

STARRING **CORTEX XDR, CORTEX DATA LAKE**
CO-STARRING **TRAPS, PANORAMA, GLOBALPROTECT, NEXT-GENERATION FIREWALLS**
DIRECTED BY **PALO ALTO NETWORKS** DISTRIBUTED BY **EXCLUSIVE NETWORKS**

AVAILABLE NOW ON PALO ALTO PRIMETIME:



CORTEX™



PLOT OUTLINE

Cortex is the industry's only open and integrated, AI-based continuous security platform – designed to simplify security operations and considerably improve outcomes. Deployed on a global, scalable public cloud platform, Cortex allows security ops teams to speed the analysis of massive data sets.



EXPERIENCE CORTEX IF:

- Your security teams are overloaded with threat data – slowing down how long it takes to detect attacks
- You are faced with a growing cybersecurity skills shortage
- You want to simplify security operations in order to cut dwell times and prevent successful cyber attacks
- You are worried that too much time is wasted deploying and managing security infrastructure instead of fighting attacks

PREVIEWS

Episode 1: Cortex XDR™ – Breaking Data Silos

Cortex XDR is the first-of-its-kind detection, investigation and response product that natively integrates network, endpoint and cloud data. Cortex XDR uncovers threats using behavioral analytics, accelerates investigations with automation, and stops attacks before damage is done through tight integration with existing enforcement points.

Episode 2: Cortex Data Lake – Storming and Norming All Enterprise Data

Cortex Data Lake is where customers can securely and privately store and analyse large amounts of data that is normalised for advanced AI and machine learning to find threats and orchestrate responses quickly.

SPOILER ALERT: HIGHLIGHTS

Reduce the risk of successful attacks:

- Automatically detect attacks by analysing rich network, endpoint and cloud data
- Uncover post-intrusion threats
- Accelerate investigations by automatically identifying the root cause and full context
- Quickly respond by tightly integrating with enforcement points

Simplify operations to maximise productivity and lower operating expenses:

- Easily store log data at cloud scale using Cortex Data Lake rather than on-premise
- Avoid the need to manually integrate/normalise data from multiple sources
- Use existing security infrastructure as sensors and enforcement points
- Consolidate detection and response across network, endpoint and cloud data to streamline operations
- Rapidly adopt deeply integrated apps of trusted innovators

Achieve visibility across network, endpoint and cloud data

Collect and correlate data at scale

Automatically detect sophisticated attacks 24/7

Use always-on machine learning and custom rules to detect APTs and other sophisticated attacks

Eliminate the alert backlog

Simplify investigations with automated root cause analysis and timeline views, lowering the cyber skills requirement

Drastically reduce false positive alerts

Apply knowledge from every investigation to refine behavioral detection rules and speed future analysis

Increase SOC productivity

Streamline to a single console by consolidating alert triage, investigation and response across environments

Remediate without business impact

Shut down attacks with surgical precision while avoiding user or system downtime

Eliminate advanced threats

Malicious insiders, policy violations, ransomware, fileless/memory-only attacks, zero-day malware, etc.

EXCLUSIVE BEHIND THE SCENES BENEFITS

JOIN PALO ALTO PRIMETIME WITH EXCLUSIVE NETWORKS AND ACHIEVE:



Increased skills on security solutions



Increased turnover and margin on solutions and related services



Premium content and bespoke marketing to differentiate yourself and go to market easily



Customised support throughout all deals and opportunities



New business opportunities