algosec | SECURELY ACCELERATE

AlgoSec SaaS Services

SECURITY PRACTICES

V17

October 2024

Revision History

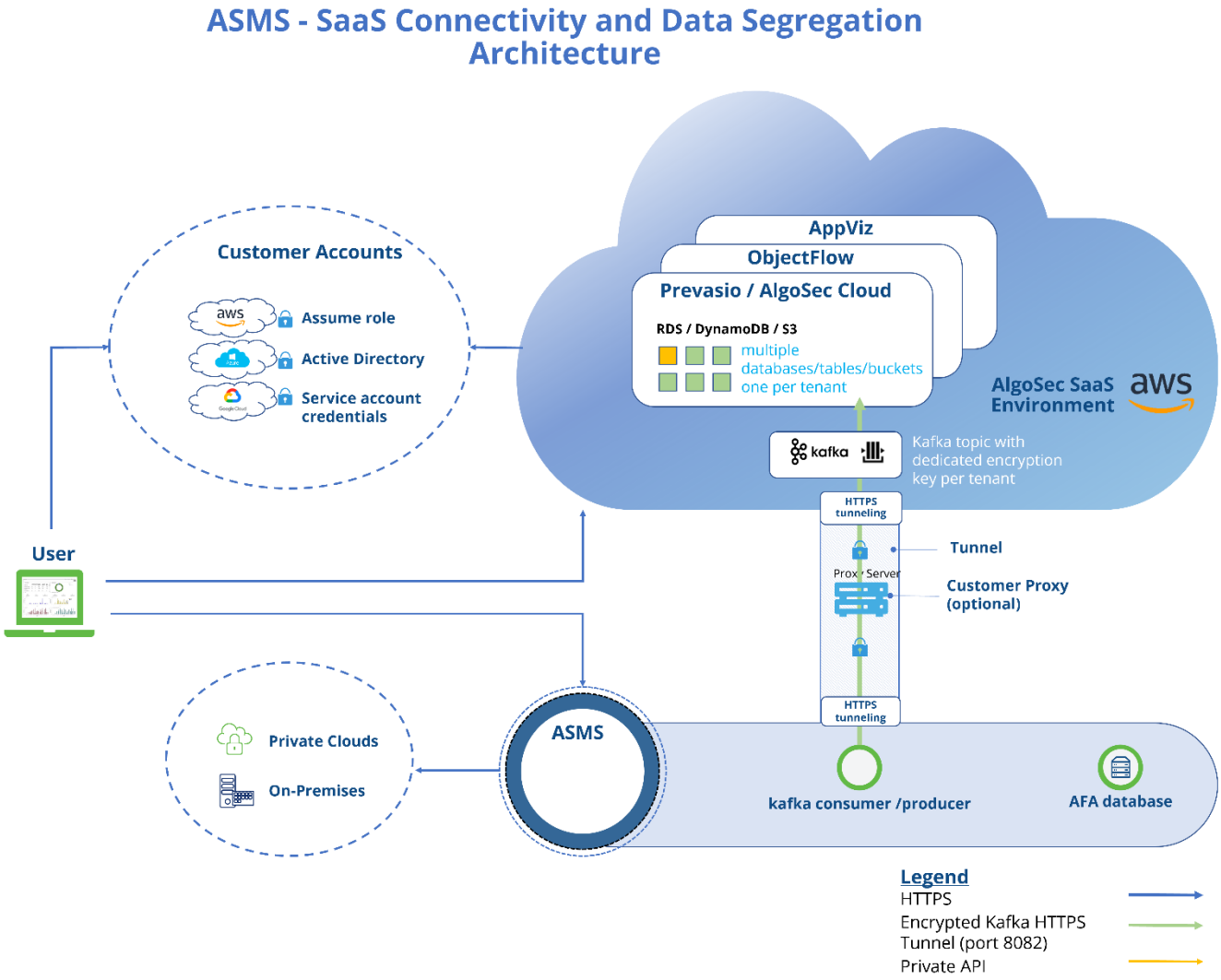
Version	Date	Changes
17	8-Oct-24	- Modified: ObjectFlow now support ME region

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 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 27001:2013 & 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.

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.**

AlgoSec Cloud, ObjectFlow, AppViz	We deploy dedicated tenant infrastructure and separate databases 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 credentials are held in AWS KMS service (see below) and are accessible only by users of that tenant.
Prevasio	Prevasio uses a multi-tenant architecture where info about different tenants is stored in separate database tables and separate S3 buckets. Encryption key management of the database tables is owned by Amazon DynamoDB. 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

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.

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/.

Prevasio adheres to the Principle of Least Privilege

For our Prevasio solution to provide the best value for our customers, we require certain read-only permissions to the customer cloud account(s).

The read-only permissions required for Prevasio are listed on the relevant web pages. These permissions are designed to align with Zero Trust principles and ensure the security of our customers' critical information. It's important to note that the Prevasio Role has no read access to nonessential but sensitive data, such as customer cloud computing secrets.

Write permissions/roles that Prevasio requests are:

- AWS ecr:*SetRepositoryPolicy*: This permission allows setting/changing a policy of a container image, detected to be a high risk, so that it could not be pulled from the registry into a workload.
- Azure *AcrPush:* This role is needed to set "canRead" property to the image metadata.
- GCP Requires the following roles to update signature of image:
  - binaryauthorization.policyEditor
  - containeranalysis.occurrences.editor
  - containeranalysis.notes.attacher
  - cloudkms.signer
  - serviceusage.serviceUsageConsumer

For more information about permissions and roles required by Prevasio, see:

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

Product	Data Encryption at Rest	Data Encryption in Transit
AlgoSec Cloud, ObjectFlow, AppViz	All data at rest is encrypted using the AES-256 algorithm.	All data in transit is encrypted using TLS 1.2.
Prevasio	All data at rest uses DynamoDB tables, encrypted with Amazon Managed Keys.	

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 not exposed to AlgoSec SaaS

AlgoSec does not access, store, or manage any highly sensitive, federally regulated PII data across its SaaS solutions. Please see data specifics for each AlgoSec SaaS solution below.

- **AlgoSec Cloud:** AlgoSec Cloud contains cloud asset inventory, cloud-native firewall, and security policy data.
- **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.
- **Prevasio**: Prevasio only 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 Prevasio 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.
- Prevasio never stores user passwords and delegates user authentication functions, such as new user registration, login, logout, and password recovery, to AWS Cognito.
- 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 AlgoSec Cloud, 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. Prevasio does not connect directly to ASMS.*

Privacy Regulations

Data gathered by AlgoSec SaaS services is almost entirely free of personally identifying information (PII). The only sensitive data that may be found in the data is names, business email addresses, and IP addresses of customer employees. 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 AlgoSec Cloud and AppViz 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
- 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.

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

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, ASMS-AlgoSec SaaS communication is securely established based on a Kafka certificate that your AlgoSec SaaS administrator downloads from AlgoSec SaaS and onboards in the ASMS host.

When a user triggers an action in AlgoSec SaaS that requires processing by ASMS, a job is pushed into a AlgoSec SaaS queue based on a Kafka topic that is unique to your specific AlgoSec SaaS account and is secured by a unique certificate. Only the specific ASMS with which trust has been established can fetch data from this AlgoSec SaaS queue and push data to it.

Protocols

AlgoSec SaaS uses the following communication protocols:

Protocol	AlgoSec Cloud, ObjectFlow, AppViz	Prevasio	
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	Prevasio	AlgoSec Cloud	ObjectFlow	AppViz
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	✓	✓		

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*

Region	FQDNs
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*

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 AlgoSec Cloud, to scan across the entire AlgoSec SaaS environment. Detected misconfigurations are handled according to severity.

AlgoSec SaaS Solutions

AlgoSec SaaS Services secure application connectivity, anywhere, for SaaS customers.

AlgoSec's current SaaS-based offering includes:

- **Prevasio:** Fast and secure agentless cloud security configuration management across multi-cloud, multi-accounts, cloud native services, and cloud assets
- **AlgoSec Cloud**: Manage security policies across the various security-control layers in your multi-cloud and hybrid cloud estate.
- **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.

Resources

- Prevasio online Tech Docs.
- AlgoSec Cloud online Tech Docs.
- ObjectFlow online Tech Docs.
- AppViz 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.