ASSURIA DataSense

CUSTOMER CASE STUDY

UK Government Chooses Assuria
for Tier 1 Azure Security Visibility

A major UK Government department selected Assuria's Security Data Platform to deliver scalable monitoring, custom analytics, and high-assurance cloud security operations.

ENVIRONMENT
Tier 1 Official Azure Cloud

COVERAGE
Azure Security + Bespoke Apps

ARCHITECTURE
Multi-AZ Resilient Deployment

The Challenge

A major UK Government department required a scalable, proven, and easily maintainable Security Data Platform capable of operating within highly sensitive environments. Their Tier 1 cloud estate underpins efficient day-to-day operations, flexible and remote working, and secure collaboration across teams.

To meet these needs, the organisation sought a security data management and analytics platform that could seamlessly onboard new data sources, support the creation of custom analytics rules, generate tailored alerts, and provide rich, role-specific dashboards. The solution also needed to monitor a wide range of cloud-native security services, including firewalls, security groups, antivirus, and the full Azure Security Center suite-Defender for Servers, Defender for Storage, Defender for Key Vault, Office 365, Azure ATP, Defender for Cloud Apps-as well as bespoke applications developed specifically for UK Government use.

The Solution

The Assuria Security Data Platform was deployed on a resilient architecture spanning multiple availability zones to ensure high availability and operational continuity. It also needed to ingest and present vulnerability-scanning results to identify and prioritise security weaknesses across the environment.

As additional projects were commissioned, the solution had to remain flexible and easily adaptable. Several internet-facing custom applications required seamless integration into the Security Data Platform, along with tailored dashboards to surface key insights, external threat activity, and overall security posture.

Outcomes

The final solution was designed to collect telemetry from 389 SIEM agents deployed across virtual machines in the Tier 1 Azure environment and ingest over 100GB daily log events while maintaining performance, scalability, and security.