

Six Degrees Secure Azure

Securing Azure with Cyber
Security Services and Microsoft
Cloud Adoption Framework

Damon Crawford & Tom Poole

March 12th 2020



6°

Adoption Challenges



Skills and Staffing



Complexity



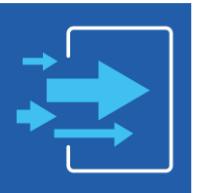
Service Level Agreements



Security



Lock-in



Migration and Architecture



Governance



Cost Management

6°

Securing Your Microsoft Azure Future



Capture
& Consult



Transform
& Harden



Manage
& Optimise



Defend
& Recover

6^o

Shared Responsibility Model

Responsibility Zones	SaaS	Paas	IaaS	On-prem	
Data governance & rights management	Customer or Partner	Customer or Partner	Customer or Partner	Customer or Partner	
Client endpoints	Customer or Partner	Customer or Partner	Customer or Partner	Customer or Partner	Always retained by customer
Account & access management	Customer or Partner	Customer or Partner	Customer or Partner	Customer or Partner	
Identity & directory infrastructure	Customer or Partner	Customer or Partner	Customer or Partner	Customer or Partner	
Application	Microsoft	Customer or Partner	Customer or Partner	Customer or Partner	Varies by service type
Network controls	Microsoft	Customer or Partner	Customer or Partner	Customer or Partner	
Operating system	Microsoft	Microsoft	Customer or Partner	Customer or Partner	
Physical hosts	Microsoft	Microsoft	Microsoft	Customer or Partner	
Physical network	Microsoft	Microsoft	Microsoft	Customer or Partner	Transfers to Microsoft
Physical datacentre	Microsoft	Microsoft	Microsoft	Customer or Partner	

Key:



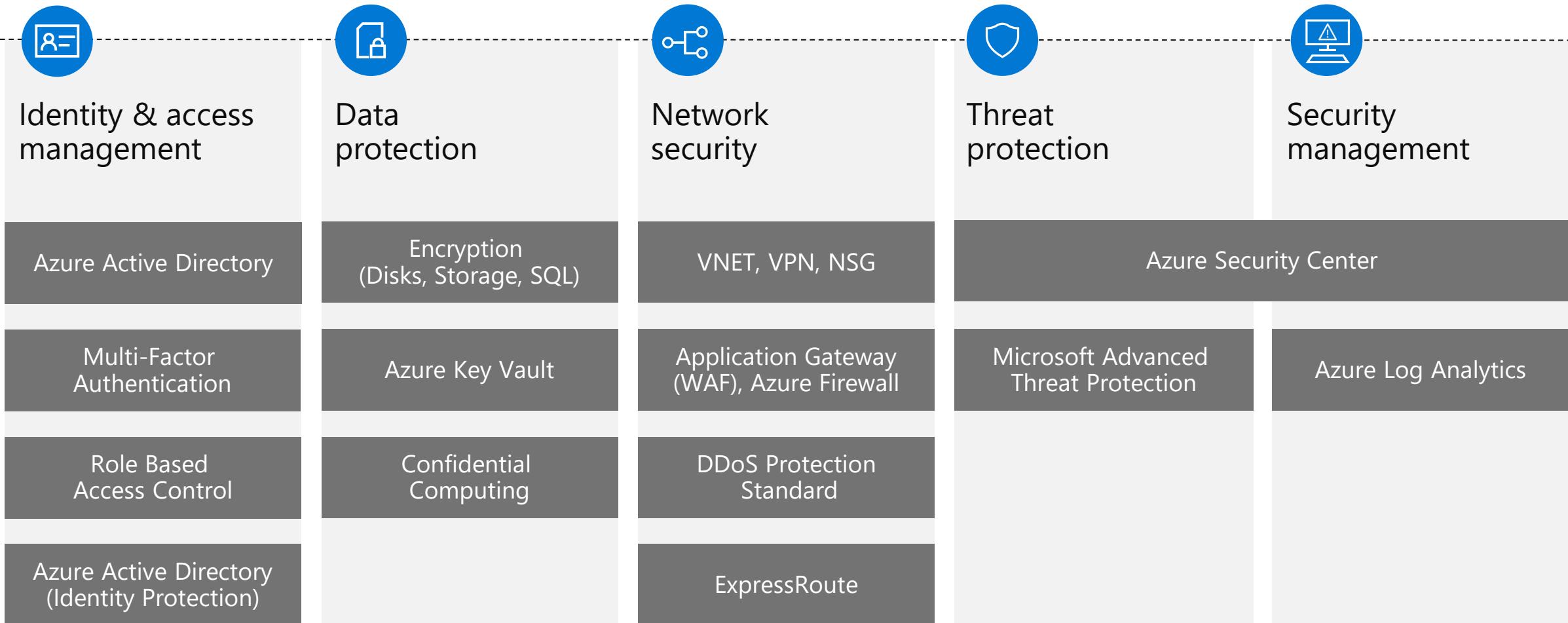
Microsoft



Customer or Partner

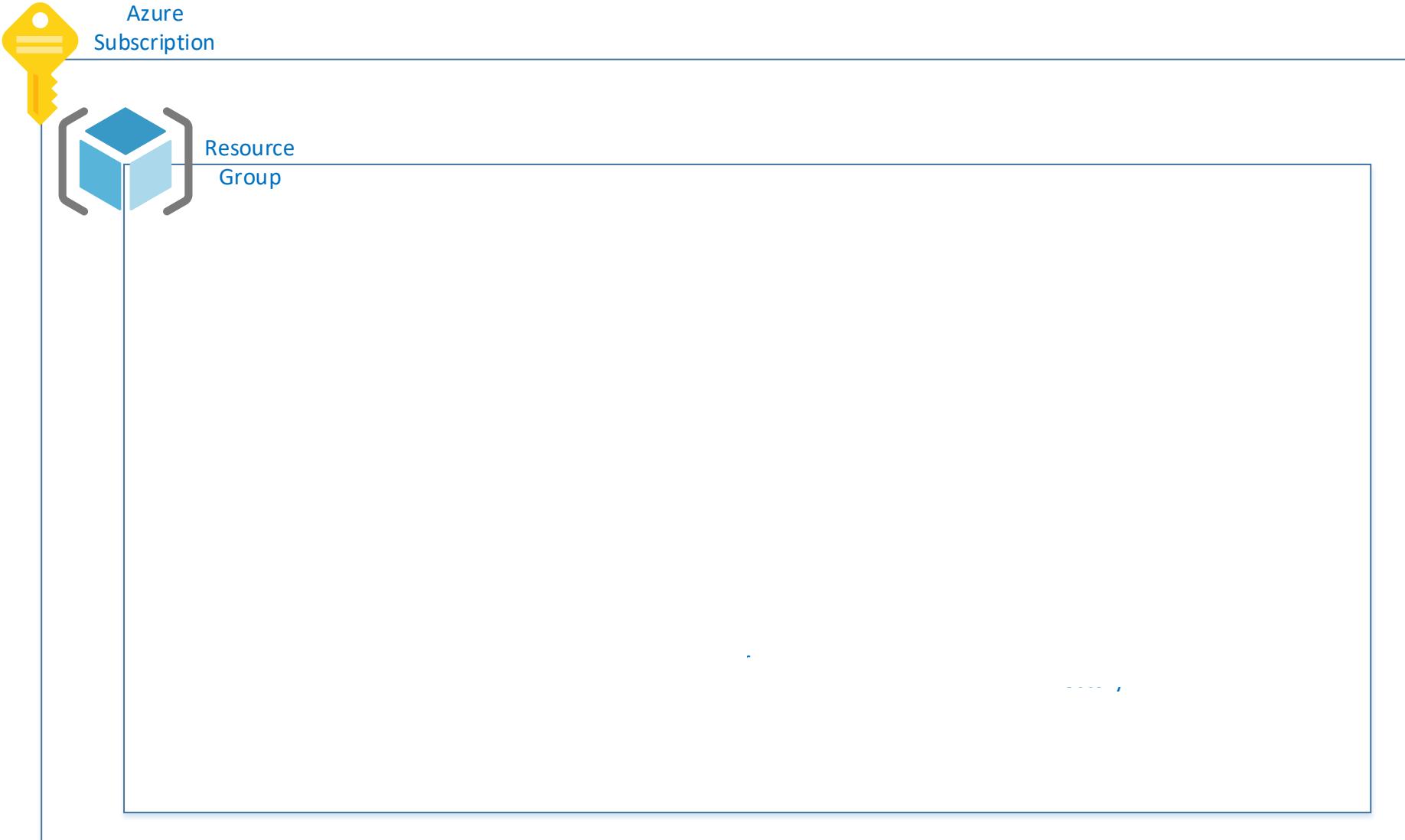
6°

Simplify Security with Azure





Blue Prints



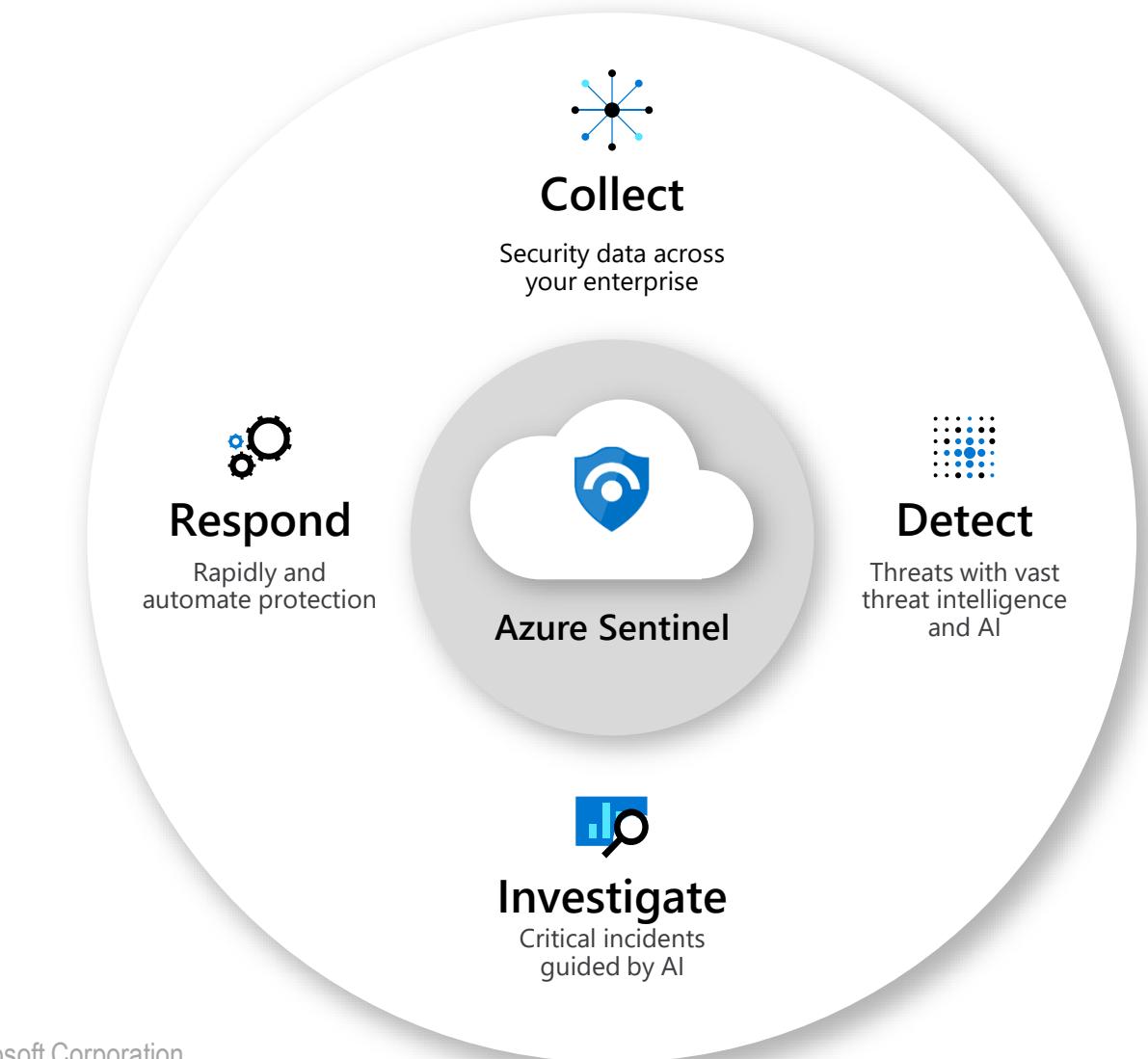
Azure Security Centre Demo



Introducing Microsoft Azure Sentinel

Cloud-native SIEM + SOAR

- Limitless cloud speed and scale
- Automatically connected across Azure & Office 365
- Easy integration with existing tools
- Artificial Intelligence



© Microsoft Corporation

Azure

6°

Secure Azure Validation

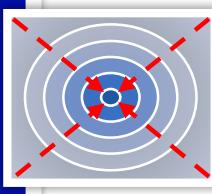
Standard Managed Service

Collection and Fusion
(mostly machine)

Solution Platform

Defense in Depth

Microsoft Azure



Security/SIEM Tool*

Azure Sentinel

Configure and Tune
(mostly human)

Possible cyber security incidents

Actual cyber security incidents

Secure Azure

Analysis and Action
(mostly human)

Six Degrees Cyber Security Operations Centre

Level 1 Triage

Analyst Analyst Analyst

Level 2 Incident Response

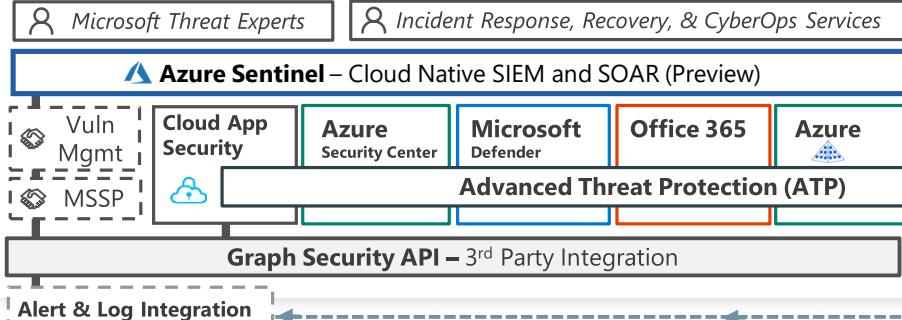
Incident Responder Incident Responder

Subject Matter Expert Subject Matter Expert

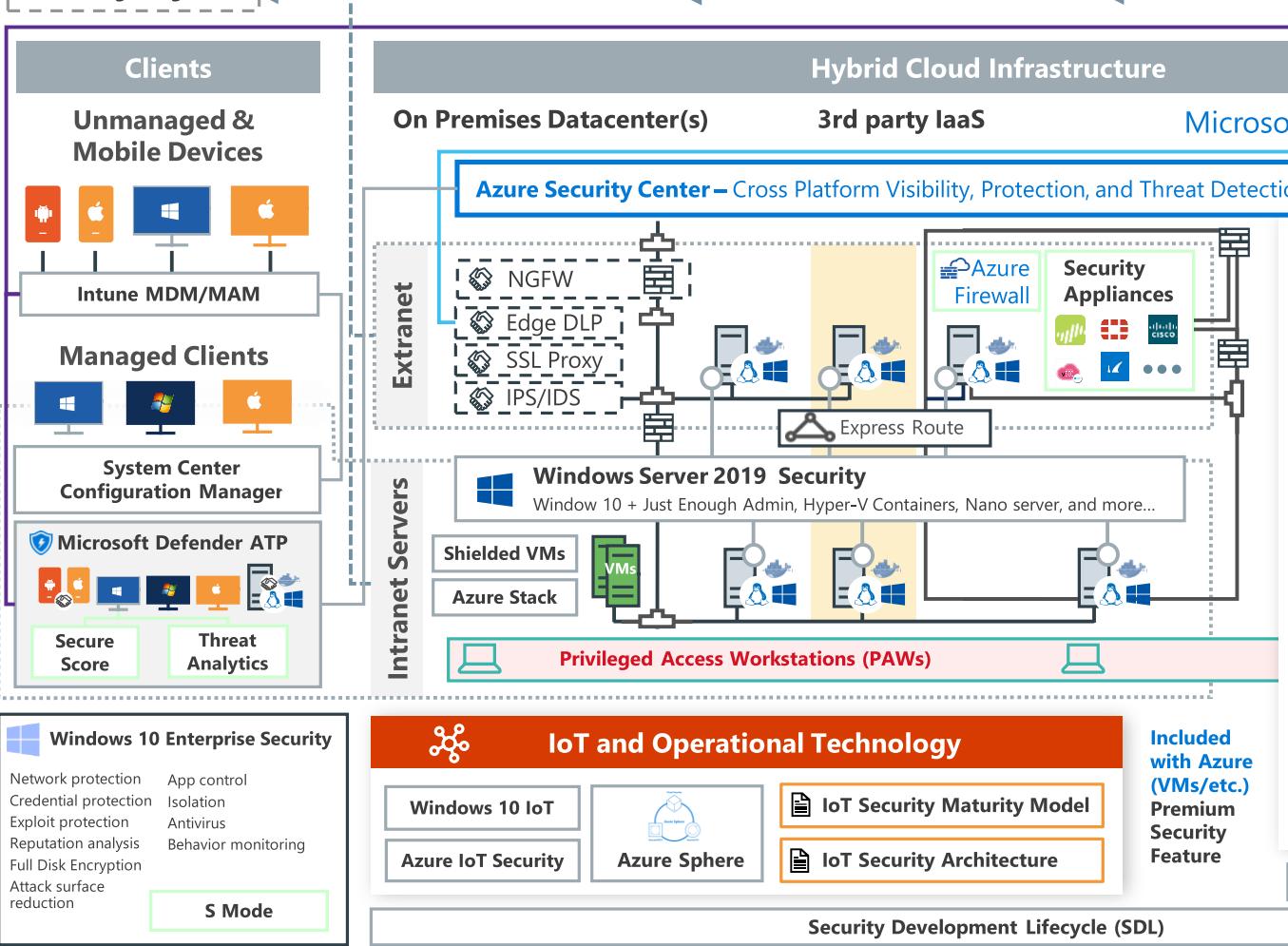
Level 3 Further Forensics

*Recommended tool. We also can work with existing SIEM tool fit for purpose.

Security Operations Center (SOC)



Cybersecurity Reference Architecture



Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365



Identity & Access

Azure Active Directory

- Azure AD Identity Protection
 - Leaked cred protection
 - Behavioral Analytics

Azure AD PIM

- Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

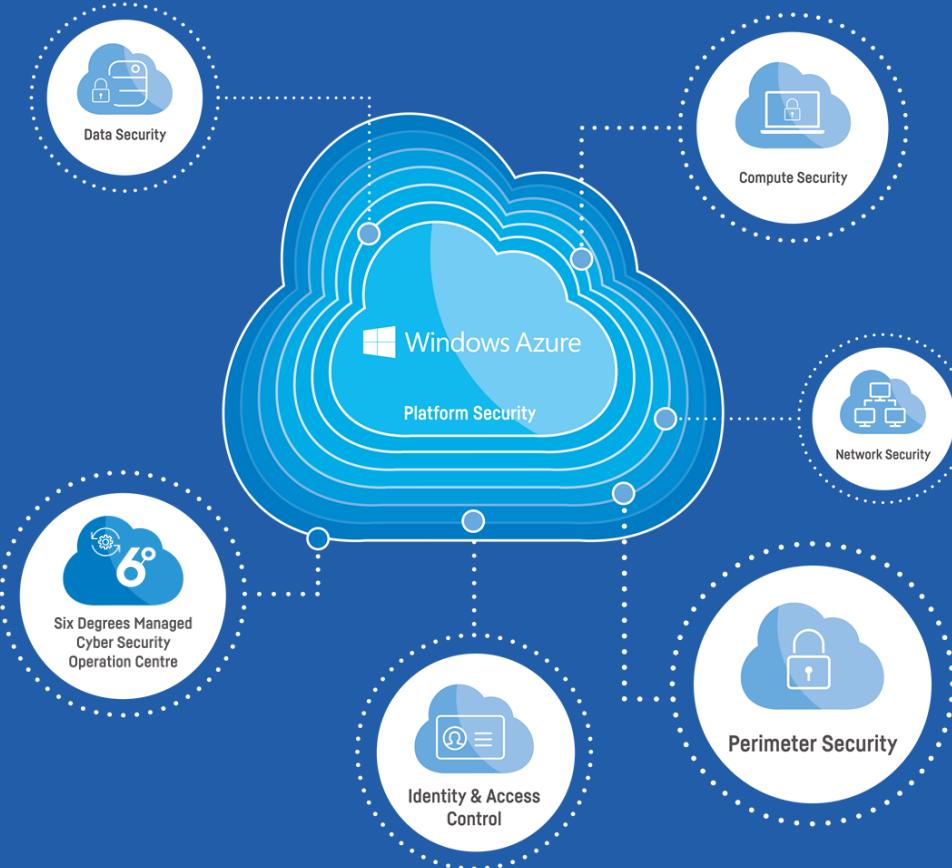


Trust Center

Intelligent Security Graph

6°

Can you do all this in-house?



UK-based CSOC facilities | Geographically-diverse Data Centre footprint
24x7x365 support | Fully scalable technology-agnostic service



Next steps – visit us on stand C1244



**Capture
& Consult**



**Transform
& Harden**



**Manage
& Optimise**



**Defend
& Recover**

- To discuss the Azure security and governance tools
- Get a demo of Sentinel and Security Centre
- Take our Aegis Security Maturity assessment
- Speak to our Security experts
- Book a free cloud adoption strategy workshop
- Book a 50% off cloud assessment
- Book your penetration testing



60°

**Enabling your
brilliance**