Six Reasons for Encrypted Traffic Visibility

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide end-to-end security over a communication network. The SSL/TLS protocol aims primarily to provide authentication, privacy, and data integrity between two or more communicating computer applications. The SSL/TLS protocols is widespread and used in applications such as web browsing, email, messaging, and voice over IP (VoIP) and many other application services. Encrypted traffic is pervasive. According to a Google report from April 2020, the use of HTTPS is increasing, and it is currently around 80%.

The reasons why enterprises implement decryption for security visibility include:

1 You Can't Manage What You Can't See

To evade enterprise security monitoring, bad actors encrypt their attacks. Without the ability to decrypt for inspection, security tools are left to pass traffic uninspected, or to potentially block legitimate traffic.

2 Fail to Detect of Encrypted Malware Traffic

It is a daunting task to detect malware traffic in clear text as attackers come up with new types of attacks and malicious behavior. Encryption makes malware traffic detection even harder.

3 Unable to Prevent Data Loss, Exfiltration

Encrypted traffic cannot be inspected by Data Loss Prevention (DLP) appliances. Stop data exfiltration and know what has been taken in case of network breach, to implement mitigating actions for regulatory compliance.

4 Incapacitated IPS, IDS and WAF Tools Are Blind, Cannot Inspect Encrypted Traffic

IPS, IDS, WAF, and other security tools cannot protect what they can't see. Maximize your investment in security monitoring tools to protect your network and assets.

5 Inhibited Network Forensic Analysis and Sandboxing

Network forensics and sandboxing tools cannot see inside the encrypted traffic causing longer dwell times and increased cyberthreats.

6 Gaps in Compliance

Don't let compliance gaps remain undetected. SSL/TLS decryption assists with cryptographic compliance, by revealing TLS policy violations, uncovering cipher suite vulnerabilities, or detecting weak ciphers that might be in use.

About NETSCOUT nGenius Decryption Appliance

NETSCOUT® nGenius® Decryption Appliance enables visibility into encrypted traffic for pervasive, high-performance security monitoring with policy management for privacy. nGenius Decryption Appliance decrypts traffic flows from the network to the security systems and monitoring tools. Our customers use nGenius Decryption Appliance to enhance both their service assurance platform and cybersecurity deployments so that they can gain visibility into encrypted traffic, increase security monitoring tool performance, and reduce total cost of security monitoring tools.

NETSCOUT®

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us