Stealthwatch Online Visibility Assessment

Security and Privacy Overview

Table of Contents

Introduction

Cisco understands that the confidentiality, integrity, and availability of customer information are vital components to their business operations and our own success.

The purpose of this document is to address Stealthwatch Online Visibility Assessment (SOVA) security and privacy concerns of interest by customers and local compliance requirements.

Infrastructure Overview

You access the service through a web-based dashboard over TLS to gain visibility into account info, configure policy and view logs generated.

SOVA uses Cloud Collectors to collect metadata from customer network traffic. The Cloud Collector is an on-premises device that transmits up to our infrastructure hosting location in Amazon Web Services (AWS). This transmission is performed via a TLS connection.

Security

This section describes the security policies and procedures in place for SOVA.

Physical Security

SOVA is collocated in top-tier data centers and resides in the Oregon (US West-2) region of AWS.

AWS compliance offers robust controls to maintain security and data protection. All data centers are ISO27001 certified and compliant with the SOC 2 Readiness Assessment. Our offices, located in Alpharetta, GA and RTP, NC have undergone a physical security assessment within the last calendar year.

Access Control

We maintain a controlled list of user accounts that have administrator privileges to production systems.

New employees must pass a background check, undergo security training, and sign a non-disclosure agreement.

Employees are granted access on a least-privilege basis. This access requires management approval.

We use AWS multi-factor authentication to grant remote access to the AWS APIs for managing the infrastructure:

Remote access to the application does not require multi-factor authentication. This access provides administration of application data, but does not provide access for altering infrastructure.

Network Protection

We ensure network protection by housing clusters inside of an AWS Virtual Private Cloud. This allows the use of AWS Security Groups to fine-tune security access.

Example: An open node on one specific port

Backups

SOVA backs up system-wide user account information and configuration data on a daily basis. It is encrypted and stored in AWS S3. For any trials needing restored, however, we recommend starting a new trial as the most effective solution.

Internal and Third-Party Testing/Assessments

Cisco defines a security vulnerability as an unintended weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of the product. The service ensures regular scans of our network and systems for security vulnerabilities using internal and third-party tools, best practices, and standards. Our engineering teams follow documented remediation procedures when new vulnerabilities arise.

Our engineers undergo Cisco Security application training in order to ensure vulnerabilities are not built into the product. We also develop the service in accordance with the Cisco Secure Development Lifecycle (CSDL). CSDL is a repeatable and measurable process Cisco designed to increase the resiliency and trustworthiness of our products.

For internal testing, the Cisco InfoSec team ensures that all Security products undergo rigorous application vulnerability assessments and penetration tests to check for weaknesses:

- How Cisco IT and InfoSec Partner to Protect Our Infrastructure and Data

For third-party Cloud Service Providers (CSPs), the service leverages the Cisco CASPR (Cloud/Application Service Provider Remediation) process. The CASPR process is designed to protect and reduce Cisco's exposure to risks in the area of compliance. This process ensures all third-party CSPs are assessed, and the appropriate visibility is available to critical stakeholders around CSP usage:

- Managing Cloud Security and Risk Exposure

Security Incidents

In the event of a confirmed incident affecting customer data, we follow Cisco data security incident policies by contacting the Cisco Product Security Incident Response Team (PSIRT). The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

Data Protection

This section describes the data protection policies and procedures in place for SOVA.

Data in Transit

SOVA stores data in Kafka topics and continues on to encrypted S3.

Results of batch calculations are stored in a secure database and presented to web browsers over secure http/ssl channels.

To access the controller web UI, authentication is required in the form of a username and passphrase.

Data Logged and Retained

SOVA stores customer data in a timeframe necessary for the entire duration of the assessment (both account information and flow data). Sales Engineers or the support team also have privileges to manually delete data during or after the assessment. The raw data is stored in an encrypted AWS S3 bucket:

- AWS S3 Service Level Agreement
- AWS S3 Frequently Asked Questions

Segregation of Clients

SOVA logically segregates and indexes customer data by using globally unique IDs per customer. Database and application level logic ensures that a customer cannot access another customer's data.

Privacy

We collect customer contact information in the form of:

- Name
- Physical Address
- Email address
- Phone number

Any contact information we collect is used solely for customer contact purposes only. We do not share or sell data to third parties. Customer users are able to modify their information within the application and can request for account closure at any time. All account information is deleted upon account closure.

As Cisco is a global organization, we may transfer your personal information to Cisco in the United States of America, to any Cisco subsidiary worldwide, or to third parties and business partners that are located in various countries around the world.

Cisco safeguards and enables the global transfer of personal information in a number of ways:

APEC Privacy Certification

The U.S. APEC Accountability Agent certified that Cisco's global privacy program complies with the Asia Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules System (CBPRs). The CBPRs provides a framework for organizations to ensure protection of personal information transferred among participating APEC economies. More information about the APEC Privacy Framework and CBPRs can be found here. Our certification applies to our business processes across our global operations that process and transfer personal information to/from our affiliates around the world.

EU-US and Swiss-US Privacy Shields

Cisco participates in and has certified its compliance with the EU-U.S. and Swiss-US Privacy Shield Frameworks and Principles as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union (EU) and Switzerland, respectively. Cisco is committed to subjecting all personal data received from European Union (EU) member countries and Switzerland, in reliance on the EU-US and Swiss-US Privacy Shield Frameworks, to the Frameworks' applicable Principles. If there is any conflict between the terms in this Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about these Privacy Shield Frameworks, visit the U.S. Department of Commerce's Privacy Shield site.

Refer to the Cisco Online Privacy Statement for additional detailed information on these programs and how Cisco protects your privacy while using SOVA.