Crown Commercial Service
Supplier

G-Cloud 15

Managed eXtended Detection & Response Service

Atos

Table of contents

Crown Commercial Service *Supplier*

Atos

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

Atos MXDR (Managed Extended Detection and Response) is a comprehensive managed security service that transforms dormant Microsoft E3/E5 security investments into active 24/7 threat protection. Operating from advanced Security Operations Centres staffed by 180+ certified 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 security professionals, ensuring consistent operational excellence and service quality.

The service addresses a critical market reality: organisations spend hundreds of thousands on Microsoft E3/E5 licences whilst using only 10% of security features, drowning in false alerts that consume valuable resources. 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 MSSPs often provide generic coverage that lacks the contextual understanding needed for effective threat response and business-aligned security operations.

By operationalising these existing investments through a dedicated Azure AD tenant architecture with enterprise-grade security controls, MXDR ensures comprehensive threat protection whilst delivering predictable operational costs, replacing volatile security spending and recruitment challenges with assured professional operations.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

MXDR delivers comprehensive managed security operations that transform how organisations achieve security excellence and operational efficiency. The service architecture ensures complete visibility and control: through Azure Lighthouse and Defender MTO Portal integration, Atos 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 by certified security professionals using advanced automation and orchestration capabilities.

This 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. The dedicated MXDR tenant provides centralised security operations with built-in resilience and high availability, ensuring continuous protection. Access to the security platform is controlled through Azure Virtual Desktop with strict conditional access policies, multi-factor authentication, and certificate-based validation—ensuring secure operations whilst maintaining customer data control.

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. Professional analysts handle what matters, when it matters—providing enterprise-grade 24/7 coverage with consistent quality. For regulated sectors, this professional managed service model delivers measurable security improvements whilst maintaining compliance with industry standards and regulatory requirements.

Core Security Operations (24/7/365 Professional Coverage)

- Continuous incident detection, analysis, investigation and response by certified SOC teams
- Proactive threat hunting and hypothesis-based investigations by experienced analysts
- Dynamic rule deployment and exception management with controlled change processes
- Automated incident response through professionally developed and maintained playbooks
- Sandbox analysis for malware detonation in isolated environments
- Complete RBAC management with privileged access controls

Service Management & Governance

- Dedicated Client Security Manager providing a single point of escalation
- Monthly/quarterly service reviews with performance metrics and trend analysis
- Compliance reporting aligned to regulatory requirements and industry standards
- Professional service desk and engineering support
- ServiceNow integration for streamlined ITSM processes
- Comprehensive audit trails and documentation

Endpoint & Server Protection

- Professional EDR policy management and optimisation
- Real-time threat detection with coordinated response
- Remote isolation capabilities with customer approval workflows
- Forensic data capture and analysis by certified specialists
- Continuous platform health monitoring
- Compliance reporting aligned to industry standards

Incident Response Capabilities

- Professional CSIRT services with 25-50 hours included monthly (tier dependent)
- Digital forensics by certified specialists (25 hours annually in enhanced package)
- Coordinated cyber recovery services for business restoration
- Expert incident management across stakeholder groups
- Comprehensive root cause analysis and improvement recommendations

Business Outcomes

- Activation of underutilised Microsoft E3/E5 security investments
- Faster threat containment with response times measured in minutes, not hours
- Significant reduction in false positive alerts through continuous tuning
- Enhanced security posture with 24/7 professional monitoring
- Reduced operational costs compared to building internal capabilities
- Scalable security that grows with business needs
- Predictable costs with transparent service delivery

Crown Commercial Service Supplier

Atos

3. What Technology Does it Use?

MXDR leverages Microsoft's cloud-native security ecosystem through a sophisticated multi-tenant architecture, maximising the value of existing E3/E5 investments whilst maintaining complete operational control. The technology stack employs enterprise-grade Azure services with built-in resilience and scalability, ensuring high availability and consistent performance. The service uses Microsoft's native delegated access capabilities—Azure Lighthouse and Defender MTO Portal—configured with stringent security controls and audit capabilities. This approach combines the power of Microsoft's security platform with professional security operations, delivered through a dedicated MXDR tenant that's purpose-built for managed security services and completely segregated from other operations.

- **Microsoft Security Stack (Core Platform)**
- **Microsoft Sentinel**: Cloud-native SIEM providing unlimited scale, AI-powered analytics, and automated SOAR capabilities for centralised security orchestration
- **Microsoft Defender for Endpoint (P1/P2):** Advanced endpoint detection and response with behavioural analysis and automated investigation
- **Microsoft Defender for Cloud:** Server workload protection with vulnerability assessment and just-in-time access controls (Defender for Servers scope only)
- **Azure Lighthouse:** Secure delegated access enabling multi-tenant management whilst customer data remains in their tenancy
- **Defender MTO Portal:** Centralised multi-tenant operations providing a unified incident response view across customer estates

Secure Delivery Architecture

- Dedicated MXDR Tenant: Purpose-built Azure AD tenant exclusively for MXDR operations, isolated from other services

Azure Virtual Desktop (AVD):

- Controlled analyst access with comprehensive security controls
- Session recording for audit and compliance
- MFA enforcement and conditional access policies
- Data loss prevention controls
- Zero Trust Access Model:
- Just-In-Time privileged access with approval workflows

- Role-based access control with least privilege principles
- Privileged Identity Management (PIM) for administrative functions
- Certificate-Based Authentication: PKI infrastructure with certificates for enhanced validation

Data Control Architecture:

- Customer data remains in the customer tenant
- Only telemetry and alerts are accessed for analysis
- No data replication or storage outside the customer environment
- Complete audit logging for all access and actions

Resilience & Availability

- High availability architecture with automated failover
- 99% platform availability SLA
- Comprehensive backup and recovery capabilities
- Disaster recovery procedures and testing
- Continuous service monitoring and health checks

Third-Party EDR Integration (Optional)

- CrowdStrike Falcon Insight for advanced threat hunting
- SentinelOne Singularity for autonomous endpoint protection
- Trend Micro XDR for cross-layer detection and response

Automation & Intelligence Layer

- AI/ML-powered threat detection and analysis
- Custom playbook development for automated response
- Behavioural analytics for anomaly detection
- Threat intelligence integration from multiple sources
- Automated correlation and enrichment of security data

Integration Capabilities

- ServiceNow for ITSM workflow integration
- Native support for all Azure-supported log sources
- API-driven integration with existing security tools

- Custom parser development for proprietary data sources (subject to professional services agreement)
- Flexible integration with customer environments

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 by certified security professionals using proven methodologies and best practices, ensuring consistent quality and measurable security improvements 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
CSIRT	Computer Security Incident Response Team
EDR	Endpoint Detection and Response
ITSM	Information Technology Service Management
MSSP	Managed Security Service Provider
MTO	Multi-Tenant Organisation
MVP	Minimum Viable Product
MXDR	Managed Extended Detection and Response
PIM	Privileged Identity Management
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation 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

105043-RR