The CRITICALSTART Buyer's Guide for Cortex XDR

A Roadmap to Supercharge Managed Detection and Response outcomes

CRITICALSTART®

EXECUTIVE SUMMARY

XDR takes endpoint detection and response to the next level, delivering comprehensive visibility into the entire security ecosystem. But to get the most performance out of XDR, you need to understand why it's different and what it takes to deploy this tool effectively. Consider this your guide to navigating through the noise around XDR to develop a plan to realize proven security capabilities far beyond the EDR and SIEM platforms of the past.

TOPICS INCLUDE

- ✓ The business case for why MDR for XDR is so important for its success
- ✓ Why organizations choose an MDR service and how MDR differs from Homegrown/MSP/MSSP
- ✓ How an MDR should work with XDR to close gaps in security coverage
- ✓ How to close gaps in security coverage to maximize protection in your environment
- ✓ How the speed of Cortex XDR + MDR = less attacker dwell time—if it's used effectively
- ✓ The advantages and disadvantages of building or buying a security operations center
- ✓ A guide to selecting an MDR for Cortex XDR provider
- ✓ CRITICALSTART MDR for Cortex XDR

The Business Case for Managed Services and XDR

WHAT IS XDR AND HOW CAN YOU MAKE THE BEST IN SECURITY BETTER

XDR. There are a significant number of buzzwords surrounding this technology and our goal is to not use any of them. Instead, we want to define clearly for you the core value of XDR and what it means for your security environment.

On the surface, XDR, or Extended Detection and Response, aggregates related security alerts. But what this really means is that XDR tells a story. It provides something that is missing from traditional Endpoint Detection and Recognition (EDR) and Security Information and Event Management (SIEM) platforms—and that something is context.

Why MDR is so important to XDR

XDR can do great things in terms of shining a light on the alerts that need the most attention, providing a clear path to mitigating threats. But this is only true if those using the tool have the right skillset and expertise necessary to conquer the strident noise coming out of XDR and drive XDR to its full potential. An organization using XDR may try to hire this skillset internally, but they will need to find someone who really knows:

- ✓ The operating system being used
- ✓ The dependencies of the libraries that will interact with the XDR and how they will all work together
- ✓ How to interpret alerts coming from XDR to understand what is normal versus concerning behavior across the network and all applications used by the organization
- ✓ How to efficiently perform a proper investigation based upon an incident that can contain upwards of 30 or 40 related alerts and know how to mount the proper response

Consider this: Two Full Time Employees (FTEs) with the necessary skills may cost over $75,000 each annually plus benefits, but that still would not provide the staffing necessary to deploy 24x7 security coverage for your organization.

You may consider a Managed Services Provider (MSP) or Managed Security Services Provider (MSSP) to fill this skills gap, but each of these still falls short in specific areas. MSPs are not security specialists and can be deficient in many of the same areas that an organization will face trying to work with XDR internally. And while MSSPs monitor networks and notify customers of security issues, they are limited in the active response services they provide, leaving the customer to deal with most issues on their own.

Why organizations choose an MDR service and how MDR differs from Homegrown/MSP/MSSP

TO UNDERSTAND A COMPLETE PICTURE OF HOW EACH TYPE OF SKILLSET TYPICALLY INTERACTS WITH XDR, CONSIDER THE FOLLOWING:

SECURITY VALUE	Internally run XDR	MSP with XDR	MSSP with XDR	MDR with XDR
Prevention from malware, exploits, ransomware, and fileless threats	✓	✓	✓	✓
Automated, machine-learning-based detection	✓	✓	✓	✓
Custom rules	✓	✓	✓	✓
Root cause analysis	✓	✓	✓	✓
Network, endpoint, and cloud prevention	✓	✓	✓	✓
Incident grouping	✓	✓	✓	✓
24/7 expert security analysis			✓	✓
Augment limited in-house security operation capabilities				✓
Optimized detections and BIOCs				✓
A “second” set of eyes				✓
Investigation of every alert				✓
Focused incident analysis				✓
Human-led threat hunting				✓
Guided remediation actions			✓	✓
Direct access to analysts	✓			✓

What is Palo Alto Networks Cortex XDR[1]?

Cortex® XDR™ is the world's first extended detection and response platform that integrates endpoint, network, and cloud data to stop sophisticated attacks. It unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency.

How MDR works with Cortex XDR to close gaps in security coverage to maximize protection in your environment

Cortex XDR[2] empowers organizations to quickly stop stealthy attacks and adapt your defenses to prevent future attacks. Cortex XDR accurately uncovers threats by applying machine learning across your network, endpoint, and cloud data. It provides a complete picture of each incident and reveals the root cause to speed up every investigation.

Now, sped up investigation and remediation are the optimal endgame. To achieve this, a robust team of highly experienced security analysts must be in place and at the ready. And with the current shortage of security professionals, achieving the optimal endgame by solely relying on in-house expertise is becoming increasingly difficult.

An MDR service extends your security team capabilities and coverage with threat detection and response expertise 24x7x365, possesses the horsepower to improve security tool detections, investigate, contain, and respond to incidents coming from Cortex XDR and often includes a range of fundamental security activities for organizations that cannot maintain their own security operations center (SOC). It enables you to leverage the collective experience of security experts across a broad range of security domains, mature operational processes and complete visibility, detection, and response across your network, endpoint, and cloud assets.

With better knowledge, process, and methodology on hand to understand the incidents coming from Cortex XDR, visibility is extended beyond the endpoint and gaps are naturally closed.

What this means:

- ✓ A more comprehensive XDR approach to identify and mitigate known and unknown threats
- ✓ More threat intelligence to expand visibility and stop attacks
- ✓ In-depth security experience to help you properly tune and manage dedicated infrastructure
- ✓ The ability to work with a team that knows what to look for, understands the priority levels within each incident and can rapidly triage the information coming from the Cortex XDR

[1,2] Palo Alto Networks Cortex XDR data sheet

What is Palo Alto Networks Cortex XDR[1]?

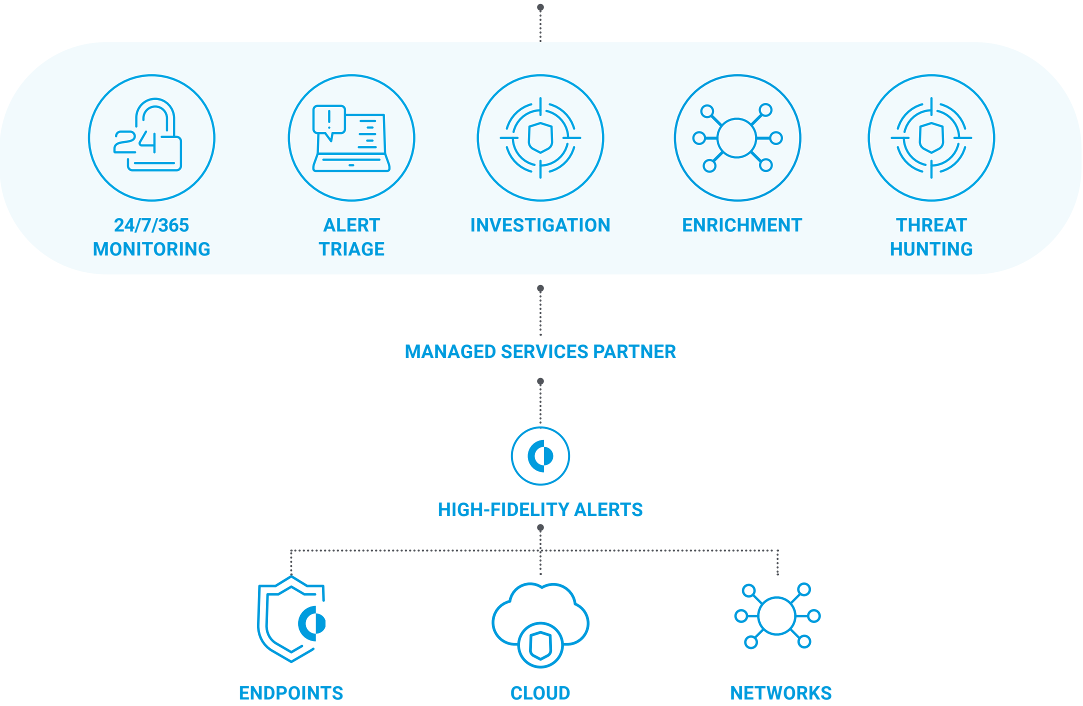
How the speed of Cortex XDR + MDR = less attacker dwell time—if it's used effectively.

Beyond the value that MDR provides in getting the most out of Cortex XDR, it's also a good idea to consider the cost of inaction. The reality is that very few attacks hit instantly. An attacker needs to gain access, examine the environment, get the right credentials, and then deploy malware like Ransomware. This process can take hours or days. If XDR identifies a low or medium incident indicating a breach that is not routed to someone who will mount an effective response—let's say for 12 hours after the initial alerts—that is 12 hours a potential attacker has to work within your environment.

What's needed to find and respond to ransomware:

- ✓ The right tools (XDR)
- ✓ The right focus (every alert without exception)
- ✓ The right people (highly trained, relentless analysts, monitoring XDR information 24/7/365)
- ✓ The right time (investigating and responding to attacks in minutes)

RAPID RESPONSE TO ELIMINATE THREATS



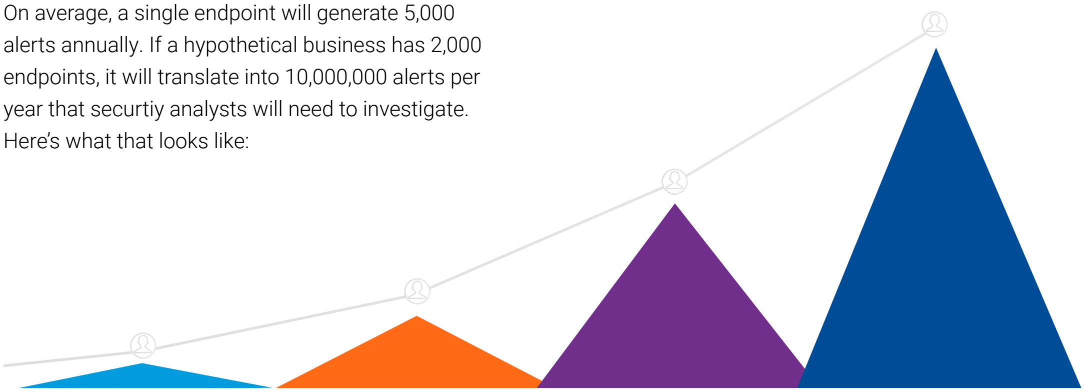
Build Versus Buy:
Bottom line advantages to MDR

Utilizing MDR with your existing Cortex XDR investment provides many distinct and serious cost advantages over trying to develop security capabilities in-house. MDR providers can help you take advantage of economies of scale to shrink total cost of ownership while increasing the expertise and resources you have at your disposal. The MDR provider will also already have the real estate, technology, and expertise to integrate efficiently with your current environment. Software license costs can be significantly reduced, since the MDR provider can purchase licenses at scale, distributed across their entire customer base.

Here's what that looks like in real terms:

Human Costs

On average, a single endpoint will generate 5,000 alerts annually. If a hypothetical business has 2,000 endpoints, it will translate into 10,000,000 alerts per year that securtiy analysts will need to investigate. Here's what that looks like:



Critical-Priority Alerts
0.1% of total events
2-3 analysts
$175,000/year

High-Priority Alerts
0.9% of total events
21-22 analysts
$1,575,000/year

Medium-Priority Alerts
29% of total events
697-698 analysts
$50,750,000/year

Low-Priority Alerts
29% of total events
697-698 analysts
$122,500,000/year

How to Select an MDR provider

The security and business case of using MDR to get the most out of Cortex XDR gets stronger with each examination. The whole premise of XDR is how it enables identification of threats quicker and provides the necessary information to enable the fastest possible response. But MDR will only pay off if you're working with a provider that has the right expertise, tools, processes, and methodology that can adapt to your environment to ensure comprehensive visibility is combined with an aggressive and proactive response. Here's what to ask and demand from any MDR provider you consider.

Do They Treat Every Alert as Critical?

Cortex XDR is a robust, integrated, and holistic product suite that empowers security teams with best-in-class detection, investigation, automation, and response capabilities. Your MDR provider should mirror the robustness of Cortex XDR to ensure quick detection and resolution of every event and response to breaches. This will help you reduce risk acceptance, eliminate alert fatigue, and demonstrate value from your Cortex XDR investment—right from day one.

To accomplish this, every alert triggered by Cortex XDR, no matter the alert level, must be treated equally. In a legacy environment, with thousands of alerts pouring in from EDR and SIEM tools, many MDR providers will disable detection logic to prevent alerts they feel do not require attention.

The problem is that attackers are increasingly being detected through medium, low, and even informational alerts. A top-down approach to dealing with alerts is simply not sufficient in today's threat environment.

A far more effective strategy is to use a trust-oriented approach to handling alerts at scale.

How do they integrate with XDR?

The MDR provider you select should have a deep integration with Cortex XDR, be able to grant you instant access to their SOC teams and deliver best practices in alert management, threat investigation, incident response, and threat hunting.

Best-in-class threat prevention working with Cortex XDR should mean:

- ✓ **Complete visibility, detection, and response across network, endpoint, and cloud assets.**
- ✓ **Expert threat hunting and forensic specialists who will reduce your time to detect (TTD) and median time to respond (MTTR).**
- ✓ **In-depth security experience to help you properly tune and manage dedicated infrastructure.**

Your MDR provider should be able to scale at the pace of your growth. Traditional approaches consistently require the addition of security analysts, technology, and operational process to stay ahead of new risks. But the right MDR provider should be simply able to expand their services as needed to keep ahead of risk. This may be especially relevant in the case of a Mergers & Acquisition situation when the MDR provider of the acquiring organization needs to ramp up quickly to accommodate the tools used by the acquired organization.

How to Select an MDR provider

Are they willing to put it in writing?

This one question is particularly critical to not only building a good working relationship, but also ensuring that the service provider you're considering is ready to deliver on their promise.

While it's common for an MDR provider to supply a Service Level Objective (SLO), that's not going far enough and here's why:

- ✓ An SLO is not committing to a MTTR.
- ✓ An SLO is not outlining any penalties if service level objectives are not met.
- ✓ An SLO is not defining a level of transparency to understand if a service provider is really measuring up to their promises.

Additional Questions to Ask for True Trust Oriented Protection

Beyond these key considerations, there are additional questions you should ask the MDR provider, including:

- ✓ Do they investigate every Cortex XDR incident and alert? If yes, what specifically are they investigating and how do they go about their investigation?
- ✓ What Palo Alto Networks certifications does the MDR provider have?
- ✓ Can they show data from your endpoint, network, and cloud environments?
- ✓ Can your MDR provider really prove the value of their approach through concrete expertise and real-world success stories utilizing Cortex XDR?

CRITICAL**START MDR for Cortex XDR**

Tim Junio, SVP of Products, Cortex at Palo Alto Networks defines the story generated by XDR as the joined relationships between different data sets. In the case of Palo Alto's Cortex XDR, that process begins with data from their endpoint agent and next-generation firewalls. But then they also include third-party data and even competitor's data.

But rather than drowning under a sea of alerts, Cortex XDR joins related alerts together into security incidents that remove security blind spots by stitching together network, endpoint, and cloud data to deliver monitoring, analysis, and coordinated response across your entire environment. These incidents provide clarity into what's really happening in an environment while requiring fewer resources to make an actual threat determination.

CRITICAL**START**™ Managed Detection and Response (MDR) service integration with Palo Alto Networks Cortex XDR™ delivers a comprehensive combination of highly experienced analysts and operational process that helps your security team to quickly detect, investigate and respond to every alert, and stop the most advanced attacks while reducing risk, alert fatigue, and analyst burnout.

HOW WE DO IT	ZTAP/TBR	Human Element	Mobility
	Leverage the Zero Trust Analytics Platform (ZTAP) platform to ingest, normalize and aggregate all alerts from Palo Alto Cortex XDR	Provide 24x7x365 human-led end to-end monitoring, investigation and remediation of alerts by Cortex XDR-certified SOC analysts	MOBILE**SOC**™ allows you to fully triage and contain alerts anytime, and from anywhere
	The platform removes the priority alert and automatically resolves all known good with Trusted Behavior Registry (TBR) • Enables the auto-resoltuion of false positives	Security experts that will deeply understand, adapt, and scale with your organization's unique needs and collaborate with you to detect, investigate, and respond to all alerts.	Collaborate with CRITICAL**START** analysts in near real-time from within the app
	ZTAP enriches our investigation of unknown alerts to ensure the escalation of the alerts that really require the attention of your security team	By simply augmenting in-house security protocols with MDR security experts, the painstaking process of building or refining your own SOC is eliminated	

Unlike other MDR services who take a "blackbox" approach, CRITICAL**START** provides 100% access to our ZTAP platform for complete transparency. You see what our analysts see period. And by providing complete visibility and access to every alert with full investigation details and every action taken, the outcome is a more effective collaboration between our teams, to remediate threats faster.

Our approach to Cortex XDR also means:

- ✓ **We investigate every Cortex XDR alert when triggered at the endpoint, network, and cloud environments**
- ✓ **We leverage incident investigations with endpoint, network, and Wildfire events**
- ✓ **We use Security Assertion Mark-up Language (SAML)/Single Sign-On (SSO) authentication for users**
- ✓ **We use Additional Behavioral Indicators of Compromise (BIOCs) curated by CRITICALSTART**

Beyond visibility into our MDR service, you will have visibility across your security ecosystem. You can better understand how your security tools are performing and validate their return on investment, as well as gain a clear understanding of the true value of your MDR service.

Capability Comparison

● COMPLETE OFFERING
◐ PARTIAL OFFERING
✗ NO OFFERING

	CRITICAL**START** powered by Palo Alto Networks Cortex XDR	**Other MDR Providers**
24x7x365 monitoring, investigation, and response by security analysts	●	●
Contractually guaranteed Service Level Agreement for Time to Detect and Median Time to Resolution for all alerts, regardless of priority level	●	✗
Native iOS and Android applications for alert investigation, collaboration, and response	●	✗
Customer and vendor work from the same platform and see the same information	●	◐
Custom Behavior Indicators of Compromise (BIOCs) Monitoring	●	✗
Two-person integrity review process that provides quality control of SOC orchestration for every customer	●	✗
Manage and maintain cross-ecosystem Behavioral Indicators of Compromise (BIOCs)	●	✗
Continuous threat hunting	●	◐
Perform configuration, deployment, and health checks without requiring additional professional services	●	●
Alert notifications that include both security event data and expert analysis	●	◐
Analyst will proactively respond to stop attacks (isolate, block, whitelist, etc.)	●	●
Managed response, policy tuning, and updating of agents	●	●
BIOCs for Windows, Mac, and Linux	●	✗
Multi-Tenant so customer can have multiple organizations with N-level hierarchy	●	✗
Bi-directional integration with Cortex XSOAR	●	◐
CRITICAL**START**™ Cyber Research Unit: • Manage, maintain, curate Cortex XDR out-of-the-box detections and IOCs • Add MITRE®-based CRITICAL**START** proprietary detections and IOCs • Curates original and 3rd party threat intelligence used to develop new detections and IOCs	●	◐

Best of all, we've built a comprehensive bi-directional integration between ZTAP and Palo Alto Networks Cortex XSOAR, a comprehensive security orchestration, automation, and response (SOAR) platform that fits right into existing workflows, provides for centralized data and visibility, and lets the customer:

- ✓ **Monitor incidents**
- ✓ **Address critical incidents in real time without leaving the XSOAR interface**
- ✓ **Speed up investigation via automated capabilities**
- ✓ **Weave in human analyst tasks and workflows to share information more effectively**
- ✓ **Reduce alert fatigue while using familiar security products**

One last thing to consider....

An MDR provider should not simply be a third-party vendor, they need to be a seamless extension of your own team. The protection of sensitive data—especially customer data—presents one of the greatest business challenges of the 21st century. You must rely on your security partners the most when your organization is facing an attack, and it's in these moments that the relationship really matters.

CRITICAL**START** holds a 99% SOC retention rate, which speaks to the value we place on our team and yours. Learn more about our strength in deploying a SOC that's fluent in Cortex XDR and how we can build the most effective security relationship to strengthen your environment against any potential threat whilst driving a return on investment.

SOC Total Cost of Ownership: Internal Versus CRITICAL**START** MDR

TOTAL COST OF SOC OWNERSHIP	INTERNAL	CRITICALSTART MDR
SOC Analysts	$750k to $100,000,000+ based on number of alerts processed	Included
Alerts Processed	Typically, critical/high only	All alerts resolved
Technology cost	$500k-$1,000,000	Included
Real-estate cost	$25-$85 per square foot	Included
Level of expertise	Varies	Very High, spanning multiple industries, security environments and threat scenarios
Level of protection	Varies	Extremely high

Ask the right questions - of your prospective MDR provider

Do you treat every alert as critical? Cortex XDR is a robust, integrated, and holistic product suite that empowers security teams with best-in-class detection, investigation, automation, and response capabilities. **The right MDR provider should mirror the robustness of Cortex XDR to ensure quick detection and resolution of every event and response to breaches. This will help you reduce risk acceptance, eliminate alert fatigue, and demonstrate value from your Cortex XDR investment—right from day one.**

How do you integrate with XDR? The Cortex XDR platform is ingesting telemetry from a whole bunch of data sources -- Endpoints, Cloud Apps and Network, so you need an MDR that can pull this telemetry together so that it is viewable through a single pane of glass. **The right MDR provider should have a deep integration with Cortex XDR, be able to grant you instant access to their SOC teams and deliver best practices in alert management, threat investigation, incident response, and threat hunting and should be able to scale at the pace of your growth.**

Are you providing a 24x7x365 service? The need for this may seem obvious, but there are MDR providers that view security as a 9x5 service. **The right MDR provider can match the timing and pace of those threats as well as your round the clock security needs.**

How many real humans will be protecting my environment? Some MDR offerings provide a chatbot that notifies you of suspicious activity and then simply give you a link to the issue. But would you rather deal with a chatbot, or a live MDR analyst that has identified the problem, taken direct action to mitigate the issue, and then is ready to make a full report to you over your mobile device? **The right MDR provider should offer you the mobile tools that empower you to take charge of your security from anywhere, and collaborate with industry-leading expertise when a threat is detected.**

How extensive are your playbooks? An MDR provider might have a playbook that details how to deal with an alert based on severity, but what about routing an alert to the right person to evaluate it? What about a playbook for resolution of alerts? And finally, can this entire process be automated to ensure alerts are arriving at the most positive outcome in the most efficient manner possible? **The right MDR provider should have a process roadmap that clearly answers the "who", "what", "when" "how" and "why" to ensure an outcome that's most beneficial for your organization.**

Are you providing us just a Service Level Objective (SLO), or a true Service Level Agreement (SLA)? Is any MDR offering you consider willing to commit their offered protection level to a contract, or are they simply talking about abstract goals around managing risk? **The right MDR provider should commit, in writing, to specific SLA's as well as consequences for not meeting them.**

Do you treat all alerts equally? Many MDR providers practice alert suppression to reduce the overall volume of alerts while only focusing on alerts categorized as critical or high. And they may not even be able to effectively automate the process for closing these alerts. But here's the real problem: Ransomware attacks can often register only a medium- or low-priority alert. **The right MDR provider should investigate every alert, in our opinion. The Trusted Behavior Registry (TBR) within the CRITICALSTART Zero Trust Analytics Platform (ZTAP) is designed to eliminate false-positives at the scale by resolving known-good and safely trusted alerts. A platform like ZTAP can consolidate alerts triggered by Cortex XDR to provide visibility across endpoint, network, and cloud so that MDR analysts can focus on remediating the true positive alerts that might indicate a threat.**

Other questions to ask service providers

Beyond issues important to the successful deployment and use of Cortex XDR, there are other questions you should ask:

- ✓ Do you investigate every Cortex XDR incident and alert? If yes, what specifically are you investigating and how do you go about their investigation?
- ✓ What Palo Alto Networks certifications do you have?
- ✓ Can you show data from endpoint, network, and cloud environments?
- ✓ Can you provide real-world success stories utilizing Cortex XDR?
- ✓ How long does your team take to respond to alerts and are there contractual obligations around this?
- ✓ Will my company have access to your SOC as needed or is that an additional charge?
- ✓ Is there any hardware associated with this service?
- ✓ If my company grows quickly, can you scale just as quickly?
- ✓ Can we investigate and respond to alerts natively from our phones?

DIAMOND

paloalto® NETWORKS

CRITICALSTART®