

# Cortex: Pioneering AI-Driven SecOps from SOC to Cloud

Palo Alto Networks Cortex® revolutionizes security operations with a unified, AI-driven platform that delivers best-in-class SOC and cloud capabilities, enabling security teams to address threats more efficiently and quickly.



✓  
**Prevent and remediate risk**

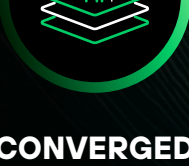
✓  
**Stop attacks**

✓  
**Detect and respond to threats**

## Cortex XSIAM

### AI-Driven SecOps Platform Purpose-Built for SOC Transformation

Rethink and transform your security operations. Combine your SOC capabilities. Connect all of your data sources, and move to a machine-led, human-empowered SOC.



#### CONVERGED PLATFORM

All core SOC capabilities are integrated into a single platform.



#### AI-DRIVEN OUTCOMES

Connect events to accurately detect and stop threats at scale with 2.4K+ AI models.



#### AUTOMATION-FIRST APPROACH

Reduce manual work to accelerate incident response and remediation.



Cortex XSIAM® integrates the entire SOC ecosystem, applying 2,400+ models curated and prebuilt AI and analytics models to deliver the highest 100% detection level, as proven by the latest MITRE ATT&CK® evaluation. Data models normalize third-party sources for seamless integration.



## Cortex Cloud

### Real-Time Cloud Security

With Cortex Cloud, we now integrate cloud and SOC capabilities in a single end-to-end platform. By bringing together code, pipeline, runtime, and application context, security teams get complete cloud visibility to eliminate risks as they occur and remediate issues at the source.



#### ELIMINATE RISK AT THE SOURCE

Secure code delivery and deployment with context-aware guardrails and CI/CD pipeline monitoring.



#### AI-POWERED SECURITY POSTURE ASSESSMENT

Comprehensive risk prioritization based on code, runtime, and application context.



#### AI-DRIVEN DETECTION & RESPONSE

Real-time protection and response capabilities; runtime insights that inform code and cloud remediation.



#### Application Security

PREVENT ISSUES



#### Cloud Posture Security

REDUCE RISK



#### Cloud Runtime

STOP ATTACKS



#### SOC

DETECT & RESPOND



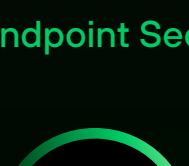
### Unified Data from Code to Cloud to SOC



The Cortex platform's best-in-class XDR, SOAR, and ASM capabilities are fully integrated into XSIAM but can also be deployed in standalone configurations, depending on an organization's needs.

## Cortex XDR

### The Endpoint Security Leader with 100% Detection in MITRE ATT&CK Evaluations<sup>1</sup>



#### PRECISE THREAT PREVENTION

**Stops attacks at the endpoint** with protection against evolving adversary techniques and **zero false positives**.



#### AI-DRIVEN DETECTION ANALYTICS

AI analyzes AI-driven investigation and response data to reveal how attacks unfold across multiple domains with **100% accuracy**.

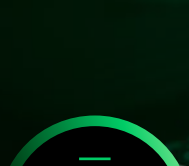


#### AI-DRIVEN INVESTIGATION & RESPONSE

Reduces alerts by **98%** and identifies the root cause of attacks so analysts can respond before a breach.

## Cortex XSOAR

### Pioneer and #1 Leader in Security Automation<sup>2</sup>



#### REDUCE MTTR FROM HOURS TO MINUTES

Facilitate and speed incident resolution across SOC, cloud, and network teams.



#### 75% LESS WORK

End-to-end workflow automations dramatically improve analyst daily productivity.



#### AUTOMATE ANY USE CASE

Completely extensible across your enterprise. **1,000+ integrations** with third-party tools.

## Cortex XPANSE

### The Market Leader in Attack Surface Management<sup>3</sup>



#### PROACTIVE ATTACK SURFACE DISCOVERY

Scans all **500B+** ports daily across all connected systems, clouds, and exposed surfaces.



#### AI-DRIVEN PRIORITIZATION

Uses ML to map attack surfaces and automate risk scoring for zero-day response.



#### AUTOMATION REMEDIATION AT SCALE

Deploys AI playbooks to identify owners and fix issues at machine speed.

### Cortex: The Only Market Leader in SOC and Cloud

Recognized by leading analysts, Cortex has led each revolution in security operations, from XDR to XSIAM and now Cortex Cloud.

<b>Gartner</b>  <b>LEADER</b> 2024 Magic Quadrant™ for Endpoint Protection Platforms	<b>FORRESTER</b>  <b>LEADER</b> 2024 Wave™ for Attack Surface Management Solutions
<b>FORRESTER</b>  <b>LEADER</b> 2024 Wave™ for Extended Detection and Response (XDR)	<b>KUPPINGERCOLE ANALYSTS</b>  <b>LEADER</b> 3X Overall Leader in Security Orchestration, Automation, and Response
<b>FORRESTER</b>  <b>LEADER</b> 2023 and 2024 Wave™ for Cloud Workload Security	<b>MITRE   ATT&amp;CK</b>  <b>100% DETECTION</b> 100% Detection and Industry-Low False Positives, Zero Delays, or Config Changes

Source:

<sup>1</sup> "2024 MITRE ATT&CK Enterprise Evaluations," MITRE, December 11, 2024.

<sup>2</sup> "Security Orchestration, Automation and Response," KuppingerCole, October 8, 2024.

<sup>3</sup> "The Forrester Wave™: Attack Surface Management Solutions, Q3 2024," Forrester, September 23, 2024.