cbts | paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

Cortex XDR managed by CBTS

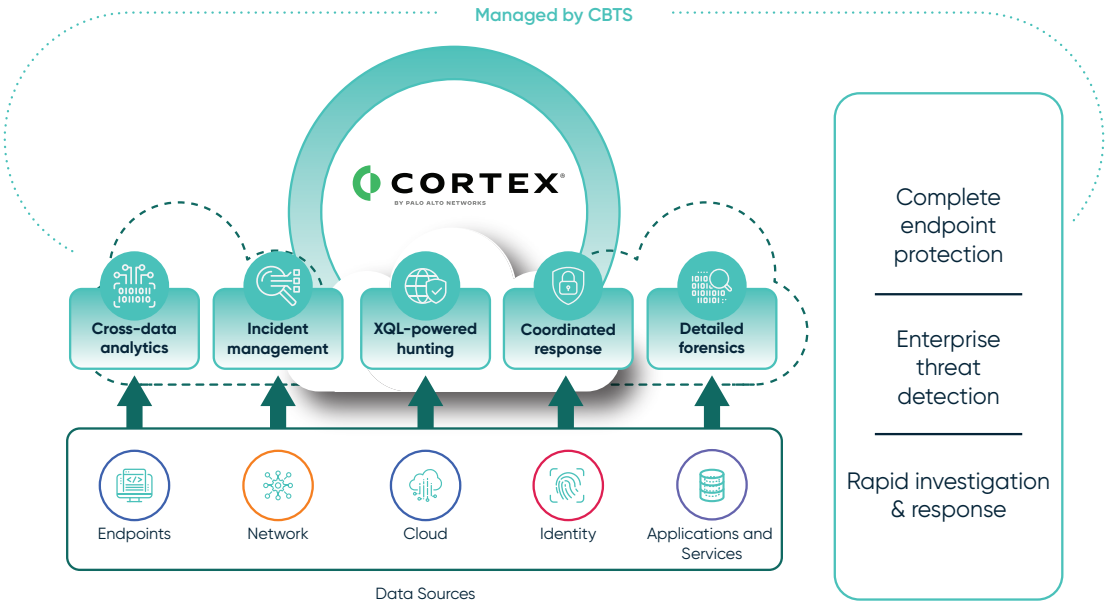
Rapid identification and remediation of cyberattacks with machine learning and enterprise-wide visibility

Cortex® Extended Detection and Response (XDR) managed by CBTS delivers complete endpoint protection across the enterprise by integrating data from any source to defend against advanced cyberattacks.

Cortex XDR security offers sophisticated capabilities for identifying and addressing threats, including:

- Identification and countering of stealth attacks.
- Analysis of the behavior of both users and technological assets.
- Threat intelligence combines locally-shared intelligence with intelligence acquired from external sources.
- Minimize false positives with automatic correlation and verification of alerts.
- Centralized management and comprehensive analysis across all channels for various threats.
- Automation and orchestration enhance numerous security operations center (SOC) processes, allowing for faster response and remediation for customers.
- Extended Threat Hunting (XTH) is an optional add-on that allows your security team to proactively detect threats with additional analytics and machine learning (ML) tools.

Benefits of Cortex XDR	
Enhanced visibility	Cortex XDR enables a centralized view of endpoint, cloud, identity, and network data to streamline investigation and speed remediation.
Triage	Assess and prioritize risk with machine learning, analytics, and cloud deployment. Rapidly sort between false and true positives.
Security automation	Speed and enhance incident response with automated root cause analysis, detection, and response actions.
De-silo security solutions	Remove siloed security tools from the enterprise security fabric to streamline customer networks.
Integration	Fully integrates with SIEM/SOAR security tools and ITSM.
Agile response	Sweep the entire environment to block rapidly spreading attacks, isolate infected endpoints, and halt attacks.
Contextual learning and AI	Context-based machine learning gathers clues over time to aid SecOps in tracking threat actor techniques.
Security for cloud and remote work environments	XDR can manage and easily scale various environments, encompassing both cloud-based systems and remote devices.
Deep forensics	Ability to carry out thorough internal regulatory inquiries, even when the endpoints are not linked to the network.



Why Palo Alto Networks?

Palo Alto Networks® first coined the term XDR in 2018 and released Cortex XDR as the world's first XDR. Cortex is the only XDR on the market to deliver 100% protection and detection based on the MITRE ATT&CK framework[2].

Why choose CBTS for managed Cortex XDR?

8x faster investigation[1]

Up to 98% less alerts[1]

Customers averaged 44% savings on TCO[1]

Cortex XDR managed by CBTS delivers the following:

- Well-integrated functionality that exceeds visibility and operational efficiency benefits from point products.
- Playbooks and workflows that support prevention, detection, and response use cases, reducing the time needed to contain threats.
- Advanced analytics that leverage multiple sources of telemetry for relevant threat detection.
- Threat intelligence from a variety of sources—OEM, third-party intelligence sources, research groups, analysts, and cross-customer information.
- Increase the value of existing investments through configuration recommendations and best practice policies and actions.
- Integrations with ITSM tooling for ticketing.
- A measurable reduction in effort, time to detect, and time to remediate incidents.

CBTS-managed Cortex XDR offers integrated threat intelligence, machine learning-based detection, fast response and investigation, manual and automated threat hunting, and detailed reporting to help protect your organization against various threat actors—all backed by the CBTS SOC, a team of process-oriented and expertly trained analysts and engineers.

Speak to a security expert today.

[1] Maximize the ROI of Detection and Response

[2] MITRE Engenuity ATT&CK Evaluations Dashboard