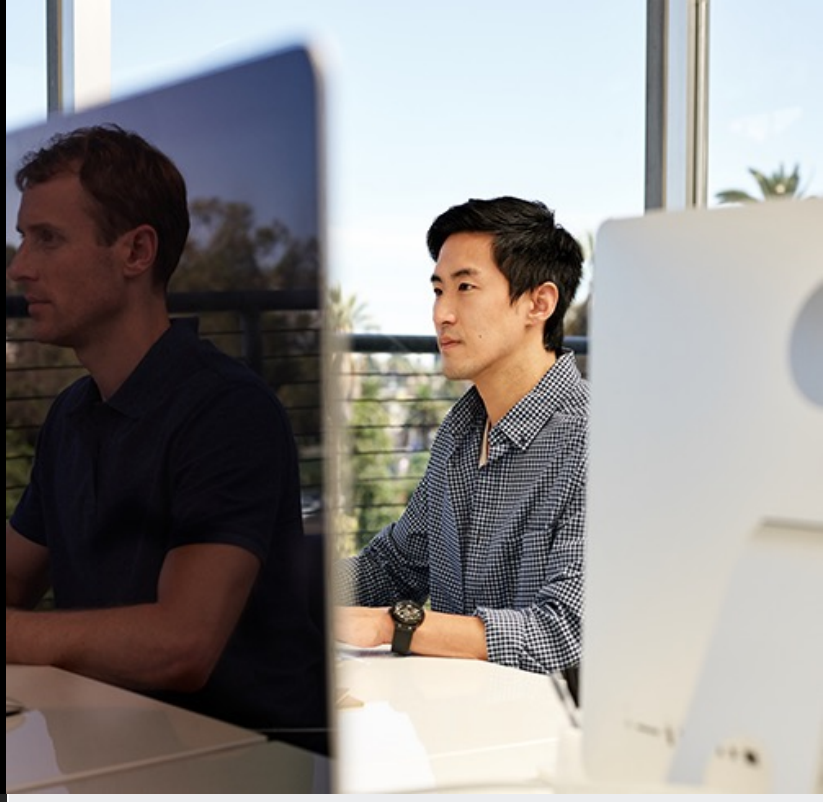
IBM Security

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



Can you relate to these security challenges in your hybrid cloud environment?

Siloed platforms

- Different geos on different detection platforms
- No common processes/governance creates a lack of visibility and stifled collaboration
- Lack of continuity driving up costs and causing inefficiencies

Information overload

- Moving to the cloud introduced the complexity of hybrid IT
- New vulnerabilities from an expanded attack surface
- Alert volume is a problem due to the increasing number of tools and device feeds

Coverage gaps

- Limited internal resources to optimize threat management
- Inability to provide 24/7 coverage due to budget constraints
- Struggling to attract and retain specialty skillsets like threat hunting

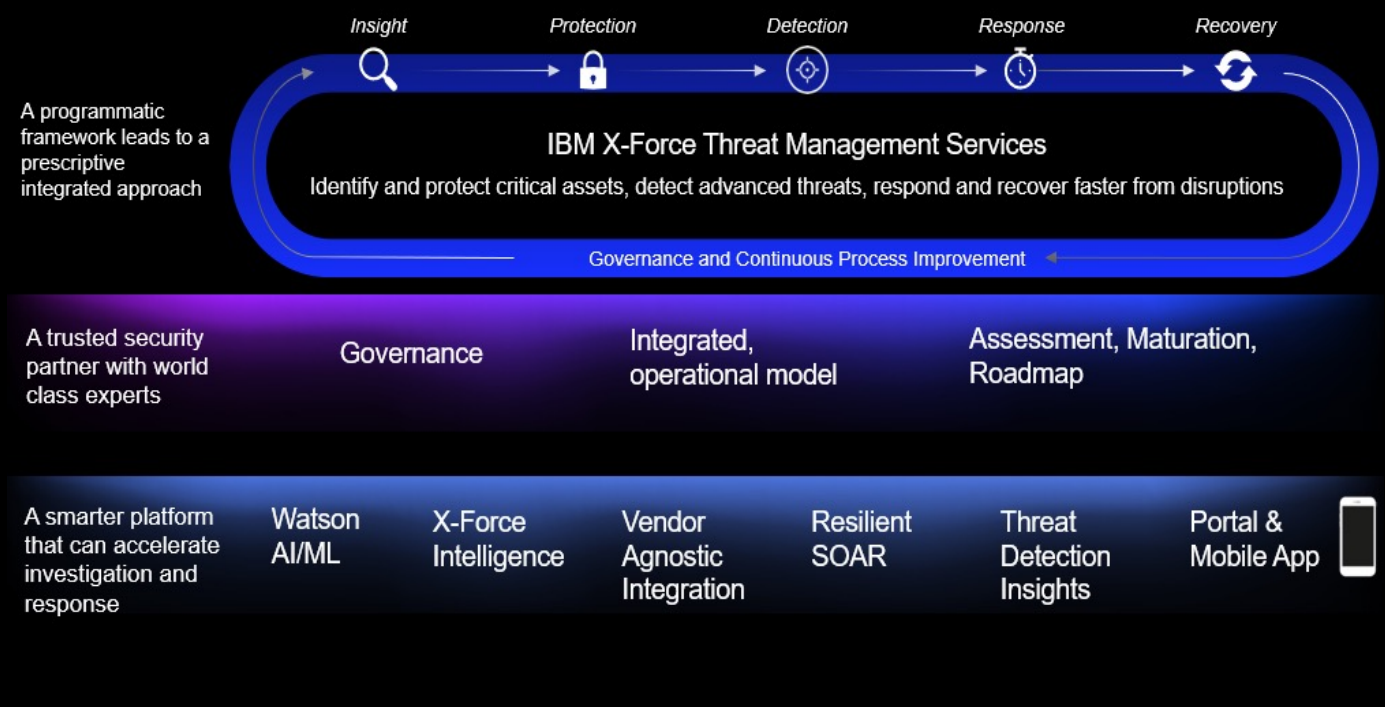
IBM

IBM Security can help you overcome those challenges

IBM Security Threat Management integrates offensive security services, full threat lifecycle management, as well as incidence response and intelligence services into a comprehensive, end-to-end program aligned to a security industry framework.

Highlights:

- **Hybrid and multi-cloud visibility:** Integrate Microsoft Sentinel and Microsoft Defender for Endpoint with enterprise security operations and workflows to quickly identify and react to 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 IBM's trusted security advisors to improve your threat management posture, and keep up with your enterprise's growing security needs



Member of Microsoft Intelligent Security Association

Gold Microsoft Partner

Success story – global retailer

Challenges they were facing

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

The solution

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

The outcomes

- 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 Microsoft Sentinel

Why IBM Security?

- One of the most advanced and integrated portfolios of enterprise security products and services. Supported by world-renowned IBM X-Force® research, it 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

Take a next step

Learn about IBM's Azure Threat Management Accelerator offer or schedule a consultation at this link.

If you're experiencing a cybersecurity issue, contact us!

- **US:** 1-888-241-9812
- **Global:** (+001) 312-212-8034

IBM **Security**