paloalto® NETWORKS

CORTEX™ BY PALO ALTO NETWORKS

Cortex XDR Managed Threat Hunting

The industry's first threat hunting service operating across integrated endpoint, network, and cloud data

Managed Threat Hunting offers round-the-clock monitoring from Unit 42 experts to discover attacks anywhere in your organization. Our threat hunters work on your behalf to discover advanced threats, such as state-sponsored attackers, cybercriminals, malicious insiders, and malware.

Our service leverages the comprehensive data and threat detection capabilities of Cortex XDR to provide industry-leading coverage of MITRE ATT&CK® techniques. With Cortex XDR and Unit 42 on your side, you can rest easy knowing that your organization is safe.

Key Benefits

With Cortex XDR Managed Threat Hunting, you can:

- Get peace of mind with 24/7 threat hunting powered by the Cortex XDR platform
- Augment your team with world-renowned Unit 42 experts armed with industry-best threat intelligence
- Instantly learn about high-risk incidents with detailed threat reports

Proactive Security with Cortex XDR Managed Threat Hunting

By proactively hunting down threats, you can unmask every adversary, reduce dwell times, and avoid successful attacks. The Cortex XDR™ Managed Threat Hunting service helps you uncover attackers wherever they hide by combining world-class threat hunters with Cortex XDR technology that runs on integrated endpoint, network, and cloud data sources. With Managed Threat Hunting, you can relax; we've got you covered.

Unrivaled Visibility Built on Comprehensive Data Sources

To detect attackers hiding in your organization, our hunters comb through integrated endpoint, network, and cloud data sources, including third-party security solutions. Our hunters can pinpoint attacks originating from any device, including unmanaged devices and remote users.

World-Renowned Unit 42 Threat Hunters Working for You

Augment your team with security experts ceaselessly searching your environment for attacker tactics and techniques. Our analysts have years of experience hunting and identifying unknown threats as well as reverse-engineering malware.

Unit 42 analysts:

- Analyze suspicious signals generated by Cortex XDR analytics, custom detection rules, and Cortex XDR research.
- Manually seek out emerging adversaries using the powerful data exploration capabilities of Cortex XDR.
- Investigate threats and determine the total scope of incidents.
- Produce detailed Threat Reports that reveal the tools and steps of attacks so you can root out adversaries quickly.
- Offer direct assistance to answer questions and provide guidance about Threat Reports and Impact Reports.

High-Fidelity Threat Intelligence

Our analysts benefit from an industry-leading repository of threat intelligence, sourced from the largest network of sensors, to find emerging attacks quickly. Leveraging AutoFocus™ contextual threat intelligence, our Unit 42 analysts can pinpoint indicators of compromise in your organization and instantly understand both the source and objective of every incident with unrivaled context.

> "With Managed Threat Hunting, we know a team of security experts have our back, helping me sleep easy at night by providing continuous monitoring to identify cybersecurity risks to stay ahead of attackers."
>
> —Johan Lelong, CISO, Petit Forestier

Unrivaled Hunting Built on Cortex XDR Analytics

Managed threat hunters have full access to all the analytics and detection rules in the Cortex XDR platform. They use these as high-quality leads to start hunting. They also have access to emerging detectors the Cortex XDR research team is working on, and they can use these detectors before they are rolled into the Cortex XDR platform.

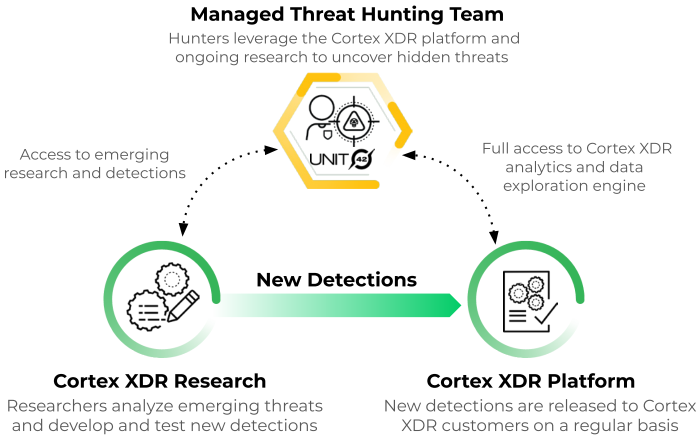
Managed Threat Hunting Team
Hunters leverage the Cortex XDR platform and ongoing research to uncover hidden threats
UNIT 42
Access to emerging research and detections
Full access to Cortex XDR analytics and data exploration engine
New Detections
Cortex XDR Research
Researchers analyze emerging threats and develop and test new detections
Cortex XDR Platform
New detections are released to Cortex XDR customers on a regular basis

Figure 1: Methods Unit 42 analysts use to find new threats

Table 1: Features of Cortex XDR Managed Threat Hunting
24/7, year-round monitoring and detection across integrated endpoint, network, and cloud data
Threat hunting by Unit 42 experts
Integrated threat intelligence from AutoFocus
Early access to new behavioral analytics and threat detection rules
Threat Reports describing critical security incidents
Impact Reports revealing emerging threats and customer exposure
Integration with the Cortex XDR management console for incident management
Direct assistance from analysts for context on Threat Reports

Clear, Prescriptive Results That Let You Act with Confidence

Managed Threat Hunting gives you the information you need to remediate threats and improve your security posture. As a Managed Threat Hunting customer, you receive:

- **Threat Reports** that provide detailed information about cyberthreats identified in your organization. You get a complete account of each security incident, including the scope of the attack, the probable source, the attack tools, and recommended guidance.[1]
- **Impact Reports** that let you stay ahead of emerging threats affecting multiple organizations. You can answer critical questions about exposure to high-profile attack campaigns from your executives or board before they even ask. With Impact Reports, you can rest assured that your organization is safe.
- **Threat hunting alerts integrated into Cortex XDR**, allowing analysts to review and triage reports using their standard investigation workflows. Threat hunting alerts are automatically grouped with related alerts into incidents, providing a complete picture of an attack.

Prerequisites for Cortex XDR Managed Threat Hunting

Managed Threat Hunting with Cortex XDR Pro for Endpoint requires a minimum of 500 endpoints.

[1] Customers will receive threat reports if attacks are observed in their environments.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com