DATA SHEET

Trustwave Managed Detection & Response

PROTECTING AGAINST ADVANCED THREATS

Benefits

- Provides 24x7 threat detection and response
- Offers real-time root cause analysis, attacker containment, and remediation
- Delivers continual application of industry-leading cyber threat intelligence
- Leverages Trustwave global SOCs and +250 security professionals
- Includes two levels of service to cater to different risk tolerance

Risky endpoints can compromise an entire network. Trustwave Managed Detection & Response (MDR) combines people, process and technology to identify & respond to advanced threats targeting endpoints. This comprehensive managed service is delivered in two service levels – Essential and Complete – catered for different customer needs. Both levels deliver 24x7 monitoring and notification, incident response and remediation. The Complete version adds a higher level of data forensics and investigation response that includes industry leading proactive threat hunting by Trustwave SpiderLabs.

Trustwave Experts Working for You

People differentiate the Trustwave Managed Detection and Response service. The global Trustwave security team is comprised of our Advanced Security Operations Centers (ASOC team) and renowned SpiderLabs Digital Forensics & Incident Response (DFIR), research, and testing security specialists recruited from top companies and programs.

Team members in global Trustwave ASOCs monitor, investigate, and remediate advanced threats around the clock. Behavioral analysis and threat intelligence from Trustwave empower analysts to resolve security incidents within the Tier 2 level of analysis. However, should the malicious activity analysis progress to Tier 3, the investigation moves directly to the Trustwave SpiderLabs teams, who use the Trustwave threat console to hunt and resolve the threat or identify that an advanced attacker is actively engaged in your environment. Throughout the journey, additional services can be engaged depending on the security roadmap of the company. Many risk averse companies also choose to have a DFIR retainer in the instance of a breach. With a DFIR retainer in place, the Trustwave DFIR consulting team can respond to an active attacker in minutes, as the MSS framework and the DFIR service are designed to interact seamlessly.

Leverage Leading Technology

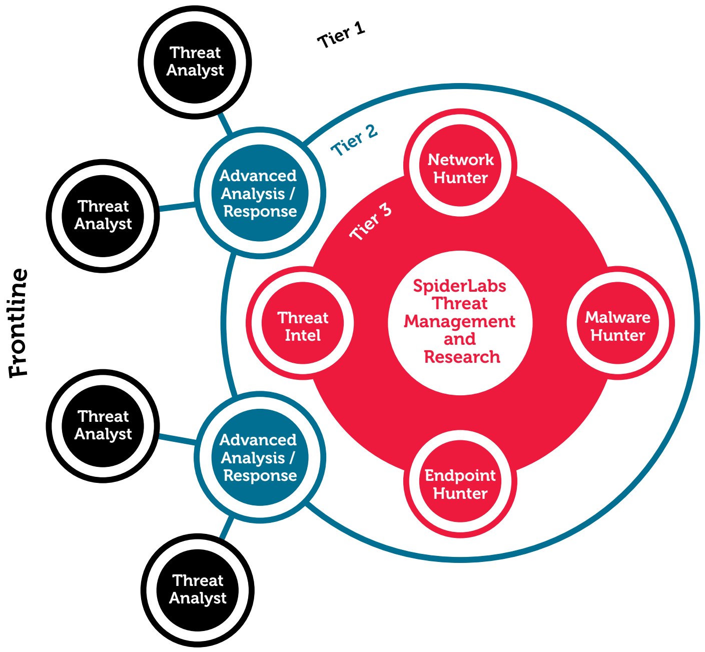
Trustwave MDR leverages advanced Endpoint Detection and Response (EDR) technology that provides real-time behavioral analytics matched with threat intelligence at the endpoint. Cloud and on-premises deployment options are available, and deployment can be done by Trustwave, a third-party, or by the client using their own deployment method.

The EDR technology serves as the front line of defense, providing automated remediation and a kill chain used to hunt advanced threats. The alert data stream is directed to Trustwave for further investigation and remediation as necessary, with the base data staying at the client site. Trustwave analysts leverage the EDR interface for deeper analysis and remediation activities within the customer environment. Clients use the Trustwave TrustKeeper portal to view data and reports and communicate with Trustwave.

In addition to EDR technology, data from 650+ additional sources can feed into the managed detection engine and provide greater visibility and insight into threats. The state-of-the-art integration between data flows from devices to the Trustwave cloud differentiates the ability to seamlessly monitor and manage device configurations.

The Trustwave team follows best practices for detection and incident response that are transparent and visible to customers through the TrustKeeper portal. Response actions are also transparent and visible and most importantly, agreed to by the customer before actions are taken by Trustwave experts in the customer's environment. The types of responses that can be taken include:

- Process or file blacklisting on the endpoint
- Endpoint quarantine or user account lockout
- Initiate interactive session on endpoint
- Download files to endpoint
- Delete files on endpoint
- Gather files and memory for host



Key Takeaways

The Trustwave MDR service blends people, processes, and technology to deliver proactive advanced threat detection and response.

The key to success of the service is that Trustwave and every client are partners. Clients deploy key technology in their environment, and Trustwave delivers value through monitoring implemented systems and their environments, maintaining technology in the case of outages, and responding to threats using global cybersecurity talent and a top-of-the-line, honed threat incident response methodology.

Cybersecurity does not have to be reactive. Partnering with Trustwave gives Trustwave MDR clients access to security experts who can actively pursue bad actors and reduce or eliminate dwell time for persistent threats. Continuous monitoring and auditing are key parts of how to survive in a world of cyberattacks. The large Trustwave portfolio provides a wide range of best of breed managed security services for managed security compliance, security technology management, and managed detection and response solutions.

For more information on these and other Trustwave products and services, visit www.trustwave.com

ANAB ACCREDITED
ISO/IEC 17021
MANAGEMENT SYSTEMS
CERTIFICATION BODY

Trustwave®
sure.business

For more information: www.trustwave.com