Cisco Secure Cloud Analytics Datasheet

October 2020
Contents

Product overview .............................................................................................................................................. 3
Features and benefits........................................................................................................................................... 3
Security for the modern network ................................................................................................................... 4
  Visibility and analytics ................................................................................................................................ 4
  Flexibility and ease of use ............................................................................................................................. 5
  Cloud security posture management ........................................................................................................... 5
  Entity modeling for advanced threat detection ............................................................................................ 5
The offering ....................................................................................................................................................... 6
  Secure Cloud Analytics .................................................................................................................................... 6
Ordering information ......................................................................................................................................... 6
Cisco Software Support for Security ............................................................................................................. 6
Protect your environment today ..................................................................................................................... 6
Cisco Capital..................................................................................................................................................... 6
  Flexible payment solutions to help you achieve your objectives ............................................................... 6
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.


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, they need the visibility necessary to detect threat actors targeting their cloud assets. In addition, they need an easy-to-use, operationally efficient solution. Secure Cloud Analytics provides the visibility and threat detection capabilities you need to keep your workloads highly secure in all major cloud environments like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

Development teams are also continuously adopting new and more dynamic compute environments like serverless and containers such as AWS Lambda and Kubernetes. Secure Cloud Analytics provides visibility into these environments as well, so that organizations don’t have to compromise on security on their path to digital transformation.

Secure Cloud Analytics provides comprehensive visibility and high-precision alerts with low noise, without the use of agents. Organizations can also monitor their cloud security posture to ensure configuration best practices and adherence to internal policies, thereby limiting potential risk and exposure of their cloud infrastructure. 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.

In addition to securing the cloud environment, Secure Cloud Analytics can also be extended to the private network with Cisco Secure Network Analytics SaaS (formerly Stealthwatch Cloud Private Network Monitoring) to provide hybrid environment visibility and threat detection using a single dashboard. The number of connected devices on the private network is increasing dramatically. Security personnel are struggling just to know what entities are operating in their environment, let alone whether they pose a threat to the organization. So, with Secure Cloud Analytics, organizations can accurately detect threats in real time, regardless of whether an attack is taking place on the network, in the cloud, or across both environments.

And 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and cloud analytics</td>
<td>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.</td>
</tr>
<tr>
<td>Feature</td>
<td>Benefit</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>High-fidelity security alerts</td>
<td>Delivers actionable intelligence while reducing false positives, enabling smarter security actions.</td>
</tr>
<tr>
<td>Built-in SecureX platform</td>
<td>Unify visibility, simplify threat response and enable automation with the industry’s broadest, most integrated security platform.</td>
</tr>
<tr>
<td>Risk and posture Monitoring</td>
<td>Quickly identify misconfigurations and changes that could introduce risk to the cloud environment, aligned with industry best practices or your internal policy.</td>
</tr>
<tr>
<td>Software as a Service (SaaS)</td>
<td>Adds the ease of use, ease of deployment, and flexibility that organizations need to deploy security at scale.</td>
</tr>
<tr>
<td>Entity modeling</td>
<td>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.</td>
</tr>
<tr>
<td>Automatic role classification</td>
<td>Identifies the role of each network device and cloud resource automatically based on its behavior.</td>
</tr>
<tr>
<td>Agentless deployment</td>
<td>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.</td>
</tr>
<tr>
<td>Monitoring private network/hybrid environments</td>
<td>Detects threats and anomalies in the private network as well as your public cloud resources using a single tool to streamline security operations and workflows.</td>
</tr>
</tbody>
</table>

**Security for the modern network**

Today’s organizations are struggling with security “blind spots.” There is an explosion of devices on the private network, and more workloads are being migrated to the public cloud. Meanwhile, security practitioners are inundated with security alerts to the point of unmanageability. Only 51 percent of security alerts are investigated, and more than half of those are not remediated, according to the Cisco 2019 CISO Benchmark Study.

Attackers are quick to take advantage of these developments to breach network defenses and remain undetected. Organizations need an easy way to see their network activity, understand what “normal” entity behavior is, and identify the signs of threats. Secure Cloud Analytics accomplishes this by consuming sources of telemetry and logs from the public cloud, 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.

Cloud security posture management

Secure Cloud Analytics begins checking your cloud resources for risky configurations and changes upon deployment. You can also create your own watchlists to be alerted to activity of interest, and to ensure cloud resources are adhering to your internal policy.

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.

Private network monitoring with Secure Network Analytics SaaS

As mentioned above, with Secure Network Analytics SaaS, users can monitor their private network as well, from the same interface as Secure Cloud Analytics. To learn more, please see the [Cisco Secure Network Analytics Data Sheet](https://www.cisco.com/c/en/us/products/endpoint-security/secure-network-analytics-data-sheet.html).
The offering

**Secure Cloud Analytics**

Secure Cloud Analytics provides visibility and threat detection in Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure infrastructures. It is a cloud-delivered, SaaS-based solution that can be deployed easily and quickly.

The solution can be deployed without software agents, instead relying on native sources of telemetry such as its Virtual Private Cloud (VPC) flow logs. 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.

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


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.