Crown Commercial Service
Supplier

G-Cloud 15

Sovereign Managed eXtended Detection & Response (MXDR) Service

Atos

Table of contents

Crown Commercial Service Supplier

Atos

1. What is the Sovereign Managed eXtended Detection & Response Service

Atos Sovereign MXDR (Managed Extended Detection and Response) is a UK-based managed security service that widens the optimisation of the Microsoft E3/E5 security investments into active 24/7 threat protection. Operating exclusively from sovereign UK Security Operations Centres staffed by 180+ UK-based, security-cleared specialists, the service provides enterprise-grade security operations without requiring organisations to build internal SOC capabilities. All platform engineering, support teams, and SOC services are delivered by dedicated UK personnel, ensuring complete operational sovereignty alongside data sovereignty.

The service addresses a critical market reality: UK organisations spend hundreds of thousands on Microsoft E3/E5 licences whilst using only 10% of the security features, drowning in false alerts, and risking £17.5M in GDPR fines as security data flows across multiple geographical locations. Building an internal UK SOC costs £2-5M upfront, plus £1-3M annually, with security roles taking 6-9 months to fill at £80-120K salaries and a 30% turnover rate. Meanwhile, global MSSPs offer offshore coverage that fails the moment regulators ask why UK citizen data is processed abroad or when you need someone who understands UK banking regulations at 2 AM.

By operationalising these existing investments through a dedicated Azure AD tenant architecture hosted exclusively in UK Azure regions—with UK West as the primary location—Sovereign MXDR ensures regulatory compliance whilst delivering predictable operational costs. The entire security platform operates within UK availability zones with built-in resilience, accessed solely by UK-based, vetted personnel through controlled access points, replacing volatile security spending and recruitment challenges with assured sovereign operations.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

Sovereign MXDR delivers comprehensive managed security operations that transform how UK organisations achieve both security excellence and regulatory compliance. The service architecture ensures complete UK sovereignty: through Azure Lighthouse and Defender MTO Portal integration configured with UK-only access controls, Atos UK SOC analysts access telemetry and security signals from the customer's Sentinel and Defender instances without any customer data leaving their tenancy. All security operations, from initial triage through incident response, are conducted exclusively by UK-based teams operating from UK facilities using UK-hosted infrastructure.

This sovereignty-by-design architecture ensures that whilst Atos analysts monitor, investigate and respond to threats 24/7, all data remains under the customer's control within their own Microsoft tenant hosted in UK Azure regions. The dedicated MXDR tenant resides in UK Azure data centres with cross-region resilience, ensuring high availability whilst maintaining data residency. Access to the security platform is restricted through Azure Virtual Desktop with conditional access policies enforcing UK-only connections, UK-registered devices, and certificates issued only to vetted UK personnel. Every byte remains in customer control, and every analyst is UK-based and understands UK threats, business, and regulations.

The service enables the transformation of dormant Microsoft investments into active security platforms with Sentinel and Defender working as intended, addressing the challenge where 95% of alerts are typically false positives through continuous tuning and expert analysis. UK analysts handle what matters, when it matters, from the UK—providing enterprise-grade 24/7 coverage that is actually UK 24/7, not handed off to offshore at 6 PM. For regulated sectors, this complete sovereignty model—spanning data, operations, and personnel—is game-changing: financial services can guarantee the FCA that data never leaves the UK and is only accessed by UK personnel, NHS trusts confirm patient data sovereignty with UK-only processing, and government suppliers qualify for contracts requiring UK-only operations.

Core Security Operations (24/7/365 UK-Based)

- Continuous incident detection, analysis, investigation and response by UK SOC teams
- Proactive threat hunting and hypothesis-based investigations by UK-certified analysts
- Dynamic rule deployment and exception management with UK-based change control

- Automated incident response through playbooks developed and maintained by UK engineers
- Sandbox analysis for malware detonation in isolated UK-hosted environments
- RBAC management with UK-only administrative access

Service Management & Governance (UK Teams)

- Dedicated UK-based Client Security Manager providing a single point of escalation
- Monthly/quarterly service reviews conducted by UK personnel
- Compliance reporting aligned to UK regulatory requirements (FCA, ICO, NCSC)
- UK-based service desk and engineering support during UK business hours
- ServiceNow integration managed by UK teams
- Audit-ready documentation maintained in UK-compliant formats

Endpoint & Server Protection (UK-Managed)

- EDR policy management by UK security engineers
- Real-time threat detection with response coordinated from UK SOC
- Remote isolation capabilities executed by UK analysts with customer approval
- Forensic data capture and analysis by UK-based DFIR specialists
- Platform health monitoring from UK operations centres
- Compliance reporting aligned to UK standards

Incident Response Capabilities (UK-Delivered)

- UK-based CSIRT services with 25-50 hours included monthly (tier dependent)
- Digital forensics by UK specialists (25 hours annually in enhanced package)
- UK-coordinated cyber recovery services for business restoration
- UK incident commanders coordinating response across stakeholders
- Root cause analysis by UK security experts

Business Outcomes

- Activation of underutilised Microsoft E3/E5 security investments with UK sovereign operations
- Faster threat containment by UK teams with response times measured in minutes, not hours
- Assured UK data sovereignty with UK-only access controls for regulatory compliance

- Mitigation of GDPR fine risk through guaranteed UK-only operations and personnel
- Qualification for UK government and critical infrastructure contracts requiring sovereign operations
- Complete audit trail of UK-only access and operations for regulatory demonstration
- Predictable operational costs with UK-based service delivery

Atos can provide continuous support and advice to help organisations adapt to evolving security challenges, update their security practices and ensure long-term protection of their cloud environments.

Crown Commercial Service Supplier

Atos

3. What technology does it use?

Sovereign MXDR leverages Microsoft's cloud-native security ecosystem deployed exclusively within UK Azure regions, maximising the value of existing E3/E5 investments whilst maintaining complete sovereignty through a UK-only multi-tenant architecture. The entire technology stack operates within UK availability zones—primarily UK West, with UK South as a failover—ensuring resilience without compromising data residency. The service employs Microsoft's native delegated access capabilities configured with stringent UK-only controls: Azure Lighthouse connections are restricted to UK IP ranges and UK-registered devices, whilst the Defender MTO Portal access is limited to verified UK personnel only. This approach combines the scalability and intelligence of Microsoft's security platform with the absolute assurance of UK-only operations, delivered through a dedicated MXDR tenant hosted in UK datacentres, managed by UK engineering teams, and accessed exclusively by UK-based, security-cleared analysts.

Microsoft Security Stack (UK-Hosted Platform)

- Microsoft Sentinel: Cloud-native SIEM deployed in UK Azure regions, providing unlimited scale with data processing remaining within UK boundaries
- Microsoft Defender for Endpoint (P1/P2): Advanced EDR with telemetry routed through UK-based collection points
- Microsoft Defender for Cloud: Server workload protection with UK-localised threat intelligence (Defender for Servers scope only)
- Azure Lighthouse: Secure delegated access configured with UK-only connectivity, IP restrictions, and conditional access policies
- Defender MTO Portal: Multi-tenant operations portal accessed exclusively through UK AVD infrastructure by authorised UK personnel

Secure Delivery Architecture (UK Sovereign Design)

- Dedicated MXDR Tenant: Purpose-built Azure AD tenant hosted in UK West region, isolated from global Atos operations
- UK Azure Virtual Desktop (AVD):
    - Hosted exclusively in UK datacentres
    - Session hosts restricted to UK availability zones
    - Access limited to UK IP addresses and UK-issued certificates
    - Session recording stored in UK-compliant storage accounts
    - MFA enforcement with UK-registered authentication methods

- Zero Trust Access Model:
  - JIT privileged access managed by UK administrators
  - Conditional access enforcing UK location and device compliance
  - Privileged Identity Management (PIM) with UK-only approval chains
- Certificate-Based Authentication: PKI infrastructure managed by the UK team with certificates issued only to vetted UK personnel
- Data Sovereignty Architecture:
  - Customer data remains in the customer's UK tenant
  - Telemetry flows through UK-only network paths
  - No data replication outside UK regions
  - Audit logs retained in UK storage accounts

Resilience & Availability (UK Infrastructure)

- Primary operations from the UK West Azure region
- Automated failover to UK South for disaster recovery
- 99% platform availability SLA across UK zones
- UK-based backup and recovery systems
- Cross-region replication within UK boundaries only

Third-Party EDR Integration (Optional, UK-Managed)

- CrowdStrike Falcon Insight with UK-localised threat hunting
- SentinelOne Singularity managed by UK teams
- Trend Micro XDR configured for UK data residency

Automation & Intelligence Layer (UK-Developed)

- Playbooks developed and maintained by UK engineering teams
- AI/ML models trained on the UK threat landscape
- UK-specific threat intelligence feeds
- Custom detection rules for UK regulatory compliance
- Automated workflows designed for UK business practices

Integration Capabilities (UK-Controlled)

- ServiceNow integration managed by UK teams
- API access restricted to UK-based systems
- Custom parsers developed by UK engineers
- All integrations tested and approved by the UK security architecture team

The service utilises a modular "pick and mix" approach, enabling organisations to select and scale capabilities aligned with their risk profile, compliance requirements, and security maturity—from SecOps Essentials providing foundation protection through to SecOps Enhanced delivering comprehensive cyber resilience with integrated CSIRT capabilities. All modules are delivered exclusively by UK teams, using UK infrastructure, ensuring complete operational and data sovereignty throughout the service lifecycle.

Crown Commercial Service *Supplier*

Atos

4. What terms apply?

To the fullest extent permitted under G-Cloud 15 Framework Agreement and the Call-Off Contract, Atos will provide the Services in accordance with the Atos Supplier Terms (which will include, but may not be limited to , the Supplier Acceptable Use Policy, Supplier Data Processing Agreement, Supplier Specific Shared Responsibility Model, Supplier SLAs and Supplier Licence Terms and any applicable Third-Party Terms outlined in this Service Description document and the Order Form) and this Service Description document.

For clarity:

- Atos Supplier Terms may be modified in accordance with the provisions of the Call-Off Contract, and remain effective except where expressly overridden.
- Hyperlinks included in the Atos Supplier Terms and Service Description document remain effective where they point to Atos' or the relevant Third-Party Terms or documents. Should a hyperlink cease to function, Atos will work with the client to update it through the agreed procedure.

Crown Commercial Service *Supplier*

Atos

5. Termination

Termination shall be in accordance with:

- The G-Cloud 15 Framework terms and conditions
- Any terms agreed within the Order Form of the relevant Call-Off Contract
- For this specific service, by default Atos ask for at least thirty (30) days prior written notice of termination without cause.

Atos commits to the continued provision of services for the duration of the Call-Off Contract subject to the terms and conditions of the G-Cloud 15 Framework Agreement, the Call-Off Contract, the Atos Supplier Terms and the applicable Third Party Agreements (as defined in the Atos Supplier Terms and indicated in the Order Form) related thereto.

Crown Commercial Service *Supplier*

Atos

6. How do I order?

Please contact our team at: gcloud@atos.net

- We will prepare a quotation for your review, including any applicable volume discounts.
- Once the quotation is agreed, we will issue the necessary documentation (as required by the G-Cloud Framework) and request a purchase order from you.
- Upon receipt of your purchase order, we will configure the services in line with the agreed requirements. Where applicable, you will also receive access to our self-service portal to begin provisioning services.
- If you are a new customer, you may need to complete additional 'new supplier' forms.
- Invoices will be issued to you and to Crown Commercial Service (CCS), quoting the purchase order number, for the services procured.
- We will also submit the required monthly management information reports to Government Procurement.

Crown Commercial Service Supplier

Atos

7. Glossary

Term	Definition
AI	Artificial Intelligence
API	Application Programming Interface
AVD	Azure Virtual Desktop
B2B	Business to Business
CRRT	Cyber Risk Response Team
CSIRT	Computer Security Incident Response Team
CSM	Client Security Manager
DFIR	Digital Forensics and Incident Response
E3/E5	Enterprise 3 / Enterprise 5 (Microsoft Licensing Tiers)
EDR	Endpoint Detection & Response
FCA	Financial Conduct Authority
GB	Gigabytes
GDAP	Granular Delegated Admin Privileges
GDPR	General Data Protection Regulation
ITSM	IT Service Management
JIT	Just in Time
KPI	Key Performance Indicator
MFA	Multi-Factor Authentication
MISA	Microsoft Intelligence Security Association
ML	Machine Learning
MSSP	Managed Security Service Provider
MTO	Multi-Tenant Operations
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond
MXDR	Managed Extended Detection & Response
NHS	National Health Service
P1/P2	Priority 1 / Priority 2 (incident levels) or Plan 1 / Plan 2 (Defender Licensing)

Term	Definition
PIM	Privileged Identity Management
RBAC	Role Base Access Control
ROI	Return on Investment
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOAR	Security Orchestration, Automation & Response
SOC	Security Operations Centre
SOW	Statement of Work
UK	United Kingdom
UKI	United Kingdom & Ireland
XDR	Extended Detection and Response

Crown Commercial Service *Supplier*

Atos

8. Why Atos

Atos has been a trusted partner on every G-Cloud iteration since the framework began, helping public sector organisations modernise with confidence. We combine global expertise with deep UK experience, delivering secure, scalable cloud solutions that meet the highest government standards.

As Europe's leading provider of cloud and cybersecurity services, Atos offers end-to-end capabilities - from migration and hosting to SaaS and consultancy - supported by UK delivery centres and strategic partnerships with hyperscalers.

Our focus on innovation, sustainability, and social value ensures that customers not only achieve operational excellence but also contribute to a greener, fairer future. With Atos, you gain a proven partner committed to driving efficiency, resilience, and transformation across public service.

About Atos

Atos Group is a global leader in digital transformation with c. 67,000 employees and annual revenue of c. €10 billion, operating in 61 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Atos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Learn more at: atos.net

105043-RR