Managed Detection and Response with Defender for Endpoint

Security

MAXIMIZE AND SECURE YOUR MICROSOFT INVESTMENT

The CDW Managed Detection & Response with Defender for Endpoint service enables advanced threat detection through automated correlation of events, resulting in faster incident qualification, response and containment of threats. We couple Defender for Endpoint's detection, prevention, investigation and response capabilities with 24x7 analyst lead monitoring, analysis and remediation.

SCOPE OF SERVICE

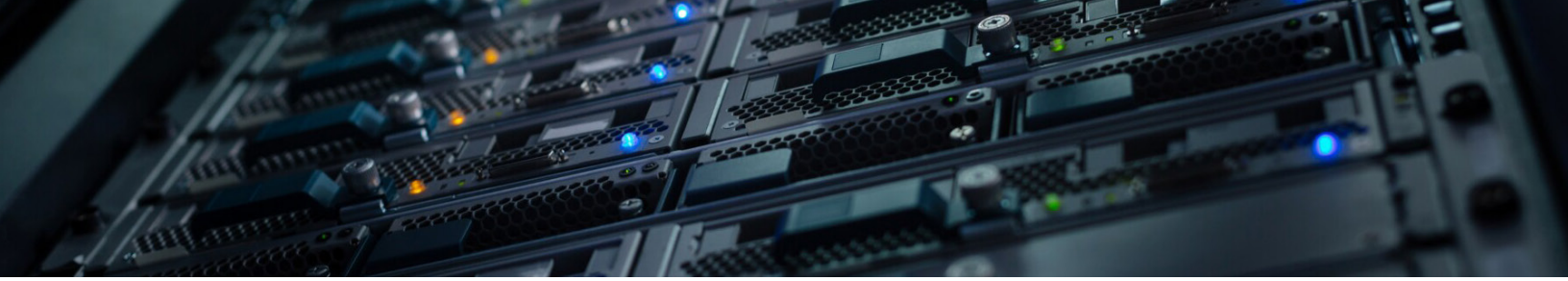
Microsoft Defender for Endpoint's robust detection, prevention and investigation capabilities allow CDW security analysts to rapidly investigate and respond to threats, reducing mean-time-to-respond (MTTR) and preventing cyberbreaches. Threat signals are stitched together as part of a chain of events, enabling our analysts to rapidly identify and investigate security incidents. When Microsoft Defender detects a threat, the ability of CDW's Managed Security Services team to quickly respond, investigate and remediate a threat sets our service apart. CDW SOC analysts can rapidly take several investigative and remediation actions to stop an attack and prevent lateral movement.

CDW MANAGED DETECTION & RESPONSE WITH DEFENDER FOR ENDPOINT SERVICE PROVIDES:

- Advanced threat detection
- Incident monitoring, triage, investigation, containment and remediation
- Microsoft Defender service and agent health monitoring
- Change and incident management
- Detailed incident investigation and response reporting

CDW CANADA'S NATIONAL OPERATIONS AND SECURITY OPERATION CENTRES

CDW operates a 24×7×365 national operations centre (NOC) to act as a single point of contact for customers experiencing issues with any CDW managed service. The CDW NOC will perform deployment, monitoring and management activities—which are part of the managed system. All monitoring notifications and service requests are directed to our security operations centre (SOC) for remediation and resolution. Our SOC will record, classify, prioritize and resolve incidents reported by our customers or alerts generated by any monitoring agent. The SOC will be available for customers to review and update their recorded incidents and produce reports of their SOC activities.



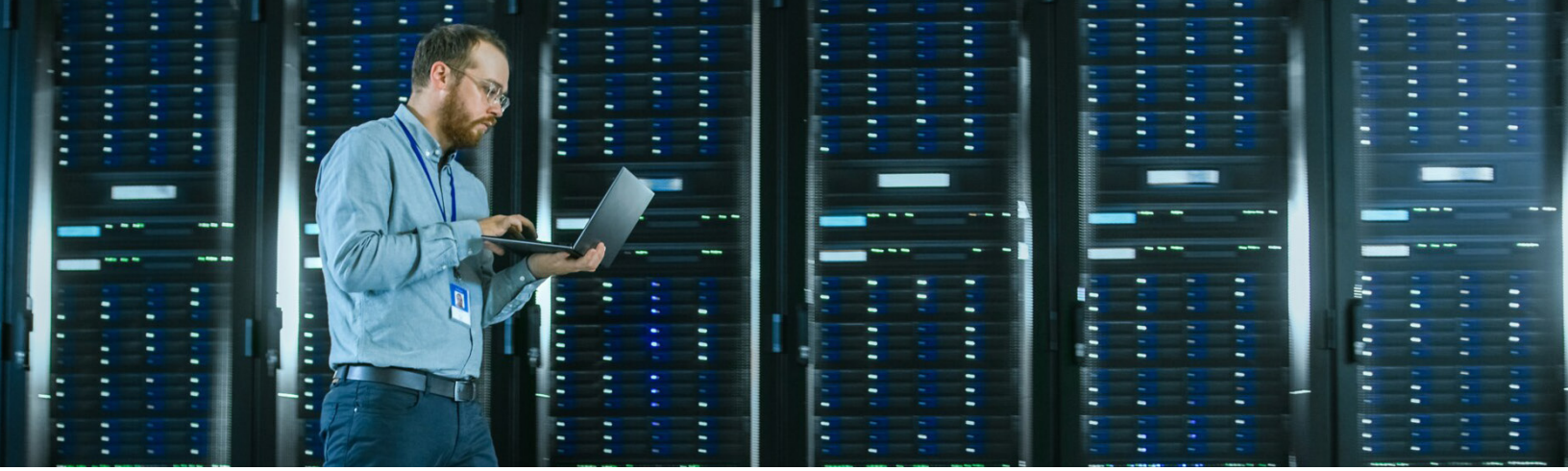
Features provided include:

- Web portal for self-service (intended for technical staff only, not end users)
- Primary contact number for reporting incidents or requesting service
- Recording and tracking of all service requests
- Proactive notification of service issues, including status updates
- NOC/SOC staff are comprised of level one, two and three specialists (as defined by CDW, solely at its discretion), who may perform their duties from any CDW office or remotely, as CDW deems necessary, to fulfill the terms and meet the requirements of any service-level objective (SLO)

SERVICE LICENSING REQUIREMENTS

The CDW Managed Detection & Response with Defender for Endpoint service is available to customers with most Defender licences. The licences required for the service are listed below.

DEFENDER LICENSING	
Enterprise	▪ M365 E5 ▪ M365 E5 Security ▪ Enterprise Mobility + Security E5 ▪ Defender for Endpoint P2 ▪ Defender for Server P1 & P2
Frontline	▪ M365 F5 ▪ M365 F5 Security ▪ M365 F5 Security + Compliance
Education	▪ M365 A5 ▪ M365 A5 Security
Business (feature limited)	▪ M365 Business Premium ▪ Defender for Business



CDW'S SECURITY APPROACH

Our risk-based approach to security is based on the NIST Cybersecurity Framework, which allows organizations to achieve their ideal security posture. We work with you to:

PREPARE

We help our clients create and align strategies and programs to address ever-evolving business risks. This includes creating a relevant and achievable security roadmap.

DEFEND

We work collaboratively with clients to decide which technologies to implement to protect against cyberthreats.

RESPOND

We monitor critical business assets, respond rapidly to incidents and validate the effectiveness of security controls 24x7x365, so you don't have to.

CERTIFICATIONS

Our service is designed to ITIL best practices. In addition to ITIL, COBIT and other certifications held by our team members, our practice is certified and compliant with:

AICPA SERVICE ORGANIZATIONS SOC aicpa.org/soc Formerly SAS 70 Reports

PCI DSS COMPLIANT

ISO 27001

NIST CSF (IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER)

For more information, contact your CDW account team at 800.972.3922 or visit CDW.ca/security

CDW

The terms and conditions of product sales are limited to those contained on CDW's website at CDW.ca. Notice of objection to and rejection of any additional or different terms in any form delivered by customer is hereby given. CDW®, CDW•G® and PEOPLE WHO GET IT® are registered trademarks of CDW LLC. All other trademarks and registered trademarks are the sole property of their respective owners.