# Cortex XDR
# At a Glance

The threat landscape can be many things, but the common attribute for everyone is that the threat landscape changes. Unfortunately, legacy endpoint security tools and narrowly focused threat detection solutions are putting organizations at risk to prevent, detect, and respond to the latest the threat landscape has to offer. Fortunately, Palo Alto Networks coined the term extended detection and response (XDR) and delivers the most effective XDR solution to protect organizations.

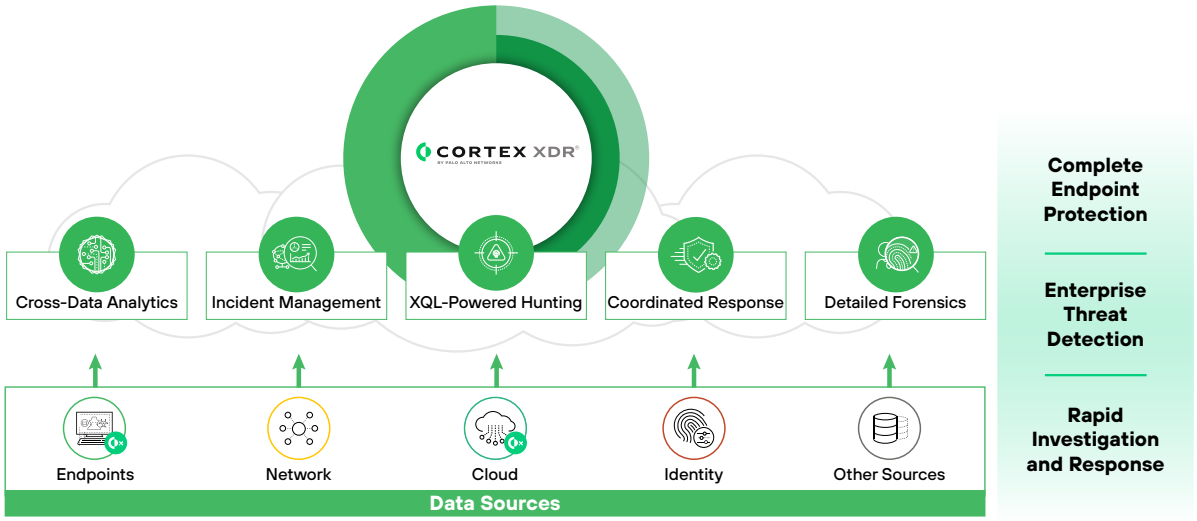


**Figure 1:** Cortex XDR: AI-powered threat prevention, detection, and response

## Cortex XDR Highlights

Cortex XDR® delivers the industry's most effective XDR solution that provides protection, detection, and response by analyzing data from the Cortex® endpoint agent, along with your cloud, network, and identity data to counter evolving cyberattack techniques.

Cortex XDR includes workflow and response automation to make security analysts more efficient in their investigation and response processes:

- Full cyberattack context across endpoint, cloud, network, and identity sources—not just endpoint.
- Mean time to detect (MTTD) reduced to near-real time and mean time to respond (MTTR) reduced to hours.
- Out-of-the-box identity analytics for initial access tactics, techniques, and procedures (TTPs) and available add-on for advanced identity-based threat detection, like insider threats.
- The only endpoint security solution in the MITRE ATT&CK Round 6 Evaluations to achieve 100% technique detection with no configuration changes or delays.
- True data science-driven detections using machine learning algorithms to reduce noise and improve efficacy for hard-to-detect threats.
- Scale to enterprise needs using the power of the cloud with no on-premises solution requirements.
- Unified agent for endpoint and cloud that delivers cutting-edge EDR capabilities including exploit prevention, AI-powered malware protection, Behavioral Threat Protection, along with host firewall, Device Control, and disk encryption. Add-ons are available for forensic collection and Host Insights for vulnerabilities and artifacts.

## Security Challenges Addressed by Cortex XDR

- Cortex XDR breaks down security solution silos by delivering an endpoint agent, a threat detection analytics engine, response workflow, identity threat detection, forensic capabilities, and a comprehensive context of attacks when combined with cloud, network, and identity data.
- A lack of current and integrated threat intelligence in security technologies is a significant challenge most organizations contend with. Cortex XDR continuously integrates curated Unit 42® and Cortex threat research, relieving clients of an extraordinary threat intelligence and detection engineering burden.

# Cortex XDR
## At a Glance

- Cortex XDR solves the challenge of missing both known and unknown threats, as proven by third-party testing, yet keeps the signal-to-noise ratio low to reduce false positives and relieve security analysts from chasing false flags.
- It's widely accepted that disparate and poorly integrated solutions are expensive and not reducing risk to an acceptable level. Cortex XDR delivers increased ROI over narrowly focused EDR solutions that create more work for the analyst and get less detection efficacy.
- EDR-focused and non-XDR solutions lack identity-based threat detection and the context of network and cloud in the same attack incident. Cortex XDR addresses insider threats, lateral movement, and anomalous user and entity behavior with the Identity Threat Detection and Response (ITDR) module.

**Table 1: Cortex XDR Features and Optional Add-Ons**

| | XDR Prevent | XDR Pro per Endpoint | XDR Pro per Gigabyte |
|---|---|---|---|
| **Next-Generation Antivirus:** Block malware, ransomware, exploits, and fileless attacks | ✓ | ✓ | |
| **Endpoint Protection:** Safeguard endpoints with device control, firewall, and disk encryption | ✓ | ✓ | |
| **Security Analytics:** Apply machine learning and UEBA detections to security data | | ✓ | ✓ |
| **Detection and Response:** Pinpoint attacks with AI-driven analytics and coordinate response | | ✓ | ✓ |
| **Third-Party Security Logs:** Send raw logs from other data sources | | | ✓ |
| **Network Traffic Analysis:** Syslog, Kafka, DB, CSV file, FTP, NetFlow, Windows events, Pathfinder | | | ✓ |
| **Prisma® and Palo Alto Networks IoT Security:** Unify cloud and/or control system environments with XDR | | | ✓ |
| **Integrations:** Threat intelligence solutions, Slack, send syslog | ✓ | ✓ | ✓ |
| **Identity Threat Detection and Response (ITDR Module):** Uncover hard-to-detect threats like insiders, lateral movement, credential compromise (includes XTH when paired with XDR Pro per Endpoint) | | | Add-on |
| **Host Insights:** Find vulnerabilities and sweep across endpoints to eradicate threats | | Add-on | |
| **Forensics Investigation:** Investigate incidents swiftly with comprehensive forensic evidence | | Add-on | |
| **eXtended Threat Hunting (XTH Module):** Collect rich data at the endpoint to support deep threat hunting operations in an environment | | Add-on | |
| **Managed Threat Hunting:** Let Unit 42 experts work for you 24/7 to discover advanced threats | | Add-on | Add-on |
| **Managed Detection and Response:** Let Unit 42 experts work for you 24/7 to detect and respond to threats | | Add-on | Add-on |