AlgoSec SaaS Services

SECURITY PRACTICES

V28

March 2026

Revision History

Version	Date	Changes	Auth/ Editor	Approved By
28	26-Mar-26	Update AlgoSec Usage of AI and LLM section	MS	LB
27	10-Feb-26	Added link to AlgoPedia article: Data exchanged from ASMS to the AlgoSec SaaS environment	MS	LB
26	17-Dec-25	Added information related to Algo New section on AlgoSec Usage of AI and LLM	MS	LB
25	10-Nov-25	Updated architecture diagram	MS	LB
24	14-Aug-25	-Added sections: • AWS Separation of onboarding and data collection • Logging and Auditing	MS	LB
23	15-Jun-25	- Modified: Description of ASMS–SaaS communication flow: Clarified that ASMS always initiates communication with Kafka hosted in the AlgoSec cloud, using outbound connections authenticated via certificate. Updated wording to remove the implication that AlgoSec SaaS pushes data to ASMS. Based on architectural review to ensure technical accuracy and alignment with security model.	MS	DL
22	24-Mar-25	- Added: Support for Singapore (SGP) region for ACE	MS	DL
21	12-Mar-25	- Modified: Modified content for ACE - Added: Support for Singapore (SGP) region for AppViz	MS	DL
20	19-Nov-24	- Modified: ObjectFlow now supports IND region	MS	DL
19	6-Nov-24	- Added: ObjectFlow now supports backup & restore	MS	DL
18	3-Nov-24	- Modified: ObjectFlow now supports UAE region	MS	DL
17	8-Oct-24	- Modified: ObjectFlow now supports ME region	MS	DL

Contents

AlgoSec SaaS Services Security Practices

The purpose of this document is to provide customers of AlgoSec SaaS Services with information needed to assess the impact of AlgoSec SaaS Services on the overall Data Management and Security posture by detailing how data may be captured, processed, and stored by and within the SaaS products used.

AlgoSec SaaS solutions

AlgoSec's current SaaS-based offering includes:

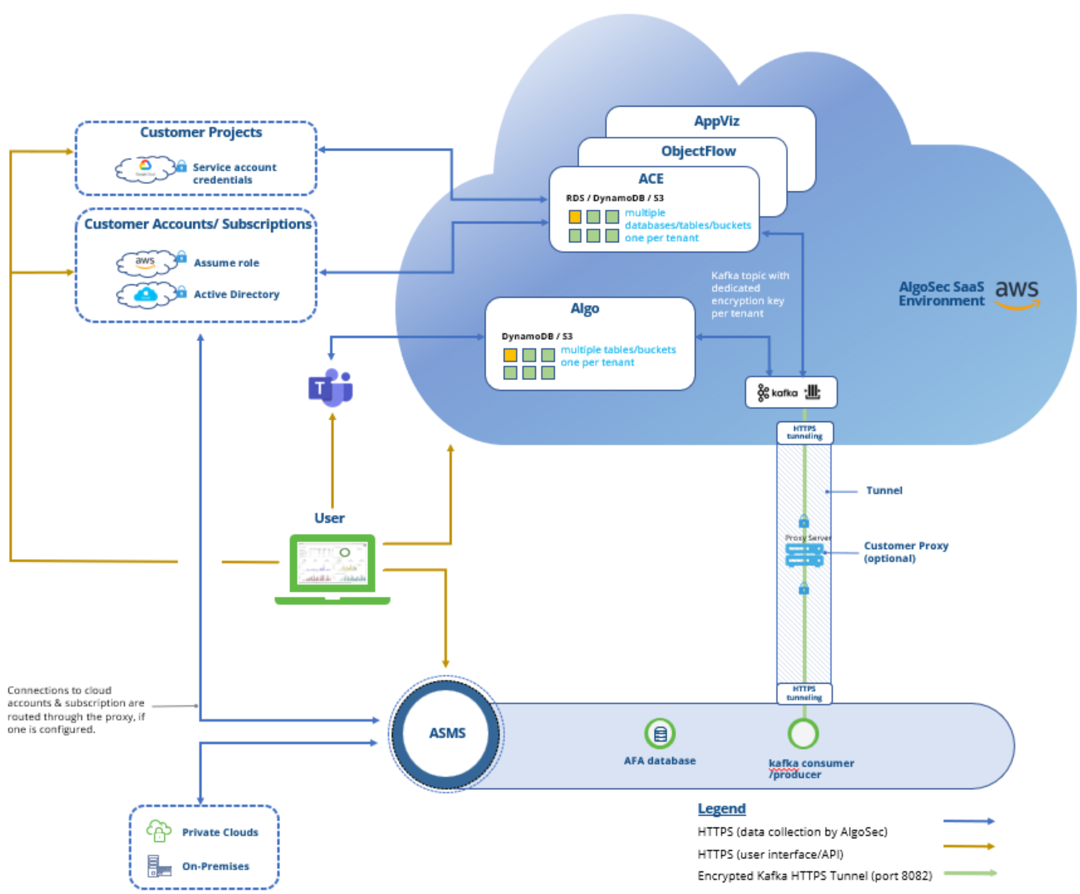
- **AlgoSec Cloud Enterprise (ACE)**: Enhance your ability to map and secure your cloud applications with deep visibility, consistent enforcement of security policies across hybrid environments, and automated change management. By combining robust network security features with advanced application analysis, ACE ensures an unmatched security posture and streamlined compliance management, empowering you to unify security across all your applications effortlessly.
- **ObjectFlow**: Simplify the task of network security object management. ObjectFlow provides a single source of truth repository for all the organization's firewall and SDN objects.
- **AppViz**: SaaS-based version of ASMS Suite AppViz that supports an application-centric approach to your network security policy management.
- **Algo**: AI-powered security assistant with advanced natural language capabilities. Algo integrates with AlgoSec products to deliver real-time access to security data, workflows, and insights.

AlgoSec SaaS services security considerations

AlgoSec is committed to upholding the highest levels of data protection. As cyber professionals, we are keenly aware of the criticality of ensuring the security and privacy of user data. Any customer data stored on or processed by AlgoSec is secured with state-of-the-art technologies. We operate ongoing rigorous technical and organizational security controls on all the services listed in this document, focusing on monitoring, change management, security updates and closing gaps from yearly penetration tests.

AlgoSec holds multiple certifications, demonstrating our firm commitment to top-tier security. We strive to comply with and maintain high-quality standards in line with globally recognized frameworks. AlgoSec is certified for the **ISO/IEC 27001:2022 & ISO/IEC 27017:2015** standards which outlines the best practices for information security management systems. In addition, AlgoSec has been certified following a **SOC 2 Type II audit** conducted by an independent service auditor. This audit evaluates the design, implementation, and effectiveness of the controls we have in place for our products.

ASMS - SaaS Connectivity and Data Segregation Architecture



Tenant and user management

Tenant and user management data is stored securely as follows:

Isolation of data between tenants

AlgoSec SaaS does the following to isolate data between tenants:

- **AlgoSec SaaS uses stateless services.** AlgoSec SaaS services do not store data of any kind in memory that may leak between actions of different tenants.
- **AlgoSec SaaS isolates data at rest.**

  We deploy dedicated tenant infrastructure and separate databases and S3 buckets for each customer. Each designated database requires access credentials. The access credentials are available only to AlgoSec services and applications and not directly to the user. These DB credentials are held in AWS KMS service (see below) and are accessible only by users of that tenant. Encryption key management of the S3 buckets is owned by Amazon S3. Refer to the diagram above.

Role Based Access Control (RBAC)

Out of the box, we provide these different roles: Admin, Cloud Security Manager & Auditor, custom roles, and other user-based custom permissions. Each role provides a specific set of allowed operations. Admin role is allowed for all operations.

User management and authentication (For Ace, ObjectFlow and AppViz)

AlgoSec SaaS uses the Cognito AWS service to manage users and create unique identities for users and federate them with identity providers (AAD). AlgoSec SaaS allocates a designated user pool for each tenant, which is isolated from other tenants. Users of one tenant cannot access other tenants, even if usernames are identical.

AlgoSec SaaS runs OAuth 2.0 authentication against these designated user pools, where each user must specify their tenant ID. The tenant ID indicates which Cognito user pool AlgoSec SaaS should redirect to.

AlgoSec SaaS provides the option of setting Multiple Factor Authentication (MFA) enforcement for each user in the system with secure MFA device setup and routine authentication powered by the AWS Cognito service.

AlgoSec SaaS service allows Single Sign-On (SSO) using external identity providers (IdP) such as How to Configure a Microsoft Entra ID Application via SAML 2.0 Authentication method.

Authentication for Algo

Algo is Microsoft Teams–integrated and uses **Microsoft Entra ID (Azure Active Directory v2)** for authentication. This enables secure, token-based access control and seamless **Single Sign-On (SSO)** within the Microsoft 365 environment.

When a user interacts with Algo through Microsoft Teams, the bot performs **OAuth 2.0 authorization** via Entra ID. Upon successful authentication, Algo obtains an **access token** representing the user's Microsoft identity, which can be validated against the Entra tenant to ensure authenticity and authorization.

Amazon Cognito

Amazon Cognito provides multi-factor authentication.

Amazon Cognito is compliant with the following standards:

- PCI DSS
- SOC
- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO 9001
- HIPAA

For more details, see https://aws.amazon.com/cognito/.

ACE adheres to the Principle of Least Privilege

The majority of permissions requested by ACE are read-only, to read config data.

To provide the best value for our customers and enable the highest level of security, ACE requires certain write permissions. These permissions are carefully selected to enable the full scope of ACE functionality. Some of them are optional as described in the documentation. For more information about permissions and roles required by ACE, see:

- **AWS** – https://techdocs.algosec.com/en/ace/content/cloud-common/ace-access-aws.htm
- **Azure** – https://techdocs.algosec.com/en/ace/content/cloud-common/ace-access-azure.htm
- **Google Cloud** – https://techdocs.algosec.com/en/ace/content/cloud-common/ace-access-gcp.htm

Data handling

AlgoSec SaaS stores sensitive data, such as passwords and tokens, encrypted using the AWS KMS service. For more details, see https://aws.amazon.com/kms/features/.

Encryption

Data Encryption at Rest	All data at rest is encrypted using the AES-256 algorithm or DynamoDB tables, encrypted with Amazon Managed Keys.
Data Encryption in Transit	All data in transit is encrypted using TLS 1.2 or 1.3

Protocol Internal communication

Each AlgoSec SaaS service communicates with others using a REST API or message queues.

- REST calls run over HTTPS, using server-side authentication.
- Queue messages are handled by AWS SQS and are accessible only for some of the services. Queue messages are not exposed to external calls. Messages to and from the queue are done via HTTPS.

Data exposed to AlgoSec SaaS

AlgoSec SaaS services may collect a small amount of personally identifiable information (PII), limited to business contact details (names, business email addresses, and employee IP addresses). Please see specifics for each AlgoSec SaaS solution below.

Note: For details what information is transferred, under which scenarios, and for what purpose, while highlighting the controls available to customers to manage or restrict these data flows, see Data exchanged from ASMS to the AlgoSec SaaS environment.

- **ACE:** ACE contains cloud asset inventory, cloud-native firewall, and security policy data. Cloud App Analyzer collects and saves data that is essential for the operation of the cloud security solution for our customers. All user data is sent and stored in a highly secure and encrypted manner to prevent any unauthorized access or data breaches. Furthermore, any data that is collected is anonymous (without any privacy identifiers).

  This data includes:

  - Cloud Asset Metadata: Metadata related to **cloud** assets and configuration is collected to facilitate the optimal operation of the ACE solution and to deliver the intended value to our customers.
  - **Docker images:**

- **Initial Storage and Analysis:** Analyzed layers of container images are initially stored in a tenant-specific cache. This method ensures that the unique data pertaining to each tenant is securely isolated.
- **Shared Caching Mechanism:** To enhance efficiency, image layers that are not unique to a single tenant and are utilized by multiple tenants are moved to a communal cache. This shared resource allows for the optimized analysis of container images while maintaining the necessary separation of tenant-specific data.
- **Metadata Storage:** For reporting and display purposes, we store only the metadata of analyzed Docker images in an encrypted format within AWS S3 Buckets. This includes crucial information such as the base image details, identified vulnerabilities and malware, and the runtime behavior of the image under isolated conditions.
- ACE never stores user passwords and delegates user authentication functions, such as new user registration, login, logout, and password recovery, to AWS Cognito.

- **ObjectFlow:** ObjectFlow contains Object name, content, and their relations (Object group members).
- **AppViz**: AppViz contains application's connectivity specifications, risk, and vulnerability data. AppViz is out of band and does not process or observe application traffic.
- **Algo**: Algo does not persist any information whatsoever.

No IPs of the end user registration is stored.

You may choose to connect your AlgoSec SaaS tenant to your on-premises ASMS system*. If you do so, your AlgoSaaS tenant is not exposed to the credentials that are used to access the security devices managed by ASMS.

**Benefits to doing this include, for example: for ACE, connectivity check, for ObjectFlow, object sync, FireFlow change requests and more, and for AppViz SaaS-version, object sync, FireFlow change requests, Application Discovery data, connectivity checks, ASMS application-level risks, scanner information sharing and more.*

Privacy regulations

AlgoSec SaaS services may collect a small amount of PII, limited to business contact details (names, business email addresses, and employee IP addresses). AlgoSec is committed to protecting personal data processed by AlgoSec SaaS. We will not access the content of the information in a way that would allow the service to acquire meaningful information about natural persons, other than in exceptional cases where it is necessary for identifying security threats or investigating suspicious behavior indicative of attack.

Any information stored on or processed by AlgoSec SaaS are secured with state-of-the-art technologies, and AlgoSec operates rigorous technical and organizational security controls.

Backup and restore

AlgoSec ensures the safety and reliability of customer data through a rigorous backup protocol. Nightly backups are carried out with a retention period of 14 days. These backups are securely stored within the same AWS region as the

SaaS account. As per AWS, each region is distributed across three Availability Zones (AZs) within the region, with each AZ approximately 100 kilometers apart, ensuring added redundancy.*

To safeguard data at rest, each backup vault is encrypted with a unique encryption key allocated per customer to ensure both security and data segregation. AlgoSec continuously monitors events that may require a recovery from a backup, with no action required from customers.

Access to these backups is strictly controlled, reserved only for privileged SRE/DevOps team members, and is granted solely for backup and restore operations.

In the event of a system restoration, our Disaster Recovery (DR) support includes:

- RTO: Maximum of 24 hours to recover the service
- RPO: Ensures that no more than 72 hours of data is at risk of being lost

All necessary actions following a backup will be clearly communicated to users as an integral component of the backup and restore process, ensuring clarity and continuity of operations.

Logging and Auditing

AlgoSec SaaS maintains detailed audit trails for critical administrative and operational actions. Token generation events for service accounts are logged and can be viewed directly within the ACE interface (in Settings>Access Management>User Activity tab) or retrieved programmatically via the Retrieve User Activity Events API. These logs can also be exported and integrated with customer SIEM platforms for centralized monitoring. Administrative activities are also logged in AWS CloudTrail, providing a secondary layer of tracking for environment-level changes.

**Out of region support: New regions can be added for an additional fee. Contact AlgoSec for more information.*

AlgoSec Usage of AI and LLM

AlgoSec currently uses AI in the following applications: **Algo** and **AppViz** (for application discovery based on FireFlow change requests and firewall rules analysis).

AlgoSec Application leverages large language models (LLMs) trained by AI model providers and delivered through a managed cloud AI service (Amazon Bedrock). The models are accessed via secured APIs and are used strictly for natural language understanding and response generation.

All AI processing and LLM operations occur exclusively within the customer's dedicated AlgoSec SaaS tenant deployed in the customer's designated AWS region (e.g., Sydney), with logical isolation enforced to prevent any cross-tenant data access or processing.

AlgoSec does not train or fine-tune AI models. Instead, AlgoSec relies on foundation models made available through **Amazon Bedrock**, including models provided by third-party AI providers (such as Anthropic, OpenAI, Meta, and others). User inputs are processed in real time to generate responses and are not retained by the AI model provider beyond the scope of the request. AlgoSec confirms that AlgoSec data and/or customer data are not used to train their models. According to AWS documentation, AWS Bedrock does not use prompts and continuations to train AWS models or distribute such data to third parties and does not store or log that data in its service logs.

AlgoSec does not persist prompts or model responses beyond the duration required to process the request, except for minimal system logs required for operational monitoring and security purposes, in accordance with AlgoSec's data retention policies.

The AI integrated within AlgoSec offerings **does not make decisions or operate autonomously**. It generates recommendations only, and the user decides whether to accept or act on them. The application may propose actions based on model interaction, but any action is executed only after explicit user approval.

All data transmitted to AWS Bedrock is encrypted in transit and processed using secure, access-controlled mechanisms aligned with AWS security best practices.

ASMS - AlgoSec SaaS trust and communication

Refer to the diagram above.

For ASMS A32.20 and above: ASMS-AlgoSec SaaS secure communication takes place over TLS, which by ASMS default is transported over an HTTPS tunnel. AlgoSec does not access, store, or manage any highly sensitive, US regulated PII data across its SaaS solutions.

The traffic that is encapsulated is encrypted with the Public Key certificate mechanism.

The HTTPS tunnel can run with or without a customer web proxy server. *

To ensure the security of your ASMS instance, AlgoSec SaaS does not establish inbound connections directly to the ASMS host. Instead, communication between ASMS and AlgoSec SaaS is securely established based on a certificate that your AlgoSec SaaS administrator downloads from the SaaS platform and onboards into the ASMS host.

When a user triggers an action in AlgoSec SaaS that requires processing by ASMS, the request is placed in an AlgoSec SaaS queue, implemented as a Kafka topic hosted in the AlgoSec cloud. This topic is unique to your AlgoSec SaaS account and is secured using a dedicated certificate. ASMS initiates the connection to Kafka over outbound TCP, using the certificate to authenticate, and either consumes messages from the topic or produces data to it. AlgoSec SaaS never initiates a connection to the ASMS host.

Protocols

AlgoSec SaaS uses the following communication protocols:

Protocol		
HTTPS	✓	Used for the following types of REST calls: Between services, and with externally available API calls. Port: 443
Kafka	✓	Encrypted messaging protocol. (no specific network configuration is required)
HTTPS tunneling	✓	Encrypted TLS over HTTPS tunnel. Used in Kafka proxy. Port: 8082

** The Proxy Content Inspection should be disabled to avoid redundant encryption and resulting degradation of the connection.*

Regions

AlgoSec deployment locations are hosted in several AWS regions and the default assignment of tenants to AWS regions is based on the customer's country of origin.

Important: To maintain the security of your ASMS instance, the SaaS product is barred from establishing inbound connections to the ASMS host. SaaS product-ASMS integration communication is always initiated by ASMS.

The following AWS regions are offered:

Region	AWS Deployment location	ACE	ObjectFlow	AppViz	Algo
North America	N. Virginia (US-East-1) region	✓	✓	✓	✓
EMEA	Frankfurt (EU-Central-1) region	✓	✓	✓	✓
APAC (ANZ)	Sydney (AP-southeast-2) region	✓	✓	✓	✓
Middle East (ME)	Bahrain (me-south-1) region	✓	✓	✓	
Middle East (UAE)	UAE (me-central-1) region	✓	✓	✓	
India (IND)	Mumbai (ap-south-1) region	✓	✓	✓	✓
Singapore (SGP)	Singapore (ap-southeast-1) region	✓		✓	

Secured connectivity endpoints

Below is a list of the necessary secured connectivity endpoints for ASMS and SaaS product integration, categorized by region:

Region	FQDNs
North America	*kafka1.us.algocare.algosec.com* *kafka2.us.algocare.algosec.com* *kafka3.us.algocare.algosec.com*
EMEA	*kafka1.eu.algocare.algosec.com* *kafka2.eu.algocare.algosec.com* *kafka3.eu.algocare.algosec.com*
APAC (ANZ)	*kafka1.anz.algocare.algosec.com* *kafka2.anz.algocare.algosec.com* *kafka3.anz.algocare.algosec.com*
Middle East (ME)	*kafka1.me.algocare.algosec.com* *kafka2.me.algocare.algosec.com* *kafka3.me.algocare.algosec.com*
Middle East (UAE)	*kafka1.uae.algocare.algosec.com* *kafka2.uae.algocare.algosec.com* *kafka3.uae.algocare.algosec.com*
India (IND)	*kafka1.ind.algocare.algosec.com* *kafka2.ind.algocare.algosec.com* *kafka3.ind.algocare.algosec.com*

Region	FQDNs
Singapore (SGP)	*kafka1.sgp.algocare.algosec.com* *kafka2.sgp.algocare.algosec.com* *kafka3.sgp.algocare.algosec.com*

AWS separation of onboarding and data collection

Algosec separates the onboarding process from the data collection.

To onboard AWS accounts to ACE via cloud formation stack, we use a dedicated API access key.
The access key generates a token which is valid for 1 hour and can be used for onboarding activities only. It is restricted by a scope for the tenant only and governed by the AlgoSec SaaS RBAC mechanism.

Using the API access key, AWS connects to ACE with the following APIs which permit only adding and removing accounts:

- `POST/DELETE /api/algosaas/onboarding/v1/aws/management-account - add\remove AWS management account`
- `POST /api/algosaas/onboarding/v1/aws - AWS Auto onboarding`

To collect data from an onboarded AWS account, like VPC policy, VM information, etc. - Algosec uses an AWS IAM role according to specific and restricted AWS permissions provided to the account. See Permissions Required for AWS Accounts.

The token scope is defined in the format:

```
json
CopyEdit
"scope": "cf_resource_server/scope_m2m_for_tenant_<tenant_ID>"
```

Session timeout

To protect your data, user sessions are automatically logged out after 60 minutes of inactivity.
Log back in to continue where you left off.

Changes to on-premises devices

Some AlgoSec SaaS services have the capability to trigger changes to the security policies and network object definitions within on-premises devices. All such changes like creating or editing network objects or filtering rules are executed by creating change requests in the on-premises AlgoSec FireFlow. The objects and policies are pushed into the on-premises devices by FireFlow which introduces additional controls (like approvers and reviewers) and is audited with the name of the user who initiated the request, approved, and executed it.

Availability

AlgoSec uses commercially reasonable efforts to make AlgoSec SaaS services available with a Monthly Uptime Percentage of at least 99.9%.

Scanning for misconfigurations

We use advanced compliance and cloud security monitoring tools, plus ACE, to scan across the entire AlgoSec SaaS environment. Detected misconfigurations are handled according to severity.

Resources

- ACE online Tech Docs
- ObjectFlow online Tech Docs
- AppViz online Tech Docs
- Algo online Tech Docs

About this datasheet

The information provided with this paper that concerns technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.