CORTEX™
BY PALO ALTO NETWORKS

Cortex XDR for Network Traffic Analysis

Hunt down and stop attackers in your network with AI-powered analytics

Why Add Cortex XDR to Your Next-Generation Firewalls?

- Detect targeted attacks, insider threats, and malware with AI-powered analytics.
- Monitor managed and unmanaged devices as well as block threats with your Next-Generation Firewall.
- Collect logs without deploying new network appliances, and store data effortlessly in the cloud.

The Easiest Decision You'll Make

With Cortex XDR, you can protect your organization from attacks while getting more value from your existing Palo Alto Networks Next-Generation Firewalls as a subscription.

Blind Spots Increase Your Risk of a Successful Attack

To catch adversaries dwelling in your network, you need the right data combined with behavioral analytics and machine learning. You should monitor internet traffic as well as internal, east-west communications between your users and servers to detect post-intrusion activity, such as lateral movement and exfiltration.

Unfortunately, most security teams today lack visibility across all their systems, especially their unmanaged endpoints. Analysts waste time triaging incomplete, inaccurate alerts and manually gathering investigative clues instead of stopping attacks. Teams need a new approach to security operations, or they will struggle to protect their digital assets.

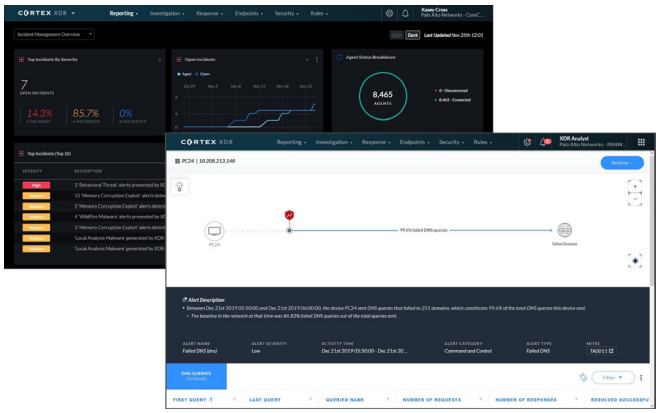

Figure 1: Machine learning and analytics to automatically find active threats

Quickly Detect, Investigate, and Shut Down Threats

Cortex XDR™ empowers you to find and stop the stealthiest network threats—fast. By analyzing rich network, endpoint, and cloud data with machine learning, Cortex XDR pinpoints targeted attacks, malicious insiders, and compromised endpoints with laser accuracy. By reviewing actionable alerts and taking advantage of flexible response options, your analysts can rapidly confirm threats with investigative context and block them before damage is done.

By thwarting every step of an attack, you can limit any opportunity for an attack to succeed. Cortex XDR detects command and control, lateral movement, data exfiltration, and malware activity by profiling behavior and detecting anomalies.

Detect Advanced Threats with Behavioral Analytics and Machine Learning

Cortex XDR reveals post-intrusion activity, cutting your mean time to detect (MTTD) and ensuring your network is free of active attackers. Using machine learning, Cortex XDR continuously profiles user and endpoint behavior to detect anomalous activity indicative of attacks. By applying analytics to an integrated set of data, including security alerts and rich network, endpoint, and cloud logs, Cortex XDR exceeds the detection capabilities of siloed tools. Automated detection works all day, every day, providing you peace of mind.

Accelerate Investigations with User, Device, and Endpoint Details

To simplify triage and analysis, Cortex XDR produces a small number of accurate, actionable alerts. Alerts include information about the user, application, and device as well as endpoint process data collected by the Cortex XDR agent or the agentless Pathfinder endpoint analysis service. Cortex XDR integrates with WildFire® malware prevention service to determine if suspicious processes are malware. By grouping related alerts into incidents and presenting all the information analysts need to confirm an attack, Cortex XDR makes investigations a snap.

Coordinate Response Across Endpoint, Network, and Cloud Enforcement Points

Your security team can instantly contain threats using multiple flexible response options. Using the Cortex XDR agent and Pathfinder, or by blocking malicious traffic with your firewalls, you can quickly stop the spread of malware, terminate processes, delete malicious files, and more. With the Live Terminal feature, your analysts can connect directly to endpoints, access graphical file and task managers, and run Python®, PowerShell®, or system commands and scripts. Integration with Cortex™ XSOAR allows you to orchestrate responses across hundreds of tools.

> "Once we got Cortex XDR in, we had the relief of knowing we were seeing real, viable data—information we could react to, information we could act on, and what the endpoints were doing. There was this tremendous relief that, now, we could be ahead of the situation."
>
> **— Greg Biegen, Director of Information Security, Cherwell Software**

Get Started in Minutes with Cloud Delivery

The cloud native Cortex XDR platform offers streamlined deployment, eliminating the need to deploy log servers or new on-premises sensors throughout your network. You can use your Palo Alto Networks Next-Generation Firewalls or third-party firewalls to collect data and easily store it in Cortex Data Lake, a scalable and efficient cloud-based data repository, reducing the number of products to manage. By automating tasks and simplifying management, Cortex XDR delivers a 44% cost savings compared to siloed security tools.

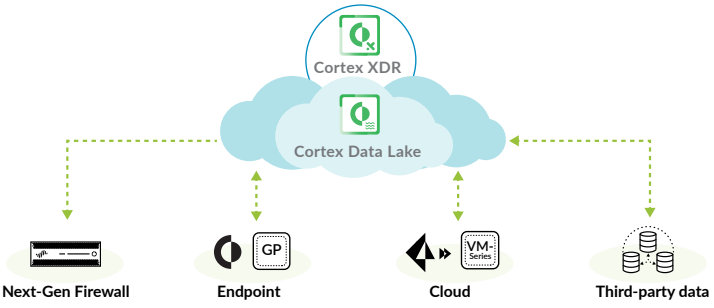

Figure 2: Cortex XDR with one or more data sources for detection and response, eliminating blind spots

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