Trustwave® | Microsoft

Trustwave Managed Detection and Response Services for Microsoft

DEFEND WITH CONFIDENCE. RESPOND WITH PRECISION.

Benefits

- Eliminate active threats with 24×7 global coverage
- Augment your team with industry-leading Microsoft experts
- Increase ROI from your existing Microsoft ecosystem
- One of the first Microsoft MSSP Partner to offer MDR Services for Microsoft Defender for Endpoint

Winner
Top Managed SOC
2021 Microsoft Security 20/20 Partner Award

Trustwave Managed Detection and Response (MDR) is an industry-leading rapid threat detection and response service. Our experts identify, investigate, and eliminate cyber threats, mitigating risk to your business. We leverage your existing Microsoft security tools and infrastructure to maximize your returns and help you realize the full power of your investments.

Improve your Threat Visibility

It starts with improving your threat visibility. Trustwave connects your Microsoft ecosystem along with your extended infrastructure to ingest high-value telemetry which enables us to expand your visibility to potential threats across your Microsoft environment. This aggregation gives you and our security engineers part of the context we need to eliminate an active threat and stop an attacker from lateral movement.

Detect and Respond Faster

Armed with greater visibility, infused with Trustwave threat intelligence, and context from your Microsoft ecosystem and security infrastructure, Trustwave detects and responds faster than anyone else. The telemetry we ingest, analyze, and enrich with our curated threat intelligence, and contextualize through the Trustwave Fusion platform, allows us to monitor your environment for threats in real-time while significantly eliminating unwanted noise.

Once a threat or anomalous behavior is detected, our team jumps into action to triage, contain, and investigate. We eliminate all the false-positives and what's left are confirmed threats that need your immediate action. This helps you to improve your security team's productivity and eliminate the wasted time investigating alert noise and false-positives from all your security tools—removing alert fatigue for in-house team. (case: "12 million events per day... into 12 priority incidents")

Most providers leave it up to you to respond. At Trustwave, an incident response action can be taken by your team or ours with your predefined instructions (response protocols) that we integrate into our SOC workflow. In the event of a breach, every second counts, that's why Trustwave SpiderLabs Remote Incident Response experts are available to deploy immediately.

Boost your Security Posture

Trustwave's Microsoft certified experts instantly become a valuable extension of your team to boost your security posture. In addition to 24×7 detection and response, our elite team of cyber experts from SpiderLabs are actively and continuously tracking sophisticated threats and threat groups to dissect the tactics, techniques, and procedures (TTPs) used by these groups to help us fortify your defenses.

The cumulative knowledge from ongoing threat research, global client engagements, and curated threat intelligence is seamlessly integrated into the Trustwave MDR service for Microsoft to protect your organization from the latest cyberthreats—coming from inside or outside your organization.
(case: "We weren't expecting... to discover that a member of our own team was spreading malware")

Moreover, unlike other MDR providers, Trustwave has a comprehensive portfolio of cyber experts and services ready to take your Microsoft investment and cybersecurity program to the next level.

Future-Proof Your Microsoft Investment

We're committed to Microsoft's forward-facing roadmaps to help you maximize your Microsoft investment well into the future.

Trustwave MDR Service for Microsoft

Service Features	MDR	MDR Elite
24/7 Threat Detection, Prioritization, and Investigation	●	●
Threat Response	●	●
Threat Hunting and Malware Reverse Engineering	●	●
Unlimited EDR Security Telemetry	●	●
Client Success Manager	●	●
Security Colony Subscription	●	●
Named SpiderLabs Threat Expert		●
SpiderLabs Remote Incident Response		●
Service Levels for MTTA and MTTR		●
Trustwave Fusion Platform	●	●
Trustwave Fusion Mobile App	●	●

Trustwave Fusion Platform

The Trustwave Fusion platform is a cloud-native threat detection and response platform, augmented by security orchestration, automation, and response (SOAR). Its primary mission is to ingest high-value telemetry and enrich it with context and threat intelligence to detect threats in near real-time. Additionally, the Trustwave Fusion platform serves as a security operations workflow engine for security operations teams during threat investigations and response activities. Via the web portal or mobile app, users can see what's happening in real-time, participate in incident investigations, chat with experts, create a ticket, and view custom reports. Take incident response actions anywhere and anytime.

Security Colony

It's likely that most of the challenges you are facing, others have faced before you. Trustwave Security Colony (included) will give you access to a library of knowledge and on-demand resources. These resources include the result of years of our team's consulting output from real client projects across thousands of companies. Cut down on the time and cost of solving common cyber security problems.

Trustwave SpiderLabs

Trustwave SpiderLabs is a world-renowned team of security researchers, ethical hackers, forensics investigators and responders. Cyber threat analysts with expertise tracking nation-state and professional criminal threat actor's offensive campaigns.
Discover how this team of elite cyber experts work to protect you: Trustwave SpiderLabs

Rapid Time-to-Value

- No one in industry is faster to value
- Seconds to ingest data, outcomes produced in 10 min or less
- Onboard in less than 10 days, the right way

Faster Response Times

- No one in the industry responds faster*
- Personalized MTTR of less than 30 minutes
- Client defined response protocol fully integrated into SOC workflows and platform

Unrivaled Threat Intelligence

- Billions of records in global threat intelligence database
- Only provider with 6 Global Cyber Threat Research Centers
- Decades of threat intelligence leadership and a team prolific in finding threats and vulnerabilities

Dedicated Cyber Success Team

- A dedicated named resource with you for the life of the service
- We detect what others can't with intimate knowledge of your environment for better tuning, faster and more efficient response

*based on review of competitors' publicly stated MTTR specifications

Member of
Microsoft Intelligent Security Association

Microsoft

Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Security
Specialist
Threat Protection

Trustwave®

www.trustwave.com