Crown Commercial Service
Supplier

G-Cloud 15

Sovereign Managed eXtended Detection & Response (Trend) Service

Atos

Table of contents

Crown Commercial Service *Supplier*

Atos

1. What is the Sovereign Managed eXtended Detection & Response (Trend) Service?

Atos UKI Sovereign MXDR (Managed Extended Detection and Response) powered by Trend Vision One is a UKI-based managed security service that transforms underutilised security investments into active 24/7 threat protection. Operating exclusively from sovereign UKI Security Operations Centres staffed by 180+ certified specialists, the service leverages Trend Micro's UK Sovereign SaaS Cloud tenancy to provide enterprise-grade security operations without requiring organisations to build internal SOC capabilities. All platform engineering, support teams, and SOC services are delivered by dedicated UKI-based security professionals certified in Trend Micro technologies.

The service addresses a critical market reality: UKI organisations deploy multiple security tools yet struggle to correlate threats across silos, drowning in uncorrelated alerts whilst risking £17.5M GDPR fines when data flows through non-sovereign infrastructures. Building an internal SOC costs £2-5M upfront plus £1-3M annually, with security roles taking 6-9 months to fill at £80-120K salaries and experiencing 30% turnover rates. Traditional global MSSPs offer offshore coverage that fails to meet sovereignty requirements—unable to guarantee that UK citizen data remains within sovereign boundaries or to provide analysts who understand UKI regulatory frameworks.

By operationalising Trend Vision One's unified XDR platform through Trend Micro's UK Sovereign SaaS Cloud tenancy with UKI-only operations, Sovereign MXDR ensures comprehensive threat protection with complete data sovereignty whilst delivering predictable operational costs that replace volatile security spending and recruitment challenges with assured sovereign operations.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

UKI Sovereign MXDR delivers comprehensive managed security operations that transform how organisations achieve both security excellence and regulatory compliance across the UKI. The service leverages Trend Micro's UK Sovereign SaaS Cloud tenancy, ensuring all security data processing and storage occurs within Trend Micro's sovereign infrastructure whilst being accessed exclusively by UKI-based security teams. Through Trend Vision One's native multi-tenant capabilities within Trend Micro's sovereign cloud, Atos UKI SOC analysts access security telemetry and correlated threat data without customer information leaving Trend Micro's sovereign environment. All security operations, from initial detection through response, are conducted by UKI-based certified professionals who understand local regulatory requirements, business practices, and threat landscapes.

This sovereignty-by-design architecture ensures that whilst Atos analysts monitor, investigate and respond to threats 24/7, all data remains within Trend Micro's UK Sovereign SaaS Cloud tenancy with guaranteed data residency and UKI-only access. The platform provides unified visibility across email, endpoints, servers, cloud workloads, and networks through a single console within Trend Micro's sovereign infrastructure, eliminating security silos whilst maintaining complete sovereignty. Trend Vision One's risk-based approach automatically correlates threats across all layers, prioritising genuine risks whilst filtering noise—addressing the challenge where 95% of alerts are typically false positives.

The service enables the transformation of fragmented security tools into a unified sovereign defence platform. UKI analysts handle what matters, when it matters, from UKI locations—providing enterprise-grade 24/7 coverage that is actually UKI 24/7, not handed off to offshore teams. For regulated sectors, this complete sovereignty model is game-changing: financial services can guarantee the FCA that data never leaves Trend Micro's sovereign cloud, NHS trusts and HSE confirm patient data sovereignty within Trend Micro's UK infrastructure, and government suppliers qualify for contracts requiring sovereign-only operations.

Core Security Operations (24/7/365 UKI-Based Coverage)

- Continuous threat detection and response by UKI-based SOC teams
- Automated cross-layer correlation within Trend Micro's sovereign cloud
- Risk-based prioritisation aligned to UKI regulatory requirements
- Virtual patching managed by UKI security engineers
- Threat intelligence contextualised for the UKI threat landscape
- Workbench access restricted to UKI-based analysts only.

Service Management & Governance (UKI Teams)

- Dedicated UKI-based Client Security Manager providing sovereign escalation
- Compliance reporting for FCA, ICO and Data Protection Commission
- Executive dashboards with UKI-specific risk metrics from Trend Micro's sovereign platform
- UKI-based service desk support during business hours
- Audit trails demonstrating UKI-only access and operations
- Regulatory alignment for both UKI requirements.

Endpoint & Server Protection (UKI-Managed)

- Trend Vision One Endpoint Security managed by UKI teams
- Response actions executed by UKI-based analysts
- Forensic analysis conducted by UKI specialists
- Virtual patching prioritised for UKI critical infrastructure
- Mobile security covering UKI corporate devices
- Policy management aligned to UKI compliance standards.

Cloud & Email Security (Sovereign Operations)

- Multi-cloud protection with UKI data residency enforcement
- Email security addressing UKI-specific phishing campaigns
- Cloud compliance scanning for UKI regulations
- CASB policies managed by UKI cloud architects
- Container security for UKI-hosted workloads.

Incident Response Capabilities (UKI-Delivered)

- UKI-based CSIRT with 25-50 hours included monthly (tier dependent)
- Digital forensics by UKI specialists (25 hours annually in enhanced package)
- UKI incident commanders coordinating response
- Threat hunting by analysts familiar with UKI threat actors
- Reporting aligned to UKI regulatory requirements.

Business Outcomes

- 70% reduction in threat investigation time through automated correlation
- Assured UKI data sovereignty through Trend Micro's sovereign cloud tenancy
- Mitigation of GDPR fine risk through guaranteed sovereign operations
- Qualification for government contracts requiring UKI-only operations
- Single platform replacing multiple tools with sovereign guarantee
- Complete audit trail of UKI-only access for regulatory demonstration
- Predictable costs with transparent sovereign service delivery.

Crown Commercial Service Supplier

Atos

3. What Technology Does it Use?

UKI Sovereign MXDR leverages Trend Vision One's unified XDR platform deployed exclusively on Trend Micro's UK Sovereign SaaS Cloud tenancy, providing a single cybersecurity platform that correlates and responds to threats whilst maintaining complete sovereignty for UKI organisations. The technology stack operates entirely within Trend Micro's sovereign cloud infrastructure, with guaranteed data residency, and is accessed solely by UKI-based personnel through controlled access points. The service combines Trend Micro's global threat intelligence with sovereign operations—ensuring organisations benefit from worldwide threat visibility whilst maintaining complete data sovereignty within Trend Micro's UK Sovereign SaaS Cloud.

Trend Vision One Platform (Sovereign Configuration)

- Vision One XDR: Unified platform hosted exclusively in Trend Micro's UK Sovereign SaaS Cloud tenancy
- Risk Insights: AI-powered risk scoring within Trend Micro's sovereign infrastructure
- Threat Intelligence: Global threat data processed within Trend Micro's sovereign cloud
- Workbench: Unified console operating within Trend Micro's UK sovereign environment
- Trend Micro UK Sovereign SaaS Cloud: Dedicated sovereign tenancy ensuring complete data residency and isolation.

Sovereign Security Architecture

- Data Residency Controls:
  - All data processed within Trend Micro's UK sovereign infrastructure
  - No replication outside Trend Micro's sovereign cloud boundaries
  - Customer data segregation within Trend Micro's sovereign tenancy
  - Complete data lineage within Trend Micro's sovereign environment
- Access Management:
  - UKI-only access to Trend Micro's sovereign cloud console
  - Certificate-based authentication for sovereign platform access
  - Conditional access policies enforcing sovereign operations
  - Privileged access managed within Trend Micro's sovereign tenancy

Security Capabilities (UKI-Operated)

- Endpoint Security:
  - Next-generation protection delivered from Trend Micro's sovereign cloud
  - EDR capabilities within Trend Micro's UK infrastructure
  - Automated response orchestrated through sovereign platform
  - Root cause analysis using Trend Micro's sovereign analytics
- Server & Cloud Workload Security:
  - Multi-cloud protection managed through Trend Micro's sovereign console
  - Container security within Trend Micro's UK sovereign environment
  - Virtual patching delivered from Trend Micro's sovereign cloud
  - Compliance scanning within sovereign infrastructure
- Email Security:
  - Protection delivered through Trend Micro's sovereign cloud
  - Phishing analysis within the UK sovereign infrastructure
  - BEC protection using Trend Micro's sovereign platform
  - Email DLP within Trend Micro's sovereign boundaries
- Network Security:
  - Network monitoring through Trend Micro's sovereign platform
  - Detection capabilities within the UK sovereign infrastructure
  - IoT/OT security from Trend Micro's sovereign cloud.

Operational Excellence (UKI Delivery)

- Multi-Tenant Management:
  - Centralised management through Trend Micro's sovereign cloud
  - Customer segregation within Trend Micro's sovereign tenancy
  - Role-based access within the sovereign platform
- Automated Response:
  - Playbooks executed within Trend Micro's sovereign infrastructure
  - Response orchestration through sovereign platform

    - Continuous improvement using sovereign cloud capabilities
- Compliance & Reporting:
    - Reporting generated from Trend Micro's UK sovereign cloud
    - Audit logs maintained within sovereign tenancy
    - Compliance data stored in Trend Micro's UK infrastructure
    - Regulatory reports from the sovereign platform.

Intelligence & Analytics (Sovereign Context)

- Threat feeds delivered through Trend Micro's UK Sovereign SaaS Cloud
- Analysis performed within Trend Micro's sovereign infrastructure
- Intelligence correlation in Trend Micro's UK sovereign environment
- Industry insights processed through sovereign platform
- Zero-day research applied within sovereign cloud boundaries.

Integration Ecosystem (UKI-Managed)

- ServiceNow integration with Trend Micro's sovereign platform
- API access through Trend Micro's UK sovereign cloud
- SIEM integration from Trend Micro's sovereign infrastructure
- Identity provider connections via sovereign platform
- Custom integrations within Trend Micro's sovereign boundaries.

The service utilises a modular approach aligned with Trend Vision One's layered architecture within Trend Micro's UK Sovereign SaaS Cloud tenancy, enabling organisations to protect across all attack vectors whilst maintaining complete sovereignty. All modules are delivered exclusively by UKI-based certified professionals operating through Trend Micro's sovereign infrastructure. Trend Micro's UK Sovereign SaaS Cloud tenancy ensures complete data sovereignty whilst providing access to global threat intelligence—delivering enterprise-grade security with the sovereign assurance required for regulated industries, government contracts, and critical national infrastructure across the UKI.

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
CSIRT	Computer Security Incident Response Team
DLP	Data Loss Prevention
FCA	Financial Conduct Authority
GDPR	General Data Protection Regulation
MSSP	Managed Security Service Provider
MXDR	Managed Extended Detection and Response
SOC	Security Operations Centre
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

Atos is a registered trademark of Atos SE. © 2024 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

105043-RR