Azure Threat Management Accelerator

Today’s data breaches can result in significant cost, liabilities and damaged reputation.

$3.86M
Average cost of data breach\(^1\)

$150
Average cost per lost or stolen record\(^1\)

Improve your Azure security posture with a targeted threat management assessment from IBM

The Azure Threat Management Accelerator identifies gaps in your Azure hybrid multicloud security posture and provides recommendations that can improve your program across security operations, incident response, compliance and governance.

Our Azure Threat Management Accelerator will include a high-level review to address the following:

**Cloud Security Strategy**
- Azure and hybrid multicloud security strategy

**Security Operations**
- Incident Response Planning
- Threat Protection, Detection and Response
- Security Orchestration, Automation and Response (SOAR): Runbooks & Playbooks

**Governance and Compliance**
- Organizational Structure
- Policies and Procedures
- Compliance Requirements

\(^1\)2020 Cost of a Data Breach Report by Ponemon Institute, sponsored by IBM
Azure Threat Management Accelerator format and deliverables

The maturity assessment format is a virtual interactive session that is facilitated by an IBM Threat Management Consultant.

A typical maturity assessment session lasts 3 days to conduct the interviews, document findings and deliver a final report.

What to expect?

The workshop focuses on the security components critical for protecting your business workloads across hybrid multicloud security operations.

IBM leads a structured conversation to review the components of your Azure cloud infrastructure, performing a map/gap exercise about related security capabilities and documenting key observations and initial recommendations.

Key benefits

• The lessons learned will help you prioritize and align your cloud security strategy to business goals and enhance your visibility into your cloud security posture.

• You’ll receive a report that outlines the information captured, identifies areas for improvement, and identifies prioritized next steps to help enhance your cloud security posture. The report is considered client confidential.