Commercial Marketplace

POC Offer Collateral / Information

Managed Azure Sentinel - Free Proof of Concept

CUSTOMER BENEFITS OF THE POC

RISK FREE Proof of Concept with minimal business impact and a new Azure subscription at no cost.

EASY TO DEPLOY with a trusted Microsoft Security Cloud Service Provider (CSP).

2 HOUR WORKSHOP to assess your cyber profile against your Microsoft ecosystem.

Your **CRITICAL** Microsoft cloud native log sources are connected in hours not days.

SPECIALISED PURPLE TEAM applying best-in-class threat hunting techniques.

Measure your security maturity using Microsoft Azure and 365 **SECURE SCORE.**

We deploy **DETECTION RULES** based on your critical logs that demonstrate comprehensive threat coverage.

AUTOMATED weekly reporting and **A FINAL REPORT** with key insights and actions to remediate risks identified.

PoC delivered by **AZURE EXPERTS** in Security and Public Cloud throughout the trial.

PoC Inclusions

☑ Free 30 Day Trial

☑ No Impact Engagement

☑ Critical Data Connectors

☑ Best-in-Class Threat Hunting

☑ Regular Updates

☑ Microsoft Security Score

☑ Tailored Final Report

☑ Microsoft Experts

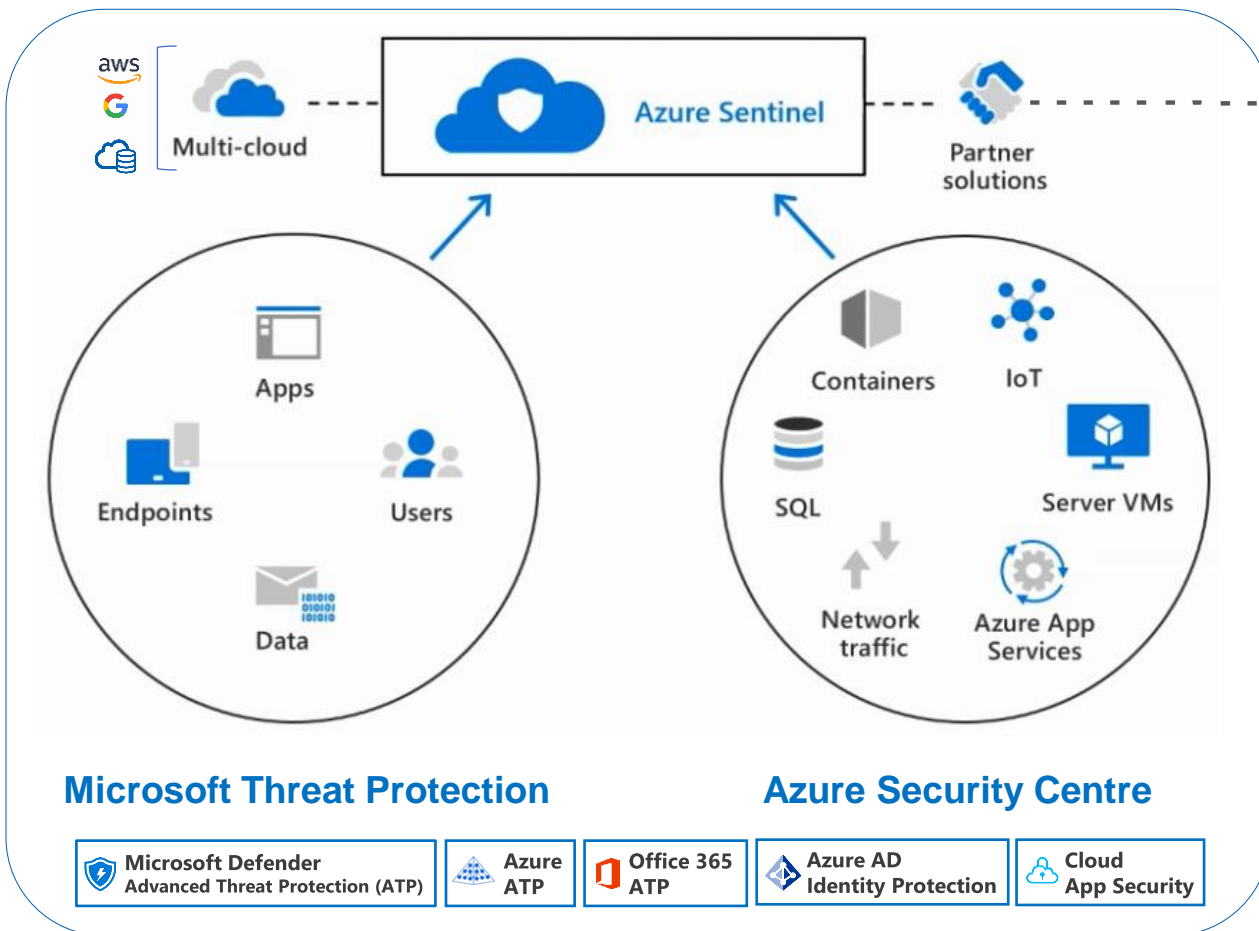☑ Easy transition into Managed Servcies

Managed Services

Results from your **Proof of Concept** will be transitioned into our Managed Azure Sentinel service by Interactive. Key features include:

▪ Deep dive **Risk Assessment** to assess your cyber risk against business operations and strategy

▪ **On-boarding your Azure Sentinel** instance to optimise managing alerts through automation, triage and investigation .

▪ Undertake an **Incident Response** (if an active threat is detected) and steps to contain and eradicate the threat.

▪ **Managed SOC** service to rapidly increase your detection and response capability supported by Interactive's 24x7 SOC
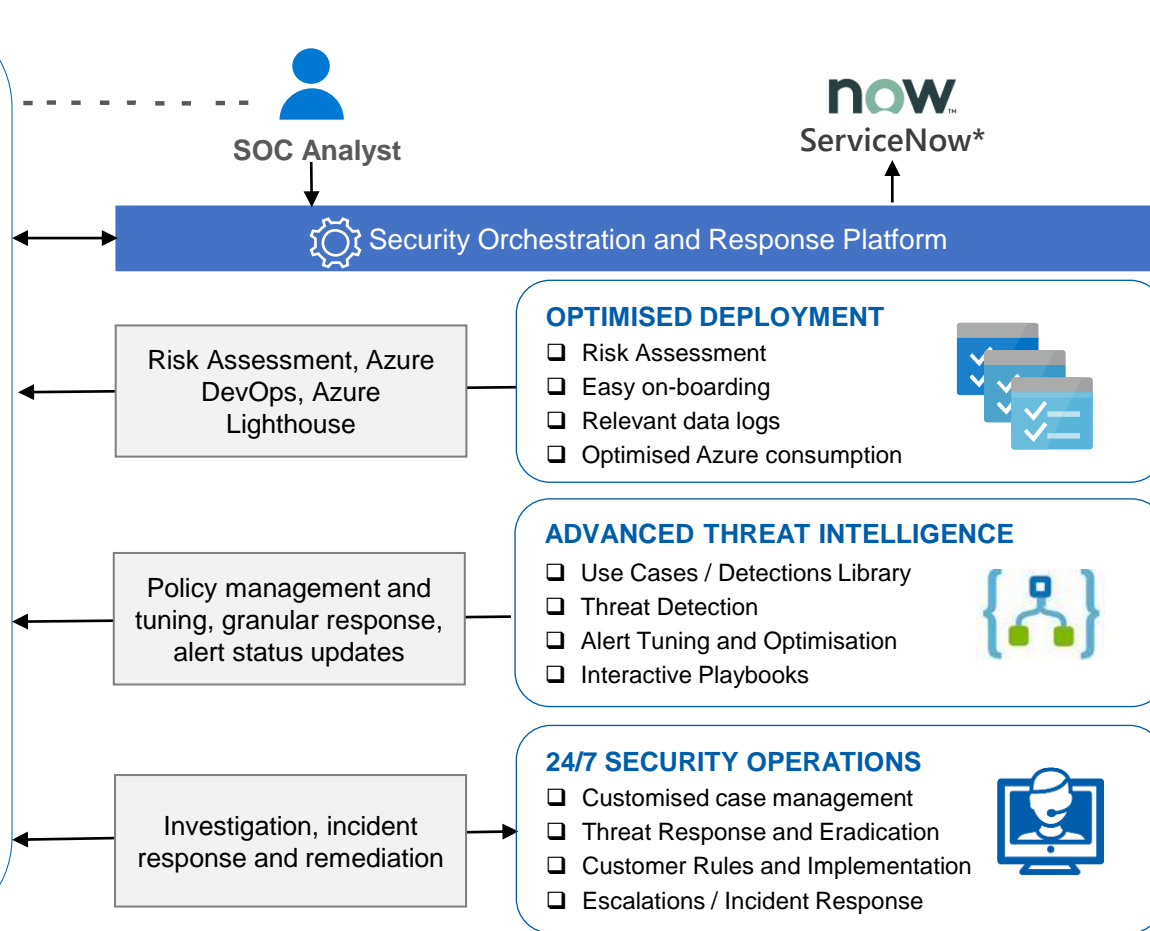
Managed Azure Sentinel by Interactive

CUSTOMER'S ENVIRONMENT

INTERACTIVE'S CUSTOMER EXPERIENCE

aws
G

Multi-cloud

Azure Sentinel

Partner solutions

SOC Analyst

now
ServiceNow*

⚙ Security Orchestration and Response Platform

Microsoft Threat Protection

Azure Security Centre

Apps

Endpoints   Users

Data

Containers   IoT

SQL   Server VMs

Network traffic   Azure App Services

| 🛡 Microsoft Defender Advanced Threat Protection (ATP) | Azure ATP | Office 365 ATP | Azure AD Identity Protection | Cloud App Security |

Risk Assessment, Azure DevOps, Azure Lighthouse

OPTIMISED DEPLOYMENT
- ❑ Risk Assessment
- ❑ Easy on-boarding
- ❑ Relevant data logs
- ❑ Optimised Azure consumption

Policy management and tuning, granular response, alert status updates

ADVANCED THREAT INTELLIGENCE
- ❑ Use Cases / Detections Library
- ❑ Threat Detection
- ❑ Alert Tuning and Optimisation
- ❑ Interactive Playbooks

Investigation, incident response and remediation

24/7 SECURITY OPERATIONS
- ❑ Customised case management
- ❑ Threat Response and Eradication
- ❑ Customer Rules and Implementation
- ❑ Escalations / Incident Response

* We can integrate with a range of support ticketing platforms.