Crown Commercial Service *Supplier*

G-Cloud 15

Microsoft Azure CloudSecOps Protection Platform

Atos

Table of contents

Crown Commercial Service *Supplier*

Atos

1. What is the Microsoft Azure CloudSecOps Protection Platform Service

Atos' Managed Microsoft Cloud SecOps Protection Platform is a comprehensive security solution that leverages a Cloud Security Mesh Architecture (CSMA) approach to enable seamless interoperability between various Microsoft security products, delivering unified visibility and protection across hybrid and multi-cloud environments.

The platform provides organisations with a fully managed security operations service leveraging Microsoft's complete cloud-native security stack to detect, investigate, and respond to threats across the entire digital estate. Our experts provide 24/7 monitoring, proactive threat hunting, and incident response to ensure your Microsoft cloud and hybrid assets stay secure, automated, and compliant.

Atos' Managed Microsoft Cloud SecOps Protection Platform, coupled with the expertise of Atos' Managed Security Service Provider (MSSP) team and cutting-edge automation, implements best practices to configure, continuously manage, and monitor the solution at peak efficiency. Whether you are an emerging startup, a small- to medium-sized public sector organisation, or a multinational enterprise, incorporating the knowledge and skills of Atos' Microsoft Azure experts provides peace of mind and robust protection against cyber threats.

Our experts provide round-the-clock surveillance and management of your Microsoft security infrastructure through Azure Lighthouse, ensuring proactive protection, timely response to potential threats, and scalable multi-tenant management without additional customer-side costs.

One of the key advantages is that it eliminates the need for dedicated in-house security personnel. However, we strongly believe in the power of collaboration and welcome the opportunity to work alongside existing security teams. By integrating our expertise with internal resources, we create a robust, comprehensive security strategy tailored to specific requirements and objectives.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

Atos' Managed Microsoft Cloud SecOps Protection platform is a security umbrella offering based on a mesh architecture approach with interoperability between distinct Microsoft security products to achieve a more consolidated security posture.

Atos' approach to cloud security extends across three simple value drivers: **PREVENT, PROTECT, and PRESERVE** security in the cloud.

- **Cloud Prevent** - Taking a preventive approach by proactively deploying controls, effectively 'shifting-left' security. This includes identity protection, endpoint hardening, and vulnerability management
- **Cloud Protect** - Implementing and continually augmenting the proper controls to maintain a secure posture across cloud infrastructure, applications, email, and data
- **Cloud Preserve** - Preserving secure posture through continuous monitoring, response, and compliance management using SIEM, XDR, and AI-enhanced capabilities.

Comprehensive Service Scope

The platform delivers protection across ten integrated modules:

1. **Identity Protection & Access Control** - Microsoft Entra ID (including Protection & Governance) and Defender for Identity
2. **Endpoint Protection** - Defender for Endpoint with EDR and vulnerability management
3. **Cloud Infrastructure Security** - Defender for Cloud (CSPM/CWPP), Network Protection, and External Attack Surface Management
4. **Application Protection** - Defender for Cloud Apps with CASB capabilities
5. **Email & Collaboration Security** - Defender for Office 365 and Data Loss Prevention
6. **Data Security & Governance** - Microsoft Purview (Security, Governance, Compliance) and Microsoft Priva
7. **SIEM & Threat Hunting** - Microsoft Sentinel with cloud-scale analytics
8. **Threat Detection & Response (XDR)** - Unified XDR Portal with Microsoft Defender Suite
9. **AI-Enhanced SecOps** - Microsoft Copilot for Security
10. **Security Operations Centre** - 24/7 managed TDIR services.

Atos helps public sector organisations ensure comprehensive security amid ever-growing digital challenges. We created a fully integrated, cloud-native security solution powered by Microsoft's leading security technologies, integrating with additional industry-leading security controls. This end-to-end solution provides necessary visibility and response capabilities to identify and mitigate cyber-attacks targeting assets and systems.

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.

With our MSSP offering, public sector organisations can expect an umbrella offering built on a Cloud Security Mesh Architecture, ensuring interoperability among Microsoft’s distinct security products in Azure. Our CloudSecOps automation, 24/7 managed security services and platform integrations help achieve a more consolidated security posture, secure multi-cloud and hybrid cloud environments, and keep organisations' systems safe from emerging threats.

Crown Commercial Service Supplier

Atos

3. What technology does it use?

Microsoft invested heavily in security for Azure, ensuring all data is stored in highly secure data centres. However, cloud security follows a shared responsibility model: Azure manages the security of the cloud, while security in the cloud is the public sector organisations' responsibility.

Atos and Microsoft will expertly guide you through securing your cloud environment by protecting and monitoring essential resources. The platform is built around native Azure capabilities, with Atos and Microsoft developing managed security service specialisations uniquely designed for comprehensive protection.

Microsoft Azure CloudSecOps Protection Platform Core Technology Components

Implementation through Azure Lighthouse:

- Multi-tenant management with scalability and enhanced governance
- Delegated resource management with secure, granular access permissions
- Centralised monitoring using Azure Portal, CLI, PowerShell, or APIs
- Improved security through Azure RBAC and Active Directory
- No additional customer-side costs.

Key Technology Capabilities:

Module	Core Technologies	Key Features
Identity & Access	Entra ID, Defender for Identity	SSO, MFA, Conditional Access, PIM, Identity Protection
Endpoint Security	Defender for Endpoint	EDR, Attack Surface Reduction, Automated Investigation
Cloud Protection	Defender for Cloud, Azure Firewall, WAF	CSPM, CWPP, Network Security, DDOS Protection
Application Security	Defender for Cloud Apps	CASB, Shadow IT Discovery, DLP, Threat Detection
Email Security	Defender for Office 365	Safe Links/Attachments, Anti-phishing, BEC Protection
Data Governance	Microsoft Purview, Priva	Classification, Information Protection, Compliance Management
SIEM/SOAR	Microsoft Sentinel	Cloud-scale Analytics, AI/ML Detection, Automation

Module	Core Technologies	Key Features
XDR	Unified Defender Portal	Cross-domain Correlation, Automated Response
AI Operations	Copilot for Security	Natural Language Queries, Automated Scripts, Guided Investigation
SOC Services	Integrated Platform	24/7 Monitoring, Threat Hunting, Incident Response

Licensing Model

The service licensing model combines Atos' operational costs with Microsoft's flexible licensing structure:

Pay-as-you-go/Consumption:

- Defender for Cloud (per resource protected)
- Azure Sentinel (log ingestion)
- Azure Network Protection (Firewall, DDoS, WAF)
- Copilot for Security (Security Compute Units).

Microsoft 365 E3:

- Defender for Cloud Apps Discovery
- Microsoft Purview basic functionality
- Entra ID Plan 1
- Defender for Endpoint Plan 1.

Microsoft 365 E5:

- Full Defender for Cloud Apps
- Unified XDR Portal
- Entra ID Plan 2
- Defender for Identity
- Defender for Endpoint Plan 2
- Defender for Office 365
- Microsoft Purview full capabilities
- 400 SCUs per 1,000 E5 users for Security Copilot.

Business Benefits

The Atos Advantage

- Long-standing Microsoft Gold partner with 13 specialisations
- Dedicated Microsoft practice with 7,800+ competency certifications
- 180+ security-certified experts for Microsoft Azure
- Member of Microsoft Intelligent Security Association (MISA)
- Global community of security experts orchestrating defence
- Proven track record in the UK public sector and healthcare.

Comprehensive Business Value

Security & Compliance Excellence:

- Unified visibility with 24/7 AI-powered monitoring
- Proactive vulnerability management, reducing attack surface
- Automated investigation and response capabilities
- Real-time compliance monitoring and reporting
- Enhanced threat intelligence from Microsoft's global ecosystem.

Operational Efficiency:

- Centralised security operations through a single pane of glass
- Reduced alert fatigue through intelligent correlation
- Automated workflows reducing manual effort by up to 70%
- Continuous tuning without additional headcount
- Faster incident response (reduced MTTD/MTTR).

Cost Optimisation:

- Tool consolidation, eliminating redundant security investments
- Flexible consumption-based pricing models
- Reduced infrastructure investments
- Lower incident costs through faster mitigation
- Predictable security spend with scalability.

Business Resilience:

- Always-on threat detection and response
- Cloud-native infrastructure ensuring continuity
- Rapid incident recovery minimising downtime

- Business-critical asset prioritisation
- Strategic continuity planning support.

Tailored Benefits by Customer Type

Greenfield Customers:

- Fast time-to-value with rapid deployment
- Low upfront investment with a pay-as-you-go model
- Enterprise-grade security without significant CapEx
- Best practices and compliance by design
- Immediate access to expert SOC capabilities.

Brownfield Customers:

- Seamless tool consolidation and vendor reduction
- Enhanced detection across hybrid environments
- Accelerated modernisation without disruption
- Improved correlation between Microsoft workloads
- Continuous optimisation of existing investments.

Implementation Methodology

Implementation Phase:

- Azure Lighthouse onboarding for delegated management
- Initial environment assessment and discovery
- Security strategy workshop and goal setting
- Resource classification and prioritisation
- Deployment and initial configuration
- Integration with existing tools and processes
- Compliance standards alignment.

Run Phase:

- Continuous fine-tuning and optimisation
- Cost optimisation recommendations
- Standard and custom reporting
- Alert/incident reduction initiatives
- Technology updates and new feature adoption
- Custom integration and automation
- Proactive security posture improvements.

Education and Training: the Atos Cloud Security Transformation Workshop service will train in-house teams on cloud security best practices, emerging threats and operational procedures. This will empower internal teams to maintain and enhance the security posture proactively

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
Azure AD	Azure Active Directory
CASB	Cloud Access Security Broker
CloudSecOps	Cloud Security Operations
CSMA	Cloud Security Mesh Architecture
CSPM	Cloud Security Posture Management
CWPP	Cloud Workload Protection Platform
DLP	Data Loss Prevention
EDR	Endpoint Detection and Response
MSSP	Managed Security Service Provider
RBAC	Role-Based Access Control
SOC	Security Operations Centre
TDIR	Threat Detection and Incident Response
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