

# Defining the cloud security services for a UK bank

Creating the architecture and roadmap to enable the client to embed security into the Microsoft cloud platform

## Fast Facts

Internal only - Remove before using

Country	UK
Industry	Banking
Deal Size	£200,000
MS Tech Used	Azure Sentinel, Compliance Manager, Intelligent Security Graph, AD, PIM, Identity Protection, Security Center, Advisor, DDoS protection, API Manager, Key Vault, App Gateway, Advisor, API Manager, Firewall, Private Link, Threat Modelling Tool
MS Tech Used	Security Platform Playbook / Portfolio Rationalisation
PwC Contact(s)	Matthew Yee

## Client need

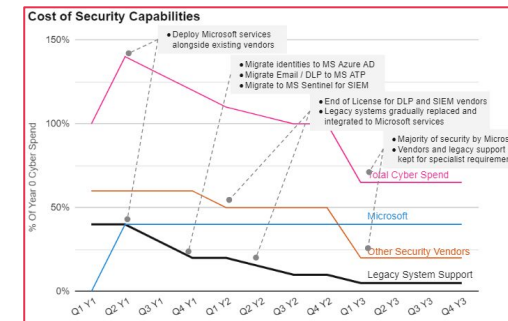
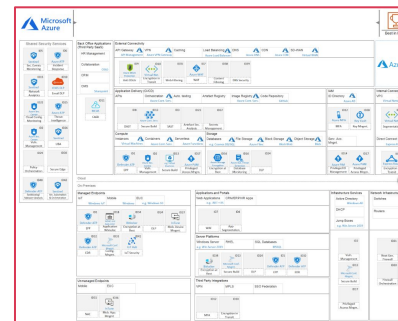
- Overhaul of processes which operated manually and introduced control challenges
- Strategic investment in data analytics and cloud technology to improve operational and cyber resilience
- Automation of processes to improve timeliness and reduce human error

## Solution delivered

- Redesigned operating model using Azure and PwC defined solutions
- Collaborated with business stakeholders, solutions architects and developers to design requirements embedded into their business and DevOps processes
- Assessed the current security capabilities against the available Azure capabilities to identify areas that could be improved and replaced

## Value unlocked

- Provided the roadmap of change to transition security services from on-premise operations to embedded services as part of the cloud estate
- Logical and physical security patterns defined for the organisation
- Key Microsoft Azure security services have been identified for configuration and additional consumption. The client will now use Microsoft for the majority of its security operations and management



Domains	Threat Detection & Response	Vulnerability Management	Identity & Access Management	Information Integrity & Protection	Infrastructure Security	Security Governance & Leadership	Security Risk & Compliance
Services	Incident Response, Event Monitored, Threat Intelligence	Penetration Testing, Code Security, Red Teaming	Security Lifecycle Mgt, Strong Authentication, Privileged Access Mgt	Data Loss Prevention, Data Discovery, Data Classification, Endpoint Protection	Network Security, Remote Access	Security Governance, Architecture & Blueprints	Policy & Standards, Risk Control Assessment, Supply Chain Risk Mgt
Technologies	SIEM, SOAR, IBA, EDR, TI, Malware Analysis	Config Mgt, Vuln scan, DAST, SAST, APT, g0terry, Code repository	MFA, Key Vault, ID Directory, Device Mgt, PAM, Secrets Mgt	Email DLP, Web DLP, CASB, Encryption, KMS, PKI, Secure FT	WAF, Cloud Protection, Change Management, Awareness & Training	Compliance Reporting	
Potential for Benefit	Low	Low	Moderate	High	High	High	High