Palo Alto Networks Cortex XDR is a detection and response application that natively integrates network, endpoint and cloud data to stop sophisticated attacks. But increased visibility is only one piece. Clients still need a team of experts to stitch the story of the attack and the root cause together and respond across the entire cyber landscape. Cortex XDR provides Trustwave the tools to conduct speedy remote investigation and root-cause analysis and additional query tools.

Trustwave Managed Detection and Response Services with Palo Alto Networks Cortex XDR

Trustwave Threat Detection and Response (TDR) services leverage Cortex XDR to monitor and escalate incidents based on behavioral analytics matched with threat intelligence across the security fabric. The development teams in both organizations have also found new and innovative ways to collaborate to allow Trustwave threat hunters deep access into Cortex XDR. The front line of defense provides a data stream that identifies anomalies that may be indicative of advanced threat actors using evasion techniques or operating system controls for malicious purposes. The alert data stream is directed to Trustwave for further investigation and remediation, as necessary. Because Trustwave SOC analysts use Cortex XDR for deeper analysis and remediation activities within the client environment, they can also inject rich security research data from the Trustwave Global Threat Database to make a world-class security product even more effective.

Trustwave Managed Detection and Response Services:

Trustwave offers two levels of the Managed Detection and Response (MDR) Service:

- **MDR Essential**: Provides 24x7 technology-based automated root-cause analysis, investigation and response to protect your environment against advanced threats.

- **MDR Complete**: Provides 24x7 advanced threat detection and investigation with containment and remediation actions on your behalf. MDR Complete provides full digital forensics investigations, proactive and continuous threat hunting, and managed Incident Response capabilities that allow the Trustwave digital and forensics incident response team (DFIR) to begin containing cyber-attacks as part of the managed security services (MSS) service.

Trustwave also offers these complimentary services to close gaps in visibility:

- Trustwave Security Technology Management and Managed Detection Services monitor and maintain Palo Alto Networks next-generation firewalls as they detect known and unknown threats.

- Trustwave MSS provide monitoring and policy management for Palo Alto Networks Prisma suite of cloud security solutions.
Trustwave SpiderLabs® Team and Palo Alto Networks Unit 42

The renowned Trustwave SpiderLabs threat hunters have decades of experience in incident response, computer forensics, cyber threat intelligence and malware analysis. These specialists work in concert identifying, tracking and collecting the latest threat intelligence including evolving adversarial tactics and techniques. From there, the teams apply appropriate actions ranging from blocking and containment to threat elimination down to the endpoint. Trustwave SpiderLabs conducts hundreds of deep investigations and thousands of penetration tests for organizations each year and are collaborating closely with Palo Alto Networks’ Unit 42 to address emerging trends and new threats.

About Trustwave

Trustwave is a leading cybersecurity and managed security services provider that helps businesses fight cybercrime, protect data and reduce security risk. Offering a comprehensive portfolio of managed security services, security testing, consulting, technology solutions and cybersecurity education, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries. For more information about Trustwave, visit www.trustwave.com.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices. Find out more at www.paloaltonetworks.com.