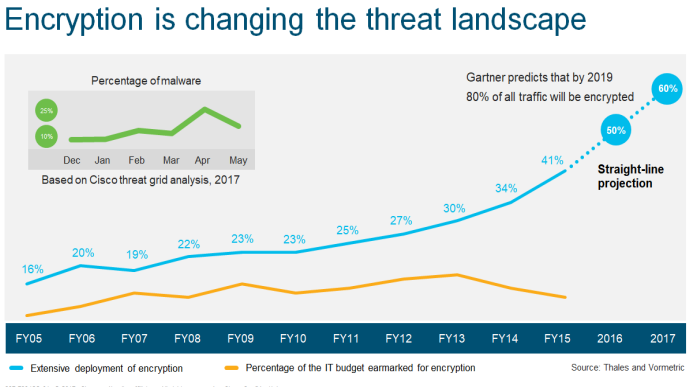
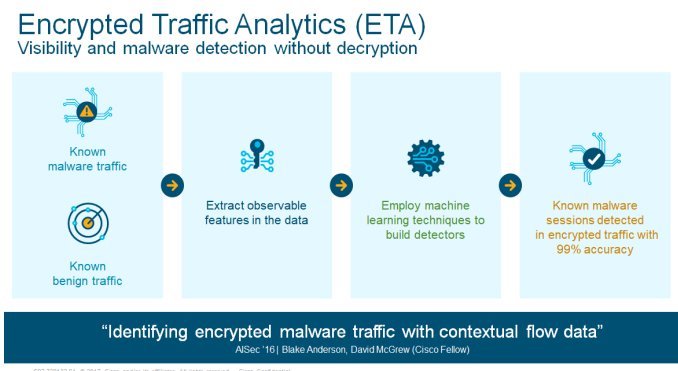
Cisco Security News Digest
10/18/2017 Issue 9

Lighting up the dark corners of your Network with Cisco Encrypted Traffic Analytics

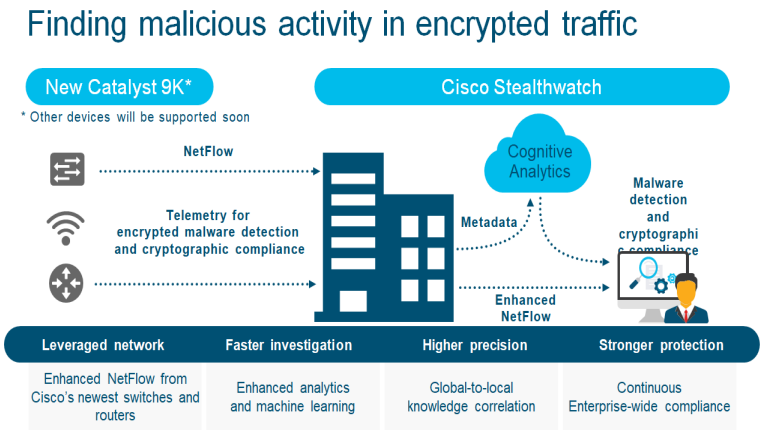
Network threats are getting smarter with sophisticated Advanced Malware Threats, Encrypted Malware, Zero- Day exploits and increased attack surface with IOT proliferation. Currently, global network traffic is increasingly encrypted using protocols such as HTTPS. The steady rise of using encryption is obviously good news for protecting application data from eavesdropping and for privacy but it's also getting misused by threat actors who are increasingly packaging malware content in encrypted channels, resulting in malware infections, data exfiltration activities etc. Decrypting data traffic for inspection purposes contributes to data privacy issues, scalability challenges and financial overhead.

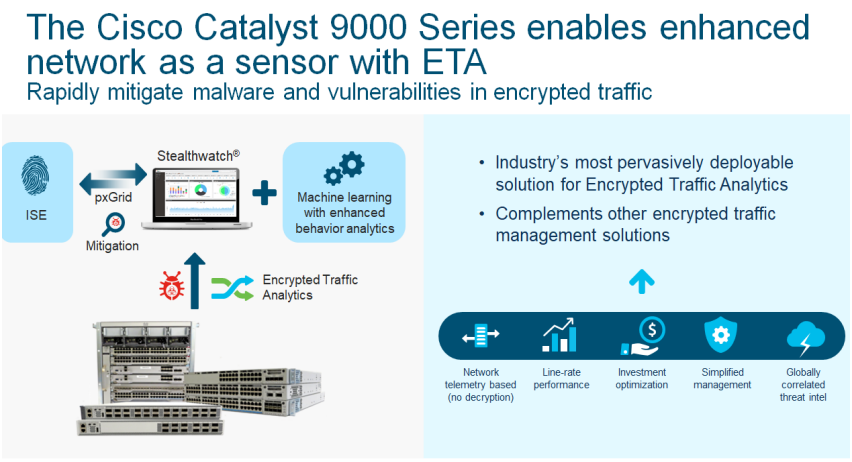




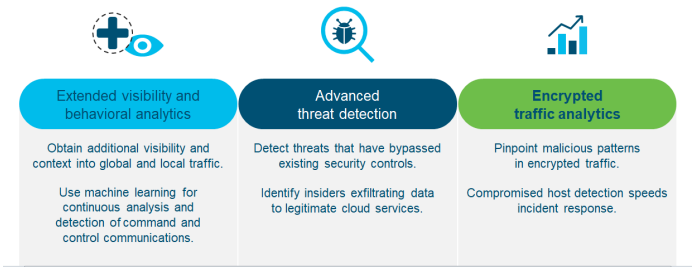
Cisco has found an unique way to watch out for the observables in data flow to indicate malicious content within encrypted data traffic. Cisco's recently launched Encrypted Traffic Analytics (ETA) offers a better balance point between privacy and security for important use cases such as identifying malware in encrypted traffic or finding out encryption compliance without the need to decrypt the traffic. Encrypted Traffic Analytics focuses on identifying malware by analyzing critical data features that are observable by passive monitoring without the need to decrypt traffic and inspect the actual content.

The enabler for ETA is the network itself. Network will generate new metadata which will provide visibility into encrypted traffic pattern. This metadata is an extension of the popular Netflow and is captured from the data headers in initial data packets of a traffic flow. The metadata is further ingested into Cisco Stealthwatch. Stealthwatch combines and correlates the information with Cognitive Analytics, a global multi-layer machine learning platform containing very broad behavioral information on Internets dark side, which will then analyze the patterns to identify security vulnerabilities hidden within encrypted data flow. This effectively allows resolution of network security incidents, mitigate malware and other vulnerabilities in encrypted traffic with higher precision.

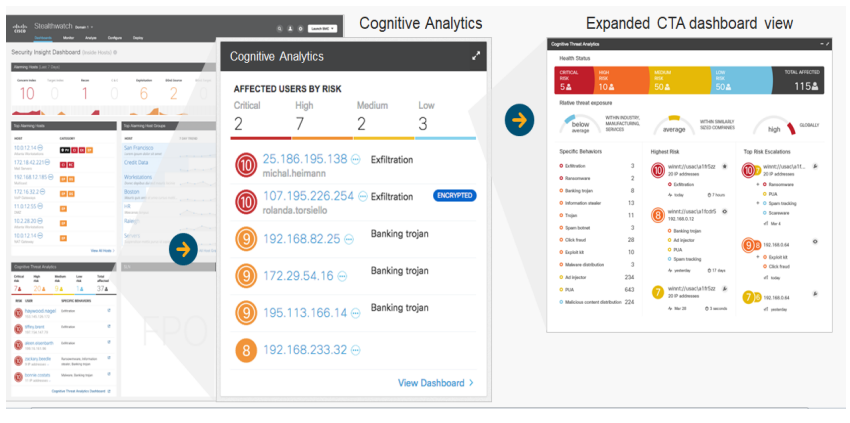




In a Digitally disrupted world, the "experience" has become a strategic imperative, whether it's for customers or employees. With the proliferation of IoT and IT managed and unmanaged user devices, it has become even more critical to put network as the first line of defense. New technologies such as ETA solves security challenges by better identifying and containing threats rapidly. Cisco's innovative ASIC chipset architecture, eg UADP 2.0 chipset in Catalyst 9300 switches enables technologies like ETA to use variety of switch analytics and still provide line-rate performance. Killing two birds with one stone– improving user experience in the network and enhanced threat visibility!



Below depicts a snapshot of the Security Insight dashboard on the Stealthwatch Management Console (SMC) with a view of affected users categorized by risk type . The threat is ranked on a scale of 1 to 10. It will also make determinations if the host identified has association to a larger threat campaign eg Wannacry. Admin can further deep dive into additional information on campaign, type of applications used by the host, communications paths internally or externally to quarantine and analysis.



ETA Video : http://cs.co/90098AaW9

ETA white paper: http://cs.co/90018Aao9

Catalyst 9000 series switches : http://cs.co/90058Aaov

For more information on Cisco Security solutions and products, please contact your **Cisco Account Manager**

Suggestions/comments on this newsletter contact Joby James at jobyj@cisco.com

Newsletter Archive: http://cs.co/SecurityNewsDigest