Trustwave®
Government Solutions

SERVICES OVERVIEW

Trustwave Managed Threat Detection & Response Services

ERADICATE THREATS. ALL DAY. EVERY DAY.

Benefits

- Detect and eradicate threats
- Extend your team with elite cybersecurity expertise
- Consolidate threat visibility across endpoints, networks, databases and clouds
- Strengthen your security posture
- Recognize value on existing security investments

Threat actors continue to develop malicious, ingenious tricks and techniques to stay one step ahead of security systems and response specialists. In addition to threat actors, the complexity of the digital landscape is a challenge security teams are facing. Choosing a partner to help you with detecting, investigating, and responding to threats doesn't have to be complex.

What we do is different

Your job is to keep your business moving. Our job is to stop threats so that your business can keep moving. Period.

We embed our elite expertise and proven threat lifecycle capabilities into your security program and environment to help you identify threats, investigate the depth and scope of those threats, and help you respond by taking containment actions.

What you get

Leveraging a global network of 24x7x365 global Security Operations Centers (SOCs), experienced Trustwave security analysts conduct advanced threat detection, analysis, investigation and response based on your organization's security needs.

Threat detection and response in the palm of your hands

Orchestrate detection and response across endpoints, networks, databases and clouds from a computer, tablet or mobile phone with the **Trustwave Fusion platform**.

- The Trustwave Fusion platform integrates and normalizes data from your disparate security tools to deliver you a panoramic view across your eco-system
- Out-of-the-box integration with 700+ data streams allows you to combine multiple detection sources, leverage existing investments and integrate with best-in-class security technologies
- Connects your eco-system, whether on-premise or in the cloud, to advanced analytics, actionable threat intelligence and a pool of elite security specialists
- Consolidates alerts, tickets and reports in one location

Trustwave® Fusion

Trustwave® SpiderLabs®

Top-notch security professionals

Our services leverage the collective experience of an elite group of top-notch security experts recruited from top companies and programs. We employ best practices for staff retainment and deeply invest in ongoing cybersecurity skills development.

- The Trustwave SpiderLabs team includes 250+ threat hunters, ethical hackers, investigators and researchers with a large depth and breadth of expertise in various security domains
- Senior staff members located across 9 Global Security Operations Centers (SOCs)
- Trustwave SpiderLabs Digital Forensics & Incident Response (DFIR) team provides multifaceted reactive emergency response and proactive incident readiness services

Proprietary threat intelligence capabilities

The Trustwave SpiderLabs team of security researchers monitor the global threat landscape to identify threats and vulnerabilities. They then develop, test and release detection rules that are applied to the telemetry you send us via the Trustwave Fusion platform, for deeper detections, investigations and resolutions.

- Comprehensive library of Trustwave SpiderLabs original research, a large incognito clientele data set, partner intelligence and open-source intelligence
- Tens of millions of new records added each week so you can stay ahead with the evolving threat landscape
- **Microsoft Active Protections Program (MAPP) Threat Indicator Top Contributor**

Human-led threat hunting

We don't wait for technology to find something – we find it first. Artificial intelligence alone is not a replacement for human expertise and experience. Our layered detection and investigation process includes hypothesis driven, intel fueled, technology enabled, and human conducted continuous and proactive threat hunting by the Trustwave SpiderLabs team.

- Blend your data with threat intelligence and human expertise to detect and understand threats
- Identify insider threat actors, unpatched vulnerabilities, network or software misconfigurations, and advanced persistent threats dwelling in your network
- With our unique customer Point-of-Delivery (POD) model we pursue threats before they pursue you by leveraging threat intelligence gleaned from similar customers like you

Containment and remediation on your behalf

We offer more than guidance. With the network support of nine global security operations centers throughout the world, we offer the ability to take response actions on your behalf, leveraging security controls to contain and eradicate threats.

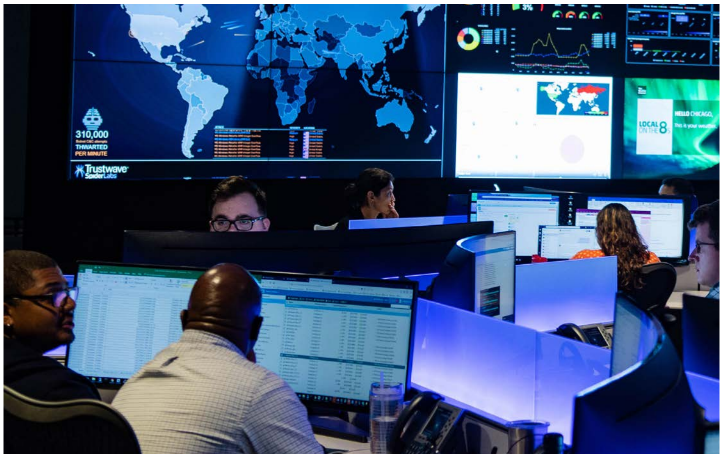
- Remediation actions include process/network blocking, file removal, device quarantine and more
- Managed remote digital forensics and incident response capabilities

Optimize and advance your security program.

Consultants and advisors help you optimize your security program and technology investments with your changing needs and the evolving threat landscape.

During onboarding, we consult with you on how to optimize existing security controls and tools in your environment for maximum protection and optimal threat detection and response. We also assist you with managing security controls, in addition to monitoring and using them.

- An available Information Security Advisor provides a named point of contact for additional content and security guidance
- The Trustwave Threat Detection and Response consulting team works with customers to solve security challenges through advisory, transformation, and operations enablement
- The Point of Delivery (POD) model allows you to leverage relationships with a virtual team within Trustwave to ensure industry specific expertise is applied to your environment



Flexible Managed Threat Detection and Response Services

Our customer-centric approach is to work with you to focus on the use cases that drive the best ability to detect and respond to threats. We'll help you choose the level of service that's right for your organization, with the flexibility to expand as your needs change.

LEVEL OF SERVICE	MANAGED DETECTION	MANAGED DETECTION & RESPONSE
Essential	Provides target automated data collection & analysis findings, provided by expert Trustwave security analysts, in a daily review.	Provides 24x7 technology-based automated root cause analysis, investigation, and response to protect your environment against advanced threats.
Complete	Provides 24x7x365 security threat monitoring, human-led investigation and notification by analysts in the nine global Trustwave Security Operations Centers (SOCs).	Provides 24x7x365 advanced threat detection and investigation with containment & remediation actions on your behalf. MDR Complete provides full digital forensics investigations, proactive and continuous threat hunting, and managed IR capabilities that allow DFIR response to target cyber-attacks in minutes.

Have an existing Security Operations Center?

No problem. With Trustwave Co-Managed Security Operations Center (SOC) services, Trustwave can integrate with your existing Security Information and Event Management (SIEM) system in order to extend your team's capacity.

- Extend or maintain continuity of your team's ability to monitor, investigate and respond to attacker activity with Trustwave Managed Detection, working as a part of your SOC
- Maintain the health, availability and function of SIEM system by leveraging Trustwave's SIEM Management services
- Receive flexibility in integration, teaming and contracting

Need to address stringent U.S. government security and compliance requirements?

No problem. Trustwave Managed Threat Detection and Response services can be delivered via the Trustwave Fusion platform hosted on AWS GovCloud. This flexible delivery model allows us to integrate with your existing security environment to detect and respond to threats, and ensure your organization meets data sovereignty requirements.

- Extend your team with elite cybersecurity experts who have U.S. citizenship
- Services delivered from our U.S. based Security Operations Centers
- Accelerate time to meet Cybersecurity Maturity Model Certification (CMMC) requirements

Service Highlights

- Out-of-the-box integration with 700+ data streams
- Best-in-class integrations with leading security technology vendors
- 250+ threat hunters, ethical hackers, investigators and researchers
- 9 Global Security Operations Centers with senior staff available 24x7x365
- Containment and remediation on your behalf
- Comprehensive, global threat intelligence library
- Supports multiple customer communication methods – web, email, phone, mobile application
- Continuous and Proactive Threat hunting led by Trustwave SpiderLabs threat hunters

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

Trustwave®
Government Solutions

For more information: www.trustwave.com