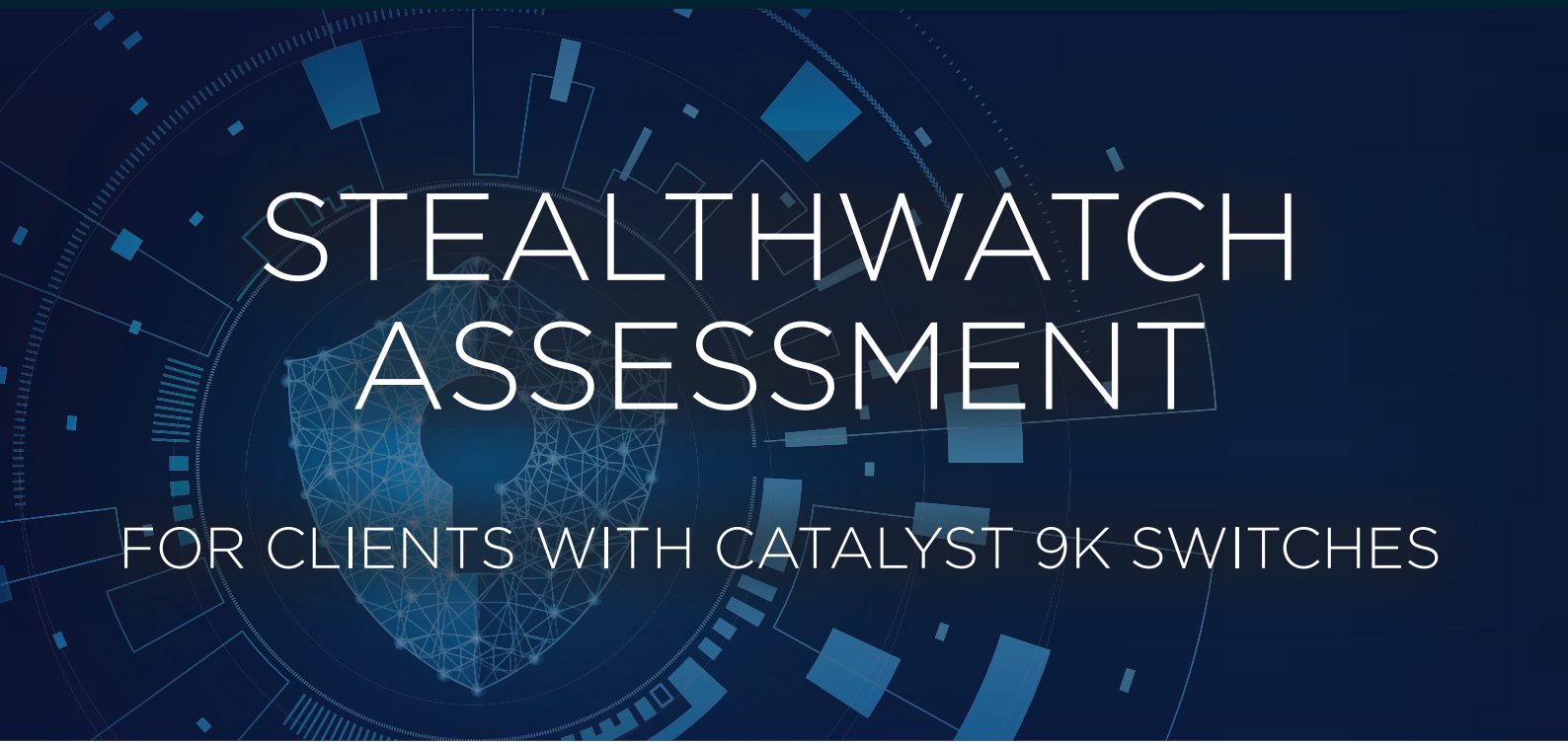
NATILIK



STEALTHWATCH ASSESSMENT

FOR CLIENTS WITH CATALYST 9K SWITCHES

CISCO STEALTHWATCH HARNESSES THE POWER OF NETWORK TELEMETRY TO PROVIDE ADVANCED NETWORK VISIBILITY, SECURITY INTELLIGENCE AND ANALYTICS. WITH INDUSTRY-LEADING MACHINE-LEARNING AND BEHAVIOURAL MODELLING, YOU CAN OUTSMART EMERGING THREATS IN YOUR DIGITAL BUSINESS.

This visibility allows a Stealthwatch database record to be maintained for every communication that traverses a network device. This aggregated data can be analysed in order to identify hosts with suspicious patterns of activity. Stealthwatch has different alarm categories using many different algorithms watching behaviour and identifying suspicious activity.

Stealthwatch leverage's NetFlow data from network devices throughout all areas of the network—access, distribution, core, data centre, and edge —providing a concise view of normal traffic patterns throughout and alerting when policies defining abnormal behaviour are matched. For more information visit www.natilik.com/sova-trial.

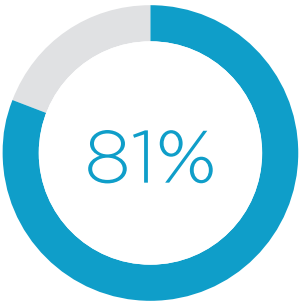
Encrypted Traffic Analytics (ETA) is available for clients using Cisco Catalyst 9K switches, when integrated with Stealthwatch Enterprise.

For more information, please contact your account manager or the Natilik team on 0203 597 8000.

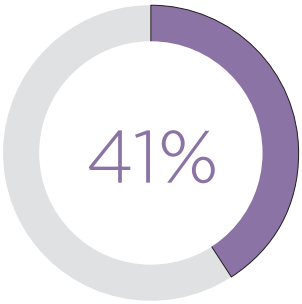
THE EVOLVING THREAT LANDSCAPE

As more businesses become digital, a significant number of services and applications are using encryption as the primary method of securing information. Mobile, cloud and web applications rely on well-implemented encryption mechanisms, using keys and certificates to ensure security and trust.

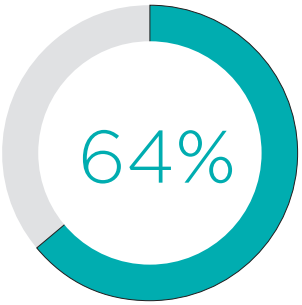
However, businesses are not the only ones to benefit from encryption. Threat actors have leveraged these same benefits to evade detection and to secure their malicious activities.



Organisation have been victims of a cyber attack



Attackers used encryption to evade detection



Cannot detect malicious content in encrypted traffic

ENCRYPTED TRAFFIC ANALYTICS

Detect malicious, encrypted traffic without the need for decrypting it.

Traditional threat inspection with bulk decryption, analysis and re-encryption is not always practical or feasible, for performance and resource reasons. Encrypted Traffic Analytics focuses on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements and supervised machine learning with cloud- based global visibility.

SECURITY VISIBILITY

- Gain insight into threats in encrypted traffic using network analytics. Obtain contextual threat intelligence with real-time analysis correlated with user and device information.

CRYPTOGRAPHIC ASSESSMENT

- Ensure enterprise compliance with cryptographic protocols and visibility into and knowledge of what is being encrypted and what is not being encrypted on your network

FASTER TIME TO RESPONSE

- Quickly contain infected devices and users.

TIME AND COST SAVINGS

- Use the network as the foundation for the security posture, capitalising on security investments in the network.