

**G-Cloud 15**

# **Google CloudSecOps Protection Platform Service**



**Atos**

# Table of contents

|                                                                     |    |
|---------------------------------------------------------------------|----|
| 1. What is the Google CloudSecOps Protection Platform Service ..... | 3  |
| 2. What does it deliver? .....                                      | 4  |
| 3. What technology does it use? .....                               | 5  |
| 4. What terms apply? .....                                          | 9  |
| 5. Termination.....                                                 | 10 |
| 6. How do I order? .....                                            | 11 |
| 7. Glossary.....                                                    | 12 |
| 8. Why Atos.....                                                    | 13 |



# 1. What is the Google CloudSecOps Protection Platform Service?

Atos' Google CloudSecOps Protection Platform is a comprehensive managed security service that leverages a mesh architecture approach to enable seamless interoperability between various Google security products, creating a unified and consolidated security posture for organisations.

The platform represents a strategic collaboration between Atos and Google, specifically designed to safeguard and continuously monitor critical Google Cloud Platform (GCP) resources. Whether serving an emerging startup, a small to medium-sized business, or a multinational enterprise, incorporating the expertise of Atos' 2,800+ Google-certified security professionals elevate the public sector organisation's cloud security posture through proven MSSP capabilities.

Our experts provide round-the-clock surveillance and management through 17 global SOC's, ensuring proactive protection and timely response to potential threats. This 24/7 managed service approach alleviates the security burden from customers, allowing them to focus on core business functions while we secure their Google Cloud-hosted environment.

One of the key advantages of Atos' Google CloudSecOps Protection Platform is its flexibility - it eliminates the need for dedicated in-house security personnel while strongly supporting collaboration with existing security teams. By integrating our expertise with the organisation's internal resources, we create a robust and comprehensive security strategy tailored to unique requirements and objectives, backed by our experience serving 700+ SOC clients globally.



## 2. What does it deliver?

Atos Google CloudSecOps Protection Platform service is suitable for cloud environments of any size and spans several critical security domains:

- **Identity and Access Management (IAM)** - Including Cloud Identity Premium integration
- **Network Security** - Cloud Load Balancing, Cloud Armor, Next-Gen Firewall, Secure Web Proxy
- **Data Protection** - Sensitive Data Protection, Secret Manager, Cloud KMS, Confidential Compute
- **Security Posture, Threat Intel, Detection** - Powered by Security Command Centre Premium
- **SIEM/SOAR** - Powered by Google Chronicle with advanced threat detection
- **DevSecOps** - Secure development and deployment practices.

The platform provides a security umbrella offering based on a mesh architecture strategy, integrating various security tools to form a collaborative ecosystem. This approach adds automation and orchestration capabilities that reduce deployment times (lowering costs) and minimise human error situations.

Atos helps public sector organisations ensure comprehensive security when facing ever-growing challenges in the dynamic cloud landscape. We have created a fully integrated, cloud-native security solution combining Google's leading security technologies with our advanced threat detection and response capabilities. This end-to-end security solution provides necessary visibility and response capabilities to identify and mitigate cyber-attacks targeting public sector assets and systems.

With our MSSP offering, public sector organisations receive an umbrella solution built on Cloud Security Mesh Architecture principles, ensuring interoperability between GCP's distinct security products. Our CloudSecOps automation and 24/7 managed security services help achieve a more consolidated security posture, secure hybrid cloud environments, and protect public sector systems from emerging threats.



### 3. What technology does it use?

Google has invested heavily in GCP security, securing all data in highly secure data centres. However, cloud security follows a shared responsibility model - Google manages security OF the cloud, while security IN the cloud remains the public sector organisation's responsibility.

Atos and Google expertly guide organisations through securing their cloud environment by protecting and monitoring essential GCP resources—Atos Google CloudSecOps Protection Platform leverages native GCP capabilities to enhance security posture. Through close collaboration with Google, Atos has developed Managed Security Service (MSS) specialisations uniquely designed to protect and monitor organisations' essential GCP resources, delivered as a fully managed service.

#### Google CloudSecOps Protection Platform Components

The platform consists of modular components tailored to organisational requirements - from one mandatory minimum to several integrated services:

Table 1: Google CloudSecOps Protection Platform Components

| Module/<br>Component           | Mandatory/<br>Optional | Functional Requirements                                                                                                                                          |
|--------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Consulting                     | Optional               | Services: Cloud Security Assessment, Architecture Design, Compliance Advisory                                                                                    |
| Identity and Access Management | Mandatory*             | Services: GCP Cloud Identity Premium, GCP IAM, Workforce Identity Federation, Organisation Policies                                                              |
| Network Security               | Mandatory*             | Firewall Services: GCP Cloud Next-Gen Firewall<br>DDoS Mitigation: GCP Cloud Armor Managed Protection Plus<br>Additional: Cloud Load Balancing, Secure Web Proxy |
| DevSecOps                      | Mandatory*             | Managed WAF Services: GCP Cloud Armor, Web Security Scanner                                                                                                      |
| Data Protection                | Mandatory*             | Services: GCP Cloud KMS, HSM, EKM, Sensitive Data Protection, Secret Manager, Confidential Compute                                                               |

| Module/<br>Component                      | Mandatory/<br>Optional | Functional Requirements                                                                       |
|-------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------|
| Threat Detection and Response (SIEM/SOAR) | Mandatory*             | Services: Cloud Logging and Threat Intelligence, Google Chronicle, SOC powered by Chronicle** |
| Security Posture Management               | Mandatory*             | Services: GCP Security Command Centre Premium                                                 |
| Cloud-Native Security Dashboard           | Mandatory              | Services: GCP Security Command Centre with enhanced dashboard functionality                   |
| Managed Detection and Response            | Optional               | Services: Advanced MDR capabilities with AI-driven threat hunting                             |

\*At least one component from the mandatory categories must be selected

## Licensing

The Google CloudSecOps Protection Platform employs a transparent dual licensing model:

- Atos Managed Services: Fixed operational costs for 24/7 monitoring, management, and expertise
- GCP Native Services: Pay-as-you-go consumption charged directly via Google's monthly billing.

This flexible model ensures cost optimisation while maintaining enterprise-grade security capabilities.

## Business Benefits

### Cloud Adoption

Expert deployment and enablement of Google Chronicle SecOps cloud instances by Atos security specialists

### Virtually unlimited compute, scale, and storage capabilities

Strengthened security posture and compliance through integration with GCP Native Security services including SCC-Premium

### Harmonised & Simplified

- Greater speed and agility in threat response through automation
- Scalable security with superior visibility and control

- Risk reduction through deeply integrated services
- Agile, homogeneous, and reliable security architecture by design
- Out-of-the-box capabilities replacing self-developed solutions
- Streamlined security surveillance and operations.

### Latest Technology

- Innovation delivered at cloud speed
- Security-by-design embedded into GCP cloud infrastructure
- Continuous compliance and posture assessment
- Comprehensive security coverage improves overall security posture
- Built with the highest standards for privacy and data security.

### Cost Savings

- Flexible pay-per-use models
- Reduced infrastructure investments through a cloud-native approach
- Transition from manual processes to automation
- Mitigated investment risks through proven solutions
- Continuous innovation without additional capital expenditure.

### Atos and Google Cloud Partnership

- Strategic partners since 2013
- 5-time Google Partner of the Year (3 for Security Excellence)
- 11 Partner Specialisations + 3 MSP certifications
- 2,800+ Google Cloud certifications
- 400+ Google client projects since 2019
- 17 Global SOC's with 24/7 coverage
- 700+ SOC clients worldwide.

Bringing together our experience, innovation, and leadership, we expertly guide public sector organisations through digital transformation, turning vision into reality.

Unleash the power of Google Cloud to modernise applications and workloads, unlock insights, and transform legacy infrastructure into a powerful platform for sustainable future growth.

It is all possible today with Atos & Google Cloud.

Together, Atos and Google Cloud bring market-leading technology, a deep understanding of legacy infrastructure, and proven experience needed to de-risk cloud migration journeys.

We understand the inherent complexity of mission-critical operations tied to legacy systems and ensure stability and continuity as key applications and services transition between environments.

We recognise that sovereignty and data protection are paramount for public sector organisations, helping embed security, compliance, and auditability into the fabric of your cloud migration.

We appreciate the realities of technical debt and help unshackle organisations from legacy constraints.

We transform legacy environments into future-proof platforms for growth.



## 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](mailto: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.



# 7. Glossary

| Term | Definition                        |
|------|-----------------------------------|
| GCP  | Google Cloud Platform             |
| KMS  | Key Management Service            |
| MDR  | Managed Detection and Response    |
| MSS  | Managed Security Service          |
| MSSP | Managed Security Service Provider |
| SaaS | Software as a Service             |
| SOC  | Security Operations Centre        |
| WAF  | Web Application Firewall          |



## 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](https://atos.net)