimum of 500 endpoints required for using Microsoft Defender XDR
3. IBM, Cost of a Data Breach Report 2023

DELL Technologies