

# Better control, easier management, enhanced security analytics, and context-aware threat mitigation

## What's new in Cisco Stealthwatch Release 7.0

Have you been compromised? How would you know? With today's evolving threats, it's a matter of time when an organization will be breached. You need eyes within your environment to be able to detect any suspicious behavior. This is where a visibility and security analytics solution like Cisco Stealthwatch® can help. Stealthwatch collects telemetry from your existing network infrastructure, and applies a funnel of analytical techniques to detect anomalies in real-time and also ties it to specific threats with a high level of confidence.

However, every organization is different with its own workflows. What might be considered suspicious activity within one, might not necessarily apply to another. And with security teams already strapped for time and resources, you don't want to spend time chasing down irrelevant alerts, or worse, miss critical threats. Stealthwatch gives you an unmatched level of control to fine-tune security and customize it to the business logic.

Stealthwatch release 7.0 introduces further enhancements to the tuning capabilities of Stealthwatch, giving you even more control and easier management of the security policies, users, host groups, and appliances, all of which are now accessible from the web interface. In addition to that, we are announcing tons of other exciting updates for faster, more advanced threat detection and response.

### New features

- Policy, user, and host group manager enhancements
- Centralized appliance and update management
- Cisco® Identity Services Engine (ISE) integration enhancements
- Stealthwatch Apps
- Enhanced security analytics
- USGv6 certification with basic IPv6 management port addressability

## Policy Management updates

All three types of Stealthwatch security policies: core events, custom events, and relationship events, can be managed centrally by the admin using the web interface. Now you can create, edit, or delete events easily. And with just one click, you can view the “effective policies” that are currently applied to a specific host, or drill down into an alarm to tune the event.

**Figure 1:** Stealthwatch Core Events control how Stealthwatch monitors and responds to host behavior that it observes. Core events can reduce unwanted alarms on your system as well as ensure that alarms are triggered in certain instances. Stealthwatch has three types of Core events – Host, Role and Default, in order of precedence.

- 1 View detailed alarm description, and modify policies based on behavioral and threshold values
- 2 Easily search for policies set for a host or host group
- 3 View, create and modify default policies, or define them by role or specific hosts
- 4 Filter Core Events by multiple parameters

Policy Management

Search for a host or select a host group

Custom Events (2) Relationship Events (352) Core Events (654)

EVENT	EVENT TY...	POLICY NAME	POLICY TYPE	HOSTS	WHEN HOST IS SOURCE	WHEN HOST IS TARGET
Ex. Anomaly	Ex. C...	Ex. Outside Hosts	Ex. Role	Ex. Network Scanners	Ex. On + Alarm	Ex. On + Alarm
Talks to Phantoms	Security	10.201.3.78	Host	10.201.3.78	On + Alarm	On
Talks to Phantoms	Security	Outside Hosts	Default	Outside Hosts	On	On
Talks to Phantoms	Security	Inside Hosts	Default	Inside Hosts	On	On
Target Data Hoarding	Security	10.201.0.23	Host	10.201.0.23	On	On + Alarm
Target Data Hoarding	Security	10.201.0.55	Host	10.201.0.55	On	On + Alarm
Target Data Hoarding	Security	Firewalls, Proxies, & NAT Devices	Role	NAT Gateway, Proxy	Off	Off
Target Data Hoarding	Security	Outside Hosts	Default	Outside Hosts	On	On
Target Data Hoarding	Security	Inside Hosts	Default	Inside Hosts	On	On + Alarm

Description  Behavioral and Threshold  Threshold Only

Tolerance 92 / 100

Never trigger alarm when less than: 476.84 M downloaded payload bytes in 24 hrs

Always trigger alarm when greater than: 931.32 G downloaded payload bytes in 24 hrs

**Figure 2:** Stealthwatch Custom Security Event (CSE) is a unique policy created for your environment that is configured based on rule types and rule values. CSEs begin as a blank slate and allow you to designate the who, what, and how for the flow that will cause an event or alarm to trigger.

- 1 Multiple rule parameters to choose from
- 2 Rules also include Encrypted Traffic Analytics (ETA) parameters to easily monitor for weak encryption
- 3 View an automatically generated easy-to-read event summary

Policy Management | Custom Security Event

NAME *	DESCRIPTION
Engineering Comms to Compliance via TLS 1.0	Prohibited comm type to Compliance

When any host within *Engineering* communicates with any host within *Compliance Systems*; using *TLS 1.0 encryption*, an alarm is raised.

FIND

SUBJECT HOST GROUPS: Engineering

PEER HOST GROUPS: Compliance Systems

ENCRYPTION TLS/SSL VERSION: TLS 1.0

Search for a rule type

- Peer TrustSec IDs
- Subject TrustSec Names
- Peer TrustSec Names
- Subject Applications
- Peer Applications
- Subject File Hashes
- Peer File Hashes

View All

**Figure 3:** Stealthwatch Relationship Events provide a way to monitor the current state of traffic between host groups with the ability to filter the traffic by applications and services.

- 1 Use relationship events to monitor policy violations by host groups
- 2 View detailed alarm description, and modify policies based on behavioral and threshold values
- 3 Easily search for policies set for a host or host group
- 4 Filter Relationship Events by multiple parameters

The screenshot displays the 'Policy Management' interface. At the top, there is a search bar with a 'Search' button and a dropdown menu for host groups. Below this, there are tabs for 'Custom Events (6)', 'Relationship Events (11)', and 'Core Events (654)'. The main content area is divided into several sections:

- Event Selection:** A dropdown menu showing 'Ex. Relationship High Traffic'.
- Policy Name:** A dropdown menu showing 'Confidential Systems <-> Out...'. A blue circle '3' is next to the search icon.
- MAP:** A dropdown menu showing 'Filter Map'.
- HOST GROUPS:** A dropdown menu showing 'Ex. "Inside Hosts"'. A blue circle '4' is next to the dropdown arrow.
- TRAFFIC BY SERVICES:** A dropdown menu showing 'Ex. "trips"'. A blue circle '1' is next to the dropdown arrow.
- TRAFFIC BY APPLICATIONS:** A dropdown menu showing 'Ex. "Corporate Email"'. A blue circle '1' is next to the dropdown arrow.

Below these sections, there is a detailed view of a 'Relationship High Total Traffic' event. It includes a 'Description' box, a 'Behavioral and Threshold' section with radio buttons, and a 'Tolerance' section with input fields for 'Never trigger alarm when less than', 'Always trigger alarm when greater than', and 'Trigger alarm when duration greater than'. A blue circle '2' is next to the 'Threshold Only' radio button.

At the bottom, there is a table listing several policies:

EVENT	POLICY NAME	MAP	HOST GROUPS	TRAFFIC BY SERVICES	TRAFFIC BY APPLICATIONS
Relationship High Total Traffic	Confidential Systems <-> Outside Hosts	Functional Map	Confidential Servers <-> Outside Hosts	All Services	All Applications
Relationship High Traffic	Confidential Systems <-> Outside Hosts	Functional Map	Confidential Servers <-> Outside Hosts	All Services	All Applications
Relationship ICMP Flood	Confidential Systems <-> Outside Hosts	Functional Map	Confidential Servers <-> Outside Hosts	All Services	All Applications
Relationship Low Traffic	Confidential Systems <-> Outside Hosts	Functional Map	Confidential Servers <-> Outside Hosts	All Services	All Applications
Relationship Max Flows	Confidential Systems <-> Outside Hosts	Functional Map	Confidential Servers <-> Outside Hosts	All Services	All Applications

## User Management and Host Group Management updates

Add Stealthwatch users and configure access to data based on their roles. Create Host Groups to effectively monitor for anomalies and threats based on the business workflows.

Figure 4: User Management

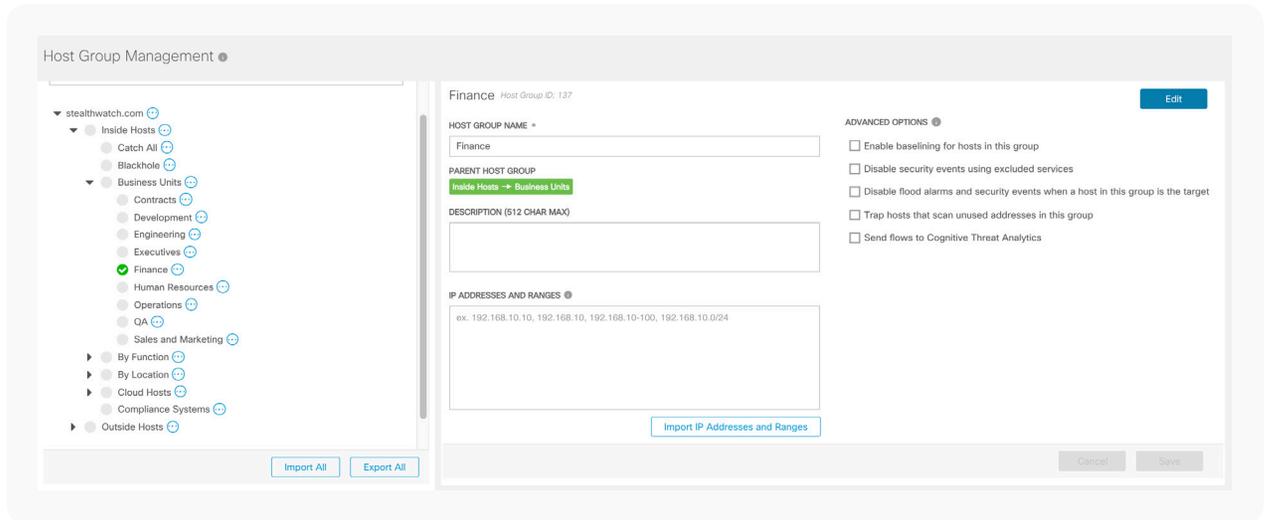
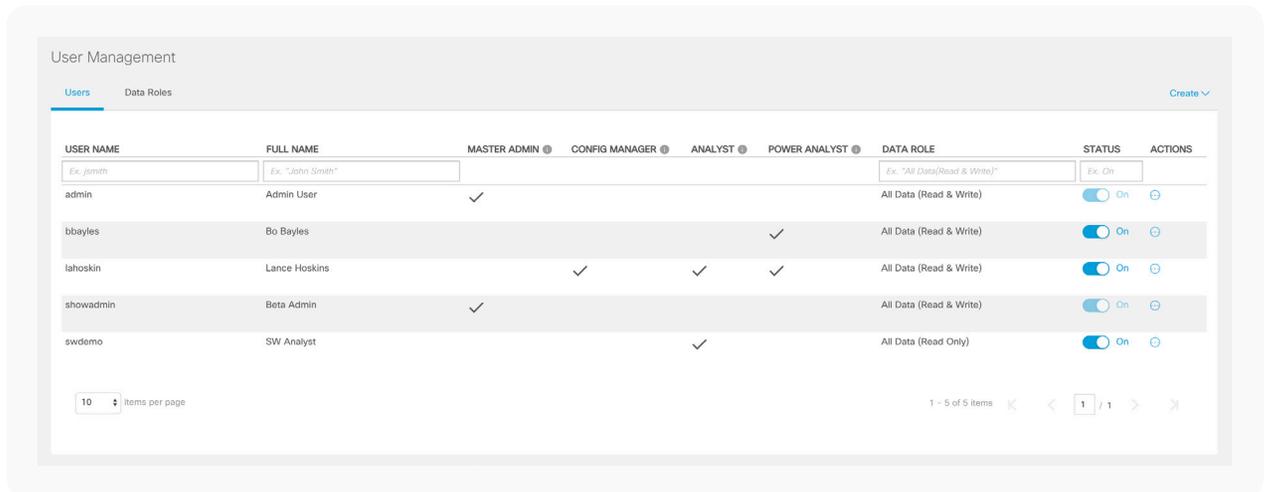


Figure 5: Host Group Management



## Centralized appliance and update management

Don't let the upgrade process get in the way of security. We have simplified management and update of all the Stealthwatch appliances like the Stealthwatch Management Console (SMC) and the Flow Collector, and it can be all be done from one place.

Figure 6: Appliance Manager

Figure 7: Update Manager

Update Information

Use the Update Manager page to apply software upgrades, updates, and patches. The SMC and Flow Collector must be on for at least 1 hour but no more than 1 week to be updated. For best results, perform the update procedures on each appliance in the following order:

- All UDP Directors (also known as FlowReplicators)
- Flow Collector 5000 Series Databases
- Flow Collector 5000 Series Engines
- All other Flow Collectors
- Endpoint Concentrator
- Secondary Stealthwatch Management Console
- Primary Stealthwatch Management Console
- All Flow Sensors

**Upload**

Upload one file at a time.

For important instructions, download the Stealthwatch Update Guide from the [Download & License Center](#).

System Updates

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
SMC	BetaSMC01	10.192.102.21	29 days ago	7.0.0 2018.07.08.0734-0	-		
Flow Collector	BetaFCNF01	10.192.102.22	29 days ago	7.0.0 2018.07.08.0732-0	7.0.0 2018.07.08.0732-0	Waiting to Install	

## Cisco Identity Services Engine (ISE) integration enhancements

Stealthwatch is integrated with ISE to provide additional user and identity context around a threat detection. This integration also allows the security professional to take action to mitigate the threat right from within Stealthwatch. With release 7.0, we are making further updates to the integration with ISE. Now you can choose from multiple ISE ANC (Adaptive Network Control) policies based on the severity of the threat, and ISE will apply the selected policy to the compromised host. Stealthwatch allows you to implement a smarter network segmentation strategy with the visibility that it provides within the environment, and now, it is further enhanced by the availability of Cisco TrustSec® Security Group Tags (SGTs). SGT fields can be used to create Custom Security Events (CSEs) or to search through the telemetry while investigating threats. The Stealthwatch and ISE integration also supports multiple ISE clusters and other performance improvements to allow larger customers to scale user sessions.

Figure 8: Stealthwatch and ISE integration

- 1 Rapid threat containment using ISE ANC policy  
– selective mitigation based on threat severity

The screenshot displays two main components of the Stealthwatch interface. On the left, a modal window titled "Applying ANC policy" is open, showing a table of ISE policies for host 10.90.90.101. The table has columns for ISE, Username, MAC, and ANC Policy. A dropdown menu is open over the ANC Policy column, listing options: "No policy applied", "ANC\_Shutdown", "ANC\_Suspicious", "ANC\_NO\_WEB", and "ANC\_Quarantine". On the right, a "Host Summary" panel for host IP 10.90.90.101 is shown, with tabs for "Flows", "Classify", and "History". The summary includes fields for Status (Active), Hostname, Host Groups (End User Devices, Main Campus Building 2), Location (RFC 1918), First Seen (6/29/18 5:57 PM), Last Seen (7/24/18 6:02 PM), Policies (Client IP Policy, Inside), MAC Address (00:50:56:b6:37:1d (VMware, Inc.)), and ISE ANC Policy (ANC\_Suspicious). Below these panels, a search query is displayed: "When any host within Compliance Systems; as a user with a TrustSec ID of 7 communicates with any host within Outside Hosts, an alarm is raise". The search criteria are: SUBJECT HOST GROUPS: Compliance Systems; PEER HOST GROUPS: Outside Hosts; SUBJECT TRUSTSEC IDS: 7.

- 2 TrustSec Security Group Tags (SGTs) are pulled from ISE and mapped to IP addresses  
– provides ability to implement more efficient network segmentation by using SGTs to create Custom Security Events

## Benefits:

- Get unmatched level of control to fine-tune security and customize it to the business logic
- Save time on managing and updating the tool to focus on better security
- Stay ahead of evolving threats with updates to the machine learning analytics
- Choose the appropriate mitigation action based on threat severity and context
- Easily detect and investigate incidents using the intuitive interface

## Next steps

For further details about this release, please refer to the [release notes](#).

To learn more about Stealthwatch, visit <https://www.cisco.com/go/stealthwatch> or contact your local Cisco account representative.

## Introducing Stealthwatch Apps!

Get exciting new Stealthwatch functionalities on-the-fly without upgrading the entire system. You can find the App Manager under Global Settings -> Central Management. Stay tuned for apps that will deliver additional features!

## Enhanced security analytics

And we continue to update and improve Stealthwatch analytics to stay ahead of evolving threats, for faster and high-fidelity threat detection. The cloud-based machine learning engine (Cognitive Intelligence) includes enhancements for more efficient botnet detection, ability to analyze and correlate proxy logs to network telemetry for increased efficacy, option to apply analytics to specific internal servers, auto-update for cryptomining classifier to detect unusual and new cryptomining pools, and more!

**Figure 9:** Example botnet detection characterized by communication to many IP addresses hosted in multiple autonomous systems.

