aa teknoloji

Cortex XDR

Designed for critical infrastructures, Cortex XDR is a next-generation cyber defense platform that integrates endpoint, network, and identity data to instantly stop cyber threats and provide operational freedom.

Enterprise Infrastructure Security Challenges

Today, cyberattacks occur three times faster than before, and in 20% of incidents, the time between initial infiltration and data exfiltration drops below one hour. Traditional security tools fail to provide proactive protection, leaving infrastructures exposed to risks.
Existing solutions generate a massive volume of low-priority alerts lacking context, crushing analysts under a heavy workload. This situation increases costs in security operations centers while escalating the operational burden.
Visibility gaps created by isolated tools operating independently across different layers allow stealthy threats to hide in the network without being detected.

⚠ Who can benefit?

- SOC teams suffering from cyber fatigue under an overwhelming volume of alerts
- Organizations looking to prevent zero-day and unsigned advanced attacks
- Institutions experiencing blind spots and visibility gaps across different layers
- Structures aiming for instant, automated response instead of manual analysis

Core Principles

Prevention
Blocks threats before they infiltrate.

Visibility
Offers full visibility across the entire infrastructure.

Automation
Automates analysis processes.

Efficiency
Lowers costs on a single platform.

How Does Cortex XDR Work?

Cortex XDR seamlessly collects endpoint, network, cloud, and identity data, unifying it into a single hub. It provides a three-step intelligent defense cycle that detects unseen threats through advanced AI analytics.

Technical Specifications

Advanced Threat Prevention
- Blocks threats via behavioral analysis
- AI-powered zero-day protection
- Known and unknown vulnerability protection
- USB and Bluetooth device control management

Data Analysis and Detection
- Rich data collection from all layers
- 98% alert reduction with artificial intelligence
- Fully compliant analysis with MITRE standards
- Tracking threats down to their root cause

Incident Response and Reaction
- Instant remote access via live terminal
- Automated response and quarantine steps
- Monitoring the attack chain on a single screen
- Advanced queries for threat hunting

Modular Security Management
- Cloud runtime and container security
- Identity threat detection and response system
- AI-based advanced email protection
- Data loss prevention integration

Hardening and Control
- USB and external device access management
- Local firewall and disk encryption
- Enterprise protection for mobile devices
- Agent-based AI assistant support

Workflow

1. Unified Visibility
- Seamlessly collects logs from all layers.
- Automatically correlates disparate data.
- Eliminates blind spots across the network.
- Provides clean and rich data for analysis.

→

2. Analysis and Detection
- Performs behavioral analysis using AI.
- Instantly detects zero-day and stealthy threats.
- Automatically filters out millions of noisy alerts.
- Presents critical cyber incidents with priority.

→

3. Investigation and Response
- Displays the root cause of the threat on one screen.
- Provides remote intervention via live terminal.
- Rapidly isolates affected systems.
- Instantly stops the threat with automated rules.

Flexible Integration and Scalability
Cortex XDR works in full harmony with your existing security investments and third-party architectures. As your infrastructure grows, its cloud-based architecture scales smoothly and flexibly without bringing additional costs.

Advantages

Artificial Intelligence Analytics
Proactively detects complex and unsigned cyberattacks missed by traditional tools using machine learning.

Unified Data Analysis
Eliminates all blind spots across the infrastructure by correlating endpoint, network, cloud, and identity data.

Intelligent Alert Grouping
Examines millions of warnings to form a single, meaningful incident chain, drastically reducing the workload of cyber teams.

Live Response Capability
Offers instant access to remote systems via the Live Terminal feature, stopping the spread of cyber threats within seconds.

aa teknoloji

AA Teknoloji is an AI-powered media technologies platform developed for modern newsrooms. Our integrated solutions, ranging from news workflow systems to digital archive solutions, real-time broadcasting infrastructure to multi-channel content management, accelerate the digital transformation processes of media organizations and offer scalable broadcasting operations.

For more information, visit aateknoloji.tr or follow the @aateknoloji LinkedIn account.