



Trustwave MXDR for Microsoft

UNIFIED SECURITY OPERATIONS TO STOP MODERN THREATS

Benefits

- Maximize value from your Microsoft investments
- Eliminate active threats 24x7, globally
- Disrupt complex threats across the attack chain
- Enhance your team Microsoft Security Advisors
- Accelerate productivity of your security operations team
- Reduce complexity and boost security posture
Unlock the full value of Microsoft Security
- De-risk transition with rapid time-to-value
- Layer detection with SpiderLabs unique threat intelligence & research
- Accelerate security outcomes with a recognized cybersecurity leader

The landscape of cybercrime has evolved dramatically, presenting significant challenges for cybersecurity. A decade ago, cybercrime's economic impact was estimated in the low billions, comparable to the global illicit drug trade. Today, cybercrime is a USD \$8 trillion industry, the third largest economy in the world, growing at an alarming rate of 15% annually. As a cybersecurity leader, this may not be a surprise to you.

To defend our organizations, we deploy varying types of security technologies. However, modern cyber-attacks often involve intricate kill chains made up of numerous low-fidelity signals. Correlating these alerts across siloed solutions to gain an enterprise-wide threat view is challenging. This issue is compounded by legacy security tools which were not designed for today's hybrid environments, leading to significant visibility and coverage gaps.

Additionally, the high demand for skilled security professionals often leaves SOCs overwhelmed with a flood of alerts and a backlog of incidents that need investigation and remediation. SecOps teams grapple with disjointed security solutions, lacking the integration, intelligence, and expertise necessary for efficient incident resolution.

Modern Tools for Modern Threats - Microsoft Defender XDR & Microsoft Sentinel

Integrated security technologies from Microsoft Security suite are essential to address these challenges and keep up with the advancement and funding of cyber threat groups.

Microsoft Defender XDR is a unified enterprise defense suite that coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications. This integration provides robust protection against sophisticated attack scenarios in concert with Microsoft Sentinel (SIEM).

By leveraging various Microsoft Security products, Microsoft Defender XDR enables security teams to piece together threat signals to determine the full scope and impact of threats. This integrated solution reveals how threats enter the environment, what they affect, and their current impact.

Enhanced with Trustwave Managed XDR (MXDR)

Having the right modern tools is only part of the equation. The other part that's needed is high-quality experts, proven SecOps process, dynamic content, and relevant adversarial threat intelligence to put organizations ahead of today's sophisticated threats.

Trustwave MXDR for Microsoft services offer 24/7 global security operations with extended detection, investigation, threat hunts, and response across Microsoft Security products:

- Microsoft Sentinel
- Microsoft Defender XDR
 - › Defender for Endpoints
 - › Defender for Identity
 - › Defender for Cloud Apps
 - › Defender for Office 365
- Copilot for Security
- Microsoft Native & External Data Sources

Trustwave MXDR for Microsoft service integrates with your deployment of Microsoft Sentinel and the Microsoft Defender XDR suite. This integration enables Trustwave to take native response actions in Defender XDR for swift and effective response to security incidents across your digital environment.

Trustwave's thorough investigation process and effective response actions aim to disrupt complex threats across the attack chain soon after detection. Trustwave is also the first in the industry to offer accelerated investigation and response capabilities within our client's deployment of Microsoft Copilot for Security for faster resolution of threats.

Trustwave Microsoft Security Advisors

Trustwave MXDR for Microsoft services include preventative configurations to maximize your organization's defensive posture and minimize overall threat exposure leveraging the Defender XDR's proactive capabilities.

Additionally, Trustwave Microsoft Security Advisors (MSA) will enhance your team and provide co-management activities—continuous technical advisory, preventative configuration reviews, dynamic emerging threat content, customization, and more—to maintain an optimized deployment. The MSA also conducts regular Microsoft Security & Exposure Score reviews to help you prioritize your team and mature your overall security posture.

Trustwave MXDR for Microsoft offers a comprehensive approach to your cybersecurity mission, providing your organization with the expertise required to actively combat the modern cyber threat.

Features:

- 24/7 global threat monitoring, threat hunting, investigation, and response
- Effective, native Defender XDR response to disrupt complex threats
- Layered threat detection with SpiderLabs threat intelligence
- SpiderLabs threat research & reverse engineering
- Proven preventative configurations and continuous tuning
- Trustwave Microsoft Security Advisors
- Microsoft Security & Exposure Score reviews
- Defender XDR Security Assessments

Unlock the full power of Microsoft Security with Trustwave, and maximize your investment, reduce complexity, and boost your SecOps team's productivity with a unified stance.



Your Cybersecurity Partner

We understand the importance of rapid time-to-value while mitigating transition risks. Trustwave will be your objective advocate for the right technology solutions within your existing heterogeneous and homogenous environments, ensuring seamless integration and interoperability.

If you have a Microsoft license, both Microsoft Defender XDR and Microsoft Sentinel may already be available to you as part of your security product entitlements. Trustwave can help you understand and unlock the full value of your security entitlements under any Microsoft license.

Let Trustwave be your trusted partner in securing your digital landscape, today and into the future. Learn more: www.trustwave.com

Microsoft Credentials & Certifications

Trustwave is endorsed and validated by Microsoft as a leading cybersecurity partner:

- Microsoft Verified MXDR Partner
- Microsoft Copilot for Security Partner
- Microsoft Intelligent Security Association (MISA) Member
- Certified Microsoft AI Cloud Solutions Partner
- Advanced Security Specialization Partner:
 - > Cloud Security
 - > Threat Protection



About Trustwave

Trustwave is a globally recognized cybersecurity leader that reduces cyber risk and fortifies organizations against disruptive and damaging cyber threats.

Trustwave's comprehensive offensive and defensive cybersecurity portfolio detects what others cannot, responds with greater speed and effectiveness, optimizes clients' cyber investments, and improves security resilience. Trusted by thousands of organizations worldwide, Trustwave leverages its world-class team of security consultants, threat hunters, researchers, and market-leading security operations platform to decrease the likelihood of attacks and minimize potential impact.

Trustwave is an analyst-recognized leader in managed detection and response (MDR), managed security services (MSS), cyber advisory, penetration testing, database security, and email security. The elite Trustwave SpiderLabs team provides industry-defining threat research, intelligence, and threat hunting, all of which are infused into Trustwave services and products to fortify cyber resilience in the age of inevitable cyber-attacks.