CORTEX XDR

Stop sophisticated attacks by breaking the traditional silos of detection and response and natively integrating network, endpoint and cloud data.

RECENT INDUSTRY INSIGHTS

Incident response times are too long. Mean time to identify: **197 days** Mean time to contain: **69 days**	Security teams receive **174,000** security alerts per week, but they can review less than **7%** of them.	Two greatest SOC challenges according to security professionals: Not enough time: **80%** Not enough people: **79%**
Cost of a Data Breach Study, 2018, Ponemon Institute	***State of SOAR Report 2018, Demisto***	***State of SOAR Report 2018, Demisto***

CORTEX XDR MESSAGING

Cortex XDR defines a new category for detection and response by fully integrating network, endpoint and cloud data to stop sophisticated attacks. With Cortex XDR, security teams can:

- Automatically detect stealthy attacks by applying behavioral analytics to network, endpoint and cloud data
- Reduce investigation time 8x by integrating data from multiple sources to reveal the root cause of alerts and grouping related alerts into incidents
- Block malware, exploits, and fileless attacks with best-in-class prevention

CORTEX XDR ELEVATOR PITCH

Cortex XDR is defining a new category for detection and response by fully integrating network, endpoint and cloud data to stop sophisticated attacks. Cortex XDR accurately detects threats with behavioral analytics and machine learning and it reveals the root cause of any alert to simplify investigations. Tight integration with enforcement points accelerates containment, enabling you to stop attacks before the damage is done.

KEY ASSETS AND SALES TOOLS

Customer Presentation | Datasheet | Sales/Partner FAQ | Competitive Battlecards | Lightboard Cortex XDR Overview | Lightboard Cortex XDR Analytics

CORTEX XDR

PROSPECT CHALLENGES AND RESPONSES

Titles and Responsibilities	Challenge Faced	Pitch and Customer Benefit
Security Operations Alert Triage Analyst (Tier 1) Incident Responders (Tier 2) Threat Hunters (Tier 3) Architects and Engineers	▪ Can't detect advanced attacks ▪ Too many alerts ▪ Don't have enough information to triage alerts	▪ **Behavioral analytics:** Automates attack detection by profiling behavior and generating a small number of accurate alerts with full investigative context. ▪ **Flexible custom rules:** Detects attacks targeting vulnerable or high-risk systems in your organization & apply knowledge gained from past investigations.
	▪ Can't efficiently investigate threats ▪ Need specialized experts to confirm attacks ▪ Searches require learning a new query language	▪ **Data stitching:** Eliminates alert fatigue by allowing analysts to quickly investigate security alerts from any source with a single click. Eliminates alert backlog and lowers experience needed for accurate analysis. ▪ **Root cause analysis:** Simplifies investigations for the entire SecOps team by identifying the sequence of events and root cause of alerts. **Powerful search tools:** Makes threat hunting easy with intuitive queries
CISO Develop and lead security programs	▪ Growing cost of security operations	▪ **Automation and efficiency:** Reduces operating costs with machine learning and by fully integrating network, endpoint & cloud data, avoiding manual correlation or costly professional services ▪ **Increased productivity:** Lowers experience needed for accurate analysis across alert triage and investigations, reducing backlog and risk ▪ **Increased ROI**: Reduces the number of security products to deploy and operate, lowering TCO 44% versus siloed tools. ▪ **Cloud-based deployment:** Lowers management costs by eliminating the need to deploy & maintain new single-purpose servers & infrastructure.
	▪ Business risks associated with breaches and data loss	▪ **Automated detection and accelerated investigations:** Stop threats that otherwise would have been missed by combining rich data, behavioral analytics and machine learning. ▪ **Full visibility to eliminate blind spots:** By stitching together network, endpoint and cloud data, you can catch all threats, including ones involving unmanaged devices and cloud assets, and thereby reduce the risk of a costly breach

COMMON OBJECTION HANDLING AND FAQ

Objections	Response
I am concerned about sending log data to the cloud	Security is our top priority. The Cortex Data Lake leverages industry-standard best practices for security and confidentiality, including app, system, network, and physical security. Data sent to Cortex Data Lake is encrypted in transmission. Cortex XDR is SOC 2 Type II Plus certified and has reached a key FedRAMP milestone. Contact Deal Desk to obtain the report.
Do I need to buy & deploy both Traps and firewalls?	No, customers only need one source of data, such as Traps or firewalls, for detection and response. Note that Cortex XDR includes Traps licenses, providing a single agent for prevention as well as data collection for detection and response.

CORTEX XDR

TOP COMPETITIVE ADVANTAGES

Competitive Advantage	Cortex XDR Capabilities
Network + Endpoint + Cloud	• Stitches together network, endpoint and cloud and third-party data to: – Provide EDR, UEBA & NTA (and endpoint protection) in one offering – Present the full context of alerts to simplify investigations – Detect advanced attacks and remove blind spots
Best-in-Class Endpoint Protection Included	• Eliminates the need to buy and manage endpoint protection separately • Offers best-of-breed prevention for exploits, malware & fileless attacks • Integrates with WildFire for cloud-based malware analysis
Behavioral Analytics to Detect Network & Endpoint Attacks	• Profiles user & device behavior to identify anomalies indicative of attack • Uses machine learning in customers' environments to detect attacks • Uses machine learning performed for local static analysis in Traps & WildFire
Accelerated Investigations with Root Cause Analysis & Incident Management	• Automatically determines the root cause, chain of events, and timeline of any alert with one click in a simple, intuitive user interface • Group related alerts into incidents to reduce individual alerts 50x
Simple Deployment & Management	• Avoids the need for on-prem log storage • Supports logs and alerts from next-gen firewalls, Traps, Prisma Access, and third-party tools, eliminating the need for new sensors and enforcement points

Competitors	Competitor Weaknesses *(Start with Top Competitive Advantages Shown Above)*
CrowdStrike	• Offers managed services to compensate for poor attack detection
Cylance	• Focused on prevention; offers weak detection & response; bought by Blackberry
Carbon Black	• Very complex; requires experienced tier 2/3 analysts to investigate threats
Symantec	• Legacy vendor with resource-intensive agents; complex EDR; bought by Broadcom
Darktrace	• Lack endpoint detection or response; generate a high-volume of false positives • Require additional network appliances • Depends heavily on a managed security service to supplement inaccurate alerts
Cisco Stealthwatch	• Primarily relies on high-level NetFlow data and detects attacks using static thresholds because it can't correctly ID devices over time in DHCP networks

CORTEX XDR

QUESTIONS TO ASK

Discovery Questions

1. How do you detect and respond to threats today?
2. What do you have in place to find an active attacker or a malicious insider in your network?
3. What percentage of security alerts can you investigate today?
4. How long does it take you to triage and investigate alerts?
   - How many alerts do you receive a week?
   - What is a typical process to investigate an alert?
5. What are your greatest security operations challenges?
6. Do you have enough staff to handle all your security alerts?
7. Do you have any active endpoint detection and response (EDR), or network traffic analysis projects?
8. Do you proactively hunt threats?

Qualifying Questions

1. Do you have a dedicated security operations team?
   - How do you handle alerts and investigations?
   - How many people are in your security team?

   Recommendation: Organizations that do not have a dedicated team to investigate alerts are not good candidates for Cortex XDR. Refer to an MDR partner.
2. What is your stance on cloud-delivered security?

   Recommendation: Qualify out organizations that aren't willing to send security data to the cloud.
3. How many users do you have in your organization?

   Recommendation: Focus on organizations with 1,000+ users and refer smaller customers to MDR partners.
4. What is your renewal cycle for endpoint products?

   Recommendation: If a customer is unwilling or unable to consider Traps, position Cortex XDR for network traffic analysis and anomaly detection based on firewall logs.