ILLUMIO ASP SECURE CLOUD

Illumio Adaptive Security Platform® (ASP) Secure Cloud secures enterprise applications in private data centers and private, public, or hybrid cloud environments by decoupling security from the underlying infrastructure. Illumio ASP delivers real-time application dependency mapping and micro-segmentation to prevent the lateral movement of bad actors inside your data center and cloud environments. It provides real-time visibility into the connectivity between workloads across heterogeneous compute environments, generates optimal micro-segmentation policies based on how workloads communicate, and programs the native stateful enforcement points in each host to enforce applicable firewall rules. Illumio ASP is unique because its architecture enables you to use the sensors and enforcement points that are natively available in your compute environment, eliminating the overhead of having to re-architect your network and deploy more networking/SDN and data center firewalls to secure your micro-perimeters. Illumio ASP delivers visibility and enables micro-segmentation for Zero Trust security at any scale. Since policy creation does not require deep familiarity with networking terminologies, you can empower different teams within your organization to create micro-segmentation policies, but retain governance over what gets provisioned.

ILLUMIO ASP SECURE CLOUD SERVICE DETAILS

Illumio ASP Secure Cloud is comprised of two primary components:

1. The **Policy Compute Engine (PCE)** is the central policy controller and is operated by Illumio.
2. The **Virtual Enforcement Node (VEN)** is a lightweight agent that gets installed from the cloud and resides on the customer's workloads.

Data Residency – Illumio ASP Secure Cloud resides in the following geographical regions:

- AWS US West-2 (Oregon)
- AWS EU West-2 (London)
- AWS Asia Pacific (Sydney)

Customers may indicate which instance they prefer for deployment. If customers do not make a request for a specific region, the closest geographical region to the customer is selected by default. All regions share the same login.illum.io login cluster, so account usernames are stored in the US.

VEN CAPACITY

Illumio ASP Secure Cloud supports up to 25,000 managed VENs. For larger deployments, contact Illumio.

DIFFERENCES BETWEEN ILLUMIO ASP SECURE CLOUD AND ILLUMIO ASP ON-PREMISES

Both Illumio ASP Secure Cloud and the Illumio ASP On-Premises platform run the same software. However, Illumio ASP Secure Cloud differs from the Illumio ASP On-Premises platform in the following ways:

FEATURE/FUNCTION	
Exporting VEN flow logs and auditable event logs	Illumio ASP Secure Cloud supports the export of Virtual Enforcement Node (VEN) flow logs and auditable event logs to customer-provided AWS S3 buckets. Splunk as well as other log aggregation systems with AWS data integration methods are supported.
Kerberos	Kerberos-based authentication with VENs is not supported with Illumio ASP Secure Cloud.
LDAP	Admin authentication via LDAP is not supported with Illumio ASP Secure Cloud. Admin authentication via SAML is supported with Illumio ASP Secure Cloud.
F5 visibility and enforcement	F5 visibility and enforcement requires a customized solution specific to the client's specific environment.
Explorer Resolve Unknown FQDNs	Illumio ASP Secure Cloud does not have access to customer internal DNS servers, so the "Resolve Unknown FQDNs" feature will only resolve publicly addressable IPs.
FIPS 140-2	FIPS 140-2 is not supported. Customers requiring FIPS 140-2 should contact their Illumio Account Representative.
Events data retention	Retention period for events stored in the database for Illumio ASP Secure Cloud is fixed and is not configurable by the users.

SERVICE LEVEL AGREEMENT

Illumio provides an uptime SLA of 99.8% for Illumio ASP Secure Cloud. For more details regarding SLA, refer to your Illumio Purchase Order as well as the Illumio Master Subscription Agreement (https://www.illumio.com/eula).

RESPONSE TIME

Illumio will endeavor to provide an initial response to support requests based on designed priority:

PRIORITY	DESCRIPTION	RESPONSE TIME
P1	Catastrophic problem; systems down and impacting ability to operate	30 minutes
P2	High impact problem; systems disrupting business operations	2 hours
P3	Medium to low impact problem; loss of non-critical functionality	4 business hours
P4	General usage issues, information requests	1 business day

Illumio manages Illumio ASP Secure Cloud uniformly so all customers receive the latest product features and security updates.

MAINTENANCE

PCE Maintenance – Illumio announces new PCE software upgrades at least 48 hours in advance. There are three types of PCE upgrades:

1. Major software upgrades: Generally occur three times per year. Major upgrades typically occur 1–3 weeks following a new GA release of the PCE software.
2. Patch software upgrades: Performed on an as-needed basis (e.g., when a released version has a customer impacting issue).
3. Infrastructure maintenance: No change to the software version but updates to the underlying PCE infrastructure.

VEN Maintenance – New VEN LTS versions are published as they become GA. When a new LTS release of a VEN is available, Illumio notifies customers so as to schedule VEN upgrades as far ahead as possible of the PCE release which drops support for the old VEN version.

SECURITY

Illumio ASP Secure Cloud is designed to protect the security and privacy of your data. Illumio segmentation policies are enforced restricting inbound and outbound access to all production data and systems. Additional security controls include:

Separation of Environments – Illumio ASP Secure Cloud uses separate environments for development, testing, and production systems. Each environment has access restricted based on the least privilege method of provisioning access and maintains a separate access listing. Production data is not replicated to non-production environments.

Cluster Hardening – Illumio ASP Secure Cloud exists in an isolated VPC in a dedicated AWS account, separate from non-production related assets. The production hosting environment is secured with micro-segmentation application rules and security groups which restrict inbound and outbound access to production data and systems.

Monitoring & Patching – Illumio ASP Secure Cloud components are regularly monitored and scanned from the OS level up to the application stack and patched as needed. Production host servers are continuously monitored using monitoring tools.

Secure Communication – All customer communication with Illumio ASP Secure Cloud uses industry standard Transport Layer Security ("TLS") encryption for the transmission of private confidential information over public networks using a web browser. External network connections are configured to be closed with only required traffic allowed for corporate administrative and internet-facing (customer) use cases.

Administrative Access – Administrative access control is enforced at several layers:

1. System OS
2. AWS Security Groups
3. PCE policy

Multi-Tenancy/Data Separation – Illumio ASP Secure Cloud is a multi-tenancy platform. Multi-tenancy enables multiple customers to access the service while isolating each tenant's (customer's) application data. Every customer ID is associated with exactly one tenant, which is then used to access the service. All instances of application objects are tenant-based, so every time a new object is created that object is also irrevocably linked to the customer. The service maintains these links automatically, and restricts access to every object based on the customer ID.

When a user requests data, the service automatically applies a filter to ensure it retrieves only information corresponding to that customer. Each request requires authentication and authorization which is tied to a specific customer and user session resulting in a distinct separation between customer accounts. Once authenticated, all requests must have a valid session ID unique to the customer ID, which cannot be used to access any other tenant. All external users have unique user account IDs and meet minimum password requirements to authenticate to their accounts.

Single Sign-On (SSO) Authentication – Illumio ASP Secure Cloud supports secure SSO via SAML authentication. SAML data transmitted to identity providers (IdP) is secured by public key cryptography and encrypted with TLS.

Personnel Screening – Illumio has established workforce conduct standards and implemented workforce candidate background screening procedures to enable it to meet commitments and system requirements as they relate to Security, Availability, and Confidentiality.

BACKUP AND DISASTER RECOVERY

Backup – Illumio ASP Secure Cloud uses backup facilities to backup system configurations, source code, and data. For customer data, snapshots are taken every 24 hours for which backups are kept for at least 30 days. Backup files are replicated in real time to backups in AWS servers on encrypted volumes. The snapshots of the volumes are also encrypted. The replicated backups are stored in a different location than the primary data center as protection in the event of a disaster.

Disaster Recovery – Illumio makes use of multiple availability zones for database redundancy and geographic diversity. The Illumio Disaster Recovery Plan includes processes, procedures, and contact information to be used in the event of an incident or disaster. The service is configured for high availability (HA) with multiple redundant nodes to provide failover capabilities in the event of outages, corruption, or system failures.

Data Residency – Illumio ASP Secure Cloud supports instances in the US, the UK, and Australia. Customers may indicate which region they would like to be invited to for deployment. If customers do not make a request for a specific region, the closest geographical region to the customer is selected by default. All regions share the same login.illum.io login cluster, so account usernames are stored in the US.

Details regarding production IPs and allowed ports for use with Illumio ASP Secure Cloud are available in the following Illumio Knowledge Base article: https://illumio.lightning.force.com/lightning/r/Knowledge__kav/ka50H00000005WzQAI/view. VEN to PCE connectivity does not support network configurations via proxy servers.

For the export of flow logs and audit events, customers are required to provide Illumio Support with an AWS S3 bucket name, account ID, and external ID. Customers are responsible for associated AWS S3 storage charges.

SUBSCRIPTIONS, ONBOARDING, DATA RETENTION, AND TERMINATION

SUBSCRIPTIONS:

Customers can add features and increase the scale of their Illumio ASP Secure Cloud deployment anytime during the term of their subscription to meet their business needs, such as:

- Customers may increase the number of workload subscriptions and pair as many workloads as needed for their deployment. Illumio Customer Success will provide a true-up during account renewals.

- Customers may add a feature license such as Vulnerability Maps at any time during the term of their subscription.
- The Illumio ASP Secure Cloud service EULA (End User License Agreement) is available for review at: www.illumio.com/eula

ONBOARDING

Illumio Support and Services onboards the primary technical contact listed on the initial sales order by sending an email invitation to that user to become the "org owner" for their Illumio ASP Secure Cloud deployment. This "org owner" user has the capability and responsibility to invite and manage subsequent owner, admin, and read-only users for their deployment. If the customer has access to a proof of concept (POC) environment, Illumio will coordinate with the customer to terminate POC access at an agreed upon date prior to on-boarding the production environment.

DATA RETENTION

If a customer decides to terminate all services with Illumio, their accounts are disabled and customer data is archived/destroyed according to Illumio's Data Retention and Disposal Standard. Backups are stored on encrypted volumes and retained for 365 days, after which they are deleted from the backup location(s). Customer workload data is removed from the system when customer accounts are offboarded and the customer user accounts are locked. Metadata is removed from the system after five years from the offboarding date.

TERMINATION

Upon receiving notice of intent to terminate Illumio subscription, the following actions are initiated by Illumio Support:

1. Lock user accounts
2. Unpair VENs
3. Remove all Illumio policy

CERTIFICATIONS & COMPLIANCE

Illumio ASP Secure Cloud has successfully completed SOC2 Type II compliance.

SUPPORTED APPS

The following apps are available for use with Illumio ASP Secure Cloud:

- **Illumio Technology Add-On for Splunk (TA-Illumio)** – This app enriches Illumio Policy Compute Engine (PCE) data with Common Information Model (CIM) field names, event types, and tags. More information is available here: https://splunkbase.splunk.com/app/3657/
- **Illumio App for Splunk** – This app integrates with the PCE to provide security and operational insights into your Illumio secured data center. More information is available here: https://splunkbase.splunk.com/app/3658/
- **Illumio App for ServiceNow CMDB** – This app permits a user of ServiceNow CMDB to sync data with PCE using a common hostname field. More information is available here: https://store.servicenow.com/sn_appstore_store.do#!/store/application/15314f1ddb882700dc9fabc5ca961943/1.0.0

The IBM QRadar app is not supported with Illumio ASP Secure Cloud.

ABOUT ILLUMIO

Illumio, a cybersecurity leader delivering segmentation solutions, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information, visit www.illumio.com/what-we-do and:

- Engage with Illumio on Twitter
- Follow Illumio on LinkedIn
- Like Illumio on Facebook
- Subscribe to our YouTube Channel

CONTACT US

For more information about Illumio ASP and how it can be used to achieve environmental segmentation, email us at illuminate@illumio.com or call 855-426-3983 to speak to an Illumio representative.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com