CRITICALSTART®

Choosing a Managed Detection and Response Partner

The Value of Augmenting Your Security Team

Whether you are a small to mid-sized company needing additional support or a larger organization that needs broader security coverage due to strategies like digital transformation, choosing a managed detection and response (MDR) partner can provide a wealth of services to strengthen your security posture.

To help determine if this approach is right for your needs, ask the questions that follow.

People and Processes

- Are you and your team lacking confidence in your security maturity level?
- Is your security team inundated with managing numerous security tools and chasing false positives or other efficiency disrupters?
- Do your security analysts spend too much time manually triaging alerts?
- Are you challenged with hiring and/or retaining experienced and skilled security personnel?
- Do you lack confidence in your security team's ability to respond to an attack immediately?

Industry

- Do you often work with third-party vendors and suppliers who can broaden an attack surface?
- Are you in a high cyber risk industry (e.g., fintech, healthcare, government, or retail)?

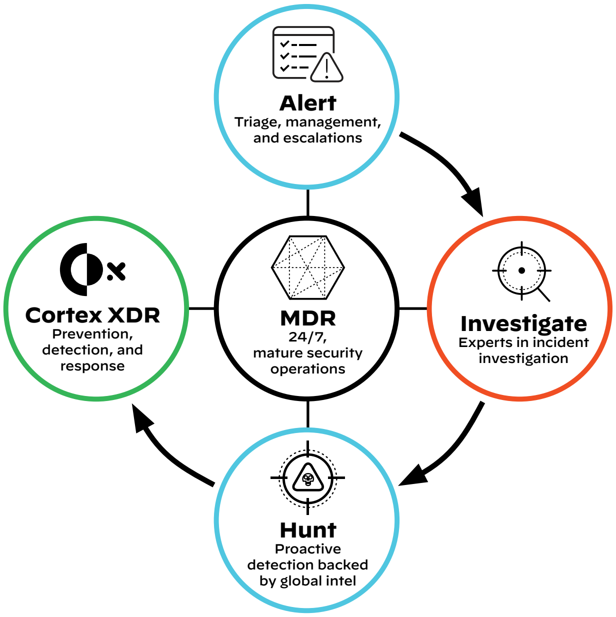
Alert
Triage, management, and escalations
Cortex XDR
Prevention, detection, and response
MDR
24/7, mature security operations
Investigate
Experts in incident investigation
Hunt
Proactive detection backed by global intel

Figure 1: Managed detection and response built on Cortex XDR matures security operations

Technology

- Do you lack confidence in the tools you have in place to investigate endpoints?
- Are you not equipped with the tools to automate threat detection?
- Do you anticipate infrastructure changes to your network that might expose security gaps (e.g., moving from legacy on-premises to cloud services)?

If you've answered "yes" to one or more of these questions, your organization may greatly benefit from working with CRITICAL**START**® because they possess the right MDR technology, skillset and expertise necessary to drive Cortex XDR to its full potential.

Cortex XDR

The success of MDR begins with the technologies used to power the service. Deep visibility and context to provide meaningful analytics are crucial for effective and comprehensive detection and response. Cortex® XDR™ lowers the risk of data breach and compromise with an integrated and holistic product suite for security teams of any size, empowering them with best-in-class detection, investigation, automation, and response capabilities.

New capabilities in third-generation Cortex XDR are described in the sections that follow.

Extending Native Analytics to Cloud Data

Cortex XDR 3.0 integrates cloud telemetry—including host data, traffic logs, audit logs and data from the Palo Alto Networks Prisma Cloud solution—with non-cloud endpoint, network and identity data, delivering organization-wide threat detection and response. Also added are dozens of cloud-specific detection rules targeting common cloud-threat vectors, like cloud escape and cloud-jacking.

UEBA Capabilities with Deeper Identity Analytics

Leverage ML-based threat detectors against an extensive set of identity data sources, including Active Directory®, Identity and Access Management products (including Okta®, PingID® and Azure® AD), human resources (HR) platforms (like Workday®) and SASE gateways.

Third-Party Data Engine

Gain the ability to ingest, normalize, correlate, query and analyze data from virtually any source:

- Ingest and normalize any data source, including databases, files, FTP, CSV, syslog, Windows Event Collection (WEC), and more.
- Allow any data to be correlated with threat activity and tagged with MITRE ATT&CK® TTPs to help provide a more detailed picture of adversarial movement.
- Facilitate ad hoc searching across all third-party data sources, using the native query language (XQL) of Cortex XDR, designed and optimized specifically for investigations and threat hunting.

Built-in Forensics Module Brings Native Forensics Capabilities

Used by Palo Alto Networks Unit 42 Elite Incident Responders, the XDR Forensics Module eliminates the need for deploying, managing and integrating a separate forensics toolkit for collecting and analyzing historical artifacts from endpoints. Cortex XDR 3.0 collects program execution, file access, browsing activity, event logs, network sessions, and other forensic artifacts and then integrates them into the Cortex XDR user interface. The Forensics Module also facilitates data collection for offline endpoints, which is important because network isolation is often one of the first response actions to an attack.

Prevention Is Not Enough

A “prevention-only” approach can introduce risk exposure and should be balanced with detection and response. Teaming up with an MDR provides alert management, investigation, response, and threat hunting for rapid threat containment. By partnering with a Cortex MDR partner, security teams can quickly ramp up the maturity of their security operations, making the leap from reactive responses to proactive and accelerating real-time remediation.

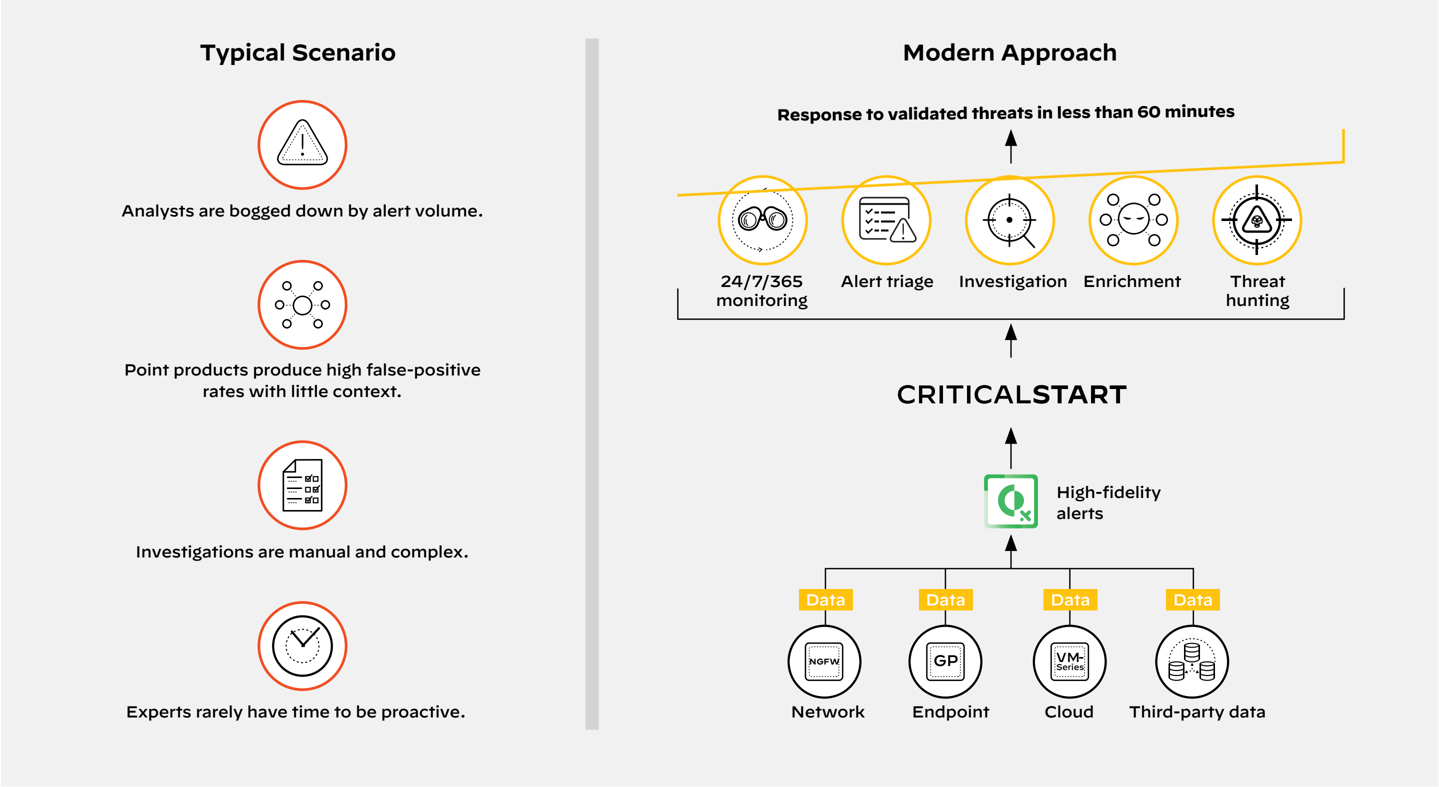
Typical Scenario
Analysts are bogged down by alert volume.
Point products produce high false-positive rates with little context.
Investigations are manual and complex.
Experts rarely have time to be proactive.
Modern Approach
Response to validated threats in less than 60 minutes
24/7/365 monitoring
Alert triage
Investigation
Enrichment
Threat hunting
CRITICALSTART
High-fidelity alerts
Data
Data
Data
Data
NGFW
GP
VM-Series
Network
Endpoint
Cloud
Third-party data

Figure 2: Modern approach to managing security operations

Combining the benefits of Cortex XDR with MDR services provides you with 24/7, year-round alert management, threat investigation, and threat hunting. Direct access to analysts with decades of experience means expert deployment of Cortex XDR for each environment, enabling you to mature your security operations in days, not years. You can instantly scale your SecOps team to defend against fast-moving threats.

Table 1: All the Benefits of Cortex XDR and More

Value	Cortex XDR	With MDR
Prevention from malware, exploits, ransomware, and fileless threats	√	√
Automated, machine learning-based detection	√	√
Custom rules	√	√
Root cause analysis	√	√
Network, endpoint, and cloud prevention	√	√
Live response	√	√
Incident grouping	√	√
24/7, year-round expert security analysis	—	√
Investigation of every endpoint incident	—	√
Focused incident analysis	—	√
Guided remediation actions	—	√
Direct access to analysts	—	√
Mobile application	—	√

About Cortex Managed Threat Hunting

Cortex XDR provides the Managed Threat Hunting (MTH) service as an add-on 24/7 proactive threat hunting service. To use Cortex XDR Managed Threat Hunting, you must purchase a Managed Threat Hunting license and have a Cortex XDR Pro for Endpoint license with a minimum of 500 endpoints. Cortex Managed Threat Hunting does not include tuning, remediation, or incident response and is often used as an additive service to MDR.

Next Steps for Improving Your Security

The straightforward path to value is to work with an MDR partner that has verified deep experience in delivering optimal MDR services across multiple industries and geographies, fits the needs of your organization and has Cortex XDR-certified SOC analysts available 24/7 to operationalize Cortex XDR, fill in security operations gaps, enhance strategic investigation and response capabilities and fully execute on threat detection and response.

CRITICAL**START** MDR compliments the capabilities of Cortex XDR by looking at and resolving every alert with the help of the Trusted Behavior Registry (TBR) built into our Zero Trust Analytics Platform (ZTAP), and by providing:

- Investigation into every Cortex XDR Incident when triggered at the endpoint.
- Relentless transparency—you see exactly what our SOC analysts see.
- Near real-time collaboration between our teams to remediate threats faster.
- Management, maintenance, curation of Cortex XDR out-of-the-box detections and BIoCs, original and third-party threat intelligence used to develop new detections and IoCs, and MITRE-based CRITICAL**START** proprietary detections and IoCs.
- Contractual SLAs for time to detect (TTD) and median time to resolution (MTTR)—we will triage every alert in minutes with a one-hour SLA, guaranteed.

CRITICAL**START** MDR powered by Cortex XDR equals endless threat protection, risk mitigation and reduction, security expertise, and is everything you need from your MDR provider.

For more information, please contact us or visit us at criticalstart.com.

About CRITICALSTART

When it comes to defending against the ever-growing number and sophistication of today's multi-vector cyberattacks, CRITICAL**START**® Managed Detection and Response (MDR) takes a bold approach to radically simplify your security. We extend your team with a comprehensive, customized enterprise solution of flexible services, exclusive technology, and well-trained, seasoned security experts who deeply understand, adapt, and scale with your organization's unique needs and collaborate with you to detect, investigate, and respond to all alerts.

Follow CRITICAL**START**: 🐦 | in | f

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

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