Trustwave Managed Detection and Response Services

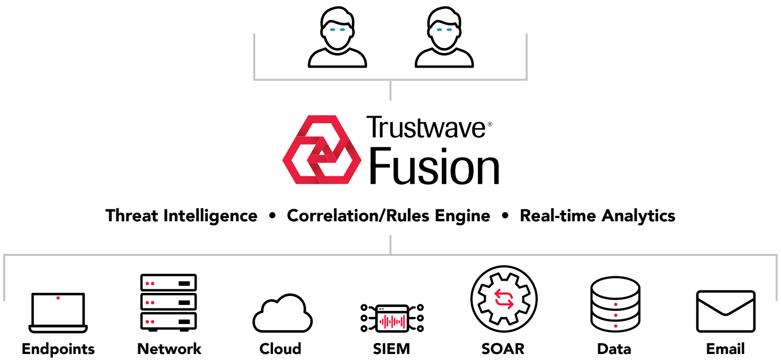
RELENTLESS THREAT ERADICATION WITH WORLD-CLASS INTELLIGENCE AND EXPERTISE

Benefits

- Value on Day 1 with agile onboarding
- Highly-available, cloud platform with worldwide points of presence
- Effective and timely, 24x7 threat detection
- Proven threat hunting capability
- Automation-enabled, expert response
- Support for hybrid operation
- Analyst-recognized service delivery excellence

Threat actors continue to develop sophisticated attacks that are increasingly difficult to detect. Meanwhile, security operations teams struggle to detect threats in a timely manner and respond effectively, given increasing IT environment complexity and limited security resources.

Trustwave provides Managed Detection and Response services, powered with our proven Trustwave Fusion platform and best-in-class Trustwave SpiderLabs® threat intelligence and expertise. Trustwave's field-proven service excellence and analyst-lauded approach drives consistent and continuous outcomes.



Trustwave Fusion
Threat Intelligence • Correlation/Rules Engine • Real-time Analytics
Endpoints
Network
Cloud
SIEM
SOAR
Data
Email

Trustwave Fusion, our cloud-based Extended Detection and Response (XDR) platform provides rich API integrations to your environment to drive fast and effective detection and response outcomes. Built-in Security Orchestration, Automation and Response (SOAR) functionality enables us to enrich environment telemetry with cyberthreat intelligence, and sync and resolve findings on your systems.

Focus on the Data That Matters

Many organizations find that they have too many security tools generating too many alerts. Trustwave Fusion connects your environment to our high-capacity, streaming detection and response platform. We focus on cloud-based connection that pulls in environment telemetry from your endpoints, networks, clouds and system logs give you more usable insights from your existing security tools.

World Class People and Processes

Expertise matters when it comes to evaluating the threats and findings, making decisions, performing investigations, and doing this consistently for a predictable service outcome. Armed with hundreds of annual training hours and seasoned by hundreds of thousands of monthly investigations, our skilled practitioners understand the threats and help you make fast, accurate decisions on responses to take.

Our investigators have access to the renowned global Trustwave SpiderLabs® team for further context and research on indicators of compromise, malware and up-to-the-minute threat intelligence.

Real-Time Monitoring and Human-Led Threat Hunting

Trustwave provides real-time, 24x7 monitoring, as well as advanced threat detection using your environment telemetry along with our proprietary threat intelligence and hypothesis-driven, human-led threat hunting.

SpiderLabs threat hunters leverage our proprietary threat hunting platform to look for suspected, but hidden threats. Our elite threat hunting team has extensive and highly specialized skillsets and a keen understanding of the tactics, techniques and procedures used by malicious actors.

Rapid Automated Response – Driven by Clients

We work with you to understand your specific needs and establish 'rules of the road' to inform how we respond. These protocols enable our skilled analysts to make fast and effective response decisions, based on your business context.

Leveraging our integrations to your environment through the Trustwave Fusion platform, we contextualize threats using your environment telemetry and our threat intelligence. Trustwave Fusion enables threat containment actions on endpoints, clouds, networks and other supported technologies, while our analysts investigate the threat.

Continuous Collaboration and Transparency

We are an open book, unwavering in our approach to drive better outcomes with you through our service delivery and platform. As part of the service, each client is assigned a named client success manager who will set up a monthly review cadence to discuss topics like support tickets, escalations, and new requests to help ensure service excellence.

Collaborate in real-time via the Trustwave Fusion platform on your browser or mobile. See what our analysts see and access all the data that is collected. Ticket and chat functions are integrated into findings so that you can communicate and make changes in a way that's most convenient for you.

Managed Detection and Response Services

SERVICE ELEMENTS	ESSENTIALS	ADVANCED
	Detect and contain threats before they compromise the larger IT environment	Expand coverage with continuous threat hunting and advanced response actions
Trustwave Fusion out-of-box rules and integrations and 24x7 platform access	●	●
24x7 global threat monitoring and incident response coverage	●	●
Guided remediation	●	●
SOAR-enabled threat containment	●	●
SpiderLabs analyst-based remote incident response		●
SpiderLabs proactive and continual threat hunting		●
Assigned client success manager (monthly review)	●	●

Extend Your Security Operations Center Capabilities

For clients with an existing SIEM, Trustwave Co-Managed Security Operations Center (SOC) services can help you get the most out of your investment, expand your team's capacity and extend the detection and response capabilities of your cyberthreat operations. We offer a comprehensive solution that maximizes SIEM ROI with proven use cases, mature SIEM management and 24x7 expert threat monitoring.

Trustwave® SpiderLabs®

Our investigators have access to our renowned global SpiderLabs team for further context and research on indicators of compromise, malware and up-to-the-minute threat intelligence. Trustwave SpiderLabs is a world-renowned team of security researchers, ethical hackers, forensics investigators and responders. Cyber threat analysts from law enforcement and military backgrounds with expertise tracking nation-state and professional criminal threat actor's offensive campaigns. Areas of expertise include:

- Security research
- Threat hunting
- Incident response
- Forensic research
- Malware reverse engineering

Trustwave®

www.trustwave.com

Copyright © 2021 Trustwave Holdings, Inc.