Crown Commercial Service
Supplier

G-Cloud 15

Secure Access Service Edge (SASE) Service

Atos

Table of contents

Crown Commercial Service *Supplier*

Atos

1. What is the Secure Access Service Edge (SASE) Service?

Atos' Secure Access Service Edge (SASE) service is a cloud-delivered, converged networking and security framework that enables organisations to securely connect users, devices, and applications regardless of their location. The service combines comprehensive security capabilities with wide area networking functionality into a unified, cloud-native architecture that replaces traditional perimeter-based security models.

The service addresses the fundamental shift in enterprise IT where users and applications have moved outside traditional network perimeters, requiring secure access to an ever-growing ecosystem of SaaS, PaaS, and IaaS resources. By converging multiple point solutions into a single framework operated and delivered as a cloud service, Atos SASE eliminates the complexity of managing disparate security products, each with its own policies and interfaces.

As a managed service, Atos SASE provides 24/7 monitoring, maintenance, and expert security management, allowing organisations to focus on their core business while ensuring a robust security posture and optimal network performance. The service is designed to support digital transformation initiatives by enabling secure, scalable, and flexible connectivity for hybrid work environments, cloud migrations, and distributed enterprises. A key differentiator is the availability of **Sovereign SASE** options, enabling organisations to maintain complete control over data residency, inspection locations, and compliance requirements - particularly critical for government, healthcare, and financial services sectors operating under strict regulatory frameworks.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

Atos's SASE service delivers comprehensive security and networking capabilities through a modular, scalable approach that addresses the critical challenges of modern distributed enterprises:

Core Security Services

Secure Internet Access

- **Secure Web Gateway (SWG)** protecting users from web-based threats while enforcing corporate acceptable use policies
- URL filtering, web visibility, malicious content inspection, and web access controls
- SWG functionality based on FortiOS explicit web proxy, captive portal, and authentication features when using Fortinet
- Application-level filtering ensuring granular control over web applications
- DNS protection for blocking malicious domains and preventing data exfiltration
- **Cloud Access Security Broker (CASB)** providing on-premises or cloud-based security policy enforcement
- Authentication, single sign-on, authorisation, and credential mapping capabilities
- Direct connections to leading SaaS providers to access usage and data stored in the cloud through Fortinet
- Shadow IT discovery and risk assessment
- Malware detection/prevention and compliance monitoring

Zero Trust Network Access (ZTNA)

- Software-defined perimeter (SDP) with adaptive trust model
- Need-to-know, least-privileged access defined by granular policies
- Universal ZTNA updates, including access support to any application from any location, and an application catalogue that automates configurations with Fortinet
- Remote user connectivity without placing users on the corporate network
- Elimination of VPN concentrators, DDoS protection, and firewall appliances

Comprehensive Threat Protection

- **Network Firewalling Services** with line-rate operation, ensuring no performance bottlenecks
- FWaaS functionality based on FortiOS Next-Generation Firewall (NGFW) features when using Fortinet
- DNS protection, including filtering, malware/botnet protection, and secure resolution
- AI/machine learning technology to identify and isolate advanced threats in real-time through FortiGuard
- API-based access to SaaS for data context and configuration information

Sovereign SASE Capabilities (Fortinet-Specific)

Data Sovereignty and Compliance

- Organisations can determine how their data is routed and where security inspections occur, whether to a data centre owned by Fortinet, a partner, or the customer
- Choice of Analytics PoP for log storage to meet compliance requirements such as GDPR
- Regional control over data processing and storage
- Support for highly regulated verticals, including finance, government, and healthcare

Business Outcomes

Complete Visibility Across Hybrid Elements

- Complete visibility over users, applications, and data
- Traffic classification by application on all ports
- Single pane of glass solution for management
- Reporting for various key metrics

Less Complexity

- Elimination of siloed point security solutions
- No need to ship, install, and upgrade hardware at remote/branch locations
- Faster deployments with a homogeneous landscape
- Out-of-the-box capabilities instead of self-developed solutions

Consistent Data Protection

- Consistency across locations and environments
- Protection for both SaaS applications and on-premise repositories
- Ease of deployment through cloud delivery

Cost Reduction

- Single solution for learning and managing
- Reduced infrastructure investments
- Simplified management with less complexity
- Licence cost reduction through consolidation

Better Network Performance and Reliability

- SLAs backed by industry-leading cloud providers
- Single high-performance SASE solution
- Zero-day support for new features and applications
- Self-healing features that rectify issues in real-time when building autonomous SD-WAN networks with Fortinet

Managed Service Deliverables

Transform & Transition (T&T) Services

- Data gathering and requirements analysis
- Design and architecture planning
- Governance framework establishment
- SSE portal setup and configuration
- Hardware and software procurement support
- Integration with Identity Providers (IdP)
- Integration with SIEM and ATF solutions
- Proof of Concept and pilot implementations
- Production user and site onboarding

Run Services - Operational Management

- Service maintenance ensuring optimal performance
- Continuous monitoring of all SASE components
- Standard reporting on metrics

- Comprehensive service management
- Engineer on standby for critical incidents
- Cybersecurity delivery management
- Service management standby support
- **Digital Experience Monitoring (DEM) - Mandatory Component**
- IT management technology measuring performance between end users and applications
- Dashboard for viewing performance data and health metrics
- Monitoring for web applications, APIs, and mobile apps
- DEM providing end-to-end visibility with improved user experience and application performance reports
- User and customer journey experience management

Platform-Specific Benefits

When Delivered Through Fortinet Unified SASE:

- Built on a unique platform with one OS, one unified agent, one management system, and one data lake
- Single data lake and unified data model for consistent policy enforcement and event tracking

When Delivered Through Alternative Platforms:

- Cloudflare One for global edge performance and cost efficiency
- Netskope for advanced CASB capabilities
- Zscaler for existing investment protection

Advanced Security Features

Data Loss Prevention

- Advanced DLP functionalities with AI/ML-driven predefined data patterns to prevent data exfiltration
- Separate category to secure GenAI applications with DLP
- Next DLP integration bringing a cloud-native SaaS data protection platform with AI/ML-based anomaly detection

Remote Browser Isolation

- RBI functionality as a core feature of FortiSASE
- RBI configured natively within the FortiSASE cloud-based management console
- Protection against web-borne attacks through isolated browsing

Service Level Commitments

Performance and Availability

- 99.99% service availability for critical security services (industry standard)
- Latency guarantee for security inspection backed by the global reach of hundreds of security PoPs
- 24/7 monitoring and incident response
- Regular security updates and threat intelligence integration

This comprehensive delivery model ensures organisations achieve their digital transformation objectives while maintaining robust security, optimal performance, and operational efficiency through a managed service approach.

Crown Commercial Service *Supplier*

Atos

3. What a technology does it use?

Atos' SASE service is primarily delivered through Fortinet Unified SASE, comprising FortiSASE (cloud-delivered SSE) and Fortinet Secure SD-WAN. The service maintains the flexibility to leverage alternative platforms, including Cloudflare One, Netskope SASE, and Zscaler SASE, based on specific customer requirements.

Core Platform Architecture

Unified Foundation (Fortinet)

- Built on a unique platform with one OS (FortiOS), one unified agent (FortiClient), one management system, and one data lake—all enhanced with FortiGuard AI-Powered Security Services
- Integrates networking and security functions like secure SD-WAN, FWaaS, SWG, CASB, ZTNA, and DLP as a single-vendor, cloud-delivered platform
- Single data lake and unified data model for consistent policy enforcement and event tracking, with regional log storage

Core SASE Security Components

Zero Trust Network Access (ZTNA)

- **Fortinet Universal ZTNA:** Access support to any application from any location with an application catalogue that automates configurations for all ZTNA application integrations
- Extends principles of ZTA to verify users and devices before every application session
- Support for both TCP and UDP-based applications
- Continuous device posture reassessment

Secure Web Gateway (SWG)

- FortiProxy: SWG functionality based on FortiOS explicit web proxy, captive portal, and authentication features
- FortiGuard Labs threat intelligence used by the FWaaS and the SWG
- URL filtering and application control
- DNS filtering integrated with security policies

Cloud Access Security Broker (CASB)

- **FortiCASB:** Directly connected to leading SaaS providers to access usage and data stored in the cloud
- Ability to scan provisioned cloud resource configurations for potential threats as well as SaaS application data
- API-based integration with major SaaS platforms
- Shadow IT discovery capabilities
- Alternative delivery through Netskope CASB or Cloudflare CASB

Firewall-as-a-Service (FWaaS)

- **FortiSASE FWaaS:** Security efficacy matches that of a FortiGate Firewall
- FWaaS functionality based on FortiOS Next-Generation Firewall (NGFW) features
- IPS, anti-malware, web security, anti-spam, sandbox capabilities
- AI/machine learning technology to identify and isolate advanced threats in real-time
- Can leverage alternative FWaaS services from other platforms

SASE Networking Components

Software-Defined WAN (SD-WAN)

- Fortinet Secure SD-WAN: Only SASE cloud with built-in SD-WAN and ADVPN (dynamic tunnels) functionality
- On-demand full mesh networks and self-healing features that rectify issues in real-time
- IPSec tunnels from SASE PoP to multiple SD-WAN Hubs
- Support for third-party SD-WAN connectivity
- Integration available with Zscaler Branch and Cloud Connector or Netskope Borderless SD-WAN

Advanced Security Technologies

Data Loss Prevention (DLP)

- Advanced DLP functionalities as part of FortiSASE with AI/ML-driven predefined data patterns
- A separate category created to secure GenAI applications with DLP

- Next DLP acquisition bringing cloud-native SaaS data protection platform with AI/ML-based anomaly detection and classification capabilities
- DLP capabilities available across all platform options

Remote Browser Isolation (RBI)

- RBI functionality as a core feature of FortiSASE f
- RBI is configured natively within the FortiSASE cloud-based management console to isolate user web browsing traffic
- Protection from web-borne attacks
- RBI services available through alternative platforms

AI-Powered Security

- FortiAI GenAI assistant now available for Fortinet Secure SD-WAN to manage and orchestrate the entire SD-WAN infrastructure
- 8 security domains using AI and 42 solutions driven by AI
- FortiAI integration with FortiAnalyzer and FortiManager

Sovereign SASE Technology (Fortinet-Specific)

Data Sovereignty Controls

- Customers can determine how their data is routed and where security inspections occur, whether to a data centre owned by Fortinet, a partner, or a customer
- Ensures robust data privacy and compliance while offering enhanced security and flexibility
- Choice of log storage location allowing organisations to meet compliance requirements such as GDPR

Platform Infrastructure

Global Network Architecture

- Global Security Points of Presence (PoPs) to provide access to remote users
- Global network of FortiPoPs with integrated SD-WAN optimisation and security processing units (SPUs) for accelerated traffic handling
- Hundreds of security PoPs with a latency guarantee for security inspection
- Alternative platforms provide their own global networks

Unified Management

- FortiSASE cloud-based management console
- Unified management console (single pane of glass) for all SSE capabilities (FWaaS, SWG, ZTNA, CASB, etc.)
- Native SCIM support, making users and groups created on the identity provider directly available in the SASE portal

Identity and Device Integration

- **FortiClient Unified Agent:** One unified agent supports multiple use cases, including ZTNA, traffic redirection to SASE, and Endpoint protection
- **Platform Support:** Wide range of OS including Windows, macOS, Linux, Android, and iOS
- **Identity Providers:** FortiTrust ID, LDAP, and RADIUS support
- **Endpoint Integration:** EDR features added to FortiClient alongside VPN, ZTNA, EPP, DEM, NAC, and SASE

Digital Experience Monitoring (DEM)

- DEM provides end-to-end visibility
- FortiMonitor platform for performance monitoring (when using Fortinet)
- Improved user experience and application performance reports with faster mean time to detection
- Mandatory component regardless of platform selection

Integration Capabilities

Fortinet Security Fabric Integration

- Integration with Fortinet Security Fabric platform using one operating system, FortiOS, across security controls
- Endpoint Management Service based on FortiClient EMS
- FortiAnalyzer for logging and analytics
- FortiManager for policy management
- Out-of-the-box SIEM and SOAR services through FortiAnalyzer

Deployment Flexibility

Multiple Deployment Models

- Agentless: Web browser-based device, low-end device, or operational technology device with explicit support
- Agent-based deployment with FortiClient
- Native SD-WAN integrations, support for thin edge locations, agent-based and agentless access
- Support for third-party SD-WAN connectivity and integrated Google Cloud and Fortinet PoPs

Platform Selection Flexibility

While Fortinet Unified SASE serves as the primary technology platform, Atos maintains the capability to deliver through:

- Cloudflare One: For organisations requiring global edge performance
- Netskope SASE: For advanced CASB requirements
- Zscaler SASE: For existing Zscaler investments

Technical Differentiators

Fortinet-Specific Advantages:

- Sovereign SASE capability for data control
- 12 years of ML and AI-powered services development

This technology foundation enables Atos to deliver enterprise-grade SASE services combining Fortinet's unified platform with flexibility to accommodate diverse requirements, with particular strength in Sovereign SASE capabilities for organisations requiring complete control over data sovereignty and compliance.

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
AI	Artificial Intelligence
API	Application Programming Interface
ATF	Advanced Threat Detection
BEC	Business Email Compromise
BYOD	Bring Your Own Device
CASB	Cloud Access Security Broker
CDN	Content Delivery Network
CI/CD	Continuous Integration/Continuous Deployment
CIA	Central Intelligence Agency
CNI	Cloudflare Network Interconnect
DDoS	Distributed Denial of Service
DEM	Digital Experience Monitoring
DFIR	Digital Forensics and Incident Response
DLP	Data Loss Prevention
DNS	Domain Name System
DNSSEC	DNS Security Extensions
EDF	Email Detection Fingerprint
FBI	Federal Bureau of Investigation
FWaaS	Firewall-as-a-Service
GDPR	General Data Protection Regulation
GenAI	Generative Artificial Intelligence
GRE	Generic Routing Encapsulation
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure-as-a-Service
IAM	Identity and Access Management
IdP	Identity Provider

Term	Definition
IGA	Identity Governance and Administration
IOC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISO	International Organisation for Standardisation
IT	Information Technology
L1/L2/L3	Level 1/2/3 Support
LLM	Large Language Model
MDM	Mobile Device Management
MPLS	Multiprotocol Label Switching
MSSP	Managed Security Service Provider
MXDR	Managed Extended Detection and Response
NGFW	Next-Generation Firewall
NHS	National Health Service
NIS	Network and Information Security
NSA	National Security Agency
OAuth	Open Authorisation
OCR	Optical Character Recognition
OpenID	OpenID Connect
OT	Operational Technology
PaaS	Platform-as-a-Service
PCI-DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PoP	Point of Presence
QoS	Quality of Service
RBI	Remote Browser Isolation
RFC	Request for Comments
SaaS	Software-as-a-Service

Term	Definition
SAML	Security Assertion Markup Language
SASE	Secure Access Service Edge
SCADA	Supervisory Control and Data Acquisition
SD-WAN	Software-Defined Wide Area Network
SDP	Software-Defined Perimeter
SEG	Secure Email Gateway
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMS	Short Message Service
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Centre
SOC2	Service Organisation Control 2
SIP	Session Initiation Protocol
SSE	Security Service Edge
SSL	Secure Sockets Layer
SSO	Single Sign-On
SWG	Secure Web Gateway
T&T	Transform and Transition
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAAP	Web Application and API Protection
WAF	Web Application Firewall
WAN	Wide Area Network
WANaaS	WAN-as-a-Service
WARP	Cloudflare WARP

Term	Definition
XDR	Extended Detection and Response
YARA	Yet Another Recursive Acronym
ZTNA	Zero Trust Network Access
ZTAA	Zero Trust Application Access

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