DELL Technologies

WHITE PAPER

DELL MANAGED DETECTION AND RESPONSE

The complete managed security solution for mid-sized and smaller organizations.

EXECUTIVE SUMMARY

Cyberattacks on businesses are on the rise. Reporting by the FBI's Internet Complaint Center in 2021 noted a 69% increase from the previous year and a total of U.S. $4.2 billion in losses.[1] Attacks against major corporations grab front-page headlines, but in reality, businesses of all sizes are vulnerable. Small businesses, lacking the extensive resources of large corporations, are particularly at risk.

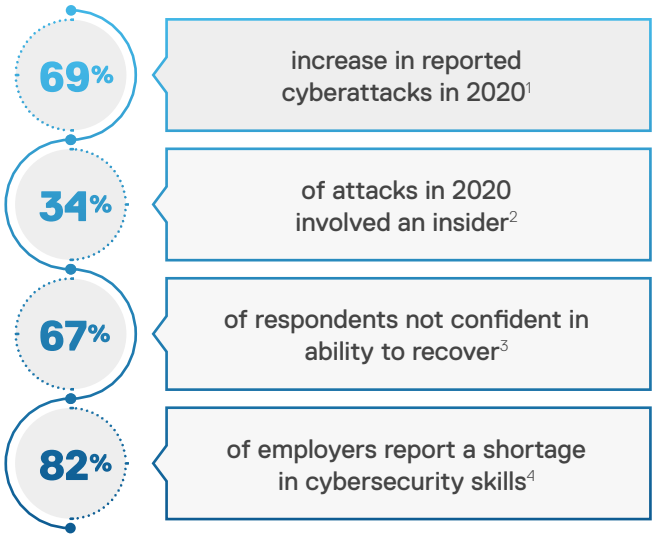
Cybersecurity is critical to protecting data assets, operations and business continuity. Large corporations often have dedicated security teams with the latest technology, methods, and intelligence. However, mid-sized and smaller companies may have only one or two security specialists who have to manage and operate increasingly complex arrays of security appliances and software tools.

A Growing IT Challenge

The onslaught of attacks on endpoints, servers, applications, networks and cloud generates immense alert volumes that quickly overwhelm security and IT teams. At the same time, threat actors continue to evolve their techniques, nimbly sidestepping yesterday's effective defense. Properly securing IT environments in the 2020s requires 24x7, 365-day monitoring and response by dedicated experts.

If IT leaders of mid-sized and smaller firms allocate sufficient IT headcount and budget to cybersecurity, important areas like applications development and DevOps will suffer. The fact is that protecting against today's threat actors necessitates an investment in talent, tools, and operations that many organizations simply cannot afford.

Cyberattacks pose a greater threat than ever



Managed Detection and Response Provides Answers

Consequently, more companies are considering managed detection and response (MDR) solutions from outside service providers. How do IT decision makers identify an outstanding MDR partner?

A viable MDR solution provider must implement technology that detects known threat types, minimizes false positives, correlates events, tracks an intruder's activity sequence, and automates containment and prevention actions. The provider requires a team of highly skilled and experienced security professionals to analyze alerts and remediate threats 24x7x365, as well as hunt for new threat types.

Providing MDR services calls for building out security operations and establishing and refining processes. Further, analysts need knowledge sharing tools and regular training to stay current on the latest threats and techniques.

Although many service providers advertise managed detection and response services, only a few have the capacity and capabilities needed to deliver excellence.

Dell Managed Detection and Response is a fully managed, end-to-end, 24x7 solution that monitors, detects, investigates, and responds to threats across an organization's entire IT environment. Whether an enterprise consists of 50 endpoints or thousands, Dell MDR quickly and significantly improves the company's security posture while decreasing the burden on IT personnel. Dell MDR takes advantage of Dell's ability to invest in people, processes, and tools to provide mid-sized and smaller businesses with enterprise-scale cybersecurity monitoring and response.

Top Reasons Why Businesses use Managed Detection and Response (MDR) Solutions

- **Access to hard-to-find cybersecurity specialists**
- **Comprehensive monitoring, detection, and response coverage**
- **Decreased burden on IT personnel enabling focus on DevOps**

TODAY'S THREAT LANDSCAPE

Modern threat actors are methodical, investing weeks or months considering how they will obtain access to valuable applications and data. Once they identify an opportunity, they may exploit an opening or send phishing emails to entice users to open a malicious attachment. Detection and response are essential elements of a comprehensive cybersecurity program, along with employee training, cybersecurity assessments, vulnerability and penetration testing, resiliency and recovery planning, and more.

If the actor obtains access, they initially want to establish a base from which to broaden the attack scope. Again, they take their time entrenching their positions within the company's infrastructure. For example, in addition to attacking business systems, ransomware attacks often aim to take a company's backup systems offline and block access to backups. This can take away a company's ability to recover, leaving paying the ransom the only option to get a business up and running.

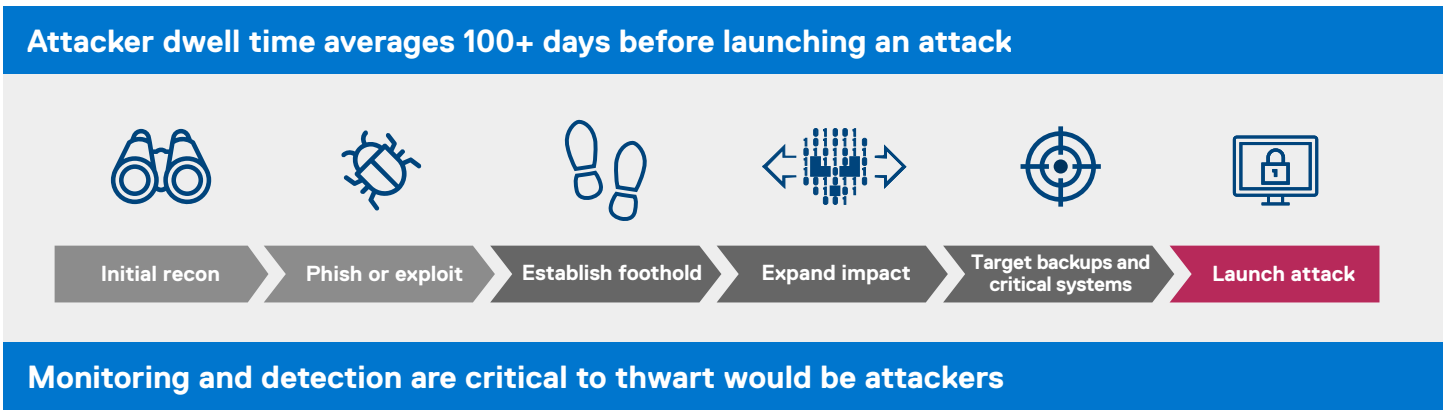
Sophisticated, constantly updated detection and response capabilities are vital to recognizing attacks and other clues. Early warning gives the organization the opportunity to lessen the damage from the assault before it spreads further.

Organizations have deployed a wide range of cybersecurity tools, such as those for password auditing, network testing, vulnerability scanning, encryption, monitoring and threat detection. Alerts come at IT from all these tools – the sheer volume of alerts is challenging, even more so when one considers the difficulty of correlating events across tools. Further, maintaining proficiency in all these technologies is a significant time commitment for IT security personnel.

The human side of the MDR equation calls for a group of professionals with years of cybersecurity experience and skills such as system administration, cyber forensics, threat investigations and penetration testing. These professionals are hard to find, expensive to hire, and constantly being recruited by more prominent, higher spending organizations. The 2021 State of the CIO survey identified cybersecurity roles as the most difficult of all IT roles to fill.[5] Retaining security analysts and backfilling those who do leave is a never-ending battle for IT leaders.

Even after acquiring the essential tools and talent, companies must build out 24x7 security operations and facilities.

Figure 1. Threat actor strategy



Dell Managed Detection and Response services put top-tier capability within reach

It's no wonder that mid-sized and smaller companies often struggle to defend themselves properly. The cybersecurity landscape has grown into an ever-shifting kaleidoscope of threats. The flood of activity has enlarged staffing requirements and the complexity of attacks has raised the level of talent needed.

Dell Managed Detection and Response extends your security team with cybersecurity experts, tools, and operations capabilities comparable to those of the very largest global enterprises. Dell MDR reduces the burden on your IT team, mitigates risk, and significantly enhances your company's security posture so you can focus on business priorities.

Dell Managed Detection and Response is a fully integrated combination of technology, expertise and operations. The service draws on the knowledge of Dell Technologies security analysts who have spent years assisting enterprises all over the world better protect their operations. Dell MDR harnesses the power of Secureworks® Taegis™ XDR—an advanced security analytics software platform that is the product of more than 20 years of proven know-how, real-world threat intelligence and research, and expertise in detecting and responding to sophisticated threats.

Secureworks Taegis XDR

Secureworks Taegis XDR is a purpose-built cybersecurity platform that brings a big data-scale solution to security concerns. A cloud-native platform, Taegis XDR includes continuous machine- and deep learning-driven assessments of telemetry and events from different attack vectors, reinforced with complete threat information.

Why Dell for Managed Detection and Response

People

- **Experienced cybersecurity experts**
- **Taegis XDR certified analysts**
- **Certifications also include CEH, GIAC SANS, CISSP, and CompTIA**

Technology

- **Industry-leading Secureworks Taegis XDR security analytics platform**
- **Continuous end-to-end threat monitoring utilizing telemetry from wide range of endpoints, network and cloud**

Process

- **Rapid time to resolution**
- **24x7/365 coverage**
- **Agent rollout assistance included**
- **40 hours per quarter of remote remediation guidance**
- **40 hours per year of incident response initiation**

Trusted Partner

- **Trusted worldwide for device and infrastructure support**
- **Over 20 years of business resiliency innovation**
- **Continually investing in people, processes, tools**

Figure 2. Threat Intelligence

The only way to identify and respond to sophisticated attacks is by first understanding how bad actors function and what motivates them. Every year, the Secureworks team behind XDR conducts approximately 1,000 Incident Response engagements. This gives them a distinct advantage in seeing how threat actor strategies, techniques, and processes that effectively penetrate client businesses change regularly.

Taegis XDR analyzes security-relevant data collected from endpoints, networks, cloud systems, and on-premise business systems to detect threats. XDR is a fully open platform that complements existing security infrastructure, ensuring comprehensive coverage and protecting prior investments.

XDR provides automated response, remediation, and insights to increase the efficiency of security operations and give response teams the visibility needed to take action when confronted by a threat. Dell MDR customers benefit from threat intelligence developed using hundreds of thousands of data points compiled across customers and shared intelligence services worldwide.

Put top security experts to work for you

A global team of highly trained security analysts are always on the lookout for trouble within your systems. Dell's skilled cybersecurity experts are experienced in all phases of threat detection and mitigation, including threat investigations, threat hunting, endpoint security, and incident response and recovery. Dell analysts are XDR certified and have a range of other governmental and industry-recognized certifications, including CEH, GIAC SANS, CISSP, and CompTIA. Dell MDR's distributed 'follow-the-sun' security operation center operates 24x7/365 days a year.

The Dell MDR team gets to know a company's operations and IT infrastructure. They use machine learning and curated threat information from thousands of IT environments, provided via XDR to monitor your environment. The Dell MDR team instantly swings into action when a warning appears, investigating the alert data to discover connections and patterns that only trained, experienced security analysts would recognize. They then advise an organization's response team members on the best course of action.

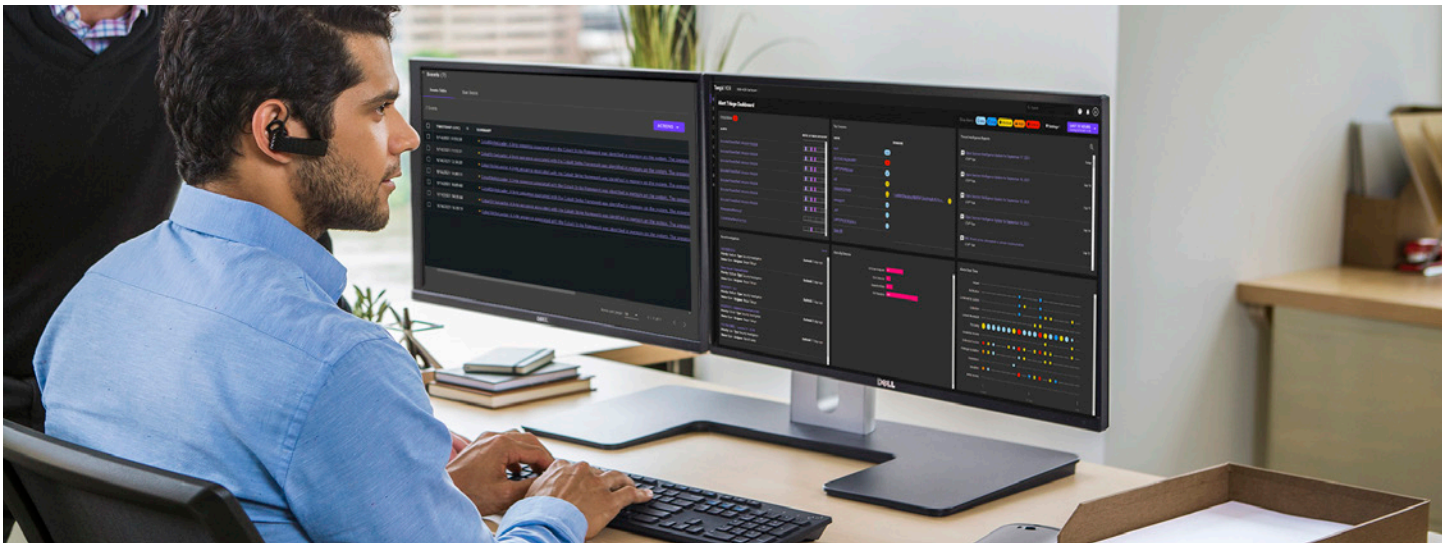
Dell MDR is part of Dell's multi-decade effort toward developing a world-class IT services organization. That means Dell MDR cybersecurity experts will not only provide exceptional guidance to remediate threats, but they also have the skills and know-how to manage it for any organization.

Threat Hunting — identifying threats that can elude automated systems

Threat actors are aware of automated detection systems, so they work to develop new attack types or variations on existing attack types in order to get past these systems. With a system such as Taegis XDR, it's not easy but it is possible.

Security analysts employ threat hunting to identify such 'stealth' threats. Threat hunting looks for indicators of compromise, which could be a series of unsuccessful logins to an account followed by a successful login; or anomalous login attempts, such as outside of regular business hours; or repeated alterations on a file in a short period of time.

Effective threat hunting is a product of technology plus people. The Taegis XDR platform offers an enormous amount of detail on an intruder's activity. Dell MDR analysts scour through this detail to recognize even well hidden activity.



GET TO KNOW DELL MDR

News media have reported on the struggles of governments and global corporations to contain cybersecurity threats. Mid-sized and smaller businesses no longer have to face that challenge alone. With Dell MDR, your organization can benefit from highly skilled security experts dedicated to protecting you, plus an industry-leading security platform, Secureworks Taegis XDR. Your organization leverages Dell's ability to invest in people, processes, and tools to create a managed security service tailored to your organization's needs. Dell Managed Detection and Response service is world-class cybersecurity made accessible to all.

Learn more about Dell MDR

Contact one of our MDR experts

1. 69% increase in attacks FBI: https://blog.isc2.org/isc2_blog/2021/03/fbi-cybercrime-shot-up-in-2020-amidst-pandemic.html
2. 34% insider: https://www.verizon.com/business/resources/reports/dbir/
3. 67% not confident in ability to recover after a destructive cyber attack: www.delltechnologies.com/gdpi
4. 82% of employers report a shortage of cybersecurity skills: https://www.csis.org/analysis/cybersecurity-workforce-gap
5. 13 most difficult-to-fill IT jobs. https://www.cio.com/article/221772/10-most-difficult-it-jobs-for-employers-to-fill.html

DELL Technologies