SOLUTION BRIEF

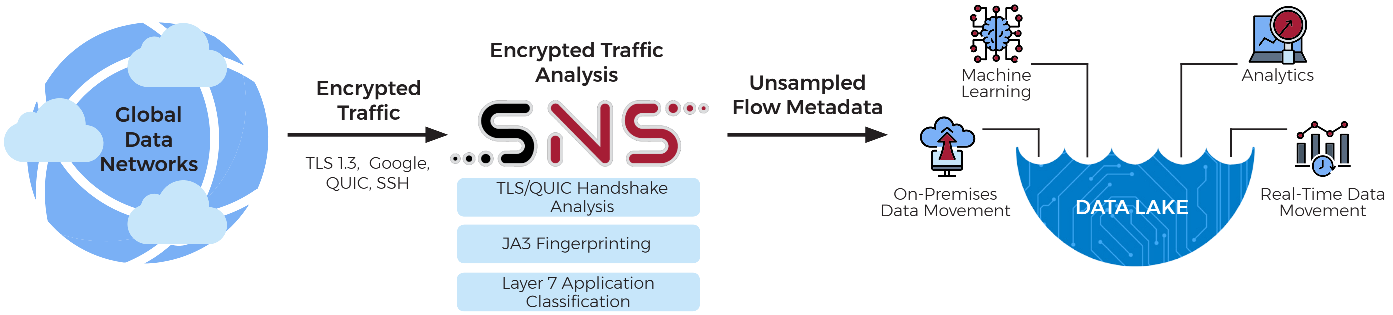
NetQuest
Monitoring Access Solutions

Encrypted Traffic Analysis for Telco-Scale Threat Hunting

The cyber threat landscape is changing every day with innovative and malicious attack techniques constantly emerging. While internet traffic is ballooning with new devices, applications and services, encryptions offers cybercriminals a safety blanket to hide behind.

We are quickly moving toward an Internet where all in-transit data is encrypted. This sounds great for privacy and confidentiality, but threat hunting teams are facing significant blind spots. With adoption of stronger encryption algorithms such as TLS 1.3 and Google QUIC, decryption is no longer a plausible solution yet visibility is still essential to defending networks from crippling attacks.

How NetQuest Streaming Network Sensors Enable Visibility into Encrypted Traffic?


Global Data Networks
Encrypted Traffic
TLS 1.3, Google, QUIC, SSH
Encrypted Traffic Analysis
SNS
TLS/QUIC Handshake Analysis
JA3 Fingerprinting
Layer 7 Application Classification
Unsampled Flow Metadata
Machine Learning
On-Premises Data Movement
DATA LAKE
Analytics
Real-Time Data Movement

NetQuest Streaming Network Sensors empower your security teams by extracting intelligence from encrypted traffic and providing essential visibility for cyber threat hunters. And this is done without decryption and maintaining user privacy.

Our technology leverages machine learning and behavioral-based techniques to statefully analyze encrypted traffic flows and identify Layer 7 applications. When combined with encryption protocol information (TLS, QUIC, SSH), NetQuest's sensors can report indicators of compromise to traditional Network Detection and Response (NDR) platforms to spot anomalous activity and potential attacks.

EXAMPLES OF DETECTED THREATS

- Malware-infected devices and end-users diagnosed by anomalies in TLS parameters
- Malware C&C center communication revealed by JA3 fingerprinting
- Man-in-the-middle attacks manifested by unusual or illegitimate certificates
- Suspicious packet size indicating data ex-filtration

How NetQuest Classifies Traffic and Detects Anomalies

NetQuest leverages embedded analytics in combination with machine learning techniques to provide high-quality encrypted traffic intelligence. This includes analysis of TLS 1.3 and QUIC handshakes to calculate unique fingerprints that can be used to track indicators of compromise.

KEY BENEFITS

- **Flow Metadata Generation** exports standards-based 1:1 unsampled IPFIX flow data, scaling from a single 10G link to multiple 100G links.
- **Application Classification** recognizes over 3,600 protocols and applications including the classification of encrypted and evasive traffic.
- **Encrypted traffic analysis** identifies powerful Indicators of Compromise (IoC) based on network protocol and traffic heuristic signatures
- **Protocol-specific metadata** helps threat hunting tools recognize anomalous activity by leveraging information carried within communications protocols such as TLS, QUIC, SSH, DNS, HTTP and BGP

CLASSIFYING ENCRYPTED TRAFFIC

The Streaming Network Sensors use the following techniques to classify encrypted traffic.

Handshake Analysis

Analysis of metadata preceding the encrypted packets in handshake messages protocols such as TLS and QUIC

Binary Pattern Analysis

Identifying & matching binary patterns against known applications and services.

Statistical Analysis

Custom models for analyzing characteristics of packets and flows

Behavioral Analysis

Encrypted session behavior analysis compared to the standard protocol behaviors.

Machine Learning

Machine learning algorithms to categorize traffic flows.

IP Address Database

Extensive continuously updated database matching known IP address/application pairs

Experience 100% Visibility with NetQuest's Streaming Network Sensors.

Request Access to the NQ Cyber Lab!