Symantec. | openreality
Making application performance great

Encrypted Traffic - What You Can’t See CAN Hurt You …

Removing the SSL/TLS Blind Spot

James Stevenson

Sales Specialist, Advanced Threat Protection

AGENDA

- THE GROWTH OF SSL/TLS TRAFFIC
- THE EMERGENCE OF ENCRYPTED THREATS
- VARIOUS SSL INSPECTION STRATEGIES AVAILABLE TODAY TO MITIGATE THIS RISK

Who are Open Reality?

10 Years

We are proud to be a Blue Coat Premier Partner and this year marks our 10th Anniversary of working together!

We specialise in:

Network Performance & Optimisation

- PacketShaper
- MACH5

Security

- ProxySG
- SSL Visibility Appliance

Our Guest Speaker

James Stevenson

Sales Specialist, Advanced Threat Protection

Blue Coat + Symantec

3 Questions to Consider Today

- WHAT PERCENTAGE OF YOUR NETWORK TRAFFIC IS ENCRYPTED TODAY?

- WHAT IS YOUR CURRENT SSL INSPECTION STRATEGY FOR INBOUND/OUTBOUND?

- CAN YOU INCREASE THE EFFECTIVENESS/ROI OF EXISITING SECURITY TOOLS?

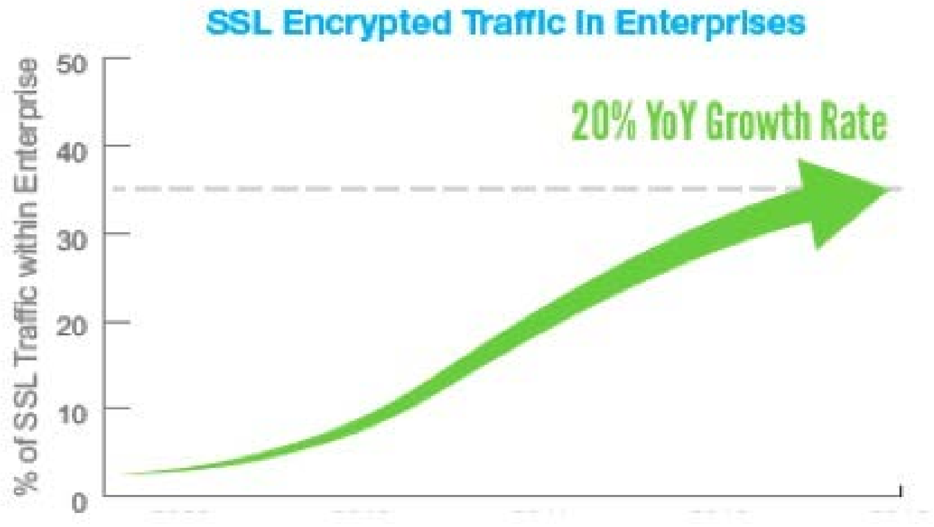
Encrypted Traffic Is Growing

- End-user privacy demands
- Mitigating risk of data loss/theft
- Legal & Regulatory Compliance
- Concerns over surveillance

amazon web services · Gmail by Google · Office 365 · ORACLE · salesforce.com Success On Demand. · SAP · f

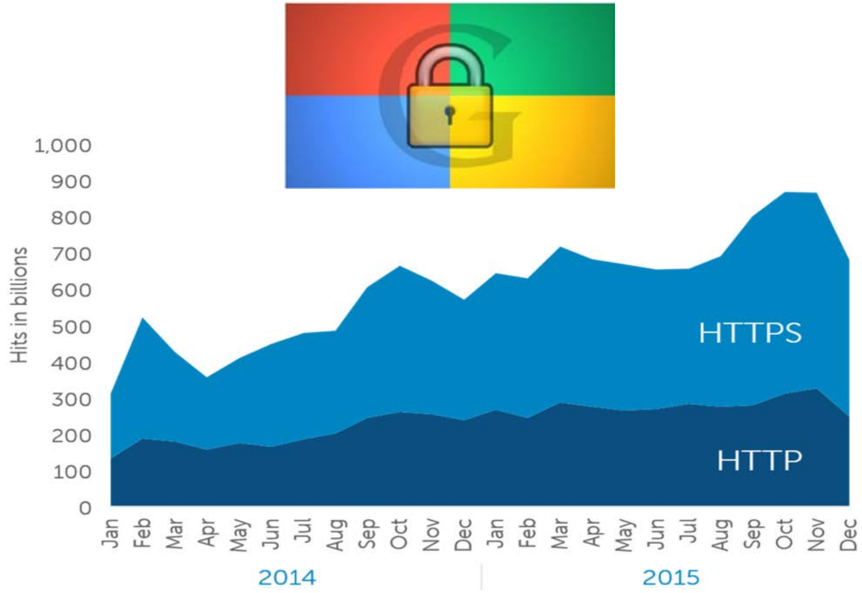
SSL is estimated at 50% of network traffic and growing 20% annually*.

- >70+% in some industries. (e.g. Gov’t, finance, healthcare)



*Source: Gartner

Google Starts Giving a Ranking Boost to Secure HTTPS/SSL Sites.



Known malware families also now leveraging SSL/TLS

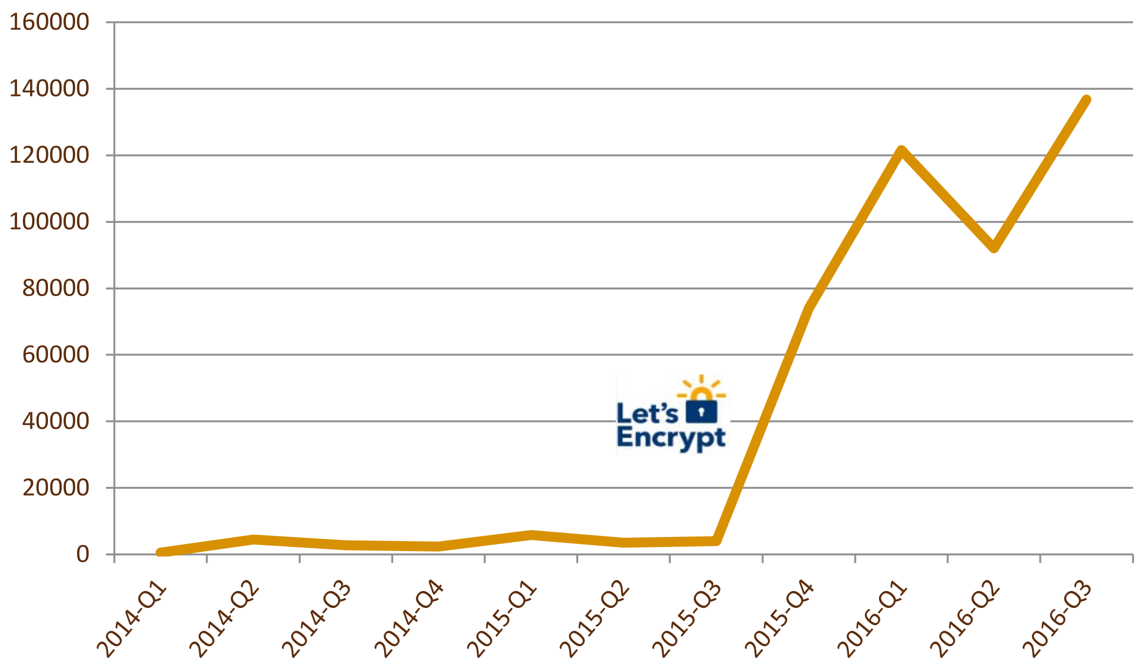
SSL based malware spiked dramatically towards the end of 2015 * †

- Dridex
- KINS
- Shylock
- URLzone
- TorrentLocker
- CryptoWall
- Upatre
- Spambot
- Retefe
- TeslaCrypt
- CryptoLocker
- Bebloh
- Gootkit
- Geodo
- Tinba
- Gozi
- VMZeus
- Redyms
- Qadars
- Vawtrack
- Emotet

* *Samples observed on VirusTotal*

† *SSL Blacklist can be viewed at https://sslbl.abuse.ch*

MALWARE SAMPLES USING SSL (2014-2016)



50% of all Malware will use SSL by 2017*.

*Source: Gartner

Command & Control Servers now leveraging SSL/TLS

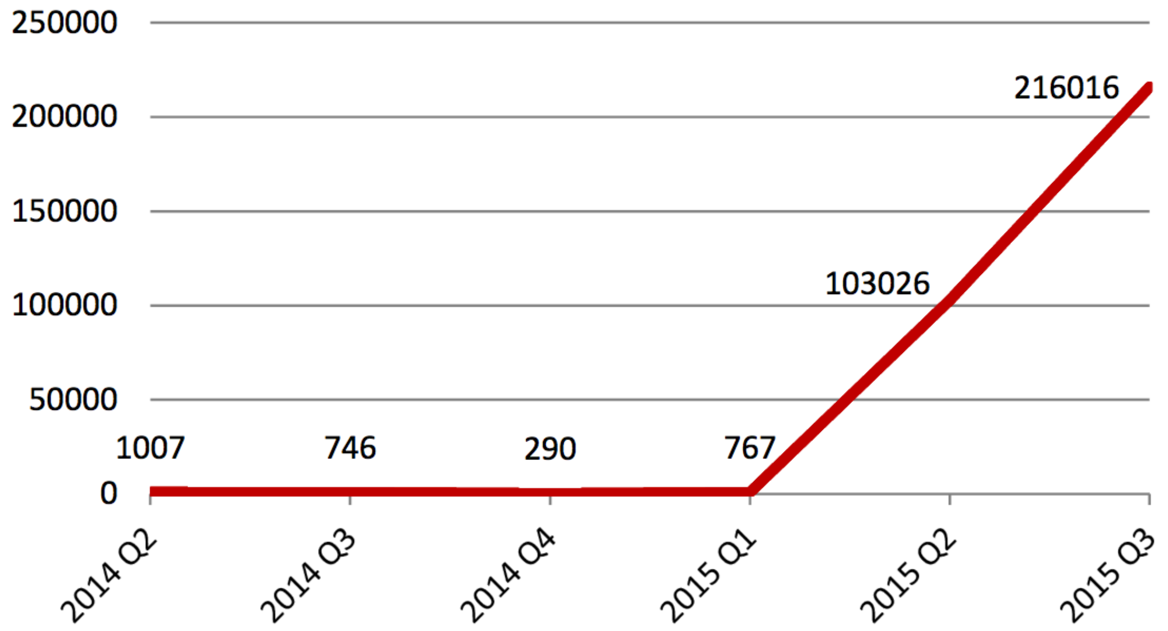
Command & Control (C2) servers using SSL spiked dramatically towards the end of 2015 *†

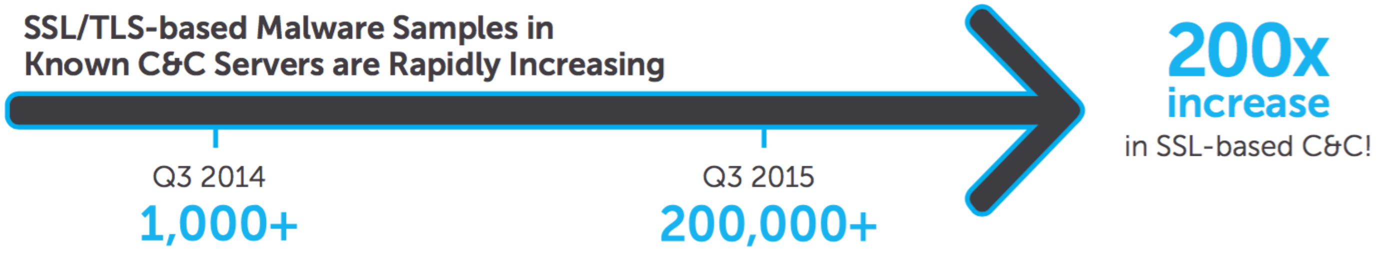
Encryption used to evade detection and conceal data exfiltration

50% of all Malware will use SSL by 2017*.

*Source: Gartner

KNOWN SSL C2 SERVERS




SSL/TLS-based Malware Samples in Known C&C Servers are Rapidly Increasing

Q3 2014
1,000+

Q3 2015
200,000+

200x increase
in SSL-based C&C!

** Samples observed on VirusTotal*

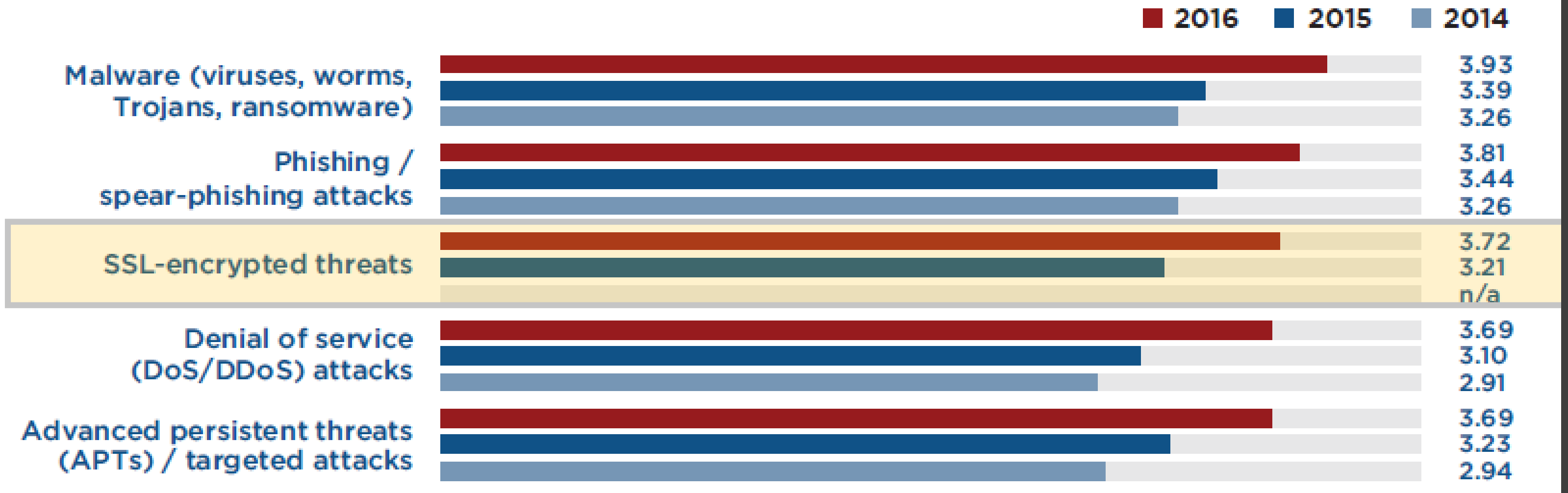
† SSL Blacklist can be viewed at [*https://sslbl.abuse.ch*](https://sslbl.abuse.ch)

SSL/TLS Threats are now a board level concern

- Malware
- Phishing
- **SSL-Encrypted Threats**
- DoS / DDoS
- APTs

TYPES OF CYBERTHREATS

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization. (n=986)



Source: CyberEdge CDR 2016 Report

Current Security Solutions Are Blind to SSL

DLP

IDS

ANTI-MALWARE / SANDBOXES

NETWORK FORENSICS

NETWORK & APP MONITORING

Limited-to-no visibility into SSL/TLS

NGFW

IPS

*Sources: NSS Labs, Gartner

Suffer ~ 80% performance degradation once SSL inspection is “turned on”

Degrades investment in security infrastructure

Limited cypher/protocol support

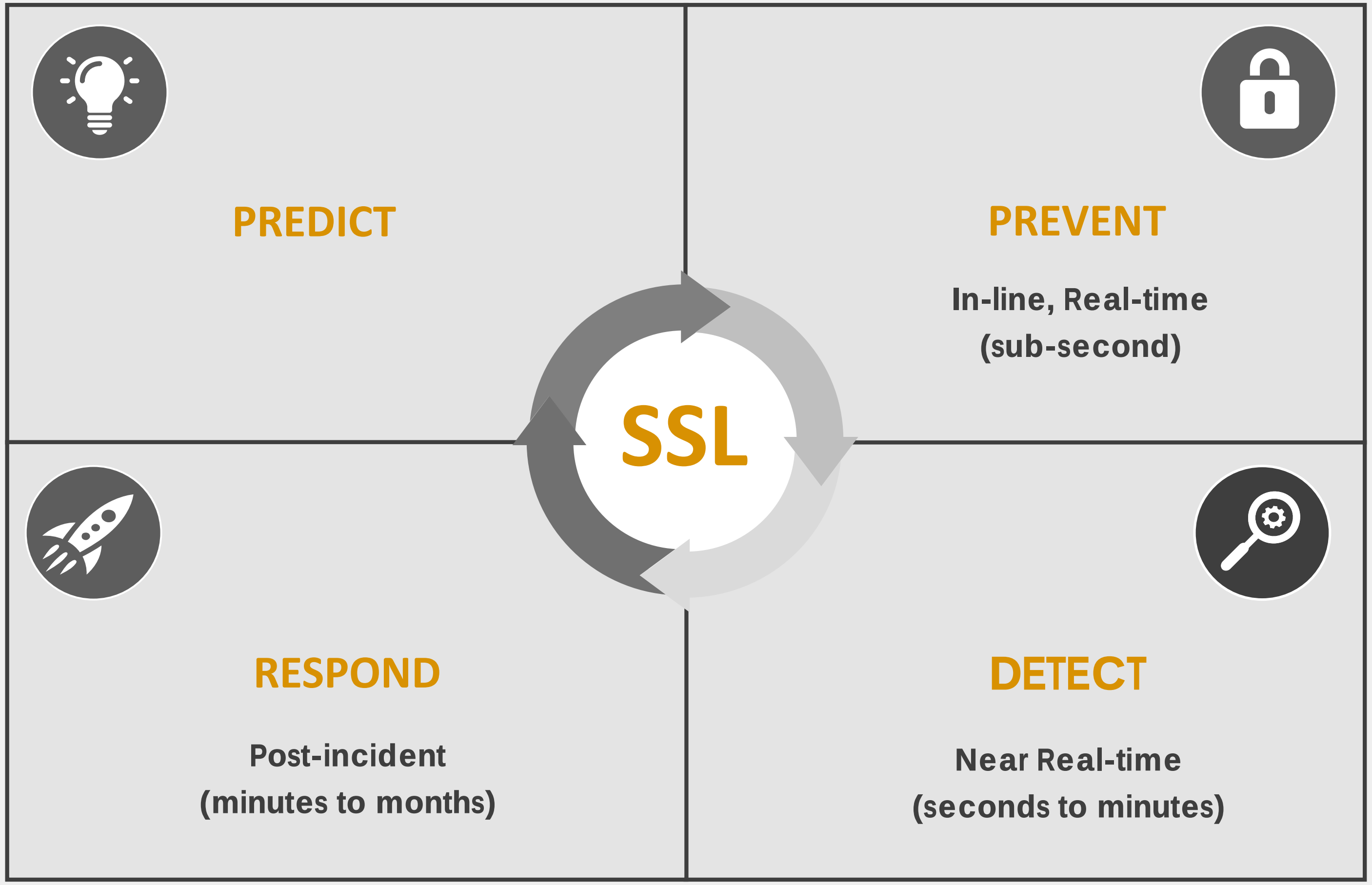
Why SSL visibility is Relevant in today's threat landscape
Strategic Shift to Rapid Detection and Response Projects

"The failure to stop targeted attacks requires security organizations to rebalance investments in all four stages"

"By 2020, 60% of security budgets will be allocated to rapid detection and response" (10% in 2014)

SSL visibility is the foundation to these projects

- Gartner, "Security Leaders Must Address Threats from Rising SSL Traffic" (December 2013)



Source: Gartner (November 2015)

Gartner®

Typical Projects at Risk without SSL/TLS Visibility

1. **Intrusion Detection/Prevention Systems (IDS/ IPS)**
2. **Data Loss Protection (DLP)**
3. **Secure Web Gateways**
4. **Anti-Malware Sandboxes**
5. **Mail Gateways**
6. **Security Analytics (Full Packet Capture)**

"41 percent of companies who were victims of a cyberattack said that the attacker used SSL encryption to hide their activities and to sneak data out of organizations"

Uncovering hidden threats within encrypted traffic, Ponemon Study 2016

Security Industry Confirmation

An ETM Strategy is Necessary

“Encrypted traffic management (ETM) has been given an increasingly important role in safeguarding infrastructures. Nevertheless, companies need to find ETM solutions capable of satisfying their needs with regard to data privacy, compatibility, security, performance, scalability and cost effectiveness, all in equal measure.”

–Fraunhofer Institute - FKIE, “Encrypted Traffic Management” (January 2016)

What You Don’t See Can Kill You

“The sooner you put an encrypted traffic management strategy and supporting network security architecture in place, the more likely you are to catch your next attacker in the act.”

—Securosis, “Security and Privacy on the Encrypted Network” (Mar 2015)

SSL Inspection is a Security Best Practice

“Implement a Secure Sockets Layer (SSL) inspection capability to inspect both ingress and egress encrypted network traffic for potential malicious activity”.

—Alert TA14-353A: Targeted Destructive Malware (Dec 2014)

Security Industry Confirmation

Enabling SSL Decryption on a Multifunction Device Isn't Sufficient

"Security leaders face limited technology choices for enterprise network traffic decryption, and these solutions often induce high costs and poor user experience."

- Gartner, "Security Leaders Must Address Threats from Rising SSL Traffic" (December 2013)

SSL Traffic Causes Wasted Network Security Investments

"Encrypted traffic is a huge blind spot for enterprise visibility. The importance of privacy will ensure this trend continues, but investments in network security are largely being wasted when encrypted traffic isn't being inspected."

- 451 Research (October 2015)

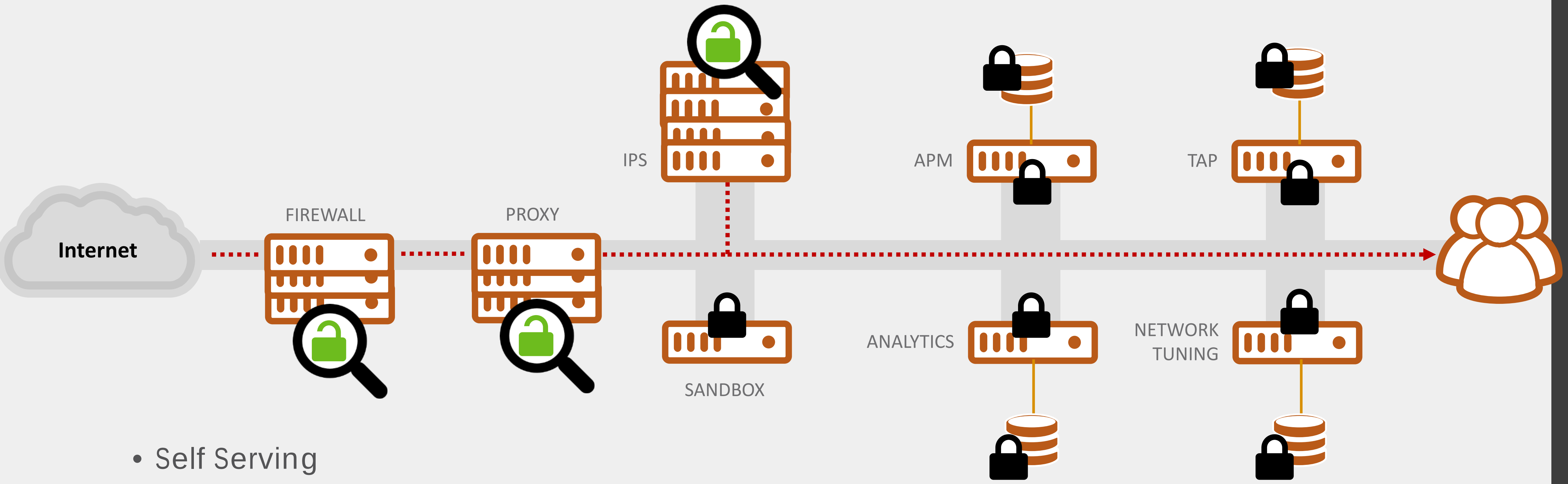
SSL Decryption Significantly Slows NGFW Performance

"The average performance loss across 7 NGFWs when SSL inspection is enabled is 81%..."

– NSS Labs, SSL Performance Problems Analyst Brief (2013)

Eliminating the SSL/Encryption Blind Spot

Enabling SSL Decryption On Each Appliance

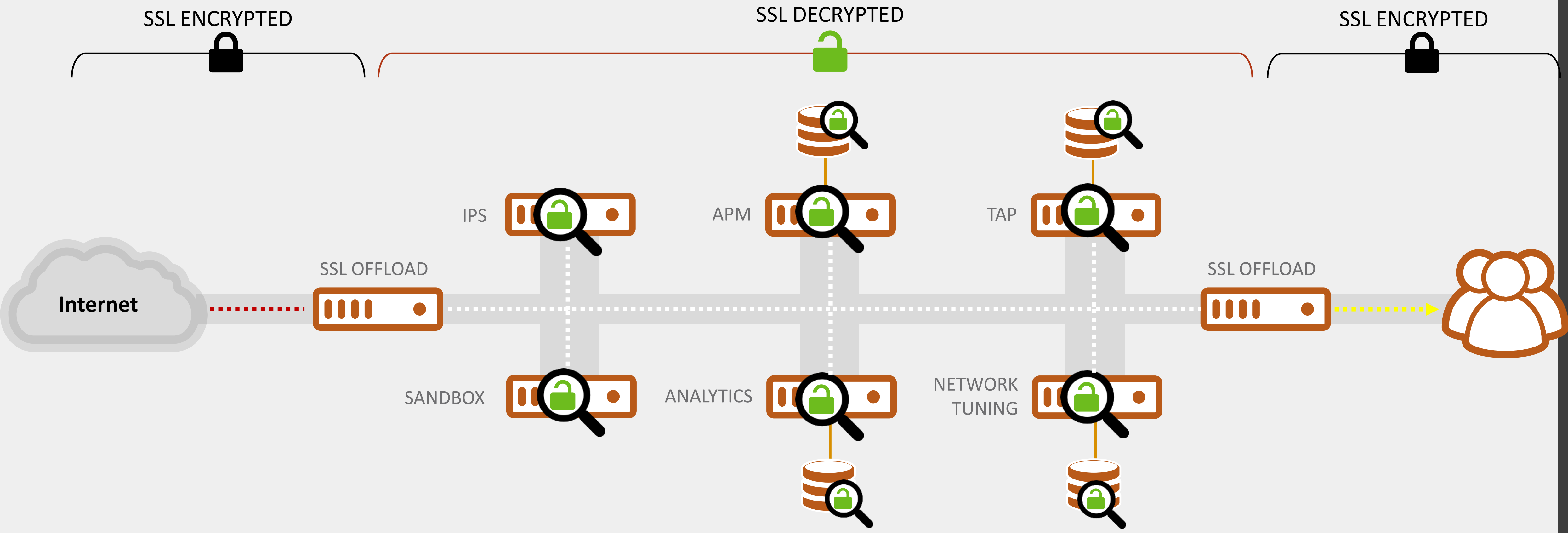


- Self Serving
- Costly and used tactically due to significant performance degradation – Up to 80%*
- Does not support latest cipher suites and key exchanges – Typically 10 vs 70+
- Only specific ports/protocols. E.g 443/HTTPS, not SMTPS, FTPS, IMAPS etc..

*Source: NSS Labs

Eliminating the SSL/Encryption Blind Spot

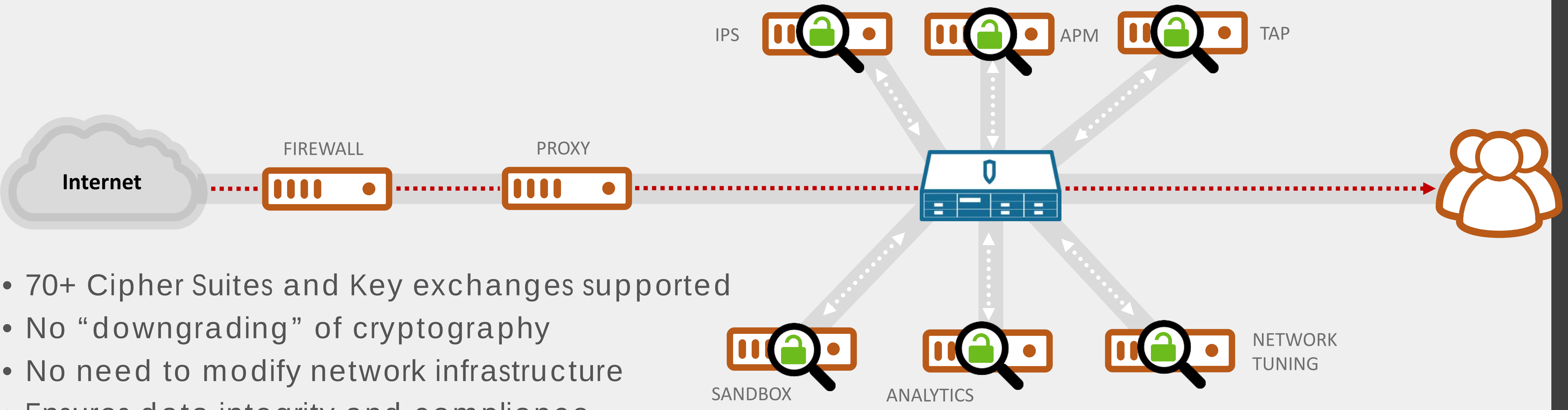
SSL with Non-Compliant Decryption Zones



- Typically requires complex scripting and network configuration = operational complexity
- Only supports a handful of cipher suites = need to “downgrade” cryptography level
- Cannot ensure data integrity and compliance. Risk of modification before re-encryption

Eliminating the SSL/Encryption Blind Spot

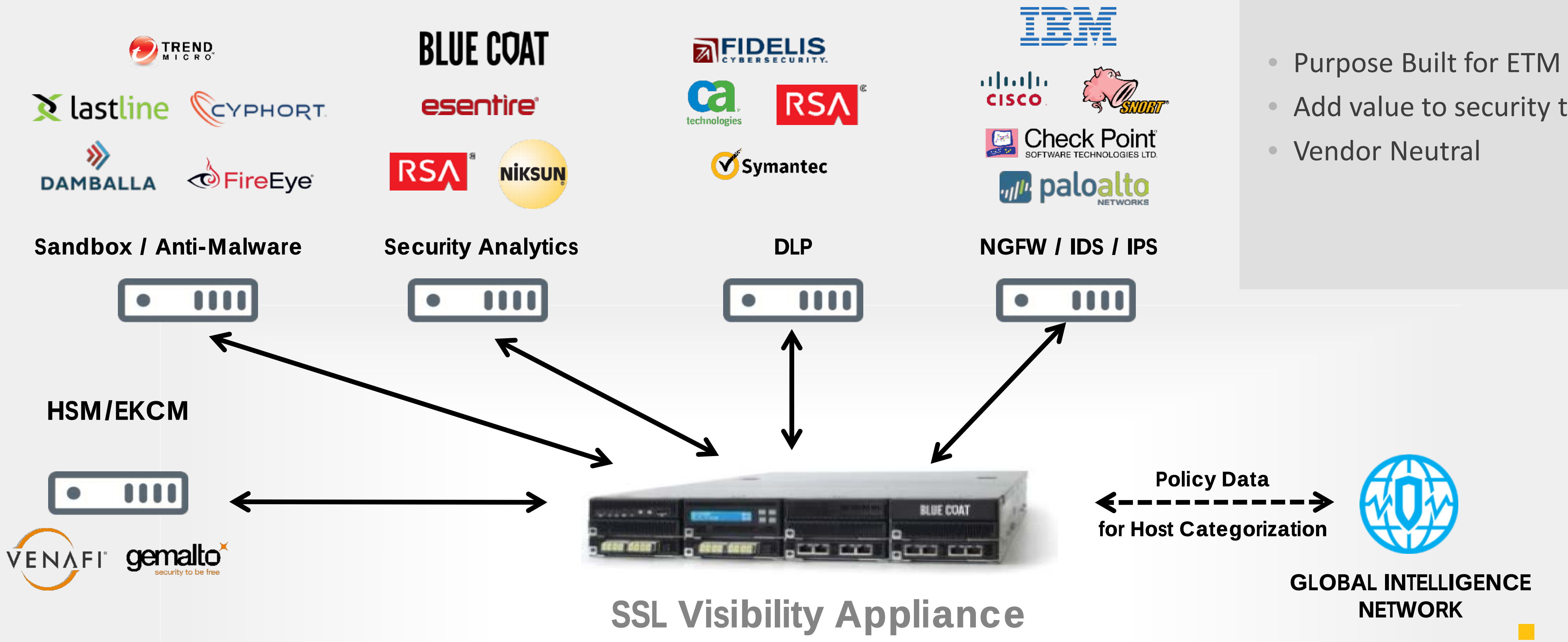
Compliant and Secure Approach to SSL Decryption



- 70+ Cipher Suites and Key exchanges supported
- No “downgrading” of cryptography
- No need to modify network infrastructure
- Ensures data integrity and compliance
- Built specifically for SSL, not a side feature of another product
- Not just HTTPS visibility. Any SSL traffic over any port. SMTPS, FTPS, POP3S, IMAPS etc..

ENHANCE EXISTING SECURITY TOOLS

DECRYPT ONCE FEED MANY



Sandbox / Anti-Malware

Security Analytics

DLP

NGFW / IDS / IPS

HSM/EKCM

SSL Visibility Appliance

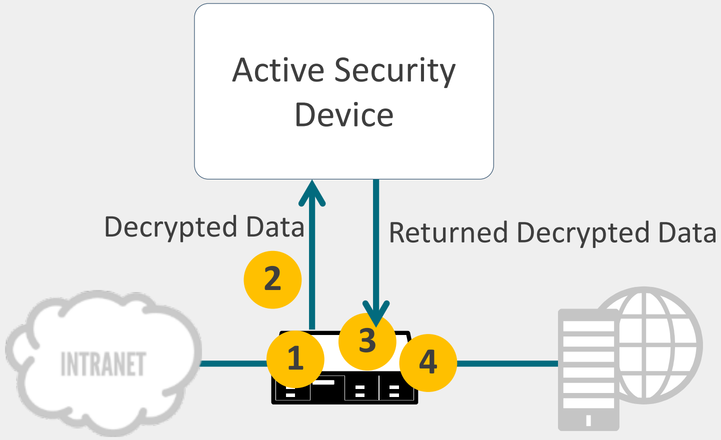
Policy Data for Host Categorization

GLOBAL INTELLIGENCE NETWORK

- Purpose Built for ETM
- Add value to security tools
- Vendor Neutral

Maintaining Data Integrity of Decrypted Data

SSLV Manages the Chain of Control



SSL Visibility Appliance

1. Decrypts data.
2. Sends a COPY to active security device
3. Checks returned data to ensure data has not been altered
4. Only forwards **original data** to assure data integrity of original info

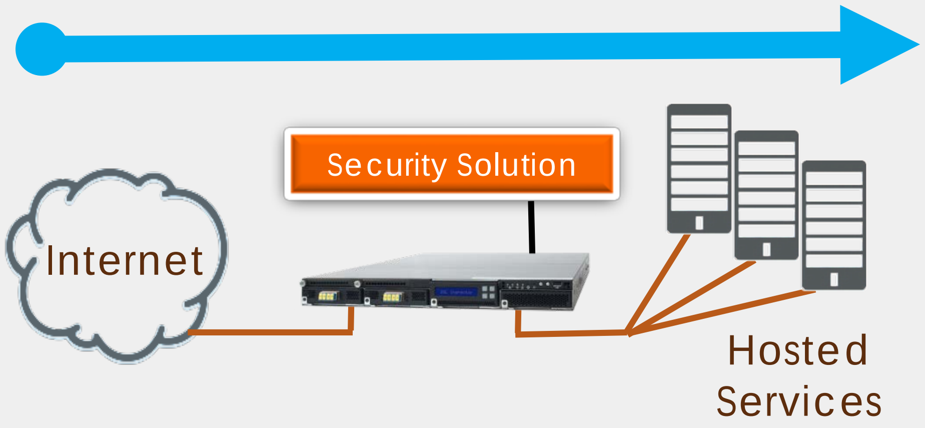
RESPONSIBLE SSL INSPECTION

TWO APPROACHES

Inbound SSL Decryption

Origin: from the Internet
Destination: your hosted services

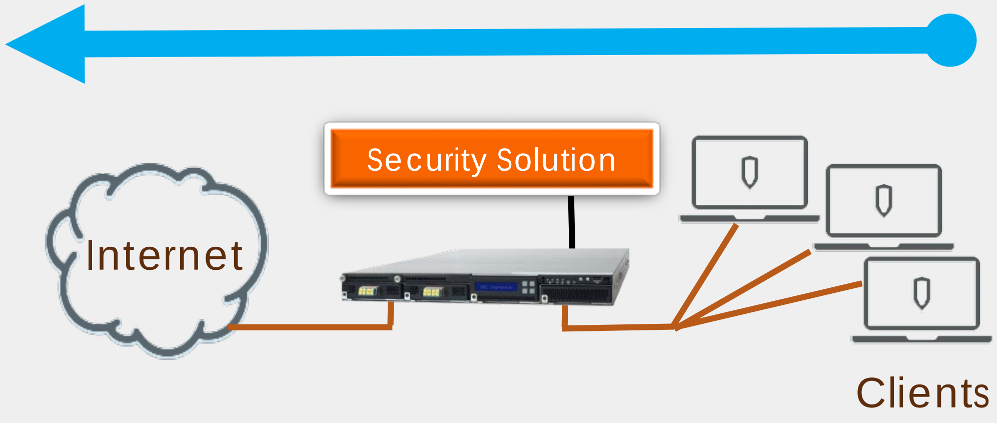
- Web Servers
- Email Servers
- Customer Web Portals



Outbound SSL Decryption

Origin: inside your network
Destination: to the internet

- Outbound Encrypted Internet Traffic
- Encrypted Email
- Shadow IT (SaaS)



Providing Visibility for the Entire Security Stack…

IPS – IDS – APT – DLP – APM – SEIM – Full Packet Capture

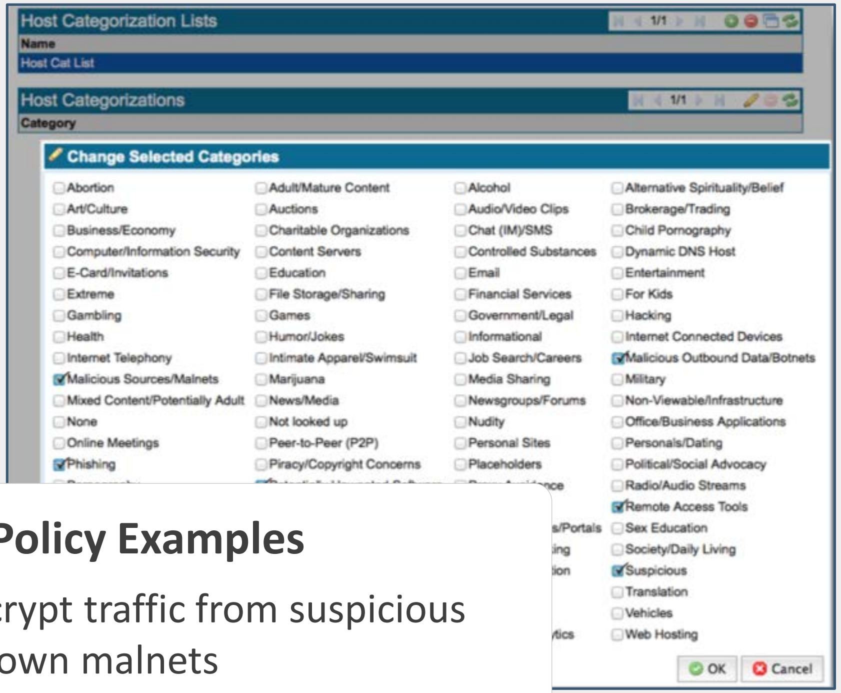
LIST (INFO)

Preserve Privacy and Compliance

Power of Global Intelligence

Set White / Black Lists automatically by category

- Host Categorization Service
- Leverages the Blue Coat Global Intelligence Network
  - Utilizes 80+ categories, in 55 languages
  - Processes +1.2B **NEW** web and file requests per day
- Easily customizable per regional and organizational needs



Host Categorization Lists

Name

Host Cat List

Host Categorizations

Category

Change Selected Categories

☐ Abortion
☐ Art/Culture
☐ Business/Economy
☐ Computer/Information Security
☐ E-Card/Invitations
☐ Extreme
☐ Gambling
☐ Health
☐ Internet Telephony
☑ Malicious Sources/Malnets
☐ Mixed Content/Potentially Adult
☐ None
☐ Online Meetings
☑ Phishing

☐ Adult/Mature Content
☐ Auctions
☐ Charitable Organizations
☐ Content Servers
☐ Education
☐ File Storage/Sharing
☐ Games
☐ Humor/Jokes
☐ Intimate Apparel/Swimsuit
☐ Marijuana
☐ News/Media
☐ Not looked up
☐ Peer-to-Peer (P2P)
☐ Piracy/Copyright Concerns

☐ Alcohol
☐ Audio/Video Clips
☐ Chat (IM)/SMS
☐ Controlled Substances
☐ Email
☐ Financial Services
☐ Government/Legal
☐ Informational
☐ Job Search/Careers
☐ Media Sharing
☐ Newsgroups/Forums
☐ Nudity
☐ Personal Sites
☐ Placeholders
s/Portals
ing
ion
tics

☐ Alternative Spirituality/Belief
☐ Brokerage/Trading
☐ Child Pornography
☐ Dynamic DNS Host
☐ Entertainment
☐ For Kids
☐ Hacking
☐ Internet Connected Devices
☑ Malicious Outbound Data/Botnets
☐ Military
☐ Non-Viewable/Infrastructure
☐ Office/Business Applications
☐ Personals/Dating
☐ Political/Social Advocacy
☐ Radio/Audio Streams
☑ Remote Access Tools
☐ Sex Education
☐ Society/Daily Living
☑ Suspicious
☐ Translation
☐ Vehicles
☐ Web Hosting

Policy Examples

- Block or decrypt traffic from suspicious sites and known malnets
- Bypass / Do not decrypt financial and banking-related traffic

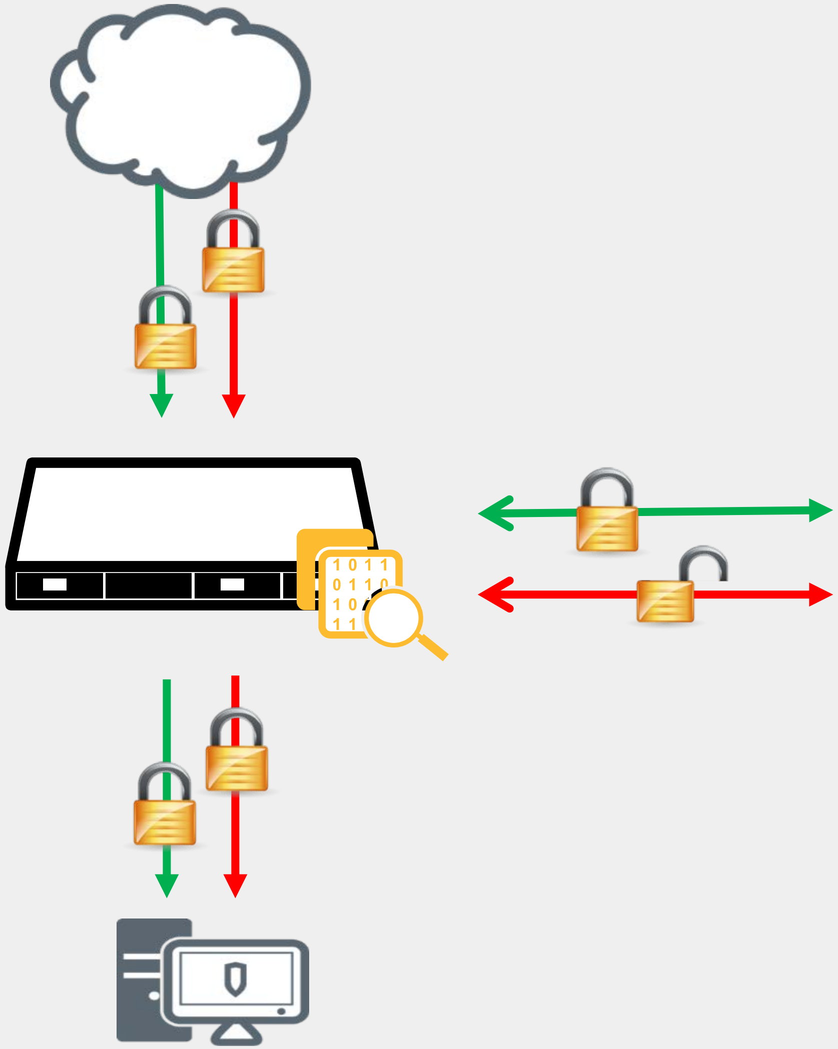
Host Categorisation

Never Decrypt: Banking/HealthCare/ Government

Decrypt: Malicious/Adult/ Unwanted Software

Same Control as a Proxy!

80 Categories, 55 Languages



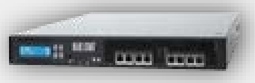
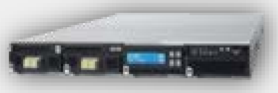
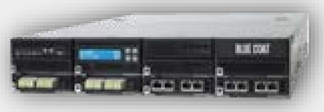
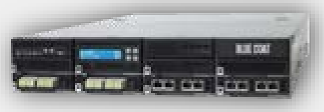
DAMBALLA CYPHORT TREND MICRO
lastline FireEye

BLUE COAT NIKSUN
RSA esentire

Symantec ca technologies
FIDELIS CYBERSECURITY RSA

SNORT CISCO Check Point SOFTWARE TECHNOLOGIES LTD.
paloalto NETWORKS IBM

SSL Visibility appliance Family

Function	SV800-250M	SV800-500M	SV1800	SV2800	SV3800	SV3800B-20
Total Packet Processing	8 Gbps	8 Gbps	8 Gbps	20 Gbps	40 Gbps	**40 Gbps**
SSL Visibility Throughput	250 Mbps	500 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	**9 Gbps**
Concurrent SSL Flow States (CPS)	20,000	20,000	100,000	200,000	400,000	**800,000**
New Full Handshake SSL sessions (CPS) (i.e. Setups / Tear Downs) • **1024-bit keys** • **2048- bit keys** • **ECDHE256**	• 1,000 • 1,000 • 500	• 2,000 • 2,000 • 1,000	• 8,000 • 3,000 • 3,500	• 12,500 • 3,000 • 6,000	• 15,000 • 6,000 • 8,000	• 30,000 • 6,000 • 11,000
Configuration	Fixed	Fixed	Fixed	Modular 3 Slots	Modular 7 Slots	Modular 7 Slots
Input / Output	8 10/100/1000 Copper (fixed)		8 10/100/1000 Copper or Fiber (fixed)	2x10G-Fiber, 4x1G Copper, 4x1G Fiber Network Mods		
Resiliency	Fail-to-Wire (FTW) / Fail-to-Appliance (FTA)					
List Price (USD)	$15,000	$25,000	$51,000 (copper) $55,000 (fiber)	$64,000 (chassis w/o Netmods)	$82,000 (chassis w/o Netmods)	$160,000 (chassis w/o Netmods)
Network Modules / Net Mods (USD)	N / A			• 4 port copper 1G : NTMD-SV-4x1G-C • 4 port fiber 1G : NTMD-SV-4x1G-F • 2 port fiber 10G SR : NTMD-SV-2x10G-SR • 2 port fiber 10G LR : NTMD-SV-2x10G-LR		

Automatic Encrypted Traffic Management

A Design Point in the Enterprise

Not a feature of another product

Automated visibility and control of encrypted traffic

Preserving the highest level of Crypto

Enhance the ROI of the security infrastructure

Data privacy and compliance while enabling security

Encrypted Traffic Management (ETM) used as Design Point for Banks Advanced Threat Detection Project

Global Top 10 Bank

- **RFP FOR THREAT DETECTION**
  - Large project with board level visibility.
  - APT / malware attacks caused “public exposure”.
  - No Encrypted Traffic Management in RFP.
  - SSL Blindspot was not considered or budgeted for.
- **SOLUTION**
  - UK team positioned need to remove SSL blind spot at RFP meeting, irrelevant of which vendor they eventually award to.
- **RESULTS**
  - SSL blind spot was put in scope to ensure project success
  - Worked with Bank in Labs to confirm our ETM solution removed SSL blind spot for **ALL** down selected vendors (FireEye, Cisco, Trend etc).
  - Our ETM solution is currently being deployed globally with Trend Micro Solution

47 SITES WORLDWIDE

Global Top 10 Bank

“Without an Encrypted Traffic Management Strategy, all threat detection solutions were 50% less effective” Project Lead for RFP.

ETM improving existing Security Investments - post breach

Global Top 10 Pharmaceutical

- **PAIN POINTS**
  - $$$ of Cancer Research Stolen
  - Encrypted Traffic >70% of Global Traffic
  - DLP, Anti-malware and Security Analytics (full packet capture) investments could not see into SSL traffic
  - Historical Compliance/HR/Legal objections with SSL inspection
- **SOLUTION**
  - UK Team enabled architects on ETM solution regarding its simple L2 implementation and policy based decryption capability
  - ETM Solution combined with DLP, Sandboxing and Security Analytics investments to improve their effectiveness
- **RESULTS**
  - ETM solution Deployed at 8 sites worldwide to improve Threat Detection and post breach investments.
  - Granular Policy Based decryption capability (e.g ignore banking/healthcare) satisfied Compliance/Legal objections.

8 SITES WORLDWIDE

ETM enabling Bank DLP project

Global Top 20 Bank

- **PAIN POINTS**
  - Compliance driven need to monitor all traffic via DLP Solution
  - Encrypted Traffic >50% of Global Traffic
  - Making bigger investment in DLP wasn’t going to happen until addressed

- **SOLUTION**
  - Educated customer on ETM.
  - ETM Solution combined with Symantec DLP Monitor

- **RESULTS**
  - Deployed ETM solution with Symantec DLP monitor
  - Deployed at multiple sites worldwide
  - Now Looking to feed other security tools and locations (decrypt once, feed many)

66 COUNTRIES WORLDWIDE

CALL TO ACTION

- EDUCATE your peers and increase awareness on this emerging risk
- Determine your current SSL/TLS Blind Spot and growth rate
- Review your current SSL Inspection strategy
  - Can you increase security tool effectiveness & ROI?

Thank you!

Sales@openreality.co.uk
01235 556 400

James_Stevenson@Symantec.com

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.