Maximize the ROI of Detection and Response

Cut Costs by 44% by Consolidating Tools and Streamlining Operations

Building a successful security operations program starts with the right detection and response tools. These tools can help security teams quickly uncover, investigate, and contain threats.

To protect their digital assets, many teams today provision countless detection, response, and analytics tools. Although each tool has individual value, these siloed products force security analysts to pivot from console to console to gather context when reviewing alerts, which slows down incident response efforts. These tools also require organizations to deploy and maintain an ever-growing array of software agents, network sensors, and on-premises log servers, putting a high operational burden on IT teams.

Cortex XDR

- Stops malware, ransomware, and fileless attacks with integrated endpoint protection.
- Detects hard-to-find unknown threats with machine learning.
- Accelerates investigations to reduce incident response time.
- Contains threats that could lead to costly data breaches.

These siloed products also add complexity, resulting in poor security outcomes. To stop sophisticated threats, security teams should consider Cortex XDR™, the industry's first extended detection and response platform. Cortex XDR lowers the mean time to contain threats and improves analyst productivity by breaking down security silos and simplifying operations.

This paper will prove how an enterprise of 10,000 users can safeguard its business against costly breaches while saving 44%—or an average US$686,599—by using Cortex XDR instead of siloed detection and response tools.

Stealthy Threats Require a New Approach to Security

Attackers continually develop new tactics to evade security defenses. They stay under the radar by stealing credentials and masquerading as legitimate users. They "live off the land," using applications already installed on endpoints to conduct attacks. They even use legitimate desktop sharing apps and VPN connections to infiltrate organizations.

To stop active threats, such as an attacker moving laterally or a malicious insider stealing data, security teams need tools that can easily pinpoint unknown threats while simplifying investigation and threat containment. Typically, this requires deploying and managing multiple disjointed tools:

- **Endpoint detection and response (EDR)** records endpoint activity on managed devices to detect potential threats, provide context for investigations, and support manual response actions.
- **Network detection and response (NDR)** monitors network traffic and detects behavioral anomalies indicative of active attacks, such as command and control, lateral movement, data exfiltration, and malware activity.
- **User behavior analytics (UBA)** profiles the behaviors of users and entities (devices) to detect threats such as insider abuse and credential-based attacks.

All three of these technologies and more should be implemented "to improve prioritization, visibility, threat detection and IR capabilities," according to research firm Gartner.[1] However, each of these tools provides a narrow view focused on one data source, forcing analysts to manually correlate details from multiple tools and requiring specialized expertise to operate.

To add to the complexity, organizations that want to use EDR, NDR, and UBA capabilities often must manage a large number of purpose-specific network sensors, endpoint agents, and log servers.

Breaking the Silos of Detection and Response

Cortex XDR is an extended detection and response platform that integrates network, endpoint, cloud, and third-party data to stop sophisticated attacks. Combining the capabilities of EDR, NDR, and UBA, Cortex XDR provides full protection while simplifying operations and allows security teams to gain enterprise-wide visibility without introducing "swivel chair" syndrome. Cortex XDR:

- Stores data in a scalable, cloud-based data repository and automatically stitches together network, endpoint, and cloud data.
- Accurately detects unknown and highly evasive threats with behavioral analytics and customizable rules. Machine learning models analyze rich data stored in Cortex XDR to uncover threats with unrivaled accuracy.
- Accelerates investigations by revealing the root cause and timeline of an incident, allowing analysts of all experience levels to quickly verify threats.

Table 1: Capabilities of Leading Security Tools

Capabilities	XDR	EDR	EPP	NDR	UBA
Endpoint-based detection, investigation, and response	●	●	◖	○	○
Endpoint-based malware, exploit, and attack prevention	●	◖	●	○	○
Network-based detection, investigation, and response	●	○	○	●	○
User behavior analytics, detection, and response	●	○	○	○	●
Automated stitching of network, endpoint, and cloud data to improve detection and simplify investigations	●	○	○	○	◖

[1] "How to Plan, Design, Operate and Evolve a SOC," Gartner, September 6, 2018, https://www.gartner.com/en/documents/3889122/how-to-plan-design-operate-and-evolve-a-soc.

Calculating Detection and Response Costs

With an average data breach costing $8.64 million in the United States and $3.86 million globally,[2] rising to $100 million or more for large-scale breaches,[3] every organization needs to invest in detection and response tools, many of which offer only limited capabilities (see table 1). An organization would need to purchase, deploy, and manage multiple siloed products to match the capabilities of Cortex XDR. To evaluate detection and response costs, consider a sample organization with 10,000 users. The estimate for the total cost of ownership (TCO) is based on an average enterprise with 10,000 users, as shown in tables 2 and 3.

Table 2: Sample Organization

Total number of users	10,000
Total number of managed and unmanaged devices	25,000
Current firewalls	Palo Alto Networks Next-Generation Firewalls
Current antivirus	Legacy antivirus agent
Project objectives	• Replace antivirus • Reduce mean time to respond (MTTR) by 50% • Improve visibility to managed and unmanaged devices • Consolidate security tools to improve operational efficiency
Cost of a cybersecurity analyst	$107,600/year[*]
Cost of an IT administrator	$81,866/year[†]

[*] Based on $79,738 average salary with 135% overhead for taxes, benefits, bonuses, and office costs. Salary information from Glassdoor.com as of June 20, 2019.

[†] Based on $60,642/year average salary with 135% overhead for taxes, benefits, bonuses, and office costs. Salary information from Glassdoor.com as of June 20, 2019.

Table 3: Comparative TCO of Cortex XDR Ownership

Capability	Palo Alto Networks Offering (List Price)	Siloed Security Tools (List Price)
Endpoint detection and response (EDR) and endpoint protection (EPP)	$385,000/year for Cortex XDR Pro per Endpoint with 30-day endpoint data collection	$385,000/year for separate EPP and EDR agents with 30 days of storage
Network detection and response[*]	$346,500/year for Cortex XDR Pro per TB with 30-day network data collection	$350,000/year for NDR appliances and network taps or flow generators
User behavior analytics	$0; included with Cortex XDR	$95,000/year for add-on UBA or subscription for SIEM
Alert triage and investigation overhead	$215,200/year for 2 cybersecurity analysts	$376,660/year for 3.5 analysts[†]
SIEM license and equipment cost savings	(- $250,000/year) due to ability to stop sending traffic logs, Windows event logs and EDR logs to SIEM	$0[‡]
SOC alert policy creation and tuning	$53,800/year for 0.5 cybersecurity analyst	$107,600/year for 1 cybersecurity analyst[§]
Operating costs for software, hardware, and log servers	$122,799/year for 1.5 IT and desktop admins	$245,598/year for 3 IT and desktop admins[||]
Total Cost of Ownership	**$873,299/year**	**$1,559,858/year**

[*] Cortex XDR includes network detection and response, but customers must collect network traffic logs, which increases storage requirements and thus subscription costs.

[†] Siloed tools reduce productivity, require more staff, and increase alert triage and investigation expenses.

[‡] Cortex XDR can reduce SIEM and log management costs 30–50% if organizations store their firewall traffic logs, Windows event logs, and endpoint data in Cortex XDR rather than their SIEM.

[§] Cortex XDR includes over 200 predefined BIOC rules as well as analytics detection algorithms out of the box. Analysis of anonymized cloud-based metrics informs development of predefined rules as part of product updates, lowering policy tuning costs.

[||] Siloed tools require extra overhead to manage and maintain separate EPP and EDR agents; NDR sensors; and on-premises log storage, analysis, and management servers.

[2] “2018 Cost of a Data Breach Study: Global Overview,” Ponemon Institute, July 2018, https://www.ibm.com/downloads/cas/861MNWN2.

[3] “The 18 biggest data breaches of the 21st century,” CSO Online, December 20, 2018, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Methodology

Operating cost estimates are based on rigorous interviews with IT and security managers and executives. Cost savings are attributed to automation; dynamic stitching of network, endpoint, and cloud data; out-of-the-box rules and response integrations; elimination of on-premises log collection and management; and consolidation of sensors and enforcement points with prevention tools. Please note these caveats:

- List prices of siloed security tools vary by provider.
- Security providers, including Palo Alto Networks, may offer discounts from list prices.

Lowering TCO with Cortex XDR

Every day, security leaders balance defensive strategies with budget realities. To keep up with escalating threats, leaders should invest in technologies that can rapidly adapt to outpace attackers without requiring the deployment of more siloed tools.

Cortex XDR is the smart choice for stopping sophisticated attacks while lowering operating costs and avoiding network sprawl. Cortex XDR:

- Reduces setup and maintenance costs.
- Decreases operating costs by streamlining investigations.
- Lowers threat hunting costs by automating detection with machine learning.
- Avoids expensive policy tuning costs and consulting engagements.

Reduce Setup and Maintenance Costs

As a cloud-based app, Cortex XDR avoids the need to provision additional on-premises software, hardware, or log storage, lowering opex and capex. It can use existing Palo Alto Networks products as sensors and enforcement points, streamlining deployment and management. Security data is stored in Cortex Data Lake, a scalable, cloud-based data repository, offering hands-free management.

Decrease Operating Costs by Streamlining Investigations

Cortex XDR dynamically stitches together network, endpoint, and cloud data, allowing analysts to investigate alerts without pivoting from console to console and performing manual analysis.

Lower Threat Hunting Costs by Automating Detection with AI

Cortex XDR accurately identifies threats unique to each customer environment by profiling user and device behavior, reducing the need to manually search for attack tactics, techniques, and procedures. Cortex XDR offered unsurpassed technique coverage out of all vendors tested in the MITRE ATT&CK® framework, so leaders can rest assured that it will uncover covert threats automatically.

Avoid Expensive Policy Tuning and Consulting

Cortex XDR offers out-of-the-box threat detection, including behavioral analytics detection algorithms and over 200 predefined behavioral rules, avoiding the need to build detection policies. Unlike most UBA tools, Cortex XDR offers immediate value without requiring protracted consulting engagements.

With Cortex XDR, security teams can consolidate multiple detection and response products into a single platform, migrate data management to the cloud, and lower log management expenses to **reduce the total cost of ownership for detection and response by 44%**. Cortex XDR is the secret weapon to improve security outcomes and maximize operational efficiency.

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