SOLUTION BRIEF

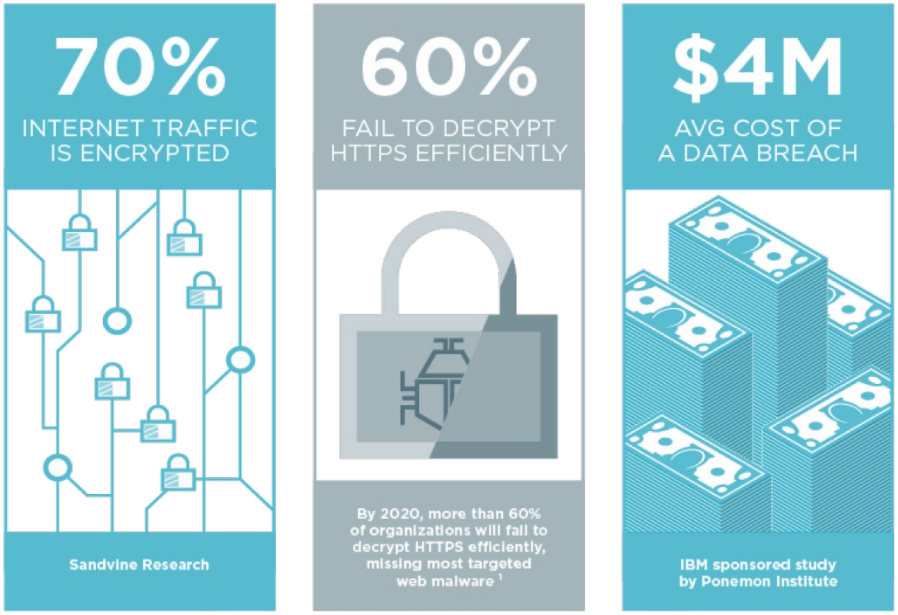
SecureStack — Optimized Handling of Secure Traffic

The Real Deal on Secure Traffic

With personal information, passwords, and other sensitive data traversing the internet, keeping your network and traffic secure is a top priority for both you and your customers. Encrypted traffic is growing and so is the use of encrypted malware to retrieve personal data. To combat malicious activity, companies must deploy robust security systems capable of handling secure traffic.

A Secure Network with Fewer Security Tools

The SecureStack feature set from Ixia adds another layer of security to your Vision ONE system. SecureStack capabilities include both active and passive SSL decryption in addition to malicious activity detection and PCI-compliant data masking. Let SecureStack do the dirty work so that your security tools can focus on what they do best.


70%
INTERNET TRAFFIC IS ENCRYPTED
60%
FAIL TO DECRYPT HTTPS EFFICIENTLY
$4M
AVG COST OF A DATA BREACH

Sandvine Research

By 2020, more than 60% of organizations will fail to decrypt HTTPS efficiently, missing most targeted web malware[1]

IBM sponsored study by Ponemon Institute

[1] Gartner, Predicts 2017: Network and Gateway Security, 13 December 2016

Highlights

Internet use is increasing and so is the need to keep data secure.

SecureStack offers a security solution without a dedicated security tool including:

- Active and passive SSL decryption with upcoming support of TLS 1.3 and ephemeral key cryptography.
- Threat insights adds another layer of detection recognizing malicious activity, malware, and more.
- Data masking plus help you meet regulatory compliance standards by masking credit card numbers, SSNs, and more.

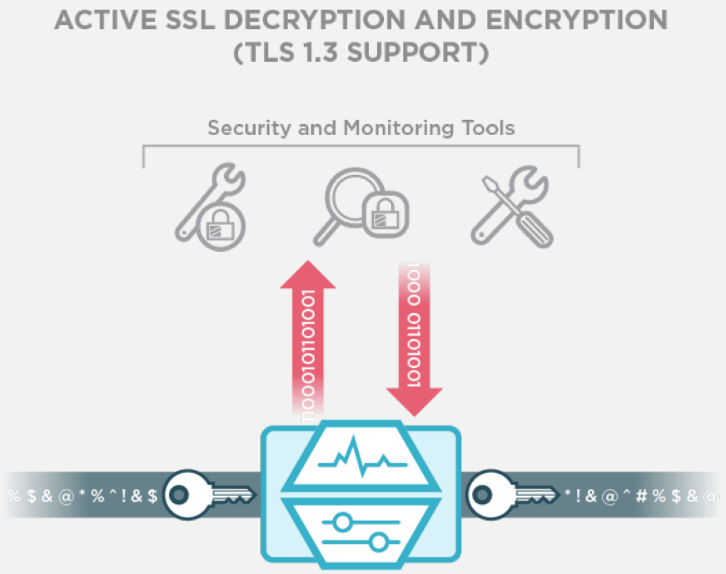
SecureStack Capabilities

Active and passive SSL

With ephemeral key cryptography and future support of TLS 1.3 standards, Keysight's SecureStack provides visibility into the encrypted traffic on your network. A dedicated cryptographic processor offers you SSL decryption with built-in policy management, upcoming URL categorization, and real-time insight through analytics reporting.

Ixia's SSL decryption allows you to:

- Decrypt once/inspect many and scale monitoring infrastructure
- Deploy inline, out-of-band (OOB), and simultaneous inline/OOB configurations
- See into both outbound and inbound traffic to inspect downloads and detect server attacks
- Decrypt without impact to NetFlow generation, data masking, PCAP, and application forwarding

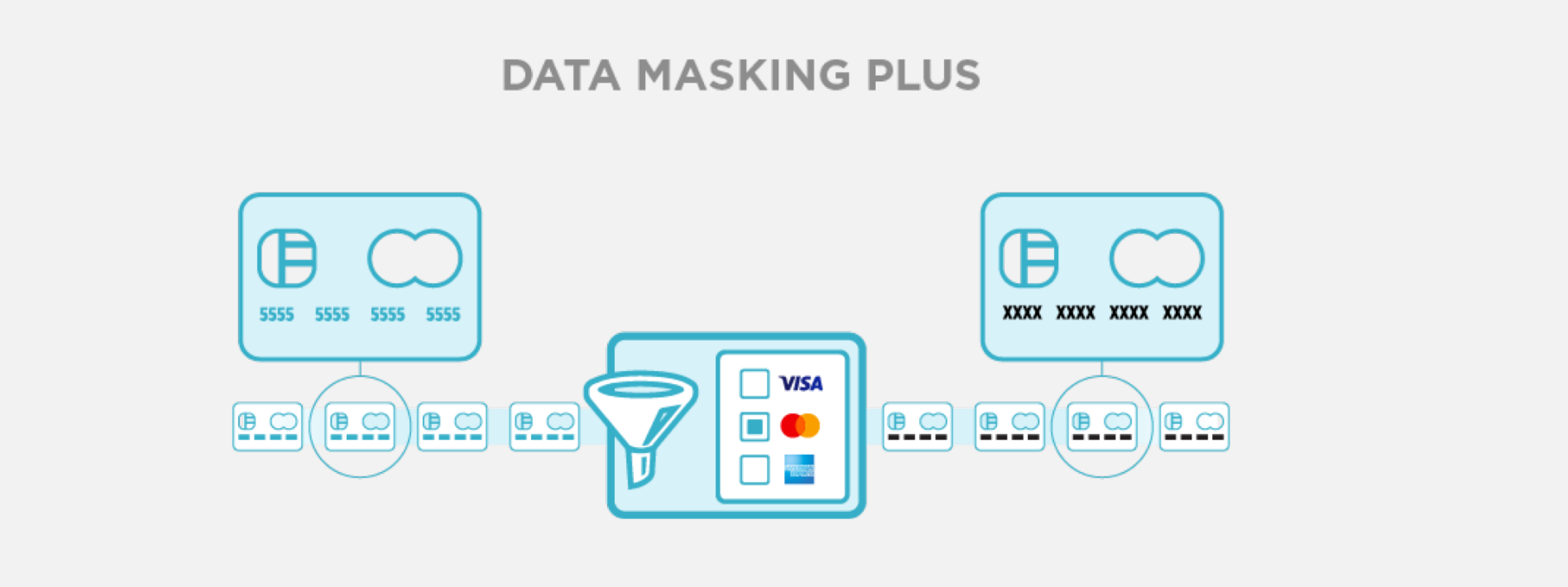

ACTIVE SSL DECRYPTION AND ENCRYPTION
(TLS 1.3 SUPPORT)
Security and Monitoring Tools

Data Masking Plus

Keysight's SecureStack helps you meet compliance regulations by securely masking sensitive data on your network. Data masking plus combines traditional data masking a configurable offset that masks a specific place in a packet- with enhanced features to increase your protection.

Ixia's data masking plus allows you to:

- Use pre-defined patterns to mask major credit cards, social security numbers, phone numbers, taxpayer IDs, and email addresses
- Reduce false positives with built-in credit card number validation using the Luhn algorithm
- Achieve Payment Card Industry Data Security Standard (PCI-DSS), HIPAA, and other regulatory compliance

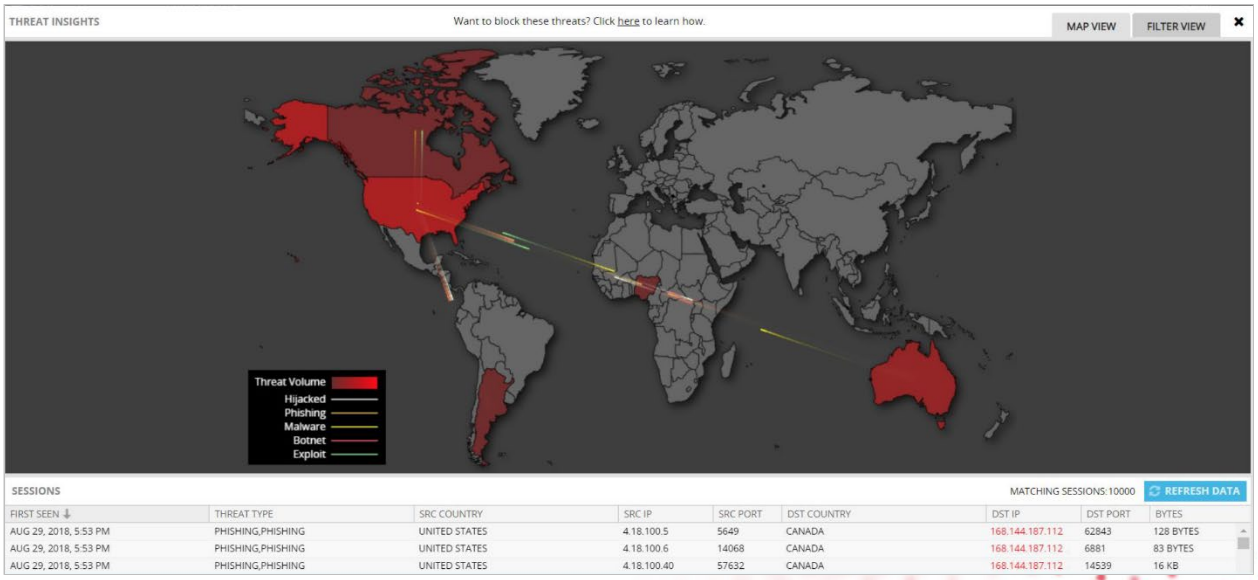


Threat Insights

Proactively prevent cyberattacks with SecureStack's added layer of threat detection. Keysight's Application and Threat Intelligence Research Center supports threat insights with a constant threat intelligence feed. Your threat intelligence database is kept up-to-date with changing geolocation data, known bad IP addresses, and known bad traffic.

Keysight's threat insights allow you to:

- Recognize malware connections, botnets, exploits, hijacked IPs, and phishing activity
- Send threat information automatically via NetFlow to existing security appliances
- Detect IoT attacks
- Tag suspicious or rogue applications and monitor them for unusual activity
- Track traffic to or from unauthorized geographies
- Track questionable file transfers and brute-force attacks



SESSIONS

MATCHING SESSIONS: 10000

FIRST SEEN ↓	THREAT TYPE	SRC COUNTRY	SRC IP	SRC PORT	DST COUNTRY	DST IP	DST PORT	BYTES
AUG 29, 2018, 5:53 PM	PHISHING,PHISHING	UNITED STATES	4.18.100.5	5649	CANADA	168.144.187.112	62843	128 BYTES
AUG 29, 2018, 5:53 PM	PHISHING,PHISHING	UNITED STATES	4.18.100.6	14068	CANADA	168.144.187.112	6881	83 BYTES
AUG 29, 2018, 5:53 PM	PHISHING,PHISHING	UNITED STATES	4.18.100.40	57632	CANADA	168.144.187.112	14539	16 KB

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at:
www.keysight.com/find/contactus

This information is subject to change without notice. © Keysight Technologies, 2018 - 2022, Published in USA, January 19, 2022, 7019-0197.EN