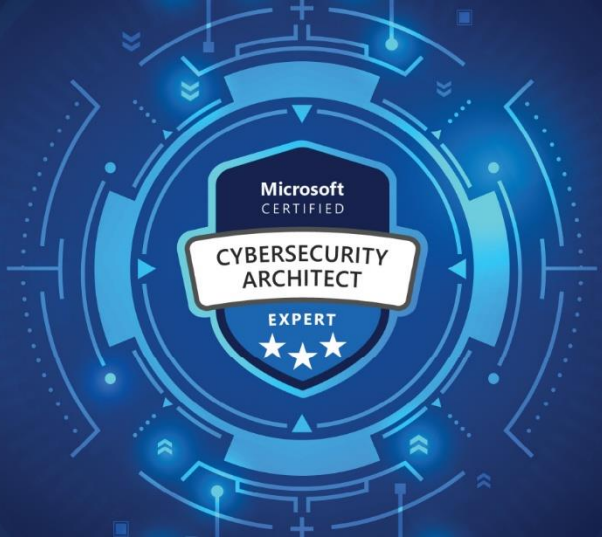
Microsoft

Case study scenario summary: Modernizing identity and data security



About the organization

- Woodgrove Bank is a US-based financial institution serving over 10 million customers.
- Offers services including consumer banking, investment advisory, and commercial lending.
- Employs thousands of staff and contractors.

Scenario & challenges

IT Infrastructure

Scenario

- Core banking systems are maintained on-premises, with customer portals hosted in Microsoft Azure and Microsoft 365
- Hybrid identity model synchronizes on-premises Active Directory with Microsoft Entra ID

Challenges

- Customer documents and regulatory reports are improperly stored in open-access team sites and guest-enabled collaboration spaces
- Past incidents of unintentional data sharing due to misplaced files in accessible collaboration spaces

Identity management

Scenario

- Microsoft Entra Guest Accounts enable partnerships with external entities
- Multi-factor authentication is consistently applied for all user and guest access

Challenges

- Independent provisioning by business units creates the risk of prolonged elevated privileges during role changes and terminations
- Guest permissions mirror internal user access, increasing security vulnerabilities
- Frequent MFA prompts and account lockouts generate excessive IT helpdesk calls

Security incidents

- Unusual sign-in patterns detected from unexpected locations with failed MFA attempts
- Investigation revealed dormant accounts executing elevated PowerShell commands and anomalous access to sensitive SharePoint files

Your role as a security architect

Analyse Woodgrove Bank's current security posture and design a resilient Zero Trust architecture that:

- Mitigates risks and enhances the overall security posture of Woodgrove Bank's hybrid environment