MANAGED CORTEX XDR

Security

SERVICE OVERVIEW

Detecting and responding to threats has never been more difficult. Attacks are more complex, sophisticated and evasive, while poorly integrated solutions, underfunded and undertrained teams, and alert fatigue make it difficult for security analyst to identify the real threats from the noise. CDW's managed XDR solution, powered by Palo Alto Networks Cortex XDR, solves this problem by simplifying threat detection, correlation and response into one complete solution.

CDW's managed Cortex XDR solution delivers the best-in-class protection against known and unknown threats by combining endpoint protection (EPP), advanced detection, qualification and response through integrated endpoint protection and response (EDR), network traffic analysis (NTA) and user and entity behavioural analytics (UEBA) into one unified and powerful platform.

ENDPOINT PROTECTION:

CDW's managed Cortex XDR solution provides advance protection against cyberthreats through its multimethod approach to stopping malware. Unknown threats are sent to Palo Alto Network's Wildfire for analysis and identification. Ransomware is stopped by disabling unsanctioned encryption processes which prevent cybercriminals from holding your data hostage. Cortex XDR stops exploit-based attacks that focuses on vulnerabilities within software and OS; as well as file-less and script-based attacks.

DETECTION/INVESTIGATION:

Powered by Cortex XDR, the CDW SOC leverages the detection of threats through AI and machine learning models. Events are stitched together into a single incident, which allows our security analysts to quickly identify root cause and respond to threats. This reduces mean-time-to-respond (MTTR) for CDW, dwell time for threat actors and reduces the cost of a cyberbreach for customers. During investigation, events are stitched together as part of a chain of events, enabling our analysts to identify the root cause of the problem.

CDW PEOPLE WHO GET IT

RESPONSE:

When the CDW managed services team detects, investigates and qualifies a threat, the ability to respond to the threat quickly and effectively is what sets our service apart. Once the threat is qualified, the CDW SOC analyst can respond quickly by isolating the infected host, which stops lateral movement of adversaries, preventing significant impact to our customers by stopping attackers in their tracks.

FEATURES:

- CDW professional services to expertly install, configure and tune the Palo Alto Networks Cortex XDR Prevent and Pro solutions

- The CDW managed Cortex XDR service includes 24/7/365 managed services, delivered by our Canadian Security Operations Centre

- Optional threat hunting service delivered by Palo Alto Networks Unit 42 Global Threat Hunting Team (minimum 500 seats)

BENEFITS:

- Best-in-class endpoint protection for virus, ransomware, exploits and zero-day threats

- Expedited detection of threats by automatically stitched events across cloud, network and endpoints, and focusing on real threats

- Reduced dwell time of threats reducing the cost of a cyberbreach

- Granular visibility of the attack chain providing greater control and targeted response

- Continuous optimization, tuning and protection through certified and experienced experts

CDW SERVICE ELEMENTS	ESSENTIAL *Powered by XDR Prevent	ADVANCED *Powered by XDR Pro
24x7x365 Expert Security Support Round the clock support from CDW Canada Security Operations Centre	✔	✔
ITIL Service Management Break-fix, change management, patch and release management	✔	✔
Threat Detection and Alert Qualification Fast detection of threats and analysis	✔	✔
Live Threat Response Respond to threats and attacks as they emerge		✔

CDW PEOPLE WHO GET IT™

RELATED SERVICES:

- Professional services to deploy and tune Cortex XDR
- Managed NGFW (Palo Alto Networks)
- Authorized Training Partner – Palo Alto Networks

WHO ARE WE?

With more than 900 coworkers in offices across the country, CDW Canada helps customers achieve their goals by delivering integrated technology solutions and services that include security, cloud, data centre, networking, collaboration and digital transformation.

WHY CDW?

We lead Canadian businesses through innovation, expertise and service.

INNOVATION

Hiring great technical talent allows us to be a truly innovative company. Our approach is to define a strategy roadmap that enhances the customer experience and provides organizations with the flexibility and vision to adapt to changes in business needs as well as technology.

EXPERTISE

We hand pick the best technical architects from across Canada, train them continuously and provide them with unique client challenges daily. In addition, we are a trusted Palo Alto Networks partner with Diamond level partnership, and a Palo Alto Networks Authorized Training Centre. We have also been named Partner of the Year from 2017 to 2021.

SERVICE

Our commitment is first and foremost to our client and we strive to become a trusted advisor and an extension of your business. This does not happen overnight, but rather through proving ourselves again and again. As a proof, we always focus on 99.99% availability and have been recognized for being one of the best service providers in Canada.

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

CDW **PEOPLE WHO GET IT**