algosec | SECURELY ACCELERATE

AlgoSec SaaS Services

SECURITY PRACTICES

V11

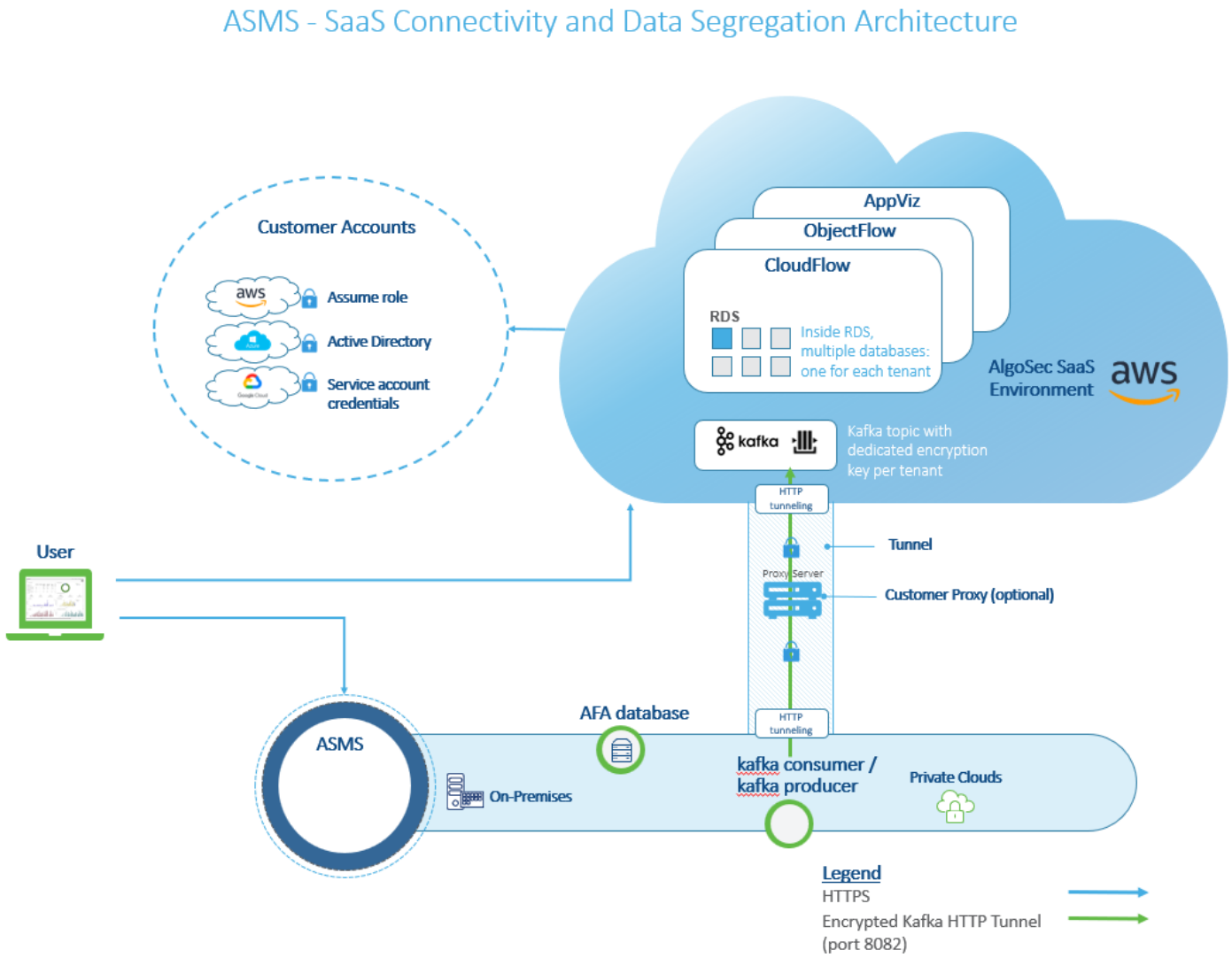
September 2023

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



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. As well, 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. 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. 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 Microsoft Azure Active Directory 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/.

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 is encrypted both at rest as well as in transit.

- Data Encryption at Rest: All data at rest (in RDS instances etc.) is encrypted using the AES-256 algorithm.
- Data Encryption in Transit: All data in transit is encrypted using the TLS 1.2

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.

- **CloudFlow:** CloudFlow 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.

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 CloudFlow, connectivity check, for ObjectFlow, object sync, FireFlow change requests and more, and for AppViz SaaS-version, object sync, FireFlow change requests, AutoDiscovery data, connectivity checks, ASMS application-level risks, scanner information sharing and more.*

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.

ASMS-AlgoSec SaaS trust and communication

Refer to the diagram above.

For ASMS A32.20 builds and above: ASMS-AlgoSec SaaS secure communication takes place over TLS, which by ASMS default is transported over an HTTP 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 HTTP 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:

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)
HTTP tunneling	Encrypted TLS over HTTP tunnel. Used in Kafka proxy. Port: 8082

** Including AlgoSec SaaS solutions like: AppViz, CloudFlow, ObjectFlow.*

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

Regions

AlgoSec SaaS deployment locations are hosted in Amazon Web Services (AWS®).

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/FQDNs	CloudFlow	ObjectFlow	AppViz
North America	N. Virginia (US-East-1) region *kafka1.us.algocare.algosec.com* *kafka2.us.algocare.algosec.com* *kafka3.us.algocare.algosec.com*	•	•	•
EMEA	Frankfurt (EU-Central-1) region *kafka1.eu.algocare.algosec.com* *kafka2.eu.algocare.algosec.com* *kafka3.eu.algocare.algosec.com*	•	•	•
APAC (ANZ)	Sydney (AP-southeast-2) region *kafka1.anz.algocare.algosec.com* *kafka2.anz.algocare.algosec.com* *kafka3.anz.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 CSPM and cloud security monitoring tools, plus AlgoSec CloudFlow, to scan across the entire AlgoSec SaaS environment. Detected misconfigurations are handled according to severity.

Current AlgoSec SaaS Solutions

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

AlgoSec's current SaaS-based offering includes:

- **CloudFlow**: 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

- CloudFlow 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.