

G-Cloud 15

Cloud Native Application Protection Platform Service



Atos

Table of contents

1. What is the Cloud Native Application Protection Platform Service.....	3
2. What does it deliver?	4
3. What technology does it use ?	8
4. What terms apply?	11
5. Termination.....	12
6. How do I order?	13
7. Glossary.....	14
8. Why Atos.....	16



1. What is the Cloud Native Application Protection Platform Service

Atos Managed CNAPP (Cloud Native Application Protection Platform) is a comprehensive security service that provides unified protection for cloud-native applications throughout their lifecycle, from development to runtime. The service eliminates the inefficiencies of siloed security tools by integrating multiple cloud security capabilities into a single platform, providing continuous monitoring and protection across multi-cloud environments, including AWS, Azure, and Google Cloud Platform.

The Atos service addresses the unique security challenges of cloud-native architectures built on containers, microservices, and dynamic infrastructure through a managed approach that combines automated security controls with Atos's expert oversight. Unlike traditional security tools that are limited to specific platforms and create fragmented protection, Atos Managed CNAPP provides holistic security coverage that adapts to the ephemeral and constantly evolving nature of cloud resources.

By unifying Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), Cloud Workload Protection (CWP), and other critical security capabilities, Atos Managed CNAPP ensures comprehensive visibility and protection across all cloud layers - compute, storage, identity, and network. This convergent approach, delivered through Atos's managed services expertise, significantly reduces the complexity of managing multiple security tools whilst providing superior threat detection and response capabilities through correlated insights across the entire cloud estate.



2. What does it deliver?

Atos Managed CNAPP delivers a transformative approach to cloud-native security, moving organisations from fragmented, reactive security operations to a unified, proactive security posture. Through the combination of Tenable Cloud Security's comprehensive platform capabilities and Atos's deep security expertise and managed services delivery, customers receive a fully-managed security solution that addresses the entire cloud-native application lifecycle.

The Atos service fundamentally changes how organisations protect their cloud environments by consolidating multiple point solutions into a single, integrated platform that provides continuous visibility, automated protection, and expert-guided remediation. Rather than struggling with tool sprawl, alert fatigue, and the complexity of securing dynamic cloud infrastructures, organisations gain a mature, intelligence-driven security capability that scales with their cloud journey. This Atos-managed approach ensures that security becomes an enabler of digital transformation rather than a barrier, delivering measurable improvements in risk reduction, operational efficiency, and compliance assurance.

Through Atos's structured implementation phases - Discovery & Scoping, Implementation, and Optimisation - combined with ongoing expert oversight and monthly reviews from Atos security specialists, Managed CNAPP transforms cloud security from a complex operational challenge into a strategic business advantage. The service delivers comprehensive security outcomes through:

Unified Security Operations and Visibility

- Single pane of glass view across multi-cloud environments through a unified dashboard managed by Atos
- Comprehensive asset inventory of all cloud resources with continuous discovery
- Real-time visibility into cloud assets, resources, and configurations
- Elimination of security blind spots across cloud infrastructures

Continuous Compliance and Risk Management

- Automated compliance auditing against industry standards, including CIS, SOC2, HIPAA, GDPR, PCI-DSS, ISO 27001, NIST, and AWS Well-Architected Framework
- Continuous assessment of cloud configurations against best practices and organisational policies
- Detailed compliance reports for audit and regulatory purposes
- Proactive identification and remediation of compliance gaps and policy violations

Advanced Threat Detection and Response

- Real-time runtime threat detection monitoring cloud workloads for active threats
- Behavioural anomaly detection identifying unusual patterns indicative of security incidents
- Automated threat response capabilities to minimise alert fatigue
- Identification of toxic combinations - security risks that, when combined, create viable attack paths

Identity and Access Governance

- Complete inventory of all human and machine identities with associated entitlements
- Just-in-Time (JIT) access management for temporary, fine-grained permissions
- Automated remediation and policy enforcement for risky entitlements
- Anomaly detection for unusual behaviours related to data access and permission changes

Vulnerability and Exposure Management

- Risk-based prioritisation using Tenable's proprietary Vulnerability Priority Ratings (VPR)
- Agentless scanning provides a comprehensive inventory of software packages, PII, file signatures, and vulnerabilities
- Continuous inspection with prompt assessment of new vulnerabilities without requiring new scans
- Container image scanning in CI/CD pipelines, registries, and running workloads

DevSecOps and Infrastructure Security

- Pre-deployment scanning of Infrastructure-as-Code templates (Terraform, CloudFormation)
- Policy-as-Code enforcement ensuring deployments meet security standards
- Integration with CI/CD pipelines to identify security gaps prior to deployment
- Secrets management validation, ensuring secure handling of API keys and passwords

Atos Expert Security Management Services

- Atos-led discovery and scoping workshops to evaluate cloud architecture and security challenges

- Monthly security reviews by Atos specialists with actionable recommendations
- Cost-benefit analysis for security improvements from Atos experts
- Architecture reviews and configuration optimisation based on real-world operational data

Container and Kubernetes Security

- Continuous scanning of Kubernetes clusters for vulnerabilities and misconfigurations
- Assessment of pod security policies, RBAC settings, and cluster networking rules
- Configuration management ensuring adherence to container security best practices
- Support for on-premises and hybrid containerised environments
- **Customer Benefits**

Atos Managed CNAPP delivers tangible business value through:

Operational Efficiency Benefits

- **Tool Consolidation:** Replace multiple siloed security tools with a single unified platform managed by Atos, reducing complexity and management overhead
- **Reduced Alert Fatigue:** Atos security teams focus on critical issues through intelligent alert correlation and prioritisation
- **Streamlined Security Operations:** Single dashboard and unified workflows managed by Atos simplify security management across multi-cloud environments
- **Freed Resources:** Enable internal teams to focus on innovation whilst Atos handles security operations

Risk Reduction Benefits

- **Comprehensive Security Coverage:** End-to-end visibility through Atos's managed service eliminates blind spots across cloud environments
- **Proactive Threat Prevention:** Continuous monitoring by Atos and automated remediation prevent incidents before impact
- **Reduced Mean Time to Remediation:** Atos's prompt vulnerability assessment and prioritisation accelerate response times
- **Minimised Attack Surface:** Automated least-privilege enforcement and continuous configuration management by Atos specialists

Compliance and Governance Benefits

- **Continuous Compliance Assurance:** Atos-managed automated monitoring ensures ongoing adherence to regulatory requirements
- **Simplified Audit Preparation:** Detailed reports and compliance scorecards from Atos streamline regulatory assessments
- **Multi-Framework Coverage:** A Single platform managed by Atos addresses multiple compliance standards simultaneously
- **Reduced Compliance Violations:** Proactive gap identification by Atos prevents audit findings

Business Enablement Benefits

- **Accelerated Cloud Adoption:** Atos-implemented security guardrails enable confident cloud transformation
- **Improved Development Velocity:** Early security integration managed by Atos that doesn't slow release cycles
- **Enhanced Security Posture:** Continuous improvement through Atos expert oversight and optimisation
- **Scalable Protection:** Platform managed by Atos grows with cloud infrastructure without proportional overhead increase

Cost Optimisation Benefits

- **Reduced Tool Licensing Costs:** Atos consolidates multiple point solutions into a single platform
- **Lower Operational Overhead:** Atos managed service model reduces the need for specialised in-house expertise
- **Prevented Incident Costs:** Proactive security from Atos reduces potential breach impact
- **Efficient Resource Utilisation:** Atos automation and expert management optimise security operations

3. What technology does it use?

Atos Managed CNAPP is powered by **Tenable Cloud Security**, an AI-driven, all-encompassing exposure management platform that Atos has integrated into its managed security services portfolio. This platform provides a holistic view of an organisation's security posture, addressing the core issue of modern security - the fragmented approach to identifying and combating cyber risks - by integrating security visibility, insights, and actions across the attack surface.

Core Tenable Cloud Security Platform Features (Managed by Atos):

- **Unified Dashboard** - Single pane of glass managed by Atos to view and manage all security risks across the organisation
- **Vulnerability Management** - Atos identifies, prioritises, and helps remediate vulnerabilities across on-premises, cloud, and hybrid environments
- **Cloud Security** - Tools configured by Atos for securing cloud environments, including configuration assessments, compliance checks, and threat detection
- **Identity and Access Management** - Atos manages and secures user access to resources with least privilege enforcement
- **Threat Detection and Response** - Real-time monitoring by Atos with actionable insights and automated response options
- **Compliance Management** - Atos ensures systems comply with industry standards and regulatory requirements
- **Risk-Based Prioritisation** - Advanced analytics configured by Atos, prioritising vulnerabilities based on potential impact
- **Asset Inventory** - Comprehensive inventory maintained by Atos of all assets, providing visibility into protection needs
- **Reporting and Analytics** - Detailed reports prepared by Atos, helping security teams understand risk posture

Integrated Security Capabilities Delivered through Atos:

Cloud Infrastructure Entitlement Management (CIEM)

- Comprehensive identity and entitlement visibility managed by Atos across cloud infrastructures
- Anomaly detection and threat investigation monitored by Atos security teams
- Just-in-Time access management configured by Atos with temporary permissions
- Automated remediation of risky entitlements implemented by Atos
- Cross-platform support for AWS, Azure, and GCP managed by Atos

Cloud Security Posture Management (CSPM)

- Automated compliance auditing configured and managed by Atos against industry standards
- Configuration management by Atos, identifying and correcting misconfigurations
- Threat detection and risk assessment within cloud environments monitored by Atos
- Automated remediation of security issues orchestrated by Atos
- Multi-cloud visibility across different platforms through Atos management

Cloud Workload Protection (CWP)

- Agentless scanning configured by Atos using API connections to extract and analyse resource snapshots
- Vulnerability intelligence powered by Tenable Research with VPR ratings, interpreted by Atos experts
- Toxic combination identification by Atos for combined security risks
- Container image scanning managed by Atos before deployment and in runtime
- Compliance with AWS Well Architected, CSA, NIST, ISO 27001, and SOC II ensured by Atos

Cloud Detection and Response (CDR)

- Agentless assessment configured by Atos without performance impact or additional costs
- Live results with continuous assessment monitored by Atos against Tenable's Vulnerability & Threat Library
- Anomaly detection by Atos, identifying misconfigurations and unauthorised access
- Unified CSPM and vulnerability management in a single solution managed by Atos
- Advanced DevOps integrations configured by Atos for HashiCorp Terraform and AWS CloudFormation

Infrastructure-as-Code Security

- Policy as Code configured by Atos, allowing teams to manage infrastructure policies within codebases
- Vulnerability detection by Atos in IaC templates before deployment
- Static analysis of IaC code performed by Atos for risks and misconfigurations
- Integration with CI/CD pipelines managed by Atos for early issue detection
- Secrets management ensuring secure handling of sensitive data validated by Atos

Kubernetes Security Posture Management (KSPM)

- Automated security scans of Kubernetes clusters configured by Atos
- Threat assessment and categorisation by Atos for prioritised remediation
- Configuration management by Atos for security best practices
- Policy enforcement across containerised environments managed by Atos
- Comprehensive visibility and reporting prepared by Atos for audit purposes

Network Security

- Network discovery and compliance assessment performed by Atos
- Built-in network security policies for AWS and Azure configured by Atos
- Analysis by Atos of security group rules and firewall settings
- Detection by Atos of misconfigurations and compliance violations
- Mitigation guidance provided by Atos for discovered vulnerabilities

Data Security Posture Management (DSPM) *(Atos Standard+ Only)*

- Data discovery and classification managed by Atos across multi-cloud environments
- Risk prioritisation by Atos with contextual analysis
- Guided and automated remediation recommendations from Atos experts
- Continuous monitoring by Atos for compliance with GDPR, CCPA, and HIPAA
- Protection of sensitive data in cloud storage and databases ensured by Atos

Atos Implementation and Integration:

- **Deployment Options** - Agentless (mandatory) and agent-based (optional) scanning mechanisms configured by Atos
- **Multi-Cloud Support** - Native support for AWS, Microsoft Azure, and Google Cloud Platform managed by Atos
- **CI/CD Integration** - Seamless integration configured by Atos with development pipelines for shift-left security
- **Geo-Location Flexibility** - Customer choice of deployment location supported by Atos for data sovereignty
- **Asset-Based Licensing** - Licensing by FQDNs, IPs, identities, workloads, and OT devices managed by Atos
- **Atos Service Delivery** - Combination of Atos operational costs and Tenable licensing costs with monthly billing.



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.



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.



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 the Government Procurement.



7. Glossary

Term	Definition
API	Application Programming Interface
AWS	Amazon Web Services
CCPA	California Consumer Privacy Act
CDR	Cloud Detection and Response
CI/CD	Continuous Integration/Continuous Deployment
CIEM	Cloud Infrastructure Entitlement Management
CIS	Center for Internet Security
CNAPP	Cloud Native Application Protection Platform
CSA	Cloud Security Alliance
CSPM	Cloud Security Posture Management
CWP	Cloud Workload Protection
DevOps	Development Operations
DevSecOps	Development Security Operations
DSPM	Data Security Posture Management
FQDN	Fully Qualified Domain Name
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
HIPPA	Health Insurance Portability and Accountability Act
IaC	Infrastructure as Code
IAM	Identity and Access Management
ISO	International Organisation for Standardisation
ITSM	IT Service Management
JIT	Just in Time
KPI	Key Performance Indicator
KSPM	Kubernetes Security Posture Management
NIST	National Institute of Standards and Technology
OT	Operational Technology

Term	Definition
PaC	Policy as Code
PCI-DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
RBAC	Role-Based Access Control
ROI	Return on Investment
SIEM	Security Information and Event Management
SOC	Security Operations Centre
VPR	Vulnerability Priority Ratings



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