# 5 Reasons Enterprises Benefit from Managed Threat Detection and Response

The modern enterprise generates massive amounts of user and system activity data that results in an avalanche of alerts. How do you keep pace with identifying what's a real threat? Do you have the right tools to help you? Does your IT security staff have the expertise needed to make sense of it all—and if so, do they have the cycles required to defend you 24/7? If your responses leave you feeling vulnerable and a bit overwhelmed, a managed detection and response (MDR) solution may be the answer to addressing these challenges.

## 1. Centralizing Your Security Information

The modern enterprise operates utilizing a complex ecosystem of devices providing diverse services. Some of them are edge devices such as firewalls and IDS/IPS systems. Others include wireless access points, anti-virus tools, endpoint threat detection, and on and on. With so many devices generating thousands of siloed event logs, it's imperative to centralize and aggregate this data into one source to identify anomalous activity that may indicate malicious activity for investigation and ease the burden of compliance reporting that mandates collection of system and user activity.

## 2. Pinpoint Threat Detection

MDR is designed to detect real threats to the enterprise. Many organizations are overrun with tools that generate waves of alerts. Too often, these alerts result in false positives that are expensive and time consuming to resolve. MDR delivers automated cross-correlation and analysis of alerts across multiple systems, providing centralized visibility to events in real time, allowing for faster and more accurate identification of what is real and truly requires prioritized response, reducing the burdens of alert fatigue.

## 3. Customizing Your System for Best Protections

Along with recognizing your network devices and understanding actual threats, a managed detection and response solution is designed to customize a tailor-made protection force tuned to the unique conditions of your network environment. This customized configuration is based on the type of servers and applications you run and the different types of user community profiles that make up your workforce. As your environment changes, the solution can be easily modified to adapt to changes in the environment, e.g., a sudden shift of office-based user activity to remote-based user activity.

## 4. Real-time Notifications and Time Efficiency

While the MDR solution constantly detects and protects against changes within routers, firewalls, and other servers, it also gathers full-configuration information and recognizes changes in threat feeds, blacklists, and geolocations. This improves the accuracy in monitoring and reporting, and when you combine that with an expert staff of security operations center analysts, you have a threat detection system that stands at the ready to identify, respond and remediate threats to your business.

## 5. Regulatory Compliance Fulfillment

All organizations with personal information must operate within the bounds of FFIEC, HIPAA, PCI, and other security regulations, and an MDR solution helps in achieving compliance. When the request comes in looking for an audit report or exam, the MDR solution can generate the needed reports on controls, such as user access logs, system changes, and any other monitoring adherence needed.

**For the best coverage and solution fit for you, give us a call to discuss how we can help you achieve better security and compliance outcomes.**

, ,
(587)776-0377
**https://www.ctechgroup.net**