Enhanced Threat Detection, Investigation, and Response

What’s new in Cisco Stealthwatch Enterprise Release 6.10.2

Cisco Stealthwatch® Enterprise is a comprehensive visibility and security analytics solution that takes full advantage of enterprise telemetry from the existing network infrastructure. It provides advanced threat detection, accelerated threat response, and simplified network segmentation by using multilayer machine learning and entity modeling across the extended network.

Now we are introducing enhanced features that will help resource-strapped security teams address the challenges of protecting the network infrastructure more comprehensively. Your team will be able to detect advanced threats faster and investigate them using intuitive workflows, without getting overwhelmed by the large number of security alerts received on a typical day.

New features

- Stealthwatch Management Console web interface updates
  - Investigate incidents faster with optimized, more granular telemetry search and contextual results management
  - Prioritize risks and respond to threats in real time with access to top security events
  - Get deeper visibility into the traffic and application patterns within the digital business
  - Enjoy better user experience through enhancements for more intuitive workflows
- Integration with Stealthwatch® Cloud to easily monitor the public cloud infrastructure
- Convenient management, better support, and product compliance features
- Enhanced security analytics to stay ahead of evolving threats (Global Threat Analytics, formerly Cognitive Threat Analytics updates)

44% of security alerts are NOT investigated

Source: Cisco 2017 Security Capabilities Benchmark Study

© 2018 Cisco and/or its affiliates. All rights reserved.
Stealthwatch Management Console web interface updates

Investigate incidents faster with optimized, more granular telemetry search and contextual results management

Cisco Stealthwatch Enterprise helps teams troubleshoot security events faster by providing a comprehensive set of search parameters for a more flexible and controlled telemetry search.

What’s new in 6.10.2

- More search parameters make it easier to perform granular investigations that return comprehensive results (Figure 1)
- Most common search parameters are organized for easy access
- Filter search results in place based on contextual information, without running a new query, to narrow down the problem quickly (Figure 2)
- Set the maximum number of records to be returned and easily export results in common (CSV) format for further analysis

With Release 6.9.2, we introduced the ability to analyze encrypted traffic to help ensure compliance. You can determine the quality of encrypted traffic using Cisco® Encrypted Traffic Analytics, a revolutionary technology within Cisco Stealthwatch Enterprise and the next-generation Cisco network. With Release 6.10.2, you can perform an advanced search on encrypted traffic based on parameters such as encryption key exchange, encryption algorithm, key length, TLS/SSL version, and more to help ensure cryptographic compliance (Figure 3)

© 2018 Cisco and/or its affiliates. All rights reserved.
Figure 2. Narrow down investigations faster by filtering query results in place.

Figure 3. Cisco Stealthwatch Enterprise is the only solution that uses the network to help ensure policy compliance without the need for additional tools.
What’s new in 6.10.2

- Immediately view the top security events for a specific host, and easily determine if the host is the source or target of an attack using the “Top Security Events” widget in the Host report dashboard (Figure 4)
- Get additional security event details, such as the policies that were violated, to understand exactly why the event was triggered (Figure 4)
- Drill down into telemetry associated with a security event with a single click for deeper investigations (Figure 4)
- Visualize traffic destinations from specific host groups, both inside and outside the organization, to assess security risks using the “Top Host Groups by Traffic” widget in the Host Group report dashboard

Prioritize risks and respond to threats in real time with access to top security events

With Cisco Stealthwatch Enterprise, you can easily tie a security event within your digital business to a specific host so you can immediately identify the source or the target of the threat and take steps to mitigate it.

**Figure 4.** Top Security Events widget in host report
What’s new in 6.10.2

- Monitor traffic passing through all the exporters in the network and view their current and maximum usage, bandwidth, speed, etc., using the Interface dashboard under the Monitor menu
- Easily analyze the type of applications passing through the exporters (Figure 5)
- Investigate alarms triggered by exporters. Filter the traffic view by time, and drill down into telemetry associated with the event

Get deeper visibility into traffic and application patterns

Cisco Stealthwatch Enterprise is a highly scalable visibility and security analytics solution because it uses telemetry from your existing network infrastructure to strengthen security. And the comprehensive visibility makes it easy to monitor the overall health of network devices.

Figure 5. Deeper visibility into traffic and applications

Enhancements for a better user experience

- Improved performance of Host List view
- Ability to Select All/Deselect All on chart legends
- Cisco Stealthwatch About page and Help page
- Multiple language support
- User interface consistencies
- Support for new tabs in context search menu

Simplified management, with improved support and compliance

Cisco Stealthwatch Enterprise is a highly mature solution built to scale with your growing business. It integrates with other security products to boost your confidence in your security posture and is compliant with major industry standards such as PCI and HIPAA.
What’s new in 6.10.2

- Stealthwatch administrators can easily sign up for Stealthwatch Cloud accounts with a free 60-day trial
- Stealthwatch users can turn on the integration after the administrator activates the Stealthwatch Cloud account (Figure 6)
- You can view alerts that are open and who they are assigned to in the “Alerts” widget. Clicking the alert name pivots to the Stealthwatch Cloud portal for more details
- The “Network Activity” graph provides a view of the traffic and the number of endpoints along with any open and closed alerts. Clicking the alert indicator pivots to the Stealthwatch Cloud portal for more details
- The “Highlighted Observation Summary” widget shows a count of observations in critical categories such as “Bad Protocol”, “Heartbeat”, etc. Observations are facts about the network automatically recognized by Stealthwatch Cloud endpoint modeling. Clicking the observation name pivots to the Stealthwatch Cloud portal for more details

Integration with Cisco Stealthwatch Cloud

Cisco Stealthwatch Cloud is a cloud-native solution that provides visibility and threat detection in your Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure environments. With Release 6.10.2, you can easily sign up for and perform public cloud monitoring with Stealthwatch Cloud from the Stealthwatch Enterprise dashboard (Figure 6). And this integration comes with a free, no-risk, 60-day trial.

Figure 6. Cisco Stealthwatch Cloud dashboard
What’s new in 6.10.2

- Improved classifiers that apply machine learning to more effectively detect advanced threats such as:
  - Command and control communication
  - Domain Generation Algorithms (DGA) or data tunneling (Figure 7)
  - Malicious Server Message Block (SMB) service discovery associated with zero-day attacks
  - BitTorrent clients
  - Cryptomining
- More contextual information for incidents and increased efficacy of the detection engine
- Option to send additional data to Global Threat Analytics to monitor specific host groups, such as internal servers, for increased protection and visibility into data exposure

Next steps

To learn more, visit https://www.cisco.com/go/stealthwatchenterprise or contact your local Cisco account representative.

Enhanced security analytics to stay ahead of evolving threats

With Release 6.9.1, we introduced the integration of Cisco Stealthwatch Enterprise with Global Threat Analytics. This cloud-based threat detection and analytics capability uses the power of multilayer machine learning and global threat intelligence to detect advanced threats. The attacks are getting smarter, and security analytics techniques need to adapt to detect those threats. Release 6.10.2 brings many enhancements to the capabilities of the machine learning cloud engine. Please note that you need to enable the integration.

Figure 7. Detection of unexpected DNS usage, caused by DGA-based malware or data tunneling