Skyhigh Security

Privacy Data Sheet

Skyhigh Cloud Platform (Security Service Edge - Skyhigh SSE)

The purpose of this Privacy Data Sheet is to provide Customers of Skyhigh Cloud Platform (aka Skyhigh SSE) with details on how Skyhigh Cloud Platform captures, processes, and stores[1] telemetry information, including personal data (or personally identifiable information), to help them understand and assess the impact of the telemetry capabilities on their overall privacy posture.

Skyhigh Cloud Platform is a cloud-native security platform that enables consistent threat and data protection controls from device to cloud. It creates an efficient and consistent security management experience by bringing together multiple Skyhigh Security products, components, and technologies on Skyhigh's Cloud Platform and is made available to companies or persons who obtain a Skyhigh Security edge base and advanced subscription.

Skyhigh Cloud Platform will process personal data in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Skyhigh Security is the Data Controller for the personal data processed to administer and manage the Customer relationship. Skyhigh Security is the Data Processor for the personal data processed by Skyhigh Cloud Platform to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Skyhigh Security Website Privacy Notice.

Skyhigh Cloud Platform Overview

Skyhigh Cloud Platform delivers more than a collection of products and technologies. We've combined industry leading cloud security products, like Skyhigh Cloud Access Security Broker (CASB) and Secure Web Gateway (SWG) with key technologies, including Data Loss Prevention (DLP), Exact Data Matching (EDM) and Indexed Document Matching (IDM), Optical Character Recognition (OCR), malware scanning, and incident management, to provide a fully converged and easy-to-use platform.

The Skyhigh Cloud Platform combines Skyhigh Security Service Edge (Skyhigh SSE), Skyhigh CASB and SWG technologies to protect data from device-to-cloud and prevent cloud-native breach attempts

[1] In this document, we adopt the broad definition of "processing" that appears at Article 4(2) of the GDPR: "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means …", which includes, but is not limited to the following non-exhaustive series of examples: "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

that are invisible to corporate networks. This creates a secure environment for the adoption of cloud services and enables access to the cloud from any device.

The Skyhigh Cloud Platform is the industry's first data-aware, cloud-native security stack that delivers unified data and robust threat protection capabilities across the web, cloud apps, email, and private apps, all from a single console.

With The Skyhigh Cloud Platform, you can achieve:

- Consistent visibility and control over data from device-to-cloud;
- Unified access control and threat protection for the cloud and web;
- Minimizes inefficient traffic back-hauling with intelligent, secure direct-to-cloud access with 99.999% availability and ultra-low latency.

The Skyhigh Cloud Platform offers the following services:

➢ **Skyhigh Security Service Edge (SSE)** - Our Security Service Edge solution is the security fabric between the Customer's workforce and the resources that enable fast direct-to-internet access by eliminating the need to route traffic through the Customer's data center for security. Data and threat protection are performed at every control point in a single pass to reduce the cost of security and simplify Customer management.

➢ **Secure Web Gateway (SWG)** - Skyhigh Secure Web Gateway protects the Customer's organization against security threats that arise when users in the Customer's organization access the web. This service:

- Scans and filters web traffic between users and the cloud.
- Blocks traffic that is not allowed by Customer configuration.
- Protects users working inside or outside Customer networks, for example, users working in a coffee shop or hotel.

➢ **Skyhigh Cloud Access Security Broker (CASB)** provides unmatched data protection, device-based controls, and online threat protection for all cloud applications using multi-mode cloud solutions— all from a single platform. The solution delivers the following capabilities:

- **Cloud Discovery and Risk Monitoring**: Processes logs and identifies all cloud services in use within the Customer's organization. Provides an objective, customizable risk assessment for each cloud service.
- **Cloud Usage Analytics**: Hadoop-based analysis engine detects usage anomalies based on statistical and behavioral models to identify risky user behavior, inconsistent policies, and underutilized subscriptions to cloud services.
- **Application Blocking:** Allows the organization to block access to applications.

➢ **Skyhigh Private Access (SPA) -** Private Access gives users seamless and secure connectivity to private applications without ever placing them on the network or exposing apps to the internet.

Private Access is a security architecture where traffic only from authenticated users, devices, and applications is granted access to other users, devices, and applications within an organization.

- **Skyhigh Cloud-Native Application Protection Platform (CNAPP)** - Secures Customers' enterprise cloud-native application ecosystem using the industry's first comprehensive, automated and frictionless platform**.**

- **Skyhigh Cloud Firewall (SCF)** - Is a cloud-based firewall solution that converges with Security Service Edge SSE to aggregate traffic from various sources that employ differing security postures. Skyhigh Cloud Firewall offers multi-layered protection and performs deep packet inspection, allowing organizations greater visibility, granular policy enforcement, and control over applications to counter web-based threats. With Skyhigh Cloud Firewall, Customers can monitor all outbound network traffic and prevent unauthorized access by enforcing firewall policies. Based on the Customer's information security policies, they can define a firewall policy to handle outbound network traffic for specific IP addresses, protocols, ports, and processes.

- **Remote Browser Isolation (RBI)** - Is a cloud-based solution that prevents web-based unknown threats from ever reaching the Customer's endpoints by integrating intelligent yet transparent Remote Browser Isolation, leveraging powerful machine learning analysis on real-time telemetry from over one billion sensors.

- **Skyhigh Client Proxy (SCP)** - Skyhigh Security Client Proxy software helps protect the Customer's endpoint users from security threats that arise when they access the web from inside or outside the Customer's network. The Client Proxy software redirects, blocks, or allows web traffic according to the Client Proxy policy and the location of the endpoints. The Client Proxy software is a unified software that works with all the Skyhigh Cloud Platform products - SWG (On-Prem & Cloud), Private Access, and Cloud Firewall.

- **Skyhigh Data Loss Prevention (DLP)** - Prevents data exfiltration, ensures compliance, and stops threats using multi-vector data protection technologies across Customer cloud, web, email, and private apps—all from one platform. Skyhigh DLP exposes visibility gaps, providing full-scope data protection for the Customer's entire workforce infrastructure. By enforcing access and data loss prevention policies and encrypting cloud data, organizations can remain compliant with regulations like FISMA, HIPAA, GLBA, PCI DSS and SOX, utilizing dashboards options to track detections, activities, and the status of their managed Windows systems within their organization.

Skyhigh Cloud Platform (SSE) via Skyhigh Client Proxy can be implemented as one of two deployments:

- **Standalone deployment:** Customers use tenant credentials via Skyhigh Client Proxy to create/deploy, manage, and enforce security policies. Customers can use the queries and dashboards options to track detections, activities within their organization.

- **Managed deployment using 3rd Party Software Deployment Tools (for example, SCCM or Jamf)**: Customers use tenant credentials via Skyhigh Client Proxy to create/deploy, manage, and enforce security policies. Customers can use the queries and dashboards option to track activities and the status of their managed Skyhigh Client Proxy client systems within their organization.
    - The Skyhigh Client Proxy is a unified client which facilitates client-to-cloud connectivity. Skyhigh Client Proxy is deployed on device end-points and authenticates end-users.
    - For specific services such as Private Access, Skyhigh Client Proxy facilitates SAML based authentication. Post authentication, all traffic that needs to be secured can be securely forwarded to the Skyhigh Cloud Platform by way of secured channels via HTTPS and isolated Skyhigh Security internal networks dedicated to Security Service Edge. When forwarding traffic, Skyhigh Client Proxy adds additional end-point context as metadata along with real-time device posture information.

Please see Skyhigh Security Service Edge product sheet for additional information.

Personal Data Processing

Skyhigh Cloud Platform is a collection of integrated, cloud-centric security capabilities that facilitate safe access to websites, cloud, and applications. The Skyhigh Cloud Platform framework converges all security services, including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Skyhigh Private Access (SPA), into a single, cloud-native framework. This integrated approach supports the digital business transformation and workforce mobility, while minimizing the impact on security performance, complexity, and cost. Because of this, Skyhigh may capture information differently depending on the Skyhigh Cloud Platform deployment version:

- **Standalone deployment:** The captured information is sent automatically by Skyhigh Client Proxy by way of SSL/HTTPS connection to Skyhigh Secure Web Gateway present within the Customer's network infrastructure.

- **Cloud deployment using 3rd Party Software Deployment Tools (for example, SCCM or Jamf):** The captured information is sent automatically by Skyhigh Client Proxy by way of SSL/HTTPS connection to Skyhigh Secure Web Gateway present within the Customer's network infrastructure.
    - With Jamf, Customers can automatically deploy Mac devices via Skyhigh Client Proxy across the enterprise without any manual intervention.

As a result, Skyhigh Cloud Platform may process a range of data potentially containing personal information. The table below shows the personal data processed by Skyhigh Cloud Platform to provide its services and describes why the data is processed.

Table 1. Personal Data Processed by Skyhigh Cloud Platform

Personal Data Category*	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General Identification Information of Administrator Access Log Data: ● AD Group ● IP Address ● Device ID ● Device Profile ● OS and Version ● Firewall and AV Status ● Device Encryption Status ● Specified Domain joined ● Name and Time of the private application accessed by the end user ● Skyhigh Security software installed, (E.g., DLP, SPA) ● MDM system ● Absolute Path of process sending web requests ● Authenticode ● Name of the signer ● A file hash of the process file ● Layer 4 protocol used for connection Provisioning Data: ● Email (Customer Email ID) ● IP Address (Customer's Public Egress IP Address) Classification Exact Data: ● Matching/Indexed Data Matching (EDM/IDM) Data (Sensitive Data): ○ Hash value associated with retained fingerprint data	Used for policy enforcement decisions based on Customer requirements. Enables Customers to be compliant with various industry specific regulations.

Generated Data	Infrastructure/Operational Log and/or Telemetry: ● Incidents/Events: ○ URL Path ○ URL Parameters ○ File Name ● Evidence: ○ File ○ Presence of File Path	Used for threat detection and response.
Collected Data	Web Evidence / Match Highlights Data: ● User Email ● File Name Configuration Information: ● Company CA Certificate present in the trust store ● Signed Client Certificate ● Skyhigh Security Software installed, (E.g., DLP, SPA) ● Policy Rules ● Policy Execution Traces	Used for Skyhigh SSE policy configuration, execution, granular policy enforcement, CA certificate validations, and overall control over enterprise applications to counter web-based threats.

*** Please note the Personal Data Categories explained below and used throughout Privacy Data Sheets for Skyhigh products and/or services:**

Administrative Data: Information to enable the service and/or manage the Customer relationship;

Generated Data: Information generated by the product (events, evidence, logs);

******Note that incident data includes logged metadata per data transaction. Customer sensitive data is not part of the logged metadata occurring per data transaction.

Collected Data: Information generated by the Customer (policies and configurations).

*******Please also note that the above lists of personal data elements per personal data category are not exhaustive and are illustrative of typical use cases.

Data Center Locations

Skyhigh Security Service Edge (SSE) and Cloud Access Security Broker (CASB)

- **For standalone deployment**, the data are located within the Customer's network infrastructure.
- **For cloud deployment**, the data are captured on globally distributed physical nodes, called points of presence (PoPs), and transferred to backend systems, all of which are maintained by Skyhigh Security.

Skyhigh also uses its own data centers as well as third-party infrastructure providers to deliver the service globally. Skyhigh SSE and CASB processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS), 365 Data Centers, Equinix, Oracle Corporation and/or Hetzer in regional clouds listed below. This means that the traffic in certain countries will be directed to a defined compute location.

Skyhigh Secure Web Gateway (SWG)

Skyhigh SWG's regional clouds provide options to address Customers' data location preferences. Customers have the choice to select a region (depending on the region where users accessed the product) or to default to their nearest region for data processing. This means that, unless otherwise modified by a system administrator, the traffic in certain countries will be directed to a defined compute location.

Table 2. Data Center and Points of Presence Locations

Data Center Provider	Data Center Location
AWS	Australia (Sydney)
AWS	Brazil (São Paulo)
AWS	Germany (Frankfurt)
AWS	Hong Kong (Hong Kong)
AWS	India (Mumbai)
AWS	Japan (Osaka)
AWS	Japan (Tokyo)
AWS	Korea (Seoul)
AWS	Singapore (Singapore)
AWS	Sweden (Stockholm)
AWS	United Kingdom (London)
AWS	United States (Ashburn)
AWS	United States (Broadman)
AWS	United States (Oregon)
AWS	United States (San Francisco)
365 Data Centers	France (Paris)

365 Data Centers	Germany (Frankfurt)
365 Data Centers	United Kingdom (London)
365 Data Centers	United States (Bridgewater)
Equinix	Colombia (Bogota)
Equinix	France (Paris)
Equinix	Germany (Frankfurt)
Equinix	Hong Kong (Hong Kong)
Equinix	Ireland (Dublin)
Equinix	Japan (Osaka)
Equinix	Japan (Tokyo)
Equinix	Netherlands (Amsterdam)
Equinix	Singapore (Singapore)
Equinix	United Kingdom (London)
Equinix	United Kingdom (Manchester)
Equinix	United States (Ashburn)
Equinix	United States (Dallas)
Equinix	United States (Chicago)
Equinix	United States (Miami)
Equinix	United States (Los Angeles)
Equinix	United States (New Jersey)
Oracle Corporation	United Arab Emirates (Dubai)
Oracle Corporation	Australia (Melbourne)
Oracle Corporation	Australia (Sydney)
Oracle Corporation	Brazil (São Paulo)
Oracle Corporation	Brazil (Vinhedo)
Oracle Corporation	Canada (Montreal)
Oracle Corporation	France (Paris)
Oracle Corporation	India (Mumbai)
Oracle Corporation	Italy (Milan)
Oracle Corporation	Canada (Montreal)
Oracle Corporation	Saudi Arabia (Jeddah)
Oracle Corporation	Seoul, (Republic of Korea)
Oracle Corporation	Sweden (Stockholm)
Oracle Corporation	London (United Kingdom)
Oracle Corporation	Newport (United Kingdom)
Hetzer	Germany (Nuremberg)

Please also see Skyhigh Service Status for more information concerning the status of Skyhigh data centers and locations of Points of Presence (POP) nodes.

Subprocessors

Skyhigh Security partners with service providers that act as subprocessors for the Skyhigh Cloud Platform service and contracts to provide the same level of data protection and information security that you can expect from Skyhigh Security. A current list of subprocessors for the service is below.

Table 3. Subprocessors

Subprocessor	Personal Data Category	Service Type	Location of Data Center
Okta	Administrative Data	Identity Management	United States
Amazon Web Services (AWS)	See Table 1.	Hosting / Co-Location	See Table 2.
365 Data Centers	See Table 1.	Hosting / Co-Location	See Table 2.
Equinix	See Table 1.	Hosting / Co-Location	See Table 2.
Oracle Corporation	See Table 1.	Hosting / Co-Location	See Table 2.
Hetzer	See Table 1.	Hosting / Co-Location	See Table 2.

Cross-Border Data Transfer

In the event of a need to share personal information with Skyhigh Security personnel in regions outside of those identified in the Data Center Locations section above, we will do so in compliance with applicable requirements for transfer of personal data, including those of the EU Standard Contractual Clauses as approved by the European Commission and/or other legal instruments recognized by EU data protection laws. For a more detailed assessment of our international data transfers, please refer to the Skyhigh Transfer Impact Assessment statement.

Access Control

Access to Customer information is subject to Skyhigh Security's Access Management Policy. Access is protected by multiple authentication and authorization mechanisms. Skyhigh Security has an account administration application that provides a central access point to request and perform administrative functions for account requests across multiple platforms. All resources have an owner who is responsible for deciding who will be granted access to that resource. Privileged access to resources is restricted to authorized users with a business need, consistent with the concepts of least privilege and segregation of duties based on roles and job functions. Shared accounts are prohibited. All usernames are traceable to a specific human user. User access credentials are promptly removed when user access is no longer authorized (e.g., Skyhigh Security employment terminates).

Remote user access by Skyhigh Security personnel is performed through a secure virtual private network (VPN) connection that requires multi-factor authentication (MFA). If remote access to production resources is required outside the VPN, then a TLS encrypted connection and MFA are required.

The table below lists the personal data used by Skyhigh Cloud Platform to carry out the service, who can access that data, and why.

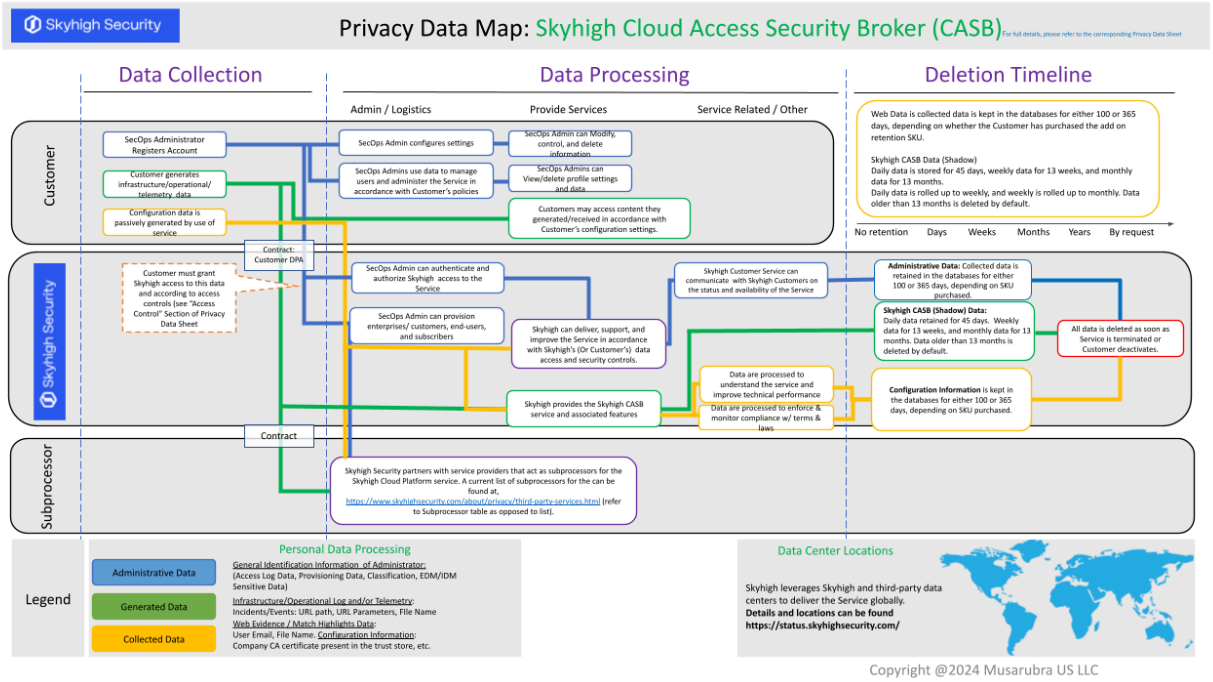
Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	**Customer**	To analyze systems involved in violations, for compliance, and for reporting.
	Skyhigh Security	To debug Customer data in event of customer service escalation.
Generated Data - Incidents/Events	**Customer**	To analyze systems involved in violations, for compliance, and for reporting.
	Skyhigh Security	To debug Customer data in event of customer service escalation.
Generated Data - Evidence	**Customer**	To analyze systems involved in violations, for compliance, and for reporting.
	Skyhigh Security	No default access.
Collected Data - Configuration Information	**Customer**	To leverage Active Directory to define end-user permissions.
	Skyhigh Security	For policy configurations, customer support, and to assist with various other functions.

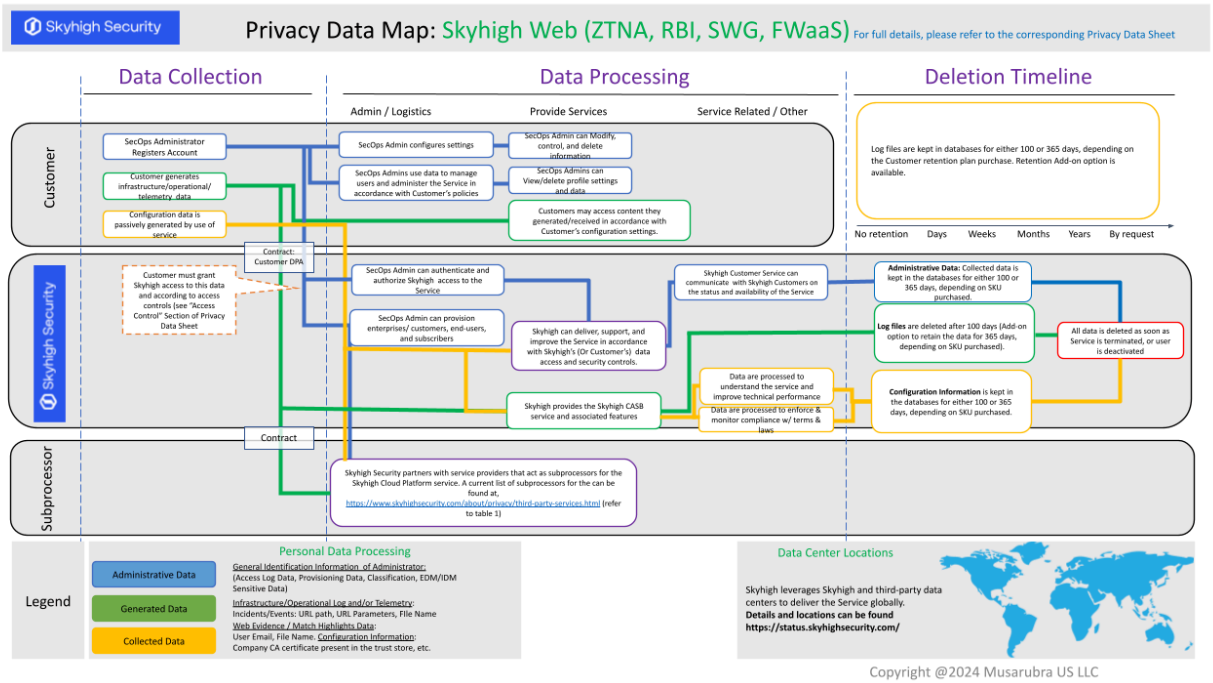
Skyhigh SSE Data Flow Diagrams

The key data flows associated with the information processing activities described in this document are shown below.

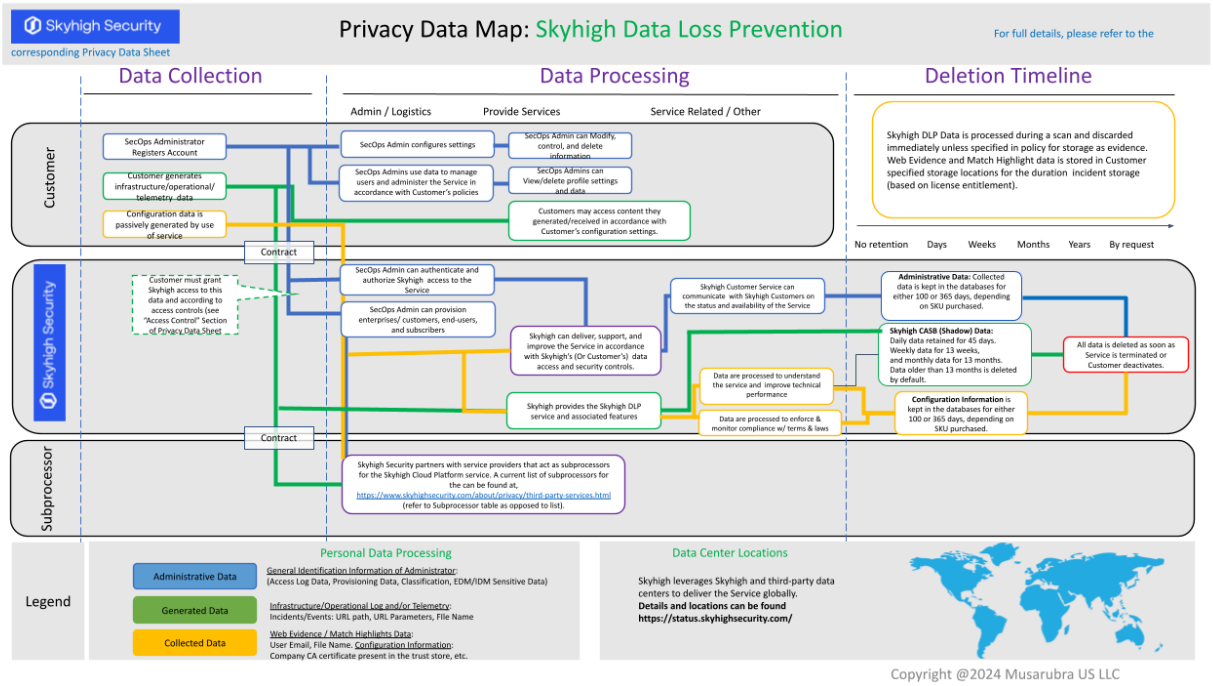
Skyhigh Cloud Access Security Broker (CASB):



Skyhigh Web (ZTNA, RBI, SWG, FWaaS):



Skyhigh Data Loss Prevention (DLP):



Customer Privacy Options

Skyhigh Security designs its products to support our Customers' compliance with global data protection and compliance obligations. It does this by addressing threat intelligence and security challenges at the application, network, and endpoint levels, and in the cloud. In addition, Skyhigh Security offers product features that help our Customers meet their EU General Data Protection Regulation (GDPR) and other legal compliance goals. Such features include, but are not limited to data localization options, policy enforcement, access controls, logging capabilities, individual rights processing, and cross-border data transfer mechanisms.

Customers control whether the Skyhigh SSE service is enabled or disabled. When it is disabled, no data processed by the service is collected and sent to the Cloud and no data is downloaded by the service from the cloud data centers.

Data Portability

Except for Registration Information, the Customer can forward the personal data processed by Skyhigh SSE to a third-party data store. If applicable, to effectuate data portability, Customers may request assistance from Skyhigh Engineering for a large-scale movement of data (e.g., the Customer does not renew subscription and asks for all data to be transferred to a third-party data store).

Data Deletion and Retention

The table below lists the personal data used by Skyhigh Cloud Platform, the length of time that data needs to be retained and why we retain it.

A data subject may request deletion of his or her Personal Data by sending a data subject request as described below in this Privacy Data Sheet.

A Customer may request data deletion by submitting a ticket to Skyhigh Security support at https://www.skyhighsecurity.com/en-us/support.html. When a Customer makes a request for deletion, Skyhigh Security will purge the requested data from its systems to the extent required by applicable law and may retain administrative data required for legitimate business purposes (e.g., billing records).

Table 5. Data Retention

Personal Data Category	Retention Period	Reason for Retention
Administrative Data	Either 100 or 365 days, depending on SKU purchased.	To conduct internal reporting and reconciliation activities, warranties or to provide Customers with feedback or information.
Generated Data	Shadow Logs: ● Daily data is stored for 45 days, weekly data for 13 weeks, and monthly data for 13 months. ● Data older than 13 months is deleted by default. Incidents, Activities, Threats, Anomalies, and Audit Logs: ● Retained for 100 days or 13 months, depending on SKU purchased.	For granular visibility into Customer cloud usage. For compliance, reporting, and troubleshooting
Collected Data	Web Evidence and Match Highlight: ● Retained for 100 days or 13 months, depending on SKU purchased. Configuration Information:	For operational needs and legal requirements. For system integrations.

	• Retained until the Customer terminates the service.	

Personal Data Security

Files stored on or processed by Skyhigh Security's systems are secured with state-of-the-art technologies, and Skyhigh Security operates rigorous technical and organizational security controls designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Skyhigh Cloud Platform uses a secure portal hosted by AWS to store product data. Data collection is accomplished by downloading an executable tool to the Customer's environment where queries and API calls are performed against Skyhigh products. The collected data is then encrypted using 256-bit encryption as an output file and uploaded via secure SSL connection to the AWS Skyhigh server where it is processed and stored in the encrypted database.

AWS regularly audits and certifies its environment by a third-party vendor. AWS is compliant with dozens of standards including NIST, ISO, SOC, CSA, PCI, GDPR, etc. The latest audit reports are available on the AWS website and can be found once logged into the AWS Console.

For additional details on AWS certifications, visit https://aws.amazon.com/.

- Search for "Artifact"
- Select Artifact from the search results
- Select View Reports from the AWS Artifact page

Table 4. Personal Data Security

Personal Data Category	Type of Personal Data	Security Controls and Measures
Administrative Data	See Table 1	Encrypted in transit and at rest
Generated Data	See Table 1	Encrypted in transit and at rest
Collected Data	See Table 1	Encrypted in transit and at rest

Additional details for product certifications are available upon request.

Compliance with Privacy Requirements

Skyhigh Security is committed to protecting personal data processed in the global and regional Skyhigh Cloud Platform clouds. We will not access the content of files in a way in which we could learn meaningful information about natural persons, other than in exceptional cases where it is necessary for identifying security threats.

The Privacy Office and Skyhigh Security Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Skyhigh Security products

and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

Further, in addition to complying with our stringent internal standards, Skyhigh Security also maintains third-party validations to demonstrate our commitment to information security.

Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will confirm identification (typically with the email address associated with a Skyhigh Security account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller may be redirected to their employer for a response.

Requests can be made by submitting a request via:

1) the Skyhigh Security Individual Data Request Form

2) by postal mail:

In the U.S. by registered mail:
Musarubra US LLC
Attn: Legal Department –Privacy
6000 Headquarters Drive, Suite 600
Plano, Texas, 75024
or call us at +1 (214) 494-9190

In the European Economic Area by registered post:
Musarubra Ireland Limited
Attn: Legal Department –Privacy
Building 2000, City Gate
Mahon, Cork, Ireland
or call us at +353 21 467 2000

In Japan by registered mail:
Musarubra Japan KK
Attn: Legal Department –Privacy
Shibuya Mark City West
1-12-1 Dogenzaka, Chibuyaku, Tokyo 150-0043

About This Privacy Data Sheet

Skyhigh Security Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. Please note that the information provided with this document concerning technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, warranty of fitness for a particular purpose, or compliance with applicable laws.