As our networks continue to evolve, so does the threat landscape. That’s why we are constantly enhancing the security analytics behind Cisco Stealthwatch Cloud – a SaaS-based network traffic analysis solution that provides visibility and threat detection across the entire network, on-premises and the cloud. We are introducing new alerts related to confirmed threats, even if they are hiding in encrypted traffic. And at no cost of effort or time to the user.

**Rise of encrypted threats**

Encryption technology has enabled much greater privacy and security for enterprises that use the Internet to communicate and transact business online. However, threat actors have leveraged these same benefits to evade detection and to secure their malicious activities.

**Solution: Encrypted Traffic Analytics**

In June 2017, Cisco announced [Encrypted Traffic Analytics (ETA)](https://www.cisco.com/c/en/us/products/solutions/encrypted-traffic-analytics.html) – a revolutionary technology that enables analysis of encrypted traffic without any decryption, using specially designed metadata generated by specific Cisco network devices that is then analyzed by Cisco Stealthwatch network security analytics. Over the years, a number of customers have adopted this technology. And we have found that among our customers who have Cisco Encrypted Traffic Analytics deployed, 63% of all threat detections and 76% of critical or high-risk threat detections were discovered in encrypted traffic.

---

**What’s New?**


Stealthwatch Cloud is also integrated with Cisco Cognitive Intelligence, a cloud-based machine learning engine integrated with other Cisco Security products. Cognitive Intelligence processes billions of connections daily and has a wealth of information on malicious domains, URLs, hostnames, and more and can be cross matched with local telemetry to generate confirmed threats in Stealthwatch Cloud.
SaaS-delivered Encrypted Traffic Analytics

Now, Stealthwatch Cloud has the ability to ingest enhanced telemetry for Encrypted Traffic Analytics to analyze and detect encrypted threats without decryption. Analytics are further enhanced by Cognitive Intelligence which brings the Confirmed Threat Service to Stealthwatch Cloud, allowing for higher fidelity threat detection.

Core benefits:

- **Confirmed threat detection**
  - Our cloud-based Cognitive Intelligence engine uses a variety of learning techniques and statistical modeling to determine malicious domains and threats across the world.

- **High Fidelity threat detection in encrypted traffic**
  - Stealthwatch Cloud analyzes network behavior and detects threats, even if they are hiding in encrypted traffic. ETA looks into attributes like the IDP and SPLT to detect encrypted malware.

- **Cryptographic compliance**
  - Stealthwatch Cloud offers an “Encrypted Traffic” report that displays various encryption parameters like protocol algorithm, message authentication code (MAC), and more.

- **Effective threat response**
  - The “Confirmed Threat Watchlist Hit” alert not only provides information about the threat and what is infected, but also provides a list of steps that can be taken to remediate the threat.

Here’s how it works:

ETA capable exporter sends enhanced telemetry to the Stealthwatch Cloud sensor. The sensor feeds enhanced telemetry into Stealthwatch Cloud, and Stealthwatch Cloud uses enhanced telemetry to provide better threat detections.

ETA capable exporters currently supported by Stealthwatch Cloud include:
- Catalyst 9300, Catalyst 9400, ASR, CSR, ISR, Stealthwatch Enterprise Flow Sensor

For more information on how to configure/enable ETA:

Software-defined access deployment guide
Configuration Guide
ETA Deployment guide

© 2019 Cisco and/or its affiliates. All rights reserved.
Cognitive Intelligence
Confirmed Threat Service

Confirmed Threat Watchlist Hit:
Notifications of high-risk threats

After correlating local customer telemetry with known IoCs (indicators of compromise) coming from Cisco Talos and Cognitive Intelligence, Stealthwatch Cloud generates notifications with information about the type of threat and threat level, and specifically calls out the IoCs used to generate the confirmed threat.

The Confirmed Threat Watchlist Hit contains a wealth of information about confirmed threats. Here you will find a list of specific observations that notify users of communication with any flagged IoCs. This reduces the amount of time you spend looking for interaction with malicious domains, hosts or IP’s, and gives you more time for remediation.
Ensure cryptographic compliance

You can also ensure cryptographic compliance with the Stealthwatch Cloud encryption report which contains information about encrypted traffic that allows you to determine the quality of encryption. Without this report, organizations often conduct tedious quarterly audits of their network traffic. With the Stealthwatch Cloud encryption report, you can see what devices are not compliant with the most up to date encryption protocol in near real time. For example, to remain PCI-DSS compliant, financial institutions cannot use TLS 1.0 or earlier. The encryption report allows you to easily fix devices that fall out of compliance.

Example High Risk Confirmed Threats:

- Click fraud
- Malware
- Exfiltration
- Spam botnet
- Cryptocurrency miner
- Ransomware
- Malicious content distribution
- Exploit kit

Don't have Cisco Stealthwatch Cloud?

- For more information on Cisco Stealthwatch Cloud click here
- Or sign up for a free 60-day trial here

Conclusion

With the integration of Encrypted Traffic Analytics and Cognitive Intelligence into Stealthwatch Cloud, users will be able to reduce the amount of time they spend searching for critical threats and put more time into remediation. Perhaps one of the best features is that you don’t need to do anything to benefit from these integrations. ETA capable exporters send enhanced telemetry directly to the Stealthwatch Cloud sensor and the Confirmed Threat Service is up and running on the Stealthwatch Cloud dashboard. All at no cost to you.