Trustwave® | Microsoft

DATA SHEET

# Trustwave Threat Detection & Response Services for Microsoft

EXTEND THREAT DETECTION AND RESPONSE ACROSS YOUR MICROSOFT ENVIRONMENT.

## Benefits

- Detect and eradicate threats
- Extend your team with elite cybersecurity expertise
- Consolidate threat visibility across endpoints, networks, databases and clouds in your Microsoft environment
- Strengthen your security posture
- Recognize value from your Microsoft 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 as more security solutions operate in silos. Trustwave removes the complexity and burden of threat detection and response with a full portfolio of solutions that work with your Microsoft investments to fight cybercrime, protect data and reduce risk.

## 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.

Trustwave Managed Threat Detection and Response Services 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 we offer

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.

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 the via Trustwave Fusion platform, for deeper detections, investigations and resolutions.

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.

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.

**Learn More:** Trustwave Managed Threat Detection & Response Services

## How We Do It

### Co-Managed Security Operations Center (SOC) Services for Microsoft Azure Sentinel

With Trustwave Co-Managed Security Operations Center (SOC) services, Trustwave can integrate with Microsoft Azure Sentinel in order to extend your team's capacity.

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

**Learn More:** Trustwave Co-Managed Security Operations Services for Microsoft Azure Sentinel

### Managed Detection and Response with Microsoft Defender for Endpoints

Trustwave offers two levels of the Managed Detection and Response (MDR) Service with Microsoft Defender for Endpoints – MDR Essential and MDR Complete.

Both levels deliver 24x7 monitoring and notification, incident response and remediation. The Complete level adds a higher level of data forensics and investigation response that includes industry leading proactive threat hunting by Trustwave SpiderLabs.

**Learn More:** Trustwave MDR Services for Microsoft Defender for Endpoints

### Technology Advisory, Enablement and Configuration

The Trustwave Threat Detection and Response Consulting team provides services to help plan, build and run a successful threat protection program utilizing Microsoft Azure Sentinel and Microsoft Defender for Endpoints as platforms integrated with the Trustwave Fusion platform and services. Services include:

- Transitional project consulting and provisioning to plan, build, and/or optimize your investments in Microsoft Azure Sentinel and/or Microsoft Defender for Endpoints to stead state
- Infrastructure and endpoint services for Microsoft Defender for Endpoints policy review and endpoint response use case guidance

Customers can also leverage an available Trustwave Information Security Advisor (ISA) who provides guidance in maturing system and process capabilities. The ISA also provides ongoing policy and rule monitoring for Microsoft Azure Sentinel and Microsoft Defender for Endpoints.

## Amplify Threat Detection & Response

### Trustwave Email Security for Office 365

Combining the proprietary defense filters in Trustwave Secure Email Gateway with the built-in security protections in Office 365 delivers unprecedented detection and extended protection in real time.

Trustwave Secure Email Gateway is the only email gateway in the market that is integrated with Azure Rights Management Services.

**Learn More:** Trustwave Email Security for Office 365

### Secure Sensitive Data in Microsoft Azure-hosted Databases

Trustwave Database Security Solutions provide proactive database security to help you get ahead of risk, respond intelligently and harden your attack surface.

Gain deep insights into vulnerabilities contained in your Azure-hosted databases as well as remediation guidance

**Trustwave AppDetectivePRO** and **DbProtect** support MySQL and PostgreSQL deployed in Azure and on-premise, Azure SQL DB service, and Microsoft SQL Server installed in Azure or on-premise, as well as all the leading database products.

**Learn More:** Trustwave Database Security Solutions

## Trustwave Partnership with Microsoft

Trustwave launched Microsoft as a Platinum Technology Partner in 2019, committing to building market-leading Threat Detection & Response offerings that leverage and support the Microsoft set of security solutions. In addition to building market-leading offers with Microsoft solutions, Trustwave is:

- A registered Microsoft solution provider for Managed Detection and Response (MDR)
- One of Microsoft's first Managed Security Services Provider (MSSP) partners for Microsoft Azure Sentinel
- A member of the Microsoft Intelligent Security Association (MISA)
- Featured by Microsoft for our Microsoft Graph Security partner solutions

For years, Trustwave has also been an active member of one of the industry's leading partnership programs, the Microsoft Active Protection Program (MAPP). In 2019, Trustwave was awarded the "Threat Indicator Top Contributor" award from Microsoft for contributions of threat indicators.

Trustwave®

For more information: www.trustwave.com



TDRM-1020