IBM Security X-Force Threat Management Services for Microsoft

Extend native Azure Sentinel and Microsoft Defender for Endpoint capabilities to transform hybrid security operations

Today, organizations must adapt to a rapidly expanding and complex security threat landscape. Whether it's growing on-premises and Azure environments, or taking advantage of multiple clouds, there is no longer a single perimeter to protect. Adding to the complexity, customers are leveraging disparate tools, workflows and controls across environments, resulting in a fragmented security posture and reduced visibility into the threat landscape. To keep pace with digital transformation, security must be programmatically woven into the fabric of business with a modern, open and unified approach across teams and environments.

IBM Security X-Force Threat Management (XFTM) Services with Azure Sentinel and Microsoft Defender for Endpoint transforms security operations, enabling intelligence-driven and agile security operations while augmenting cloud-native detection, investigation and response capabilities. IBM Security patented AI and alert dispositioning models enhance cloud-native detection capabilities, while enhancing investigation and response with security orchestration, automation and response (SOAR) capabilities. As a Gold Certified Microsoft partner and a

Highlights

- **Hybrid and multicloud visibility**
  Integrate Azure Sentinel and Microsoft Defender for Endpoint with enterprise security operations and workflows to quickly identify and react threats
- **Proactive threat hunting**
  Operationalize the MITRE ATT&CK framework using IBM Security proprietary techniques and tactics combined with Microsoft threat intelligence
- **Accelerate time to remediation**
  Refine the handling of alerts by force-multiplying cloud native detection and response capabilities with IBM Security AI machine learning and SOAR capabilities
- **Extend your security team**
  Team with our trusted security advisors to improve your threat management posture and combat advanced threats

recognized market leader by analysts for our threat management capabilities, our services align to the NIST framework and provide end-to-end visibility and actionable insights across Azure hybrid and multicloud environments.

End-to-end threat management designed for cloud-speed

XFTM integrates offensive testing, artificial intelligence and incident response into a comprehensive program offering consulting and managed services for the native Azure stack

Use cases

IBM Security simplifies the process of achieving a comprehensive, next-generation security approach:

Detect cloud misconfigurations: Protect against potential threats by detecting and resolving misconfigurations and policy drift

Near real-time security analytics: Accelerate and enhance the accuracy of threat detection across users, endpoints, and networks

Offensive testing: Uncover known and unknown vulnerabilities to harden your defenses and protect your most critical assets

Address regulatory requirements: Enable continuous compliance and proactively manage security risk with tailored and proven frameworks

A global retailer success story

Customer Challenges

- Recent merger and acquisition leading to process inefficiencies
- Safeguarding migration to Azure
- Designing and building a secure landing zone
- Aligning native controls with enterprise security operations
- Ensuring compliance to new regulatory requirements

Solution

- Designed architecture and deployed Azure native security controls
- 24/7 managed security and offensive security services
- Integrated with on-premises, legacy Security Information and Events Manager (SIEM) deployment to provide a unified workflow
- Comprehensive threat management solution with Azure Sentinel and Microsoft Defender for Endpoint

Outcome

- Shared insights and cross-functional workflow efficiencies
- Continuous compliance enabled via Azure Security Center
- Faster threat response with Microsoft Defender for Endpoint
- Improved threat management by centralizing monitoring Azure Sentinel

Next steps

Learn about the Azure Threat Management Accelerator Offer
– www.ibm.com/security/partners/microsoft-azure

Call Sales
1-877-426-3774
Priority code: Security

Experiencing a cybersecurity issue, contact us!
US hotline: 1-888-241-9812 Global hotline: (+001) 312-212-8034

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development, and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM X-Force Threat Management Services for Azure Sentinel and Microsoft Defender for Endpoint please contact your IBM representative or IBM Business Partner, or visit the following website: www.ibm.com/security/partners/microsoft-azure