CISCO
SECURE

Data sheet
Cisco public

Cisco Secure Cloud Analytics Datasheet

December 2022

CISCO The bridge to possible

Contents

Cisco Secure Cloud Analytics Datasheet 3
Product overview 3
Features and benefits 4
Network visibility is essential 4
The offering 6
Ordering information 6
Cisco software support for security 6
Protect your environment today 7
Cisco Capital 7

Cisco Secure Cloud Analytics Datasheet

This document describes a product overview and ordering information for Cisco Secure Cloud Analytics, formerly Stealthwatch Cloud Public Cloud Monitoring.

For more detailed information on the product, go to https://www.cisco.com/go/securecloudanalytics.

Gain the visibility and continuous threat detection needed to secure your public cloud and hybrid environments.

Product overview

As organizations move more IT resources to the public cloud, disperse business services, and enable employees to connect from anywhere the opportunity is big for potential threat actors to infiltrate an organizations environment without being seen. Security organizations need a solution that works with other tools in their security suite to extend visibility to the various corners of their network and services and to spot a potential threat actor lurking in the noise of their everyday environment. Secure Cloud Analytics provides the visibility and threat detection capabilities you need to keep your organization secure across all major cloud environments like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, to their existing networks on premise, and their employees connecting to these services.

Secure Cloud Analytics provides comprehensive visibility and high-precision alerts with low noise, without the use of agents. Secure Cloud Analytics is a cloud-based, Software-as-a-Service (SaaS)-delivered solution. It detects ransomware and other malware, data exfiltration, network vulnerabilities, system, event and configuration risk, and role changes that indicate compromise offering anomaly and behavioral detections that complement endpoint detection and cloud security solutions which are focused on protecting individual workloads and computers by extending visibility from these assets, so a more complete picture is understood, threats are caught quicker, and response times are lowered.

To enable integration and response, Secure Cloud Analytics also comes with Cisco SecureX, the broadest, most integrated security platform, to unify visibility, simplify threat response and enable automation across every threat vector and access point.

Features and benefits

Feature	Benefit
Network and cloud analytics	Provides fully automated, real-time analysis of device-level network traffic and patterns of communication for visibility across all devices and resources operating in the public cloud and on the private network.
Reduce mean time to detect with high-fidelity security alerts	Delivers actionable intelligence while reducing false positives, enabling smarter security actions, lowered meant time to detect and respond to threats.
Built-in SecureX platform	Unify visibility, simplify threat response and enable automation with the industry's broadest, most integrated security platform.
Findings mapped to MITRE	Most of the alerts in Secure Cloud Analytics are mapped to MITRE Tactics and Techniques, offering an industry standard way to understand and respond to findings.
Software as a Service (SaaS)	Adds the ease of use, ease of deployment, and flexibility that organizations need to deploy security at scale.
Entity modeling	Provides a behavioral model of every device and entity on the network that is used to automatically identify sudden changes in behavior and malicious activity that is indicative of a threat.
Automatic role classification	Identifies the role of each network device and cloud resource automatically based on its behavior.
Agentless deployment	Consumes native sources of telemetry and logs from the network and Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) cloud instances, with no need for specialized hardware or software agents.
Reduce mean time to respond with pervasive visibility	Understand the blast radius of devices across your network and public cloud, offering a quick way to understand and remediate an active incident that may have been found with Secure Cloud Analytics or other tools such as an Endpoint Security solution or Firewall.

Network visibility is essential

Today's enterprises are dealing with security "blind spots," as the number of devices on the private network grows and more workloads shift to the public cloud. Meanwhile, security practitioners are being flooded with security alerts to the point of incapacity. This necessitates a focus on a variety of security measures that provide a line of protection, including endpoint, network, and cloud security. Anomaly, behavioral, and IOC detection all provide varying levels of visibility to catch an adversary in situations where no single method guarantees success. Many attacks require adversaries to interact with the network in order to achieve their goal. Combining these detection approaches and coverage regions results in a more robust solution for detecting an adversary when they enter an organization, regardless of how advanced they are.

Secure Cloud Analytics provides Anomaly, Behavioral Threat, and IOC detection across the network and public cloud, enabling visibility to areas not seen by other security products and helping to spot attackers that go unseen by point security solutions. Secure Cloud Analytics accomplishes this by consuming sources of telemetry and logs from the public cloud, private network, and then modeling behavior to identify threat activity.

Visibility and analytics

This telemetry is processed in Secure Cloud Analytics to provide visibility of all active entities across your modern network, including the private network, branch, and public cloud. Through entity modeling, the solution can detect a variety of threat activities with a high degree of accuracy. The high-fidelity security alerts support smarter security decisions, reduce the number of false alarms, and shorten the time spent conducting investigations.

Flexibility and ease of use

Secure Cloud Analytics is delivered as Software as a Service (SaaS), making it easy to try, easy to buy, and simple to use. There is no specialized hardware to purchase, no software agents to deploy, and no special expertise required.

From the moment the solution begins receiving data, there is no additional configuration or device classification required. All the analytics are automated and as a result it requires very little management or security expertise to operate.

Entity modeling for advanced threat detection

As telemetry is collected, Secure Cloud Analytics creates a model—a sort of simulation—of every active entity on the network or in the monitored public cloud. This use of modeling helps you rapidly identify early-stage and hidden indicators of compromise. There are no signature lists to update or software agents to deploy.

Each model consists of five key dimensions of entity behavior:

- **Forecast:** Predicts entity behavior based on past activities and assesses the observed behavior against these predictions.
- **Group:** Assesses entities for consistency in behavior by comparing them to similar entities.
- **Role:** Determines the role of an entity based on its behavior, then detects activities inconsistent with that role.
- **Rule:** Detects when an entity violates organizational policies, including protocol and port use, device and resource profile characteristics, and block listed communications.
- **Consistency:** Recognizes when a device has critically deviated from its past behavior, in both data transmission and access characteristics.

Entity modeling allows the solution to detect a variety of behaviors associated with potential threats. For example, Secure Cloud Analytics auto-classifies a public cloud resource. This resource's behavior will be compared to the behavior of similar entities over time. These communication patterns build a baseline for 'normal' behavior, and if there is traffic that deviates from this baseline, users can receive custom alerts via email, other Cisco apps, and even remediate the threat through the Cisco SecureX platform or other third-party solutions. Secure Cloud Analytics can identify roles for all major public cloud providers. It will detect any new behavior, in near-real time and will generate an alert with details of the suspicious traffic.

DNS abuse, geographically unusual remote access, persistent remote-control connections, and potential database exfiltration are examples of Secure Cloud Analytics alerts. In addition, network reports for the top IPs, most used ports, active subnets with traffic statistics, and more are available.

Through pervasive visibility across the network and cloud and leveraging the powerful behavioral analytics, Secure Cloud Analytics is able to not only help spot unknown, advanced, or missed threats more easily and quickly, but this same visibility enables quicker response when a threat is caught by another security solutions such as with Endpoint security.

The offering

Secure Cloud Analytics

The solution can be deployed without software agents, instead relying on native sources of telemetry such as its Virtual Private Cloud (VPC) flow logs or IPFIX on premises. Secure Cloud Analytics models all IP traffic generated by an organization's resources and functions whether they are inside the VPC, between VPCs, or to external IP addresses. It integrates with additional Cloud Service Provider APIs like Cloud Trail, Cloud Watch, Config, Inspector, Identity and Access Management (IAM), Lambda, and many more to look for adversary behavior on the network and infiltrating deep into organizations cloud environment.

Ordering information

Secure Cloud Analytics Product ID: ST-CL-SUB

The licensing is subscription-based and 1-, 12-, 24-, 36- and 60-month terms are available. There's also an option provided for 1- and 12-month auto-renewals. After selecting the term options, you can add the Public Cloud Monitoring and/or Private Network Monitoring offers.

To place an order, contact your Cisco account representative.

Cisco software support for security

The basic online support option of Cisco Software Support for Security is available for Secure Cloud Analytics subscriptions. Basic online support provides foundational support for the full term of the purchased software subscription, including:

Access to support through online tools. (Telephone access is not provided.)

Response from Cisco to a submitted case no later than the next business day during standard business hours.

When a Secure Cloud Analytics subscription is ordered, basic online support is embedded as part of that subscription. It is not a separate orderable service. Therefore, when a Secure Cloud Analytics subscription is renewed, basic online support will also renew with the same term. No additional products or fees are required to receive this support with a SaaS subscription.

For more information about Cisco Software Support, refer to the service description.

Protect your environment today

Try Secure Cloud Analytics today with a free 60-day no-risk trial. To learn more, go to https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html, or contact your local Cisco account representative.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services, and complementary third-party equipment in easy, predictable payments. Learn more.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

990837995 12/22