SOLUTION BRIEF

# Evaluating a Managed Detection and Response Provider

## What's Inside?

This brief details the key requirements you should consider when evaluating managed detection and response services. It then shows how Dell Managed Detection and Response uses a combination of security analytics software, deep threat intelligence, and leading security expertise to significantly improve threat detection and response times. Links to useful resources like webinars and videos are included throughout to give you quick access in case you have additional questions.

Security teams of all sizes and maturity levels are struggling with larger attack surfaces, disparate tools, and insufficient staff and skills. Dell Managed Detection and Response powered by Secureworks Taegis® XDR™ solves these challenges, but not all managed detection and response providers are equal in today's market. Read this brief to learn what requirements to look for in a managed detection and response solution and how Dell stands out in a crowded, changing market landscape.

## Detection and Response Challenges

**76%**

of cybersecurity professionals in a recent survey by ESG[1] found that threat detection and response is more difficult than two years ago. Our experience with customers shows this is a result of amplified threat volume, staff shortages, excessive manual work, and a widening attack surface.

**89%**

of respondents in the ESG[1] survey said they plan to increase funding for threat detection and response activities. But choosing a provider to partner with isn't easy. The number of vendors in the market attempting to address detection and response has increased dramatically. But most of these providers are missing the mark.

[1] Source: ESG Master Survey Results, The Threat Detection and Response Landscape, April 2019

## Buyer Requirements Table

The following table outlines how any managed detection and response solution you're evaluating must meet certain minimum requirements to solve the challenges above.

| Component | Description | Vendor Vetting Questions |
|---|---|---|
| **Sofware-Driven Detection Speed** | Analytical speed is a powerful weapon in security operations. Any proposed solution needs to be architected around the latest analytics technology, even if you're not directly using it. Be on the lookout for true cloud-native architectures that incorporate data science methods such as machine and deep learning. | 1. Describe how quickly you detect <insert threat here> and can you show us how you will respond to it on our behalf?<br>2. Explain how your cloud-native analytics technology works. Was it built in-house or are you partnered with another vendor?<br>3. Discuss how you incorporated data science into your software development process. |
| **Software-Driven Detection Precision** | Quickly detecting a false alarm is not very effective. Precise detections fuel precise responses. AI-based Detectors should be purpose-built and used in provider's daily operations. These Detectors are used to find behavioral anomalies such as command and control, brute force attempts, and stolen credentials. | 1. Describe how accurately you can detect <insert threat here> and can you show us how you will respond to it on our behalf?<br>2. Tell us about the experience you have in responding to and evicting threats from organizations?<br>3. Can you show me a demo of how your solution will apply that experience to keep us safe?<br>4. Is your software proprietary or via a third party? Does our team get access to your software as part of the solution? |
| **Diversity of Threat Data and Research** | When a threat actor has infiltrated your environment, they often use legitimate tools to evade detection by traditional security controls. In fact, research shows that the average dwell time of attackers is 111 days. Detecting and evicting these threats requires a vast amount of threat data combined with a deep understanding of how threats behave. | 1. How many professionals do you have keeping up to speed on the threat landscape?<br>2. Show us how your software infuses a diversity of data on historical, current, and potential threats.<br>3. Does the solution adapt to new attack patterns or is it a static set of rules that are easy to figure out and bypass?<br>4. Describe the process for how you find threats on other customer environments and feed that data into our defense posture. |
| **Proactive Threat Hunting** | Collaboration and transparency between the provider and your team is a key success factor. There needs to be collaborative investigation capabilities and open channels of communication. Threats don't sleep, and neither should your provider's ability to keep you up to speed on a risk to your business. | 1. Please show us a demo of the user interface you provide to support co-hunting and collaborative investigations.<br>2. Describe what happens when we have questions – can we call or live chat with you at any time.<br>3. Describe how you know what to search for in our environment and what would trigger a hunt with us? Can we initiate a request for help in this area? |
| **Incident Response Support** | Your team needs to be able to rely on experienced security professionals to help during critical events. Any provider should provide evidence on how exactly remote incident response hours are a part of their managed detection and response solution without any hidden fees or costs. | 1. Are incident response hours included in the managed solution?<br>2. How quickly will you respond in the event of a validated incident?<br>3. Tell us more about the experience your incident response team has – are they recognized by industry analysts? |

**Watch a video about Dell Managed Detection and Response**

Watch the Video

**Watch an Advanced Threat Detection and Investigation webinar**

Watch the Webinar

**Watch a Threat Hunting webinar**

Watch the Webinar

**Download the datasheet on Managed Detection and Response**

Download Datasheet

The answers to these questions will reveal if the proposed managed detection and response solution can improve your defense posture, or if it will waste your limited time and resources. Of course, each environment has unique variables to consider, such as staff size, existing technology investments, and industry or geographic nuances. But this basic list of considerations will help you avoid making a regrettable decision.

## Dell Managed Detection and Response

Fully protecting your business requires quick detection and effective response to ever-evolving security threats. Dell Managed Detection and Response is a fully managed, end-to-end, 24x7 service that monitors, detects, investigates and responds to threats across your entire IT environment, helping you quickly and significantly improve your security posture—while reducing the burden on your IT team.

**Our 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
- The power of the open Secureworks Taegis XDR security analytics software, built on 20+ years of SecOps know-how, real-world threat intelligence and research, and experience detecting and responding to advanced threats

Managed Detection and Response enables your team, however advanced, to deal with an increasing workload and threat volume. We bring our expertise into your daily operations. Your team can collaborate with us on hunts, chat with our analysts, and periodically assess your security posture.

SOLUTION BRIEF

# 10 Reasons to Consider Dell for your MDR Needs

**Experiencing an Incident?**

If your organization needs immediate assistance for a potential incident or security breach, email us at Incident.Recovery@Dell.com

**Email Us**

For more information, go to Dell.com/MDR or contact your sales representative.

**Visit Website**

## 1 Benefit from the power of Dell

The company you trust to deploy and support your devices and infrastructure is the same company you can trust to help secure your environment with a team of highly trained, certified security analysts monitoring your environment 24x7.

## 2 Partner on investigations

Raise the skill level of your team by partnering on investigations with our experts.

## 3 Live Chat with our security analysts

Instantly pull up a chat window to get expert help whenever you need it.

## 4 Enhance your security posture with frequent reviews

Continuous improvements to your security posture with periodic reviews and reports.

## 5 See more threats with uniquedata diversity

Act on threat knowledge from over 1,400 IR engagements, a team of 80 threat researchers, and our experience protecting over 4,000 customers globally.

## 6 Act with confidence – backed by human and machine intelligence

Save time and increase effectiveness through automation of basic tasks and collaborative investigations.

## 7 Detect and respond to unknown threats

Find evasive threats like fileless malware and know exactly how to respond.

## 8 Hunt threats proactively to check anomalies

Our experts help you hunt for persistence mechanisms, threat actor tactics, anomalous networks communications, and anomalous application usage.

## 9 Incident response is included

Incident response hours are included for added peace of mind and to help you get a fast start on recovery.

## 10 Protect your cloud deployments

Use our cloud-native architecture to detect and respond to events from your AWS, Office 365, and Azure environments.



DELL Technologies