WE GET DETECTING AND PRIORITIZING THREATS IS A TOP PRIORITY.

CDW Amplified™ Detect and Respond
CDW Managed Detection and Response

CDW Managed Detection and Response leverages End Point Detect and Respond (EDR), Network Detect and Respond (NDR) and Automation technologies to help you stop and remediate threats. Our team focuses on security telemetry and utilizing industry-standard frameworks for tactics and techniques, such as MITRE ATT&CK. We can eliminate your security blind spots and enrich your alarm analysis for investigations, allowing our analysts to recommend the best course of action for remediation.

CDW Managed Detection and Response can help you achieve:

- Operational Efficiencies
- Faster Innovation
- Reduced Risk

Orchestrating the Right Solution

With CDW Managed Detection and Response, you will have 24/7 detection and response capabilities utilizing Managed Detection and Response (MDR) and NDR services. This service provides a skilled team to monitor alarms around the clock, looking for abnormal behavior and other indicators of attack.

MDR service helps to:

- Prevent attacker lateral movement within the network
- Monitor and alarm on registry editing and process/service creation
- Identify potentially malicious connections from the network
- Provide quick detection of malicious activities

Each of these enables your organization to respond to threats faster.

Offered as a stand-alone service or a complement to your Managed SIEM solution, CDW's MDR service offers expertise for your team in the areas of Automation Development, Incident Triage and Escalation, and Remediation Response. We focus on telemetry collection from EDR Agent or certain third-party EDR toolsets to gain visibility into events on the endpoint. To further enhance your visibility and reduce your potential risk, consider pairing with NDR Service to collect and alarm from both endpoint and network telemetry data. CDW can be your partner to address any security challenge.

CDW GETS SECURITY

CDW understands it takes a team to address security. Outside of our MDR service, we have Automation, Threat Hunting, and Content and Incident Response teams that can be leveraged. We help customers address remediation activities and strive for an end-to-end security solution.

Certifications

CDW and our partner have earned the following certifications:

- SOC II Certified
- Ranked Top 50 in MSSP Alert
- Awarded LogRhythm's 2019 Global Managed Service Partner of the Year
- Awarded LogRhythm's 2020 Growth Service Partner of the Year

CDW's full lifecycle of Services can support your organization no matter where you are on your journey

Design → Orchestrate → Manage

On-Premises → On-Journey → Cloud-Based

CDW AMPLIFIED™ SERVICES

Services Overview

CDW Managed Detection and Response includes the following core activities:

Core Activity	Included
Detection: Data collection through the deployment of the EDR agent is the first step to reliable detection of potential indicators of compromise (IOC). Once deployed, the agent begins to monitor and collect telemetry data, sending it back to the centralized database where that data is analyzed by policies, detection, intelligence and enriched data created by CDW and the partner research team. Through the detection process, CDW also implements tuning activities to optimize the detection rules to rule out noise and focus on the high confident alerts.	✓
Response: When anomalous behaviors are detected, CDW's security staff is notified and an initial review is performed. During the response phase, staff members need to perform triage by identifying if the alert itself is a false positive or contains elements of known or potential malicious activity. Successful triage is a critical step in reducing time to respond.	✓
Investigation: Once an alert has been deemed a potential or known risk, the CDW team initiates the investigation process. Utilizing investigation methodologies built by CDW, the investigation team works their way through the available data to determine what may be taking place, when it first occurred and the risk of the scope. Investigation results and further actions will be escalated to the customer through previously established communication channels.	✓
Remediation: In many cases, automated or staff-driven actions can start the remediation process. Depending on the nature of the events and activities identified, controls built into the EDR platform provide CDW the ability to stop processes, quarantine/isolate hosts or delete files. If these are not available, then CDW will coach the customer through remediation activities on their end.	✓
Automation (Optional): CDW offers integrations within our Palo Alto Networks XSOAR automation platform to address automated workflows. CDW's automation service allows customers access to playbooks specific to service desk, phishing or other automation use cases aimed at decreasing MTTR.	✓
Manual Threat Hunting (Optional): CDW threat hunting methodologies use a combination of data stacking and pattern searching. CDW Threat Hunters utilize SIEM logs, network connections, DNS requests, running processes and any other available metadata for analysis. Threat Hunters leverage their extensive experience of attacker TTPs (Tactics, Techniques and Procedures) and real-world attack analysis to look for previously undetected evidence of malicious behavior.	✓
Network Sensor (Optional): Increase the visibility and alerting capabilities of the MDR service through the deployment of CDW's optional network sensor. The sensor focuses on network telemetry, allowing alerting from network traffic to be combined with alarming from the endpoints. The network sensor allows full packet capture, heuristic- and signature-based IDS capabilities and network traffic analysis and anomaly detection to allow for even quicker threat detection within the enterprise.	✓

CUSTOMER SUCCESS STORY

CHALLENGE: An existing CDW MDR customer was hit by BlueCrab Ransomware.

SOLUTION: With the CDW MDR service in place, CDW was able to contain the initial infection before it was able to move laterally across the enterprise. CDW was able to search and monitor all of the customer's hosts for BlueCrab IOCs to verify the malware was not found anywhere else on the network.

RESULT: The customer experienced no downtime and CDW prevented the spread of the malware. CDW was able to determine the root cause of the infection and provide the customer with recommendations on how to improve their security posture.

To learn more about CDW Managed Detection and Response, contact your account manager or call 800.800.4239.

CDW AMPLIFIED™ SERVICES