Whitepaper

Encrypted Traffic Analysis:

The Future of Network Analytics for CISOs

Networks are becoming increasingly encrypted, and the need for more visibility creates a significant challenge for security teams. Threat actors routinely use encryption to help hide data exfiltration and control with victim networks, making it extremely difficult for security teams to detect and prevent potential security threats. Therefore, the implementation of encrypted traffic analysis (ETA) is growing in importance to help CISOs gain visibility into encrypted traffic and ensure the security of their networks.

One of the biggest challenges facing organisations today is understanding their encryption landscape to expose risks and vulnerabilities. Without understanding the encryption used within their networks, businesses may be more vulnerable to cyber-attacks, resulting in financial loss, reputational damage, regulatory violation and associated fines.

The accepted approach for many years has been the static analysis of certificates on a server to provide a single view: verify the certificate's digital signature, check the certificate's expiration date, and validate that a trusted certificate authority issued the certificate. However, this needs to be revised in a world where most communications are now encrypted.

ETA involves analysing the traffic between endpoints in real-time to understand the negotiated encryption and any potential risks or vulnerabilities to maintain privacy and compliance. This provides the necessary information and clarity around the encryption actively negotiated for each session, allowing security teams to understand the encrypted communications.

The current best-practice encryption protocols are designed with privacy and zero interference, meaning the traditional decryption, inspection, and re-encryption approach will not work. Therefore, CISOs need to adopt a new strategy to gain visibility into encrypted traffic and ensure the security of their networks.

As privacy, regulation, and security have intertwined, businesses have had to prioritise privacy to comply with regulatory requirements and protect their sensitive information. Encryption is a critical tool that companies use to protect their communications. However, with the increasing prevalence of encrypted communications, businesses must ensure that their applications and network communications comply with regulatory standards. Failure to comply with these regulations can result in significant financial and reputational harm.

“ETA is now essential to a CISO’s strategy to understand encrypted network communications.”

ETA is now essential to a CISO’s strategy to understand encrypted network communications. This approach allows CISOs to identify suspicious behaviour and vulnerabilities in their networks, detect and prevent potential data breaches, and ensure compliance with regulatory standards. Additionally, it helps businesses mitigate the risks associated with third-party/supply chain risk. Enabling organisations to include a new data source in their risk management plan that provides real- time encrypted communications analytics to ensure contractual agreements and third-party providers are accountable for protecting sensitive information.

As the world moves towards a post-quantum era, CISOs must be prepared for the changes it will bring. Quantum computing has the potential to break current encryption methods, making it essential for businesses to understand their current encryption usage and allow the measured and managed transition to more secure encryption methods that are resistant to quantum computing. By preparing now for the post-quantum era, companies can ensure that their networks are secure and avoid potential risks and liabilities in the future.

As a CISO dealing with regulators and auditors, it is a requirement to be able to evidence the effectiveness of security controls; with encryption being so prevalent and with so many legacy solutions, coupled with the fact that encryption protocols may negotiate weak ciphers, it’s a huge challenge to establish the required high degree of assurance. CISOs must make tacit assumptions based on what is believed to be the case rather than what is necessarily the reality. Thus, CISOs may be left with nagging doubts, couched in terms of residual risk. The same may be true for auditors, given the limitations of traditional tooling. The gap in perception between the actual and the reality may go unnoticed until an auditor identifies a weakness through a configuration anomaly.

“Quantum computing has the potential to break current encryption methods, making it essential for businesses to understand their current encryption usage,”

“Encrypted traffic analysis is the future of network analytics.”

Encrypted traffic analysis is the future of network analytics. By implementing ETA, CISOs can ensure their networks are secure and gain visibility of their encrypted traffic, mitigating risks and vulnerabilities. The need for more visibility of encrypted traffic is a significant challenge for CISOs, and businesses must prioritise encrypted traffic analysis to protect their sensitive information from potential security threats. Companies can mitigate the risks associated with third-party/supply chain risk and prepare for the post-quantum world. By understanding their encryption usage, complying with privacy and regulatory standards, and preparing for the post-quantum era, businesses can ensure their networks are secure and avoid potential risks and liabilities.

About Colt

Colt aims to be the leader in enabling customers' digital transformation through agile and OnDemand, high bandwidth solutions The Colt IQ Network connects 900 data centres across Europe, Asia and North America's largest business hubs, with over 29,500 on net buildings and growing Colt has built its reputation on putting customers first Customers include data intensive organisations spanning over 212 cities in nearly 32 countries Colt is a recognised innovator and pioneer in Software Defined Networks (SDN) and Network Function Virtualisation (NFV) Privately owned, Colt is one of the most financially sound companies in its industry and able to provide the best customer experience at a competitive price For more information, please visit www.colt.net.

For more information visit www.colt.net

Tel: +44 (0)20 7863 5510
E-mail: sales@colt.net