Cisco Stealthwatch Cloud

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

Product Overview

Cisco® Stealthwatch Cloud improves security and incident response across the distributed network, from the private network and branch office to the public cloud. This solution addresses the need for digital businesses to quickly identify threats posed by their network devices and cloud resources, and to do so with minimal management, oversight, and security manpower.

The network is evolving. IT resources are frequently being moved into the cloud. At the same time, 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.

Stealthwatch Cloud addresses this problem by providing comprehensive visibility and high-precision alerts with low noise, without the use of agents. 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. Stealthwatch Cloud is a cloud-based, Software-as-a-Service (SaaS)-delivered solution. It detects ransomware and other malware, data exfiltration, network vulnerabilities, and role changes that indicate compromise.

Features and Benefits

Feature	Benefit
Network visibility	Provides fully automated, real-time analysis of device-level network traffic and patterns of communication for better awareness of what devices and resources are operating on the network and in the public cloud
High-fidelity security alerts	Delivers actionable intelligence while reducing false positives, enabling smarter security actions
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) cloud instances, with no need for specialized hardware or software agents

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 and more workloads are being migrated to the public cloud. Meanwhile, security practitioners are inundated with security alerts to the point of unmanageability. Only 56 percent of security alerts are investigated, and more than half of those are not remediated, according to the Cisco 2017 Annual Cybersecurity Report.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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. Stealthwatch Cloud accomplishes this by consuming sources of telemetry and logs from the private network and public cloud, and then modeling behavior to identify threat activity.

Visibility and Analytics

This telemetry is processed in Stealthwatch Cloud to provide visibility of all active entities across your network, including the private network, branch, and public cloud. Through the use of entity modeling, Stealthwatch Cloud 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

Stealthwatch Cloud 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 Stealthwatch Cloud begins receiving data, there is no additional configuration or device classification required. All the analytics are automated. Because of this, Stealthwatch Cloud requires very little management or security expertise to operate.

Entity Modeling for Advanced Threat Detection

As telemetry is collected, Stealthwatch Cloud 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 blacklisted communications.
- **Consistency:** Recognizes when a device has critically deviated from its past behavior, in both data transmission and access characteristics.

This use of modeling can detect a variety of behaviors associated with potential threats. For example, Stealthwatch Cloud autoclassifies a printer, but later that printer starts scanning the network and establishes a heartbeat connection to an outside server. Those new communication patterns are not consistent with a printer or the specific behavioral model of that device, which could be a sign of compromise. Stealthwatch Cloud will detect this new behavior, and more, 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 Stealthwatch Cloud alerts. In addition, network reports for the top IPs, most used ports, active subnets with traffic statistics, and more are available.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Two Offerings

Cisco Stealthwatch Cloud consists of two primary offerings, Public Cloud Monitoring and Private Network Monitoring.

Public Cloud Monitoring

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

In AWS environments, Stealthwatch Cloud can be deployed without software agents, instead relying on native AWS sources of telemetry such as its Virtual Private Cloud (VPC) flow logs. Using VPC flow logs, Stealthwatch Cloud 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. Stealthwatch Cloud is also integrated with additional AWS services like Cloud Trail, Cloud Watch, Config, Inspector, Identity and Access Management (IAM), Lambda, and more.

In Microsoft Azure environments, Stealthwatch Cloud relies on a software sensor that must be deployed to all of the Linux servers where entity modeling is desired.

Public Cloud Monitoring can be used in combination with Private Network Monitoring or Cisco Stealthwatch Enterprise to provide visibility and threat detection across the entire network.

To enable Stealthwatch Cloud in Amazon Web Services:

- A policy with the appropriate permissions needs to be created.
- A role needs to be created for Stealthwatch Cloud.
- Amazon VPC flow logs need to be enabled.

To enable Stealthwatch Cloud in Microsoft Azure, a software sensor must be deployed on every Linux server to generate flow logs. There is currently no Microsoft Windows sensor available.

Private Network Monitoring

Cisco Stealthwatch Cloud Private Network Monitoring provides visibility and threat detection for the on-premises network, delivered from a cloud-based SaaS solution. It is the perfect solution for organizations that want better awareness and security in their on-premises environments while reducing capital expenditure and operational overhead.

It works by deploying a lightweight virtual appliance in a virtual machine or server that can consume a variety of native sources of telemetry or extract metadata from network packet flow. It encrypts this metadata and sends it to the Stealthwatch Cloud analytics platform for analysis. Stealthwatch Cloud consumes metadata only. The packet payloads are never retained or transferred outside the network.

Network interfaces	1 if only collecting NetFlow, IPFIX, or JFlow; 2 if attaching to a SPAN or mirror port
Memory	At least 2 GB
CPU	At least 2 cores
Disk space	At least 32 GB

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

For Private Network Monitoring, the Flow Rate License is required for the collection, management, and analysis of flow telemetry. The Flow Rate License also defines the volume of flows that may be collected and is licensed on the basis of flows per second (fps).

Ordering Information

The Cisco Stealthwatch ordering guide, section 3, will help you understand Stealthwatch Cloud components and licensing types. 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 Cisco Stealthwatch Cloud 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 Cisco Stealthwatch Cloud subscription is ordered, basic online support is embedded as part of that subscription. It is not a separate orderable service. Therefore, when a Cisco Stealthwatch Cloud 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 Stealthwatch Cloud today with a free 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

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. 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**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C78-739619-00 09/17

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.