Building a Virtual SOC with Cortex

How XDR, XSOAR, and Xpanse Deliver World-Class Outcomes Without Deploying a Traditional SOC

Don't have a security operations center (SOC) yet still want similar outcomes? From continuous protection with uninterrupted monitoring to threat detection and prevention, having the ability to holistically organize and manage security operations is paramount for a healthy security posture.

In addition to increasing attack frequency and sophistication, attacks are becoming more costly, many driven by the surge in ransomware bolstered by rising cryptocurrency prices. Unfortunately, an attack can go undetected for a long time, leading to increased dwell times and further delaying investigation, mitigation, or remediation. While reasons for operational inefficiencies differ among organizations, many of them include:

- Limited visibility into their devices, applications, networks, and systems.
- Not knowing which assets to protect.
- Not understanding which tools to use and integrating them with the existing infrastructure.

Cortex Is a Holistic Ecosystem for Proactive Security Operations

A solution to address the above challenges is a suite of products that enables tighter control of security operations: a holistic ecosystem with a view of the security posture for targeted threat detection, behavioral monitoring, intelligence, asset discovery, and risk assessment—a virtual SOC that can be managed without dependencies on a physical location or assets.

You can now achieve this reality—SOC virtualization—with the Cortex suite of products: Cortex XDR, Cortex Xpanse, and Cortex XSOAR, which seamlessly work together as a force multiplier across your security operations regardless of team size or scope.

Our Approach

While each product brings unique features and benefits, the positive results exponentially increase when combined. These three products help lower the risk and impact from breaches with a comprehensive product suite for teams of any size, with best-in-class detection, investigation, automation, and response capabilities, bar none.

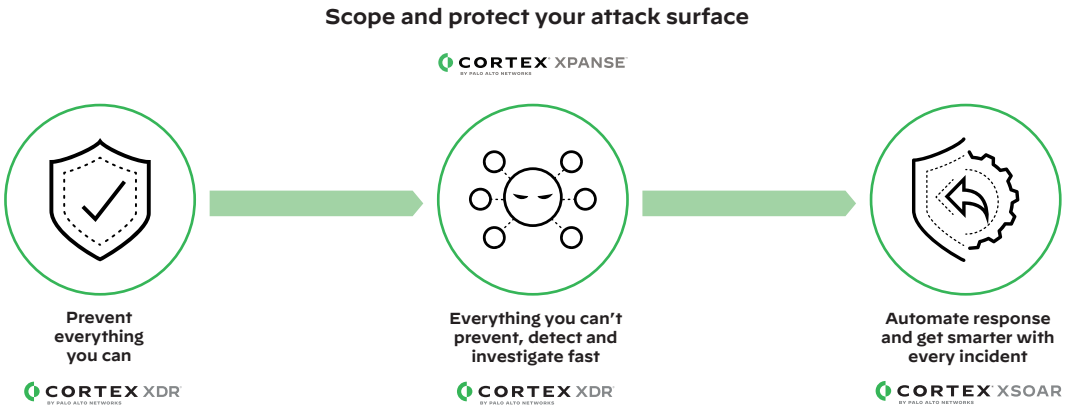

Figure 1: High-fidelity detections and alerts help drive orchestrated workflows

With end-to-end native integration and interoperability, security teams can close the loop on threats with continual synergies across the Cortex ecosystem. All three products work in concert to monitor the threat landscape and provide the most robust prevention, detection, response, and investigation capabilities:

- Cortex XDR provides endpoint security and EDR to block sophisticated attacks using AI-driven analysis and a range of protection modules.
- Cortex XDR and Cortex Xpanse provide the ultimate visibility and detections across the internet attack surface, endpoints, cloud, and network.
- Cortex XDR and Cortex Xpanse leverage Cortex XSOAR for full orchestration, automation, and response capabilities.
- Cortex XSOAR leverages Cortex XDR and Cortex Xpanse to provide high-fidelity detections and alerts to drive orchestrated workflows.

Cortex XDR for Endpoint Protection *and* Extended Detection and Response

Cortex XDR can stop attacks at the endpoint and host with world-class EDR for Windows and Linux hosts with:

- AI-driven local analysis and ML-based behavioral analysis that is updated regularly.
- A suite of endpoint protection features such as device control, host firewall, and disk encryption.
- A range of protection modules to protect against pre-execution and post-execution exploits.

Once you prevent everything you can at the endpoint, Cortex provides detection and response that focuses on incidents by automating evidence gathering, groups of associated alerts, putting those alerts into a timeline, and revealing the root cause to speed triage and investigations for analysts of all skill levels.

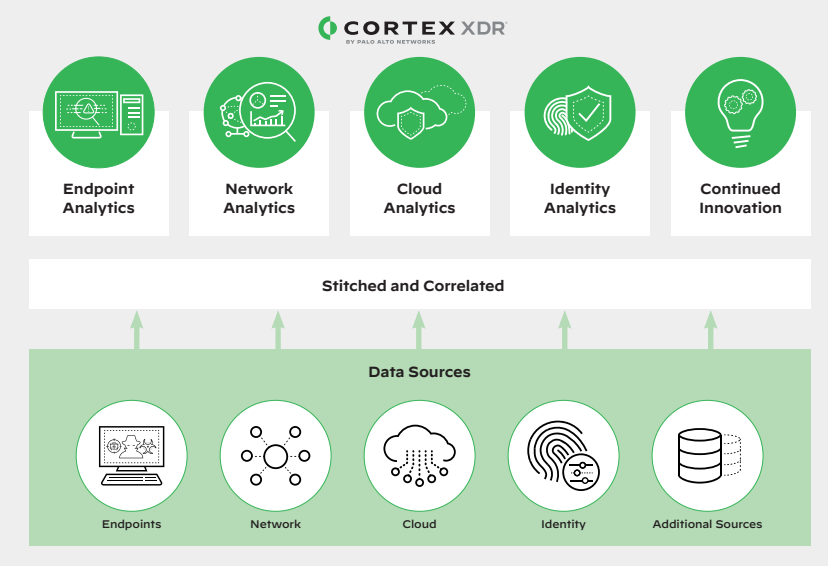

Figure 2: Faster detection and response with AI/ML analytics with Cortex XDR

The Next Logical Evolution of EDR

The product vision for extended detection and response (XDR) was created by Nir Zuk, CTO and co-founder of Palo Alto Networks, in 2018. The reason for creating XDR was to stop attacks more efficiently at the endpoint, detect attacker techniques and tactics that cannot be prevented, and help SOC teams better respond to threats that require investigation. The vision is to automate many of the SOC analyst tasks, like writing detection logic, gathering evidence, building an incident from alerts, enriching the incident with identity and threat information, and pulling disparate telemetry together from multiple (and in some cases, complementary) sources, including EDR, network traffic analysis (NTA), user and entity behavior analytics (UEBA), and indicators of compromise (IoCs).

XDR lets security teams stop attacks more efficiently and effectively, eliminating blind spots, reducing investigation times, and ultimately improving security outcomes using XDR. And with XDR's ability to stop attack sequences at critical stages such as execution—before persistence techniques result in broader lateral damage—security teams finally have a solution to "head attacks off at the pass."

In round 3 of MITRE testing, Cortex XDR's results against TTPs used by Carbanak and FIN7 blocked 100% of attacks in the protection evaluation on both Windows and Linux endpoints and achieved 97% visibility of attack techniques which represents the best detection rates of any solution that also got a perfect protection score.[1] Of the attack techniques used, Cortex XDR identified 86% with an analytics detection, defined by MITRE as detections that provide additional context beyond telemetry.[2] Notice

1. Peter Havens, "Cortex XDR: Best Combined Prevention and Detection in MITRE Round 3," Palo Alto Networks, April 21, 2021, https://www.paloaltonetworks.com/blog/2021/04/mitre-round-3-protecting-against-carbanak/.
2. Ibid.

those legacy endpoint vendors that only provide EDR/ESS/NG-AV solutions scored poorly in protection efficacy, visibility, and techniques detection.

As an evolution of existing threat detection and response solutions, XDR includes features such as:

- Integrated threat intelligence
- Network analysis
- Machine learning-based detection
- Investigation response orchestration
- Dynamic deployment
- Integrated sandbox capabilities with WildFire

Factors driving the adoption of XDR include simplified visualization of complex attacks across the kill chain, presenting information within the MITE ATT&CK framework, more robust automation, advanced analytics, and machine learning.

XDR's value is gaining momentum due to the need in the market for tighter third-party integrations, better analytics, and faster response capabilities—especially when one considers that organizations may use up to 45 security tools on average while responding to an incident that requires coordination across approximately 19 tools.

XDR Fills the Detection and Response Void

Before XDR, correlating telemetry from endpoints with other event data was an exercise in sifting through large volumes of data and false positives cluttering analysts' dashboards. Stitching disparate events together is resource-intensive and dependent on seasoned analysts to determine if alert escalations are warranted. As a result, SOC teams could find themselves wasting time verifying the accuracy of low-fidelity alerts while compromising the time needed to investigate legitimate alerts.

XDR combines the SIEM-like features of alert integration, normalization, and correlation with SOAR-like automated investigation and remediation.

Impeded by this nonstop version of security "whack-a-mole" and an increase in attack sophistication and frequency, forward-thinking security organizations are beginning to take advantage of all the efficiencies gained from an XDR approach to security architecture.

According to Forrester analyst Allie Mellen, who covers SecOps, "XDR and SIEM are not converging but colliding."[3] In a recent blog post, Mellen explains further:

> *"XDR will compete head-to-head with security analytics platforms (and SIEMs) for threat detection, investigation, response, and hunting. Security analytics platforms have over a decade of experience in data aggregation; they apply to these challenges but have yet to provide incident response capabilities that are sufficient at enterprise scale, forcing enterprises to prioritize alternate solutions. XDR is rising to fill that void through a distinctly different approach anchored in endpoint and optimization.*
>
> *The core difference between XDR and the SIEM is that XDR detections remain anchored in endpoint detections, as opposed to taking the nebulous approach of applying security analytics to a large set of data. As XDR evolves, expect the vendor definition of endpoint to evolve as well based on where the attacker target is, regardless of if it takes the form of a laptop, workstation, mobile device, or the cloud."*[4]

Takeaway: XDR can address SIEM use cases by providing threat detection, investigation, response, and hunting rooted in endpoint threat detection and response with the ability to scale to cloud environments.

Xpanse for Complete, Accurate and Continuously Updated Inventory of All Global Internet-Facing Assets

Cortex Xpanse provides a complete and accurate inventory of an organization's global, internet-facing cloud assets and misconfigurations to continuously discover, evaluate, and mitigate an external attack surface and evaluate supplier risk or assess the security of M&A targets.

3. Allie Mellen, "XDR Defined: Giving Meaning To Extended Detection And Response," Forrester, April 28, 2021, https://go.forrester.com/blogs/xdr-defined-giving-meaning-to-extended-detection-and-response/.
4. Ibid.

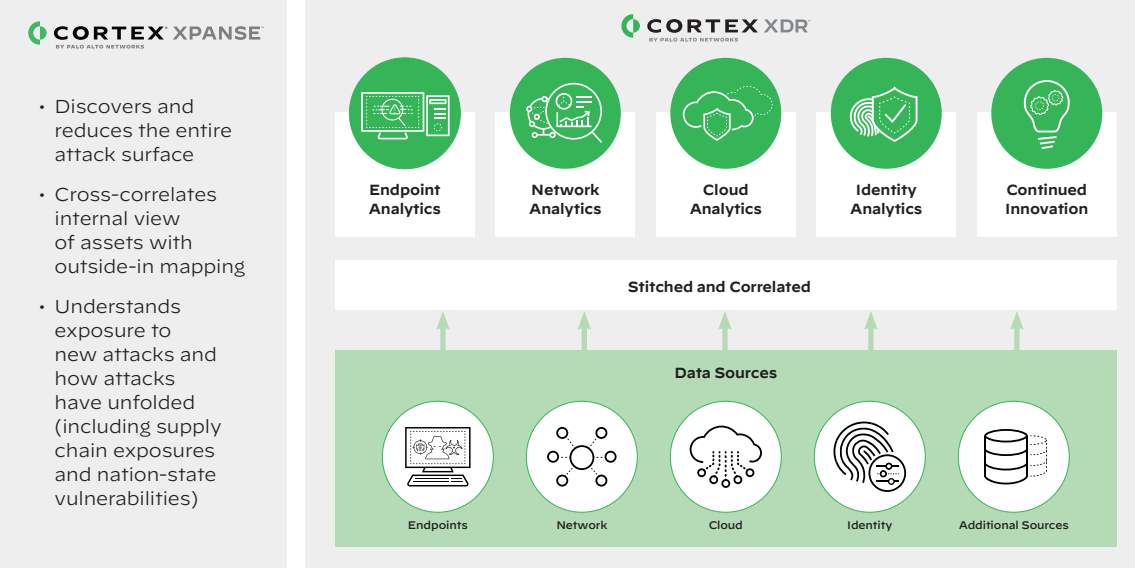

Figure 3: Ultimate visibility and detection across the internet attack surface, endpoints, cloud, and network

In our report, 2021 Cortex Xpanse Attack Surface Threat Report: Lessons in Attack Surface Management from Leading Global Enterprises, Palo Alto Networks outlined some key findings from their research of the public-facing internet attack surfaces of some of the world's largest businesses. From January to March, their team monitored scans of 50 million IP addresses associated with 50 global enterprises to understand how quickly adversaries can identify exposed systems for fast exploitation.

One interesting discovery was that nearly one in three exposed assets they uncovered was due to unnecessary use of Remote Desktop Protocol (RDP), which has surged in use since early 2020 as enterprises expedited moves to the cloud to support remote workers affected by new WFH protocols due to the COVID-19 pandemic. Other findings in the report include:

- **Adversaries scan more frequently than companies.** In a game of never-ending "cat and mouse," threat actors were found to conduct a new scan once every hour, whereas global enterprises can take weeks.
- **Adversaries scan within 15 minutes of new vulnerabilities.** Attackers began scanning within 15 minutes following announcements of new Common Vulnerabilities and Exposures (CVE) released between January and March and launched scans within five minutes of the Microsoft Exchange Server zero-day security update.
- **Exposed systems every 12 hours.** Cortex Xpanse discovered that, on average, global enterprises present a new serious exposure every 12 hours or twice daily. Issues included insecure remote access (RDP, Telnet, SNMP, VNC, etc.), database servers, and exposures to zero-day vulnerabilities in products such as Microsoft Exchange Server and F5 load balancers.
- **Cloud comprised almost 80% of the global enterprise security concerns.** Cloud footprints were responsible for 79% of the most critical security issues found in global enterprises, reiterating the inherent risk of cloud-hosted/based services, compared to 21% for on-premises.

Understanding the Attack Surface

One foundational component of a SOC transformation is to have a strong continuous risk management function. Identifying the "things" you are trying to protect and identifying what is exposed that allows it to be attacked is a logical segue into a risk management process that establishes the context for a risk management plan or strategy, whether basic or more robust. By starting with identification, the ability to prioritize what's at risk makes it easier to analyze what it would take to actually mitigate each risk.

A critical step to informing any risk management function is to have a clear understanding of one's attack surface—you can't protect what you can't see.

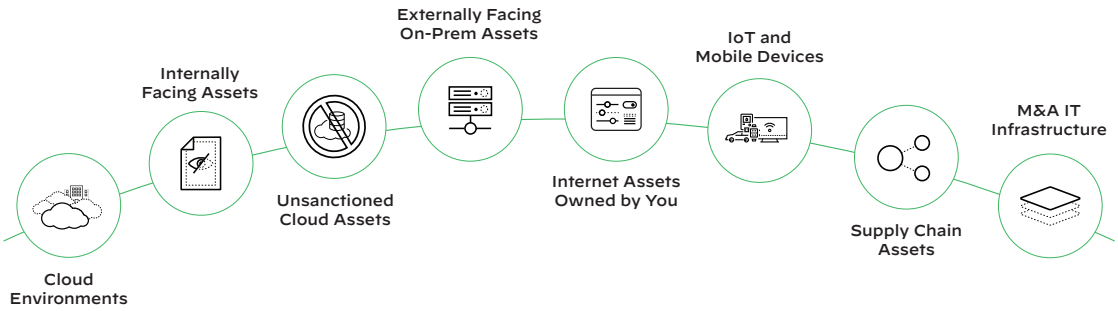

Figure 4: Components of your attack surface

Defined by SANS Institute:

> *Attack surface management (ASM) "is an emerging category of solutions that aims to help organizations address this challenge by providing an external perspective of an organization's attack surface. An organization's attack surface is made up of all internet-accessible hardware, software, SaaS and cloud assets that are discoverable by an attacker. In short, your attack surface is any external asset that an adversary could discover, attack, and use to* gain a foothold into your environment."[5]

SANS lists some common use cases for the adoption of an ASM solution, including:

- Identification of external gaps in visibility
- Discovery of unknown assets and shadow IT
- Attack surface risk management
- Risk-based vulnerability prioritization
- Assessment of M&A and subsidiary risk

Yet, whether one chooses to deploy ASM solutions or perform proactive assessments like penetration testing or vulnerability scanning, what is clear is the need to identify both product and operational requirements to determine the best fit. Product and operational requirements can include functionality, feature(s), capability, and evaluation criteria to help summarize the features and capabilities you might expect in an ASM solution or tool.

Takeaway: Advancements in scanning technologies allow attackers to locate attack vectors quickly and easily, revealing abandoned, rogue, or misconfigured assets that can become backdoors for compromise. Deploying an attack surface management solution is the best way to continuously assess an organization's external attack surface in a cost-effective, repeatable, and scalable manner.

Cortex XSOAR for Security Orchestration, Automation, and Response

Cortex XSOAR provides end-to-end incident and security operational process lifecycle management, helping companies accelerate security operations, reduce the time it takes to investigate and respond to security alerts and incidents, and handle more incidents. Security teams of all sizes can orchestrate, automate, speed incident response and any security workflow or security process across their environment by leveraging the extensive vendor integration and 725+ pre-built integration content packs to maximize enterprise integration coverage.

Companies realize that integrated threat intelligence management, the ability to automatically map threat information to incidents and operationalize threat intelligence with automation—security teams gain access to a central threat library from several threat intelligence sources—from tactical (machine-readable based) to strategic sources (report-based).

5. Pierre Lidome, "The SANS Guide to Evaluating Attack Surface Management," SANS Institute, October 26, 2020, https://www.sans.org/reading-room/whitepapers/analyst/guide-evaluating-attack-surface-management-39905.

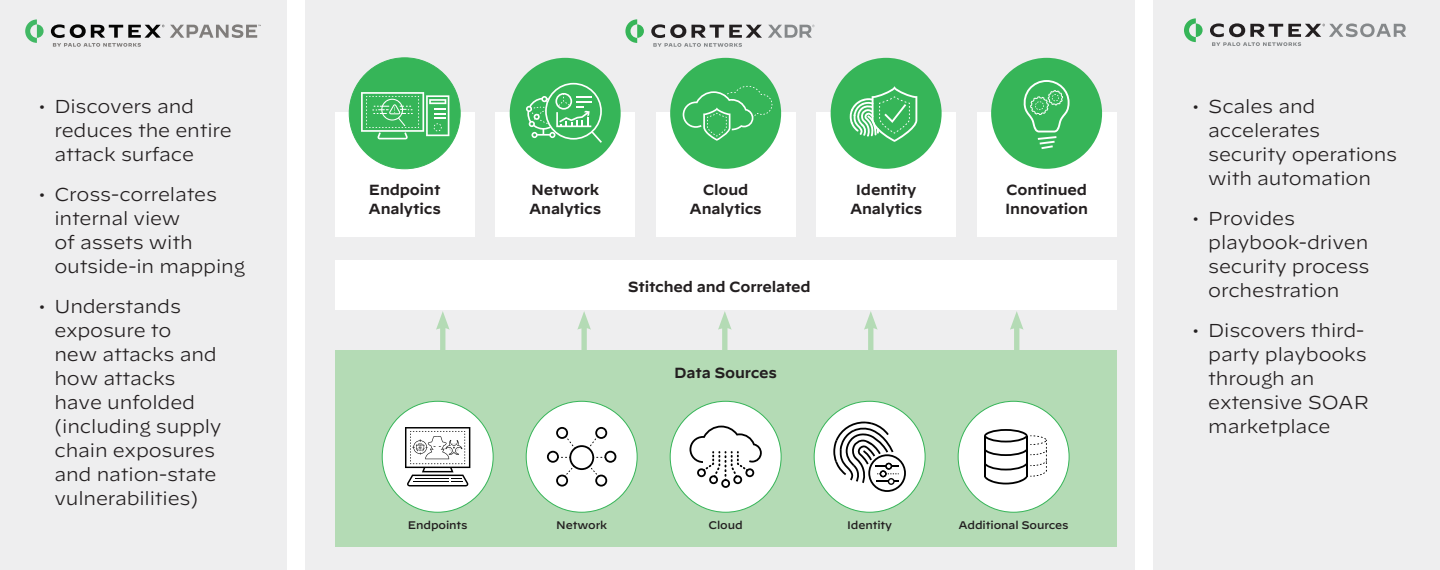

Figure 5: End-to-end workflow automation for security operations

Orchestrating Across Your Product Stack for Efficient Incident Response

Gartner defines security orchestration, automation, and response (SOAR) as "solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format."[6] Workflows can be orchestrated via integrations with other technologies and automated to achieve desired outcomes, such as:

- Incident alert triage
- Threat qualification
- Incident response
- Threat intel curation and management
- Compliance monitoring and management

How a Security Company Automates Security

Cortex XSOAR is leveraged within the Palo Alto Network SOC to minimize the repetitive and time-consuming tasks discussed in the above sections. Below is a snapshot of top automation "timesavers" for the month of February 2021.

Automation Type	Times Ran	Hours Saved
Artifact Enrichment	1195	697.08
Dedupe	12744	1062
Email User	822	342.5
Password Reset	4	1.67
GCP Remediation	34	17
Other Jobs*	*	74.73

Repetitive, tedious SOC work that nobody wants to do

*PhishMe metrics, RSS feed job, content update job, hunting assignments and metrics, daily monitoring ticket creation, and JIRA ticket pull

Total hours saved in February 2021

XSOAR automates the workload of 13.72 FTEs

Figure 6: Cybersecurity automation in Palo Alto Networks SOC

6. Claudio Neiva, Craig Lawson, Toby Bussa, and Gorka Sadowski, "Market Guide for Security Orchestration, Automation and Response Solutions," Gartner, September 21, 2020, https://www.gartner.com/en/documents/3990720-market-guide-for-security-orchestration-automation-and-r.

When it comes to SOAR, solutions running a playbook outlining response workflows may come to mind, yet an effective SOAR strategy goes beyond just leveraging automation to streamline and eliminate manual tasks. A comprehensive SOAR platform that addresses all aspects of incident management needs to provide comprehensive out-of-the-box integrations of commonly used tools in the SOC, best-practice playbooks to aid in automating workflows, integrated case management and real-time collaboration to enable cross-team incident investigation.

Last but not least, the ability to serve as a central repository for threat intelligence (both internal and external) enables automated correlation between indicators, incidents, and intel, so security analysts and incident responders get enriched strategic intelligence for added insight into threat actors and attack techniques.

SOAR solutions continue to build toward becoming the control plane for the modern SOC environment, potentially becoming the control plane for various security operations functions. To achieve this end, SOAR solutions are integrating threat intelligence and expanding automation to use cases beyond the SOC. Leading security vendors are also embedding SOAR and incident management capabilities into their products which are preprogrammed and optimized for the specific technology.[7]

Takeaway: At the heart of any SOAR solution is the ability to set priorities and build streamlined workflows for security events that require minimal human involvement. Improved efficiencies are the result of a SOAR platform that can automate processes and provide a single platform for minimizing complex incident investigations.

Added Support with Our Extended Expertise Professional Services

Our Extended Expertise Program provides you with experts focused on your organization and is uniquely qualified to advise you on getting the most out of your Palo Alto Networks deployment. In as little as 90 days, utilizing our Professional Services options such as the "Quickstart Service for Cortex XDR" can provide planning, remote configuration, and project management to jumpstart operations.

Figure 7: Build a virtual SOC team with Cortex Professional Services

7. Ibid.

Launch a Virtual SOC Today

Driven by innovation to protect and defend our customers' most valuable resources, Palo Alto Networks is committed to bringing the newest and most advanced security solutions to market. We invite you to look at our solutions, reach out, and talk to us. We're here to help you learn more, do more, and secure more.

Visit our web pages for more information about:

- Cortex XDR
- Cortex Xpanse
- Cortex XSOAR
- Professional Services

Interested in scheduling a demo? Get started today.

Unit 42 MDR

The Unit 42 Managed Detection and Response (MDR) service puts Unit 42 experts to work for you to detect and respond to cyberattacks, 24/7, and allows your team to scale fast and focus on what matters most. We use Cortex XDR so our analysts have unmatched visibility across all data sources to quickly identify and stop malicious activity most likely to impact your organization.

When choosing Cortex XDR, why not also choose the only MDR service modeled after the SOC protecting the cybersecurity leader, Palo Alto Networks.

Unit 42 MDR is:

- Built on Cortex XDR technology
- Backed by Unit 42 expertise
- Enriched with world class Unit 42 threat intelligence

paloalto NETWORKS

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