Cortex: Proactive Security Operations from End-to- End

Security operations centers (SOCs) have been around for approximately 15 years, yet have only become critical in the last five. With a need to prevent cyberattacks and the adoption of centralized security operations (SecOps), security teams are challenged by a lack of qualified personnel (staff, skills, knowledge), budgetary constraints, and a barrage of complex solutions on the market.

Attacks are becoming more frequent, sophisticated, and costly, driven by the surge in ransomware. Unfortunately, attacks can go undetected for too long, leading to increased dwell times and delayed investigation, mitigation, or remediation. While reasons for operational inefficiencies differ among organizations, common issues include:

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

In order to keep pace with threats on a global scale, and remain agile, security teams are increasingly turning to comprehensive cloud-delivered solutions. This approach enables tighter control of security operations, a holistic view of the security posture, and an integrated best-in-class offerings for asset discovery, vulnerability assessment, threat detection, behavioral monitoring, intelligence, and automated response.

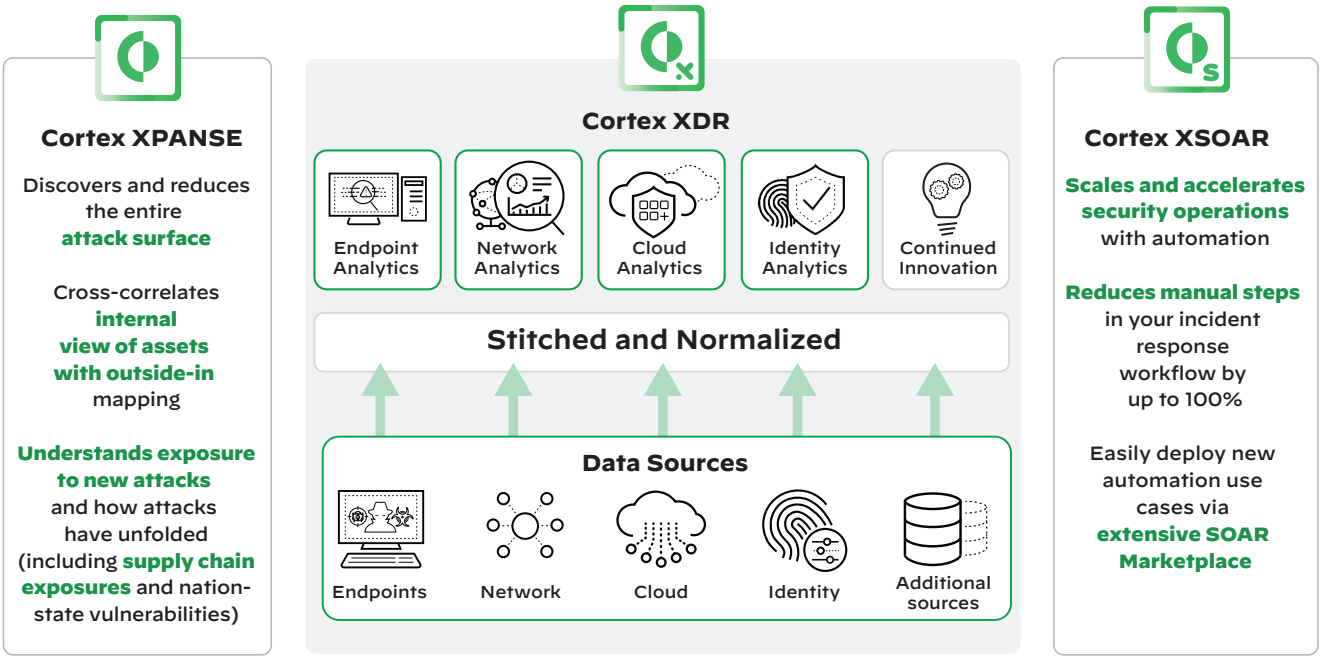

Figure 1: End-to-end workflow automation for security operations

Cortex Xpanse: Internet-Connected Asset Discovery and Mitigation

The rise of the cloud and remote work means attack surfaces are constantly moving, changing, and becoming more complex. Additionally, advancements in scanning technologies allow attackers to scan the entire internet quickly and easily to locate attack vectors, revealing abandoned, rogue, or misconfigured assets that can become backdoors for compromise. Deploying an attack surface management solution can provide a continuous assessment of an organization's external attack surface.

Cortex® Xpanse™ provides a complete and accurate inventory of an organization's global, internet-facing cloud assets and exposures to continuously discover, evaluate, and mitigate an external attack surface and evaluate supplier risk or assess the security of acquired companies.

Discover your attack surface: Automatically inventory all internet-connected assets to find unknown risks.

Prevent ransomware: Discover exposed remote access before attackers do.

Infrastructure governance: Monitor security across federated environments.

Cloud security: Eliminate cloud sprawl and enforce cloud policies centrally.

Third-party due diligence: Identify risk introduced from relationships with suppliers and acquired companies.

Cortex XSOAR: Security Orchestration, Automation, and Response Plus Threat Intelligence Management

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 minimize complex incident investigations in a single platform.

Cortex XSOAR provides end-to-end incident and security operational process lifecycle management, helping companies accelerate security operations, reducing the time it takes to investigate and respond to security threats. Security teams of all sizes can orchestrate, automate, and speed up incident response for any SecOps workflow by leveraging the extensive vendor integrations and 725+ pre-built content packs available via the XSOAR Marketplace to maximize enterprise coverage.

With XSOAR, security teams gain access to a central threat library from diverse threat intelligence sources—including tactical (machine-readable) to strategic sources (report-based)—providing the ability to automatically map threat information to incidents and operationalize threat intelligence with automation.

Automation & Orchestration

Respond to security incidents with speed and scale:

- 100s of product integrations
- 1,000s of security actions
- Intuitive, visual playbook editor

Real-Time Collaboration

Improve investigation quality by working together:

- Virtual War Room for every incident
- ChatOps and real-time security actions
- Auto-documentation of playbook and analyst actions

Case Management

Standardize process across products, teams, and use cases:

- Real-time ChatOps, integrated with case management tools
- Custom views by incident type
- Customizable dashboards and reporting

Threat Intel Management

Take full control of your threat intel feeds:

- Automate repetitive daily indicator management tasks
- Get instant ROI from existing threat intel feeds
- Gain confidence in incident response decisions

Cortex XDR: Endpoint Threat Prevention, Endpoint Detection and Response, Behavior Analytics, and Managed Detection and Response

Cortex XDR is a viable alternative approach to SIEM solutions by providing threat detection, investigation, response, and hunting rooted in endpoint threat detection and response with the ability to scale to cloud environments which is where enterprise data is moving. Once you prevent everything you can at the endpoint, Cortex XDR 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.

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

Cortex XDR brings tighter third-party integrations, better analytics, and faster response capabilities—a must when one considers that organizations may use up to 45 security tools while responding to an incident.[1]

Security teams can stop attacks more efficiently and effectively, eliminating blind spots, reducing investigation times, and ultimately improving security outcomes using Cortex XDR. And with Cortex 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."

Detect advanced attacks with analytics: Uncover threats with AI, behavioral analytics, and custom detection rules.

Focus on incidents, not alerts: Avoid alert fatigue with a game-changing unified incident engine that intelligently groups related alerts into incidents.

Investigate eight times faster: Verify threats quickly by getting a complete picture of attacks with root cause analysis.

Stop attacks without degrading performance: Obtain the most effective endpoint protection available with a lightweight agent.

Maximize ROI: Use existing infrastructure for data collection and control to lower costs by 44%.

1. *2020 Cyber Resilient Organization Report*, Ponemon Institute, June 30, 2020, https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839.

Great on Their Own, Yet Better Together

The Cortex portfolio offers an end-to-end security solution that ensures every step of security processes are covered.

To start, Cortex Xpanse ensures that your organization has a comprehensive and up-to-date view of your entire attack surface and risks. This includes not just a view of potential exposures, but an easy view of which assets are and are not being protected by Cortex XDR. Additionally, Xpanse can use data from Cortex XDR to provide critical information about the security of remote worker environments.

As new risks and threats are discovered by Xpanse or Cortex XDR, Cortex XSOAR reduces the manual human effort to remediate those risks and respond to threats. With Cortex XSOAR, an alert about a newly discovered asset or exposure can automatically be routed to the responsible stakeholder to ensure only those directly tasked with handling an issue are notified.

Cortex is the industry's most comprehensive security operations product portfolio with end-to-end solutions to ensure enterprises are being proactive with security, not reactive. This begins with attack surface management for complete visibility of assets and risks, to best-in-class prevention, detection, and response on endpoints, and powerful automation capabilities to reduce human effort. By taking a portfolio approach, teams benefit from integrated solutions for continuous protection with uninterrupted risk management.

For more information on how the Cortex suite of products can deliver best-in-class threat detection, prevention, attack surface management, and security automation capabilities, download our white papers:

Building a Virtual SOC Platform with Cortex

How to Plan for Tomorrow's SOC, Today

Visit our product pages:

Cortex Xpanse

Cortex XSOAR

Cortex XDR

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