CORTEX™
BY PALO ALTO NETWORKS

## Business Benefits

- **Remove the burden of detection and response:** Reduce MTTD and MTTR to a guaranteed 60 minutes or less.
- **Boost your security maturity:** Gain a proactive SOC with 24/7 coverage, from alert management to incident response.
- **Go beyond managed EDR:** Expect complete coverage across network, endpoint, and cloud data.
- **Make impactful security investments:** Free up investment with a predictable opex model, helping you bolster your security posture.
- **Benefit from decades of experience:** Get forensic expertise for threat investigation, response, and hunting.

# Managed Detection and Response

## Benefit from decades of experience and instantly move to a proactive, 24/7 SOC for alert management, incident response, and threat hunting

Security operations has become a never-ending battle of managing alert volume and trying to proactively combat attackers. Security teams of all sizes, struggling to keep up, have turned to managed security services to help with the volume of work siloed prevention and detection technology generates.

## MDR Services Reduce MTTD and MTTR

Organizations realize security-positive outcomes more quickly by acquiring managed detection and response (MDR) services, avoiding the painstaking process of building or refining their own security operations centers (SOCs).

Palo Alto Networks has teamed up with industry-leading MDR service providers to offer the most comprehensive combination of experienced analysts, mature operational processes, and market-leading security products. These partnerships deliver:

- Best-in-class prevention from Palo Alto Networks enforcement points.
- Complete visibility across network, endpoint, and cloud assets via Cortex XDR.
- Expert threat hunting and forensic specialists who will reduce your mean time to detect (MTTD) and respond (MTTR) to 60 minutes or less, guaranteed.
- Years of experience in security services to properly tune and manage dedicated infrastructure.

This represents a fundamental shift in the way MDR services are delivered—toward a focus on enabling positive outcomes and customer choice, not increasing point product sales. Traditional managed security services have focused on alert management and notification of critical threats, placing the onus of time-intensive investigations on the customer. MDR offerings from most technology vendors hide shortcomings of limited point products under the veil of services. This is evident in a lack of concrete detection and response service-level agreements (SLAs).

## Instantly Scale Your Security Operations

Our hand-picked MDR partners grant you instant access to their SOC teams and best practices in alert management, threat investigation, incident response, and threat hunting. Decades of experience means expert deployment and fine-tuning of Cortex XDR for each environment, providing a mature SOC in days, not years.

Our MDR partners scale with you as your organization grows. Traditional approaches consistently require the addition of security analysts, technology, and operational process to stay ahead of new risks. Our MDR partners simply require your latest employee count, and their services expand to keep risk in check—all handled for you.

## Powered by Cortex XDR Technology

Cortex XDR™ defines a new category of enterprise-scale extended detection and response that runs on fully integrated network, endpoint, and cloud data. Cortex XDR provides best-in-class prevention, utilizing machine learning to stop threats and detect advanced attacks. Taking advantage of analytics to integrate data from any source reduces alert volume, simplifies investigations, and gives forensic security experts the visibility they need to rapidly remediate threats.

In a market flooded with detection and response technology, our MDR partners selected Cortex XDR to power their services. The proven visibility leader in Forrester's MITRE ATT&CK® framework evaluation, Cortex XDR allows our MDR partners to deliver the best detection and response SLAs in the market. This partnership of best-in-class technology with security services ensures customers realize positive outcomes across all threat vectors, not just the endpoint.

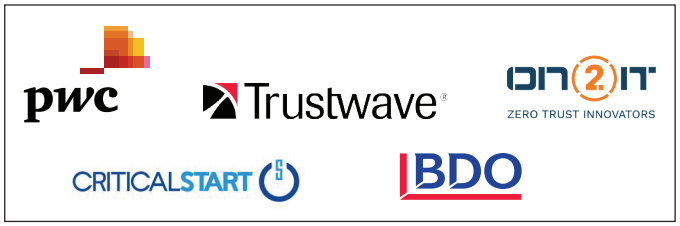


**Figure 1:** MDR providers with services built on Cortex XDR

## Key Capabilities Across Our MDR Partners

### 24/7 Year-Round Coverage

Instantly mature to a proactive SOC. Maintaining staff for continuous coverage is difficult and costly. Our partners provide around-the-clock coverage of your environment with expert analysts who manage alerts, proactively hunt threats, and respond in accordance with your SLAs.

### Alert Detection and Triage

Reduce MTTD to less than 60 minutes. On average, security teams look at less than 7% of their alerts, prioritizing to address only the most critical alerts.[1] Our MDR partners have processes in place to address every alert from Cortex XDR, ensuring no threat across your networks, endpoints, or clouds goes unchecked.

### Lightning-Fast Investigation and Response

Reduce MTTR to less than 60 minutes. Investigations are time-consuming and complex, leaving analysts to manually piece together conclusions. Backed by Cortex XDR, our partners' world-class forensic analysts investigate every threat with speed and precision, defining an attack's root cause, scope, and trajectory for targeted response.

1. Read more in The State of SOAR Report, 2018, at start.paloaltonetworks.com/the-state-of-soar-report-2018.

## Enrichment

Bolster your security with global intelligence. Gathering and maintaining intelligence to aid detection and investigations requires dedicated personnel. Our MDR partners use their experiences across customers around the world, in every industry, to steadily improve detection and response times. By natively integrating threat intelligence feeds with shared analyst experiences, every customer is protected from today's emerging threats.

## Threat Hunting

Leverage dedicated, proactive threat hunters. Even organizations with established SOCs struggle to find people and time for threat hunting. Benefit from our partners' scale and visibility across varying industries, with instant access to dedicated threat hunters experienced at finding today's stealthiest attacks.

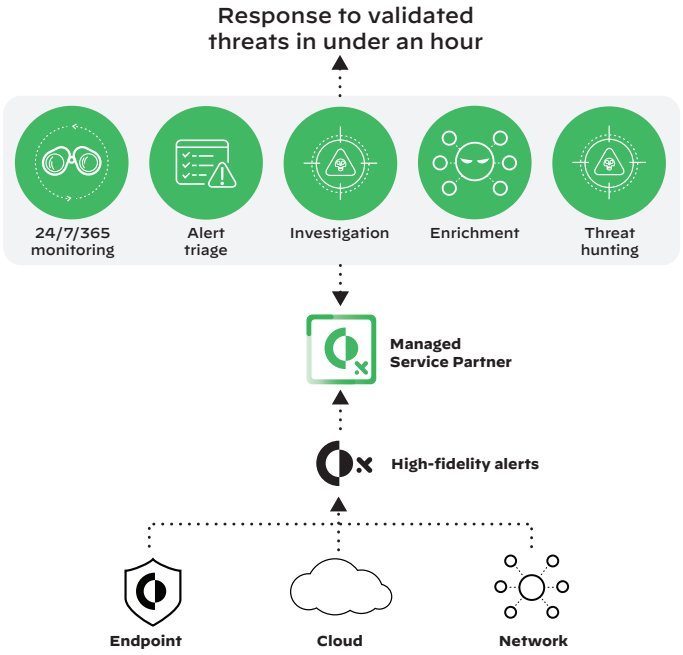


**Figure 2:** Overview of our partners' MDR services benefits

**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 alert | – | ✓ |
| Focused incident analysis | – | ✓ |
| Dedicated, proactive threat hunters | – | ✓ |
| Guided remediation actions | – | ✓ |
| Direct access to analysts | – | ✓ |
| Mobile application | – | ✓ |

paloalto NETWORKS

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