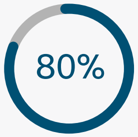
Encrypted Traffic Analytics with the New Cisco Network and Stealthwatch

Increase confidence in encrypted traffic without compromising on data privacy

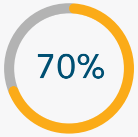
The rapid rise of encrypted traffic is changing the threat landscape. Digital businesses, with their growing complexity due to the large number of devices and applications accessing their network, are increasingly using encryption to secure information. It has been reported that as of 2017, nearly half of all Internet traffic is protected by HTTPS.[1] And the amount of encrypted traffic on the network will only continue to increase.

Encryption enables greater privacy and security, which is particularly necessary for mobile, cloud, and web applications. However, attackers are also using encryption to conceal malware and evade detection by traditional security products. So what used to be a safe and reliable protocol has now become an opportunity for cyber criminals. Data breaches can have a significant impact on an organization. Research has found that the average time to detect a breach on the network is around 200 days, and the average cost of a breach is approximately $3.62 million.[2] Unfortunately, many organizations do not have a way to detect malicious activity in encrypted traffic without decryption.

By 2019:



of all traffic will be encrypted



network attacks will use encryption

Source: Gartner

Benefits of the solution

- **Enhanced visibility:** Gain insight into threats in encrypted traffic using network analytics and machine learning. Obtain contextual threat intelligence with real-time analysis correlated with user and device information.
- **Cryptographic assessment:** Help ensure enterprise compliance with cryptographic protocols and visibility into and knowledge of not only what is being encrypted in the network, but also the strength of the encryption.
- **Faster time to response:** Quickly contain infected devices and users by detecting threats within encrypted traffic in real time without relying on slow, decryption-based methods.
- **Time and cost savings:** Use the network as the foundation for the security posture, capitalizing on security investments in the network.

> **“Identifying threats contained within encrypted network traffic poses a unique set of challenges. It is important to monitor this traffic for threats and malware, but in a way that maintains the integrity of the encryption.”[3]**
>
> **– Blake Anderson, Advanced Security Research Group**

How does it work?

Solution elements:

- Enterprise switches: Cisco® Catalyst® 9000 switching platform (starting with Cisco IOS® XE Software release 16.6.1)
- Branch routers: Cisco ASR 1000 Series, 4000 Series ISRs, 1000 Series Routers, Cloud Services Router 1000V, and Integrated Services Virtual Router (starting with Cisco IOS XE Software release 16.6.2)
- Network visibility and security analytics: Cisco Stealthwatch® Enterprise (starting with release 6.9.2)

The burden of determining that encrypted network traffic is trustworthy has become too onerous for most incident response teams. Traditional threat inspection with bulk decryption, analysis, and reencryption is impractical because of the tremendous cost and time overhead. Even when inspection is possible, solutions that decrypt network traffic weaken the privacy of the users and do not work for all types of encryption.

Encrypted Traffic Analytics

Cisco, with its expertise in the network infrastructure market, conducted extensive research and has introduced an innovative and revolutionary technology, Encrypted Traffic Analytics. It helps illuminate the dark corners in encrypted traffic without any decryption by using new types of data elements or telemetry that are independent of protocol details.

Encrypted Traffic Analytics extracts four main data elements:

1. **Sequence of Packet Lengths and Times (SPLT):** SPLT conveys the length (number of bytes) of each packet’s application payload for the first several packets of a flow, along with the interarrival times of those packets.
2. **Initial Data Packet (IDP):** IDP is used to obtain packet data from the first packet of a flow. It allows extraction of interesting data such as an HTTP URL, DNS hostname and address, and other data elements.
3. **Byte distribution:** The byte distribution represents the probability that a specific byte value appears in the payload of a packet within a flow.
4. **TLS-specific features:** The TLS handshake is composed of several messages that contain interesting, unencrypted metadata used to extract data elements, such as cipher suite, TLS version, and the client’s public key length.

Using these data elements or enhanced telemetry, Encrypted Traffic Analytics can help detect malicious activity in encrypted traffic by applying advanced security analytics. At the same time, the integrity of the encrypted traffic is maintained because there is no need for bulk decryption.

Detect malware hidden in encrypted traffic

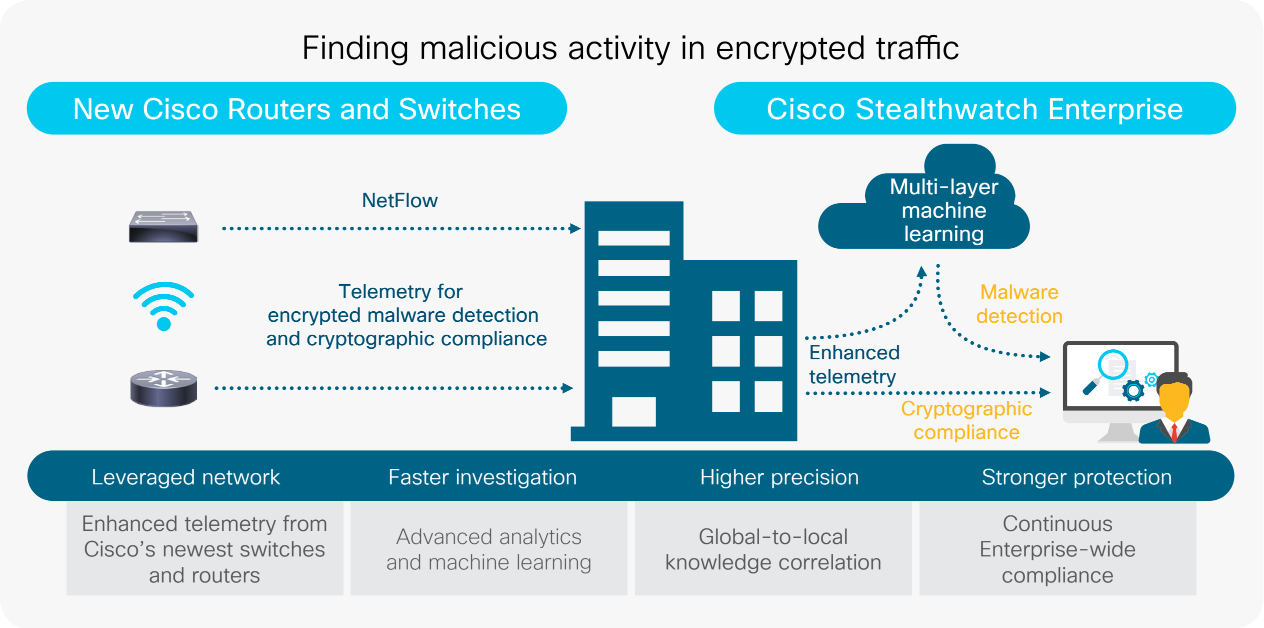
The enhanced network telemetry from the latest Cisco routers and switches is collected by Cisco Stealthwatch Enterprise, a comprehensive network visibility and security analytics product. It uses advanced entity modeling and multilayer machine learning, constantly identifying who is on the network and what they are doing, and can detect anomalous behavior in real time to identify threats. It also uses a global threat map to identify and correlate known global threats to the local environment. This considerably improves the fidelity of malware detection in encrypted traffic, and at the same time provides end-to-end confidentiality and maintains channel integrity because there is no decryption—an industry first.

Conclusion

Network and security teams must work together to gain visibility into all traffic across the enterprise. Cisco's intuitive network can help detect hidden security threats, even those lurking in encrypted traffic. To learn more about how Cisco security solutions can help you gain visibility into all areas of your network, visit https://www.cisco.com/go/eta.

Sources:

1. Electronic Frontier Foundation, February 2017, https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web.
2. Ponemon Institute, June 2017.
3. Blog: Detecting Encrypted malware traffic without decryption, June 2017.


Finding malicious activity in encrypted traffic
New Cisco Routers and Switches
Cisco Stealthwatch Enterprise
NetFlow
Telemetry for encrypted malware detection and cryptographic compliance
Multi-layer machine learning
Malware detection
Enhanced telemetry
Cryptographic compliance
Leveraged network
Faster investigation
Higher precision
Stronger protection
Enhanced telemetry from Cisco's newest switches and routers
Advanced analytics and machine learning
Global-to-local knowledge correlation
Continuous Enterprise-wide compliance

Achieve cryptographic compliance

While using encryption for data privacy and protection, an organization should be able to answer the questions, How much of the digital business uses strong encryption? What is the quality of that encryption? This information is very important to prevent attackers from getting into the encrypted stream in the first place. Today, the only way to ensure that encrypted traffic is policy compliant is to perform periodic audits to look for any TLS violations. However, this is not a great strategy due to the number of devices and the amount of traffic flowing through the business. Encrypted Traffic Analytics provides continuous monitoring without the cost and time overhead of decryption-based monitoring. Using the collected enhanced telemetry, Stealthwatch Enterprise provides the ability to view and search on parameters such as encryption key exchange, encryption algorithm, key length, TLS/SSL version, etc. to help ensure cryptographic compliance.