

Enabling Full Visibility for Zero Trust Networks

SSL Insight Solution Overview

A10

Always Secure. Always Available.

Cyber Crimes are on the Rise!



\$3.92 M

Average cost of a
Data Breach



650%

Increase in
Trojan-based
malware threats



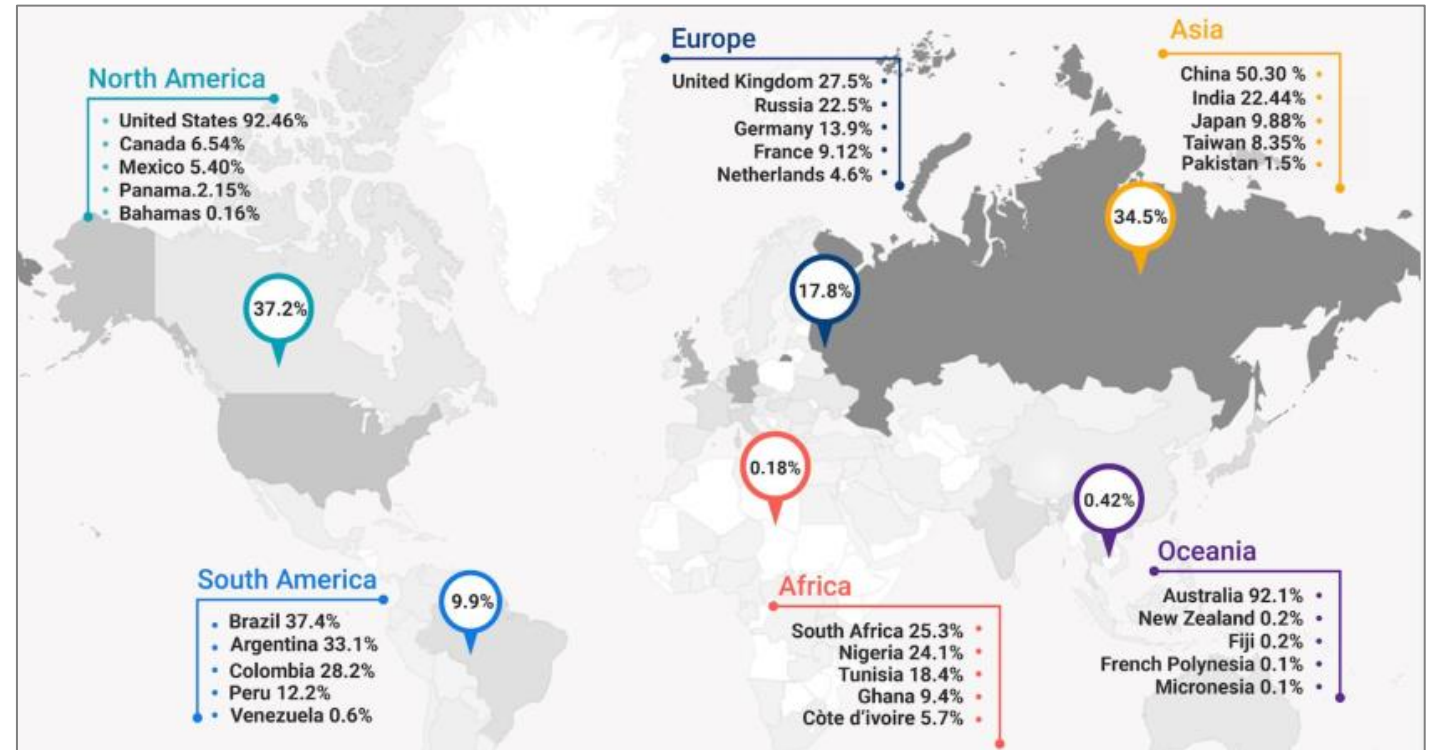
90%

Breaches caused by
Phishing

*A lot of these attacks are enabled by
Internal Threat Actors*

Impact of Data Breaches

- Ransom
- Lost revenue
- Brand damage
- Regulatory fines e.g. GDPR
- Investigation costs
- Lawsuits



Data Breaches can happen anywhere, at any time

Are All Attacks Launched From The Outside?

- More than often, Internal Threat Actors are to be blamed for such attacks
- Who is an Internal Threat Actor?
 - Any user within the trusted internal network
 - Has legitimate access to resources
 - Has conscious intent to cause harm
 - Malicious insider or disgruntled employee
 - An imposter who technically is an outsider
 - Corporate spies
 - Has no conscious intention of causing harm
 - Careless or negligent insider
- Internal Threat Actors are generally not aware of the damage they are causing

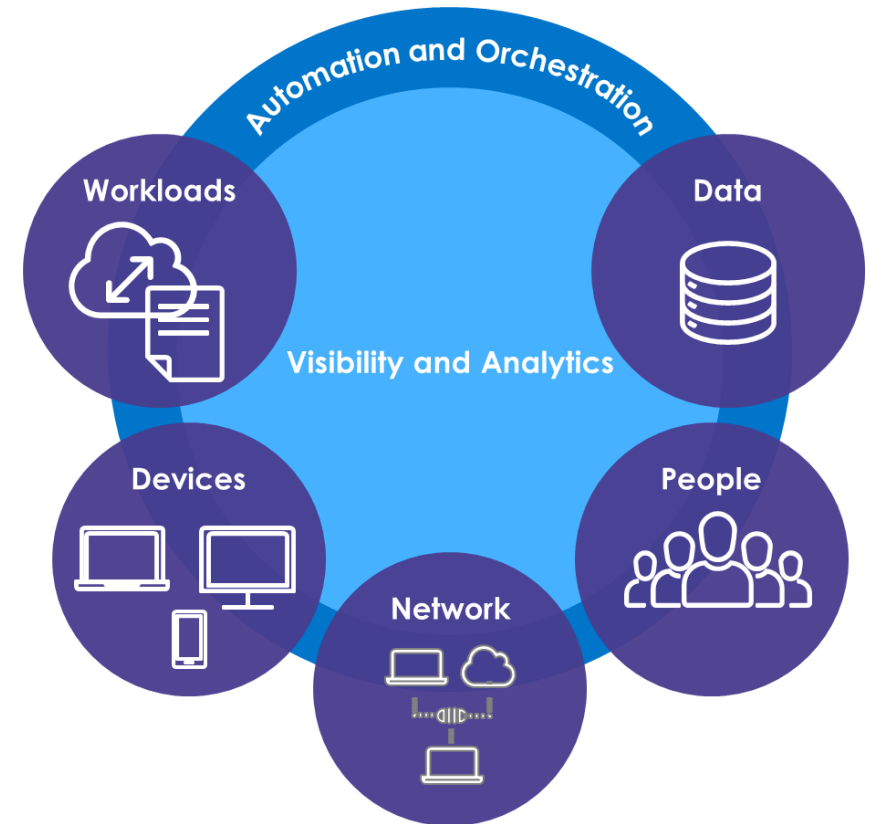
Zero Trust Aims to Solve These Security Issues

- What is Zero Trust?
 - Conceptual model driving architectural changes
 - The concept has been around for long
 - Vendors and customers finally implementing the model
 - Demands major architectural changes
 - In the Zero Trust model, visibility is key
 - Visibility into users, data, workflows etc.



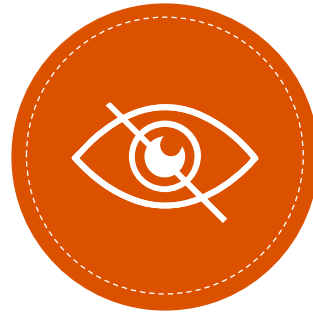
Basic Principles of Zero Trust

- “Trust Nobody”
 - Redesign networks into secure **micro-perimeters**
 - Limit **excessive user privileges**
 - Improve detection and response times through **analytics and automation**
 - Enable **compliance**
 - Improve security detection and response with **centralized visibility & control**
 - Avoid solutions that are **too complex to deploy and use**
 - Avoid solutions that don’t support **diverse integrations**



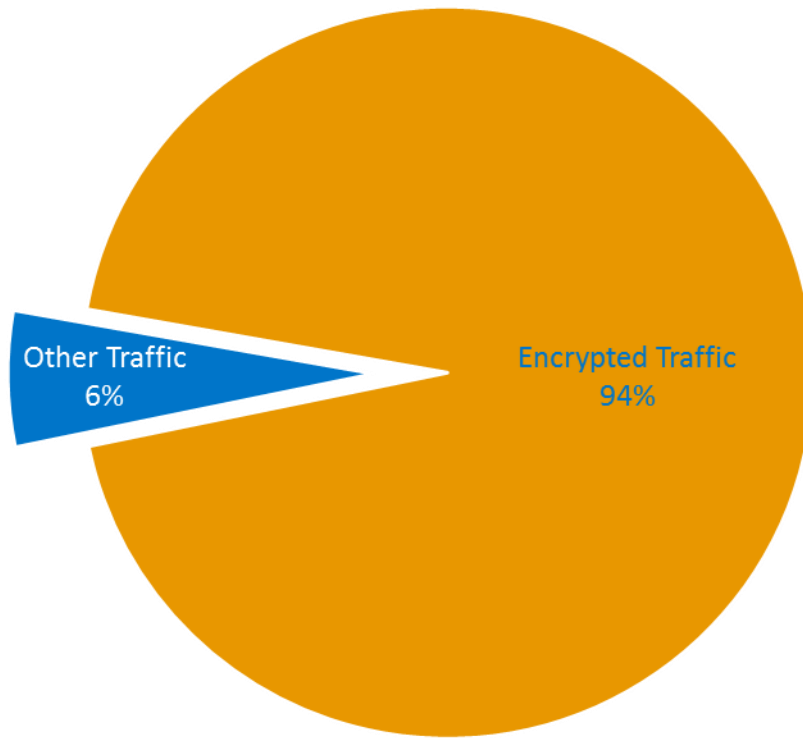
Encryption Introduces New Challenges & Complexity

*Encryption gives you **Privacy***

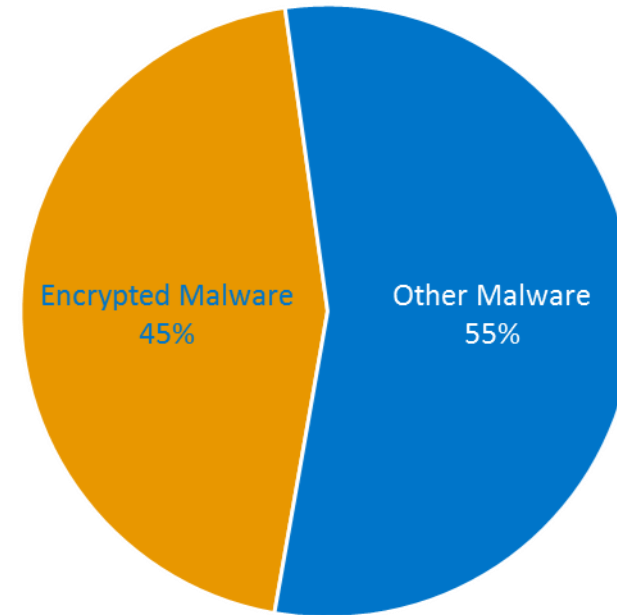


*But it can hurt your **Security***

Exploiting The Growing Encrypted Blind Spot



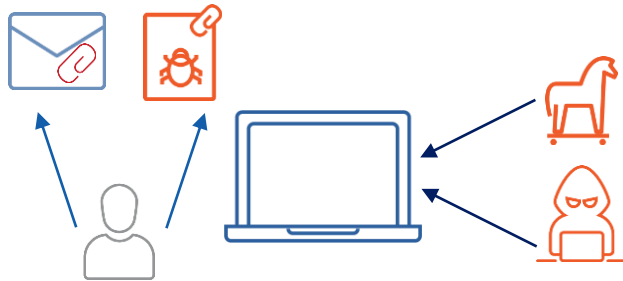
94% of all internet traffic is encrypted



Almost half of cyber attacks use encryption to evade security

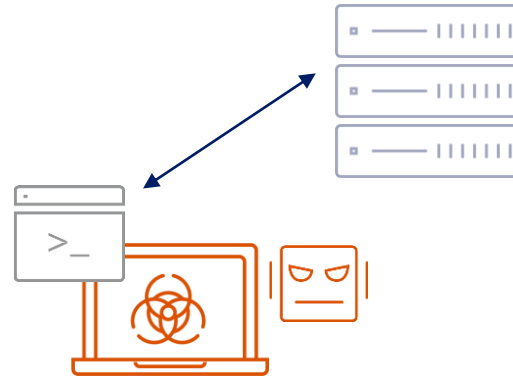
Encryption Makes Traditional Defenses Ineffective

Infiltration



Intrusion Prevention System (IPS)
Firewall
Secure Web Gateway (SWG)
Anti Virus System

Command and Control



Advanced Threat Protection (ATP)
Anti Malware System
Sandbox

Exfiltration



Data Loss Prevention System (DLP)
Forensics

Before

During

After

The Cyber Attack Continuum

Zero Trust Model Will Also Fail Without Decryption Because

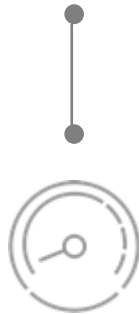
Visibility Is Key

But Visibility Requires More Than Simple Upgrades



Existing Solutions are Inefficient, Expensive and Complex

Inferior
Performance



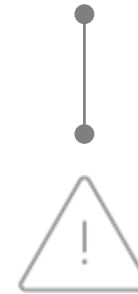
Costly & Not
Purpose Built

Inflexible
Deployment



Disruptive &
Incomplete

Difficult
Operationalization

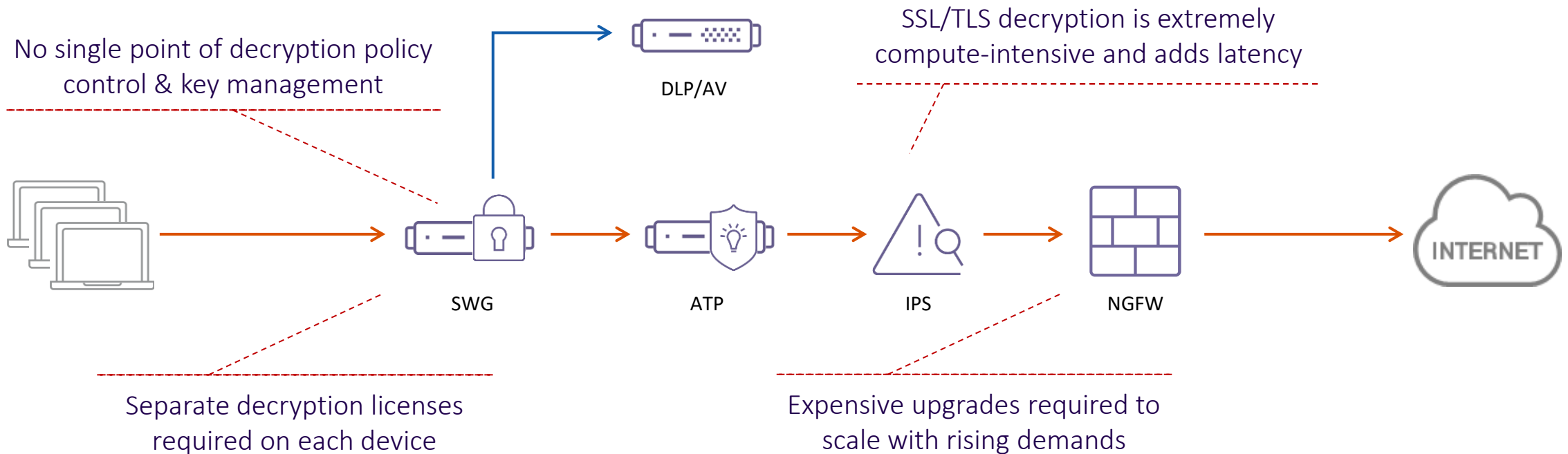


Complex UI &
Incomplete Analytics

Decryption Scale and Security Problems

→ Encrypted Internet Traffic
→ Decrypted Internet Traffic

Each device must decrypt and re-encrypt its own traffic for full visibility



So What's The Solution?

Performance Hit at Every Appliance

OR

No TLS/SSL Inspection?

The Solution – Dedicated and Centralized Decryption

A Solution That:

- Provides full visibility to the entire security infrastructure
- Enhances efficiency and efficacy of existing security infrastructure
- Is vendor agnostic and provides flexible deployment options
- Is easy to operationalize and use
- Provides centralized visibility and analytics
- Provides centralized management
- Centralizes decryption, policy control, key management

“Dedicated Decryption” is the Preferred Solution



DO IT WELL, DO IT ONCE

To minimize the risks described above, breaking and inspecting TLS traffic should only be conducted once within the enterprise network. Redundant TLSI, wherein a client-server traffic flow is decrypted, inspected, and re-encrypted by one forward proxy and is then forwarded to a second forward proxy for more of the same, should not be performed. Inspecting multiple times can greatly complicate diagnosing network issues with TLS traffic. Also, multi-inspection further obscures certificates when trying to ascertain whether a server should be trusted. In this case, the “outermost” proxy makes the decisions on what server certificates or CAs should be trusted and is the only location where certificate pinning can be performed. Finally, a single TLSI implementation is sufficient for detecting encrypted traffic threats; additional TLSI will have access to the same traffic. If the first TLSI implementation detected a threat, killed the session, and dropped the traffic, then additional TLSI implementations would be rendered useless since they would not even receive the dropped traffic for further inspection. Redundant TLSI increases the risk surface, provides additional opportunities for adversaries to gain unauthorized access to decrypted traffic, and offers no additional benefits.

flows, establishing TLS sessions, and issuing trusted certificates. Risks become apparent as the detailed mechanism TLSI employs is understood.

Forward Proxy Traffic Flows

A forward proxy is a network device that intercepts requests from internal network clients and forwards those requests to servers on external networks. When the external servers respond, the responses are sent to the forward proxy and then the forward proxy sends the responses to the internal network clients. A TLSI capability implemented within a forward proxy between the edge of the enterprise network and an external network such as the Internet protects enterprise clients from the high risk environment outside the forward proxy.

U/OO/212028-19 PP-19-1471 18 November 2019

1

Introducing SSL Insight[®]

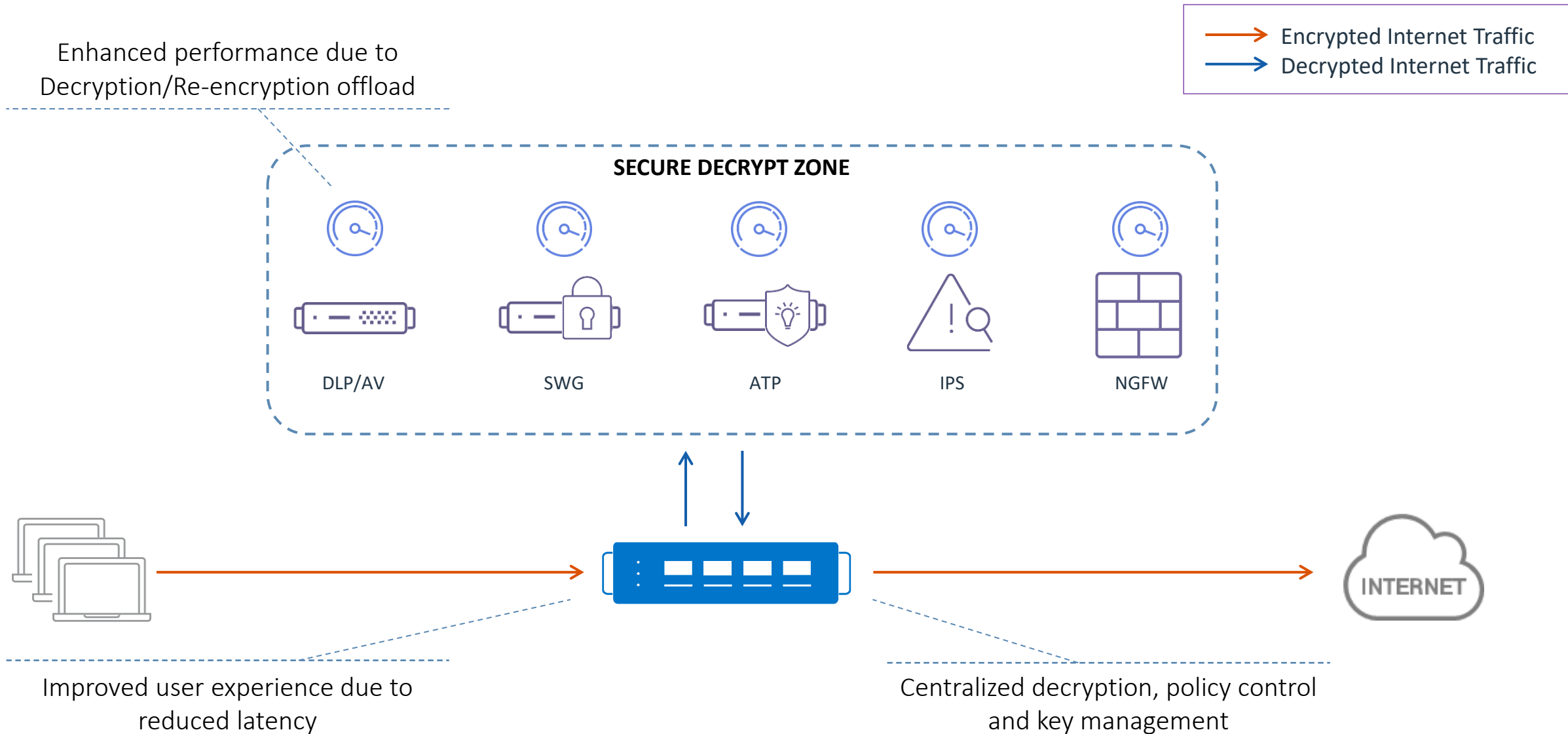
A10

Always Secure. Always Available.

SSL Insight is at the Core of the Zero Trust Model

- With most of internet traffic being encrypted, SSL Insight enables other Zero Trust security devices and improves their efficacy
- Multi-Layered Security Services:
 - Enable compliance
 - Restrict and scrutinize user access
 - Provide consolidation of multiple security services in one platform
- “Ease Of Use Matters” – Forrester
 - Centralized visibility, management and policy control with uniform UIs help position us as a strong contender
- Seamless integration with other security solutions

Enhance Performance with Secure Decrypt Zone



Solution Components – A Deeper Dive



FULL TRAFFIC VISIBILITY



MULTI-LAYERED SECURITY



ANALYTICS & EASE OF USE



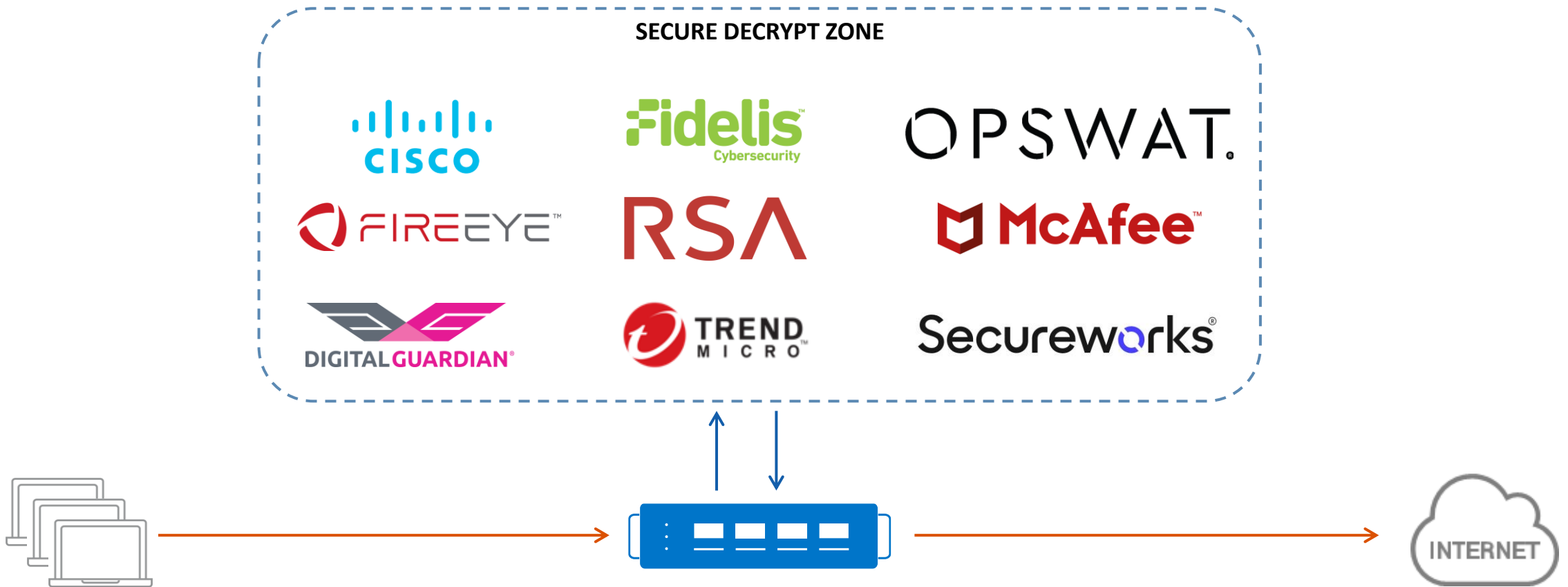
Full Traffic Visibility

- Full Visibility, including PFS, at industry's highest performance
 - Decrypt across all multiple protocols including SSL/TLS, SSH, STARTTLS, XMPP, SMTP and POP3
- Dynamic port inspection to identify and decrypt SSL/TLS over any port
- Full proxy architecture ensures granular control over traffic
- SSL Insight is non-disruptive, integrating seamlessly into any network
 - Can be deployed as an L2 bump-in-the-wire or L3 device
 - Can be deployed as a transparent or explicit proxy

Secure Decrypt Zone

- Decrypt once, inspect many times
- Flexible interoperability
 - Supports inline, passive or ICAP-enabled devices
 - Works with transparent and explicit proxies
 - Supports proxy chaining for connecting to upstream proxies
- Service chaining can be used to steer traffic through different security devices based on
 - Source and destination IP addresses
 - Protocol type
 - User and group ID
 - Application ID

What Goes in the Secure Decrypt Zone?



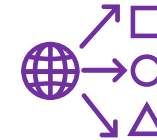
Note: Logos of only some of our validated security partners are shown here

Compliance

- Selective bypass for compliance with privacy regulations e.g. HIPAA, SOX, PCI/DSS etc.
- Examples:
 - Healthcare websites due to HIPAA regulations
 - Personal financial data due to EU General Data Protection Regulation
- Decrypt traffic to stop data breaches, ensuring GDPR compliance
 - Ensure your organization is safe from large fines and lawsuits
- High speed and detailed logging for PCI/DSS compliance

Web Classification Service

- Classifies web traffic into 83+ site categories in order to bypass decryption of specific, sensitive data
- On-box database of 20 million domain entries & 600+ million domains in the cloud
- Powered by Webroot



WEB CLASSIFICATION SERVICE

- 600+ million domains
- 27+ billion URLs classified
- 83+ site categories
- 45+ languages
- 12 million dangerous IPs correlated with URLs

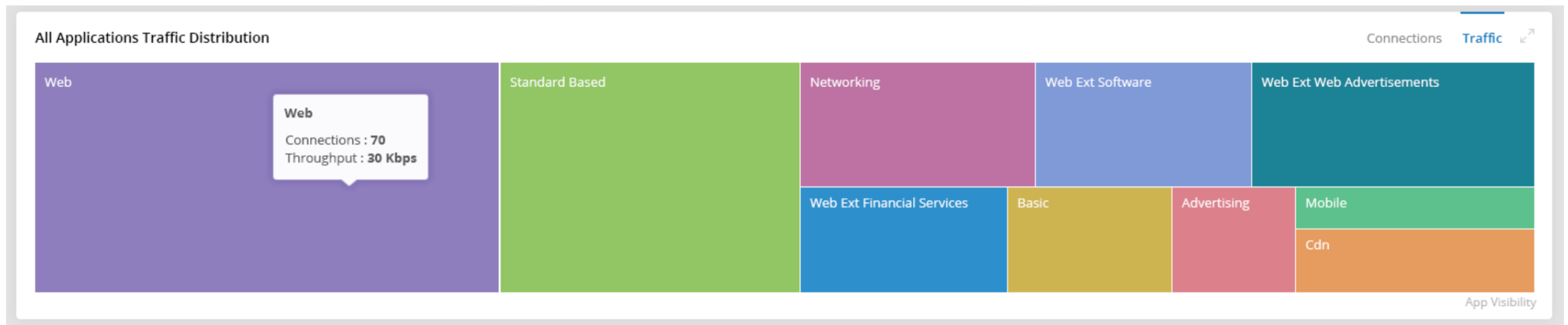
Multi-Layered Security Services



...And More

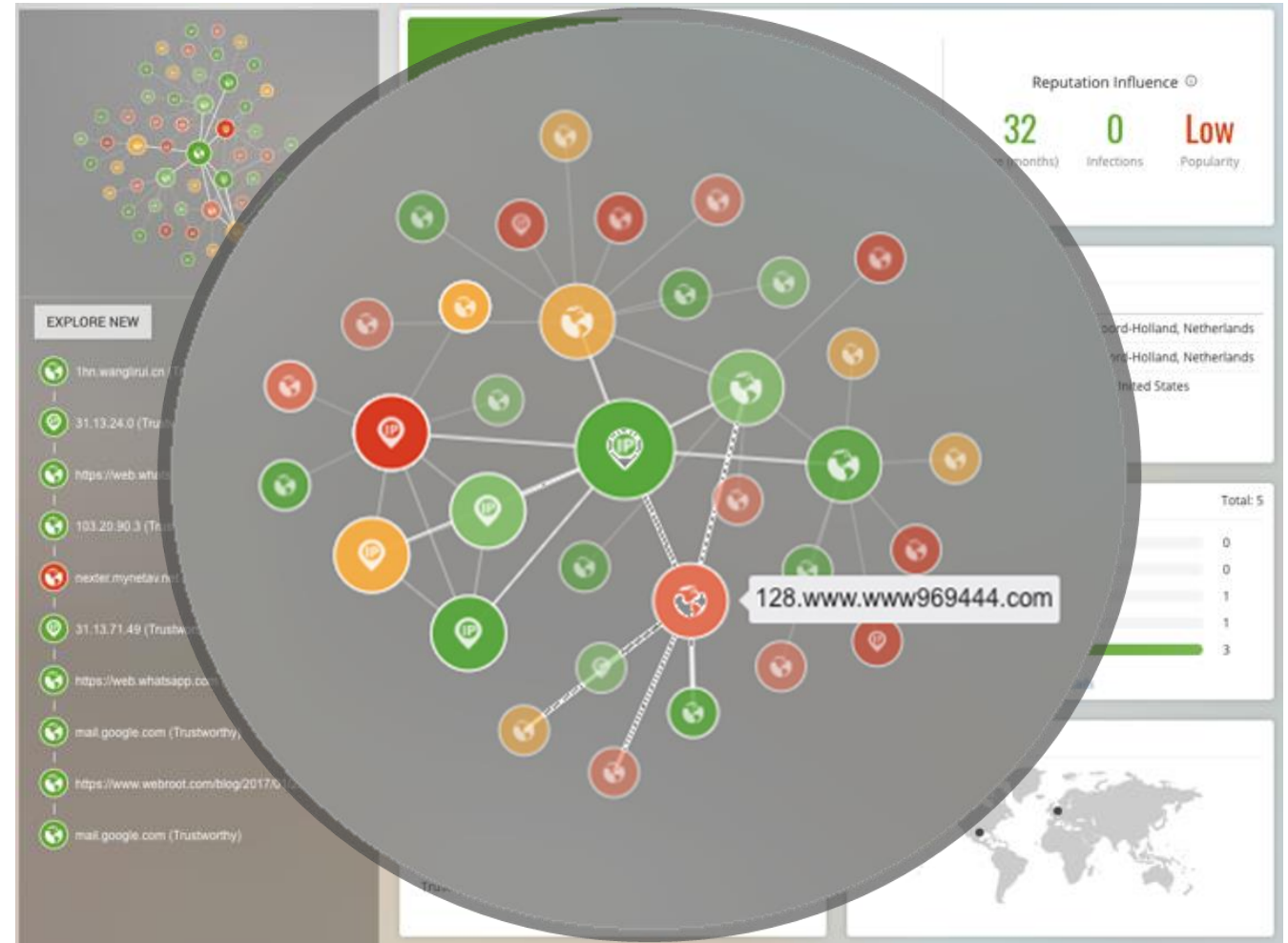
Application Visibility

- Identify applications irrespective of port, protocol, or evasive tactics
- Identify applications based on bandwidth or connections consumption
- Restrict applications based on security and performance concerns
- Steer traffic through different security devices based on Application ID



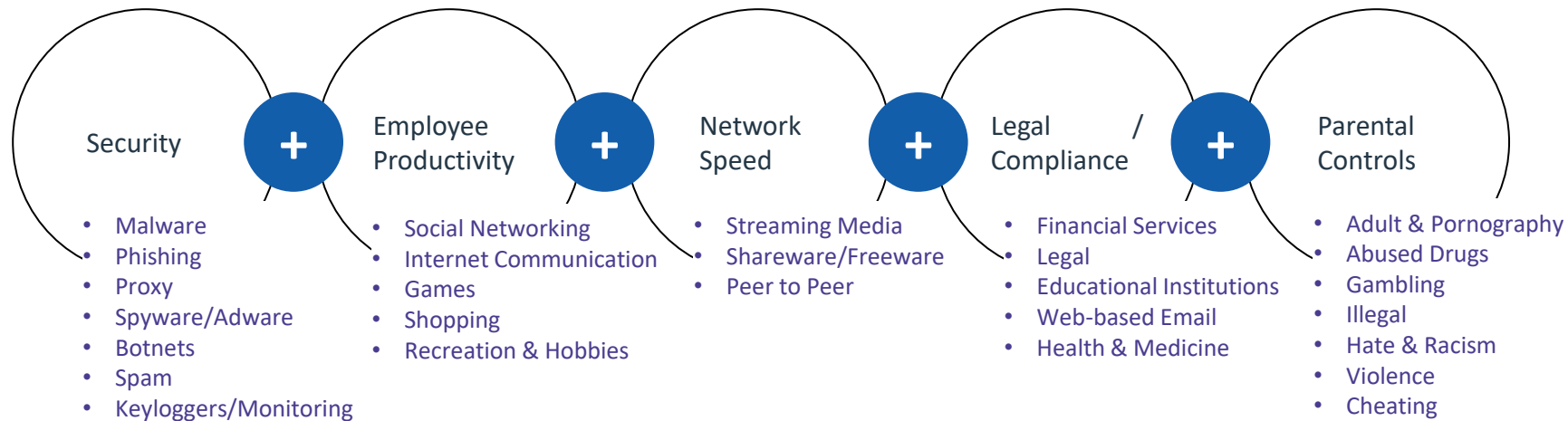
Threat Investigator

- Investigate threats & gain valuable insights
- Risk score assessment for domains, IPs, Apps & Files
 - Reputation index scores from 0-100
- Detailed graph of all linked actors and their reputation index
- Integrated into Access Logs for ease of use



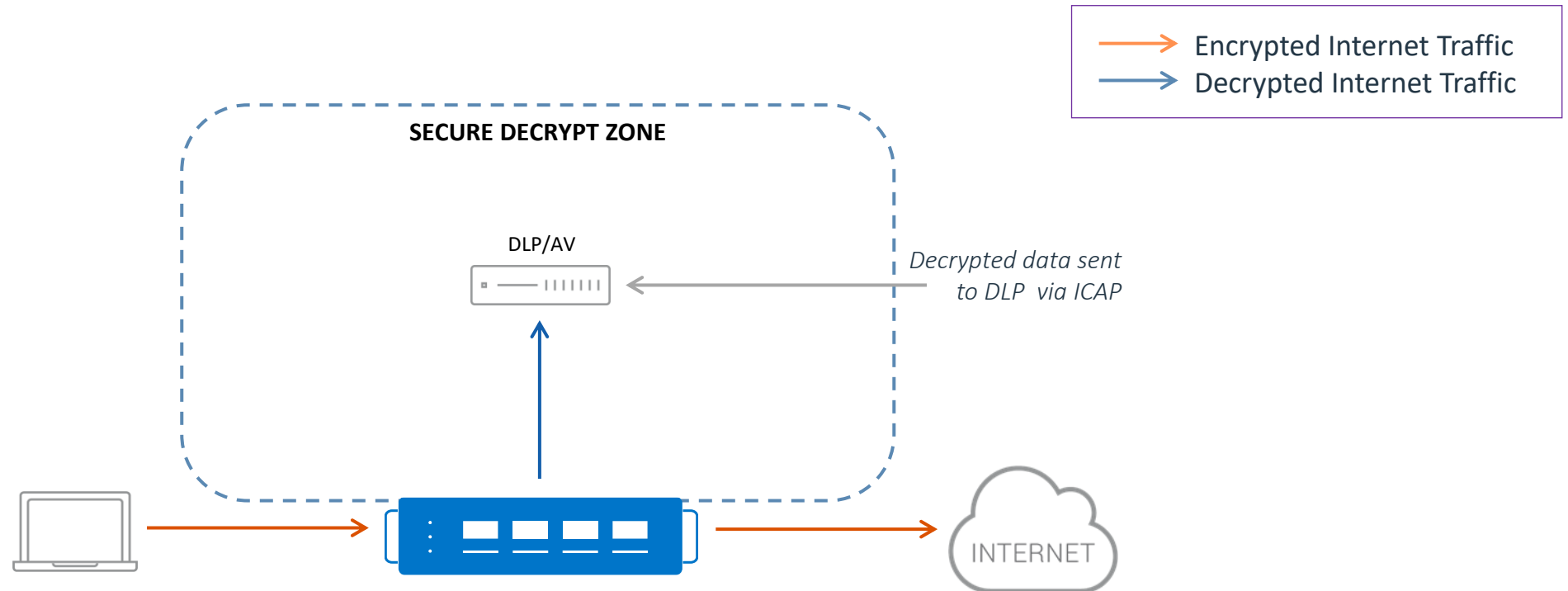
URL and Web Filtering

- Preventive security service
- Block access to known malicious and harmful content
 - Specific categories for K-12 user protection
 - Block access based on security concerns (malware, phishing etc.)
 - Stop users from bypassing security (proxies, VPNs)
- User-ID/Group-ID based filtering for granular control



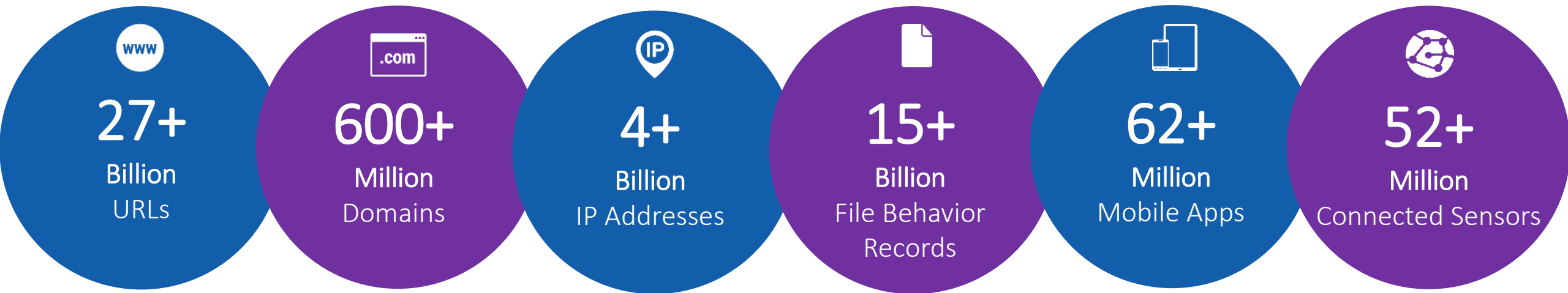
ICAP Support

- Extends TLS inspection support to ICAP based security appliances
 - ICAP Request Mode for Data Loss Prevention (DLP) appliances
 - ICAP Response Mode for Anti-Virus/Malware appliances
 - Pre-Filtering of traffic based on request method, payload or preview length



Threat Intelligence

- Continuously classifies and scores 95% of the Internet, and monitors the entire IPv4, and in-use IPv6 address space
- Enhances security efficacy to cover a broad range of attacks originated by different IP threat categories
- Applied through Thunder CFW firewall rules



Note: Web Classification service subscription is required

User-based Policies

- Authentication and Authorization services for internal users
- Provide Identity-based access control
 - Connect to Active Directory for User/Group IDs
- Define User-ID/Group-ID based policies for Traffic Steering, URL Filtering and more
- Provide detailed activity logs
 - Enable SIEMs for high-speed, extensive logs to track malicious activity

CLIENT LOGIN	METHOD (AUTHENTICATION SERVERS)
HTTP Basic	LDAP, RADIUS, NTLM, Kerberos, Token (Active Directory and OpenLDAP)
NTLM	NTLM (Active Directory)
Kerberos	Kerberos (Active Directory, MIT Kerberos Server)
Form	LDAP, RADIUS, NTLM, Kerberos
SAML	SAML IdP (ADFS 2.0/3.0, Ping Federate, Shibboleth, OKTA, Sailpoint, CA SiteMinder)
2 Factor Auth	RSA SecurID, Entrust Identity Guard, Duo, Censornet
MS SQL TDS	LDAP, RADIUS, NTLM, Kerberos (Active Directory)
OCSP	OCSP (MSFT Enterprise CA, OpenSSL)



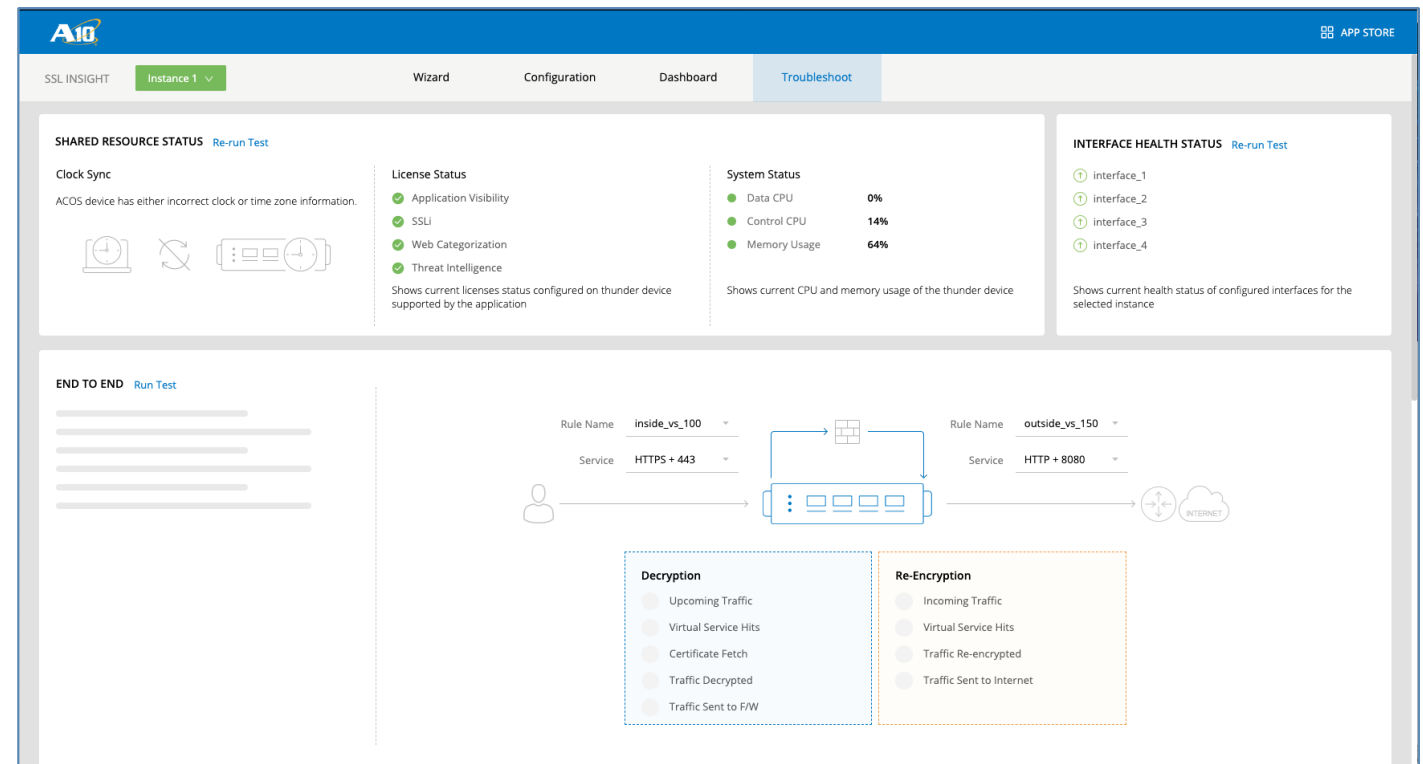
Analytics & Ease of Use

A10

Always Secure. Always Available.

Simple and Easy to Use

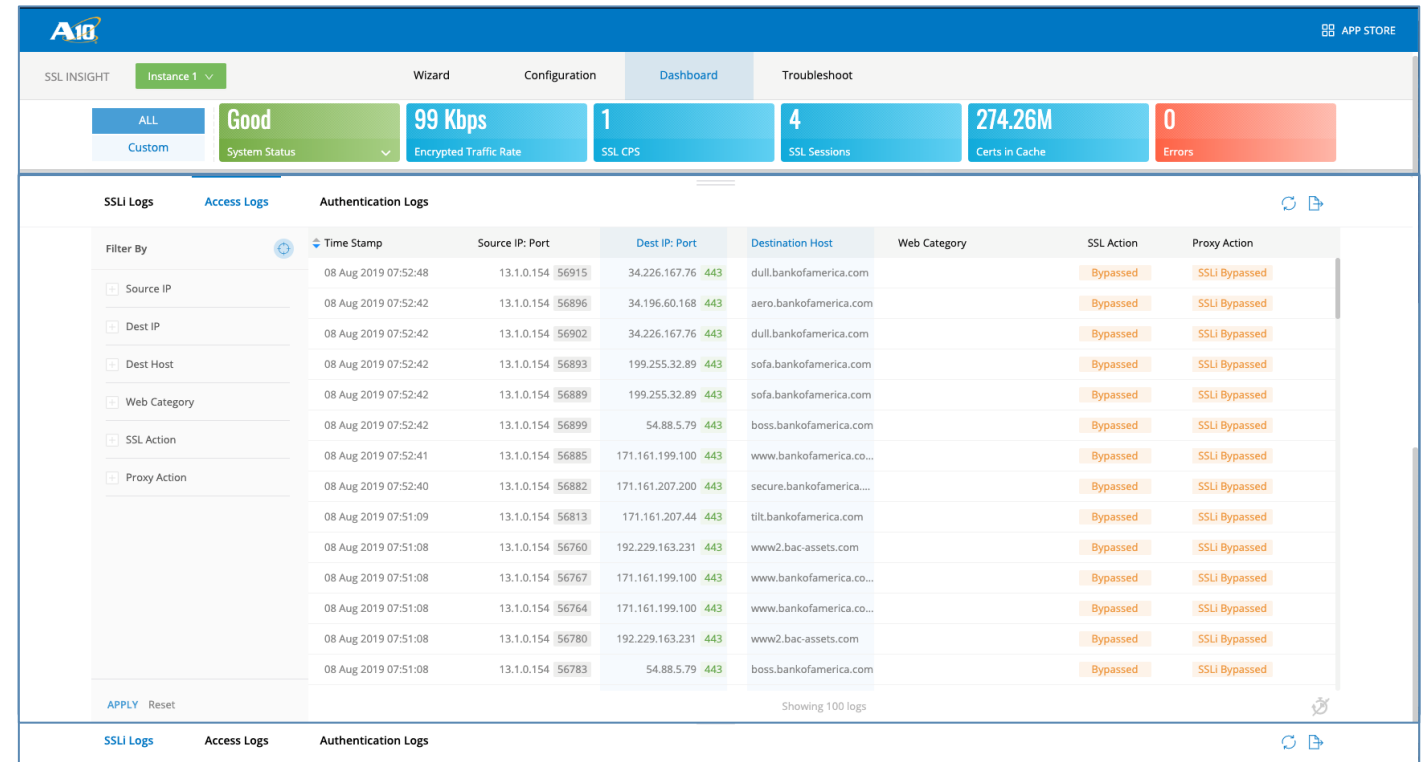
- AppCentric Templates
 - Streamlined Wizards
 - Wider coverage of use cases
 - Configuration Dashboard
- 3-step configuration
- Streamlined, single device deployments
- Simplified, wizard-based troubleshooting



Configuration Dashboard helps you troubleshoot configuration problems before making edits

Intuitive Dashboards and Detailed Visibility

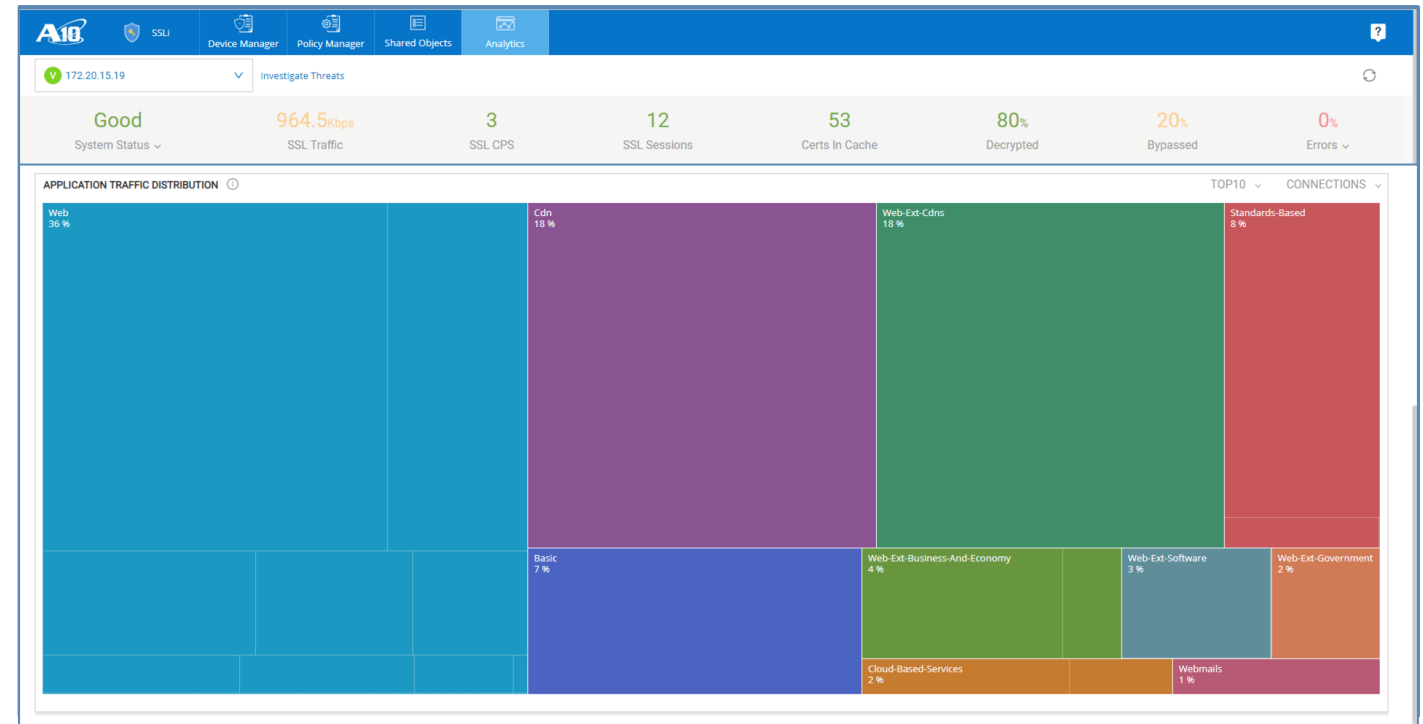
- Customizable Dashboards
 - Intuitive Widgets and Tiles
 - Grouped by service type
- Detailed Access Logs
 - Exportable logs
 - Threat Investigator Integration
- Instantaneous Reports



SSLi, Web Security, SSL/TLS, HTTP, HTTPS, and more. Threat investigation

Centralized Management and Visibility

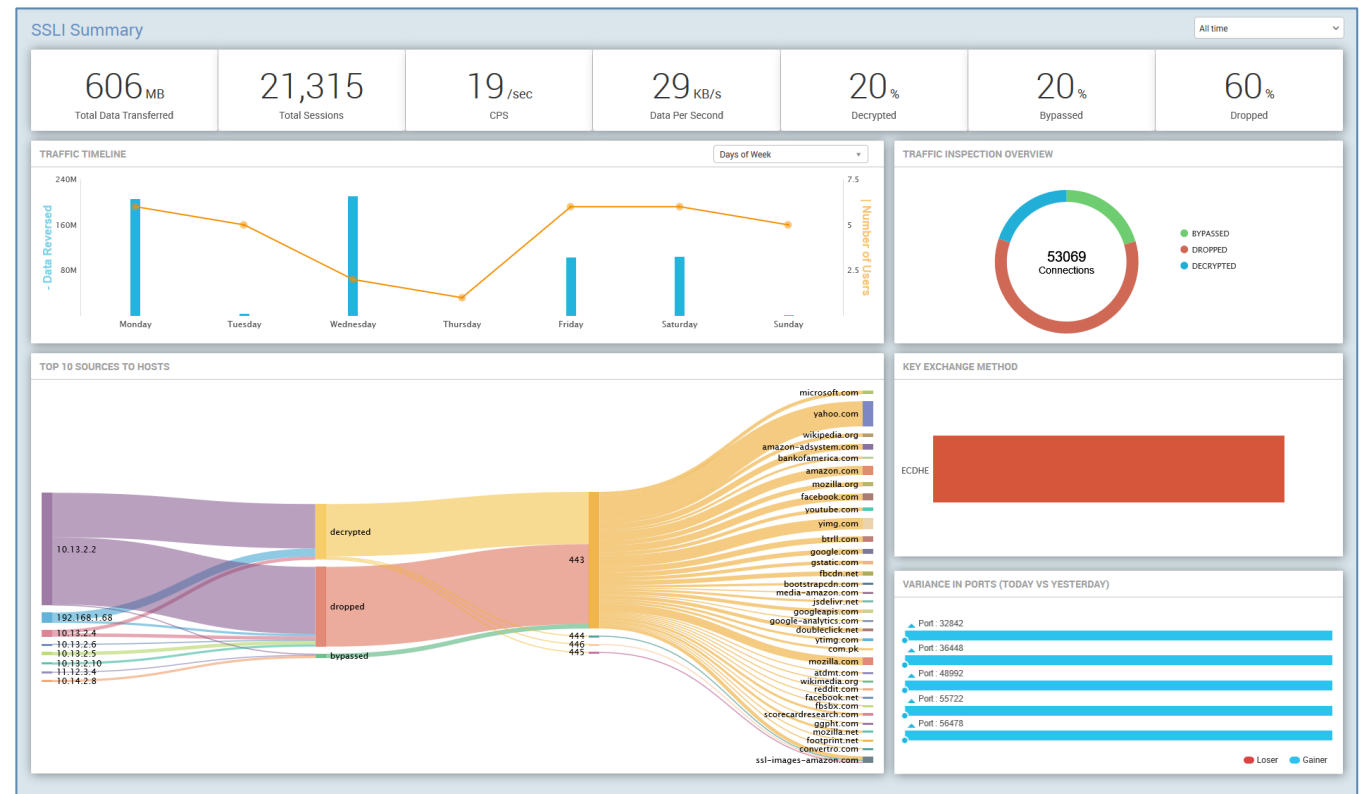
- Harmony Controller SSLi App
 - Streamlined Wizards
 - Device and Policy Manager
 - Wider coverage of use cases with shared objects
- Multi-device, Multi-site deployments
- Enhanced operational efficiency



The dashboard provides a centralized view of SSL traffic and system health, enabling administrators to monitor and manage SSLi deployments across multiple devices and device groups.

Enhanced Logging

- High speed logging to syslog, SIEM etc.
 - Comprehensive SSLi logging and stats for all SSL sessions
 - Shows detailed traffic and connections statistics
- Dedicated Splunk Enterprise App



Case Study – Secure Decrypt Zone in Education

Customer - Klein ISD

- NA, USA (Education)
- Klein ISD is a school district in Harris County, Texas. It has 32 elementary schools, 10 intermediate schools, and 5 high schools.

Challenges

- K-12 education is constantly under threat of attacks and content that is inappropriate for students to access
- With a rise in IoT devices, the infrastructure, including the firewall, intrusion prevention system, and content filter couldn't scale

Business Impact

- Protect 53,000 students and 6,500 staff against cyberthreats and maintain federal compliance
- Decrypt all content for inspection without compromising performance
- Proactively adapt controls and policies based on new visibility into anomalies and threats
- Maximize the investment in the existing security infrastructure

Solution

- Thunder CFW
 - SSL Insight
 - URL Filtering service
- Harmony Controller

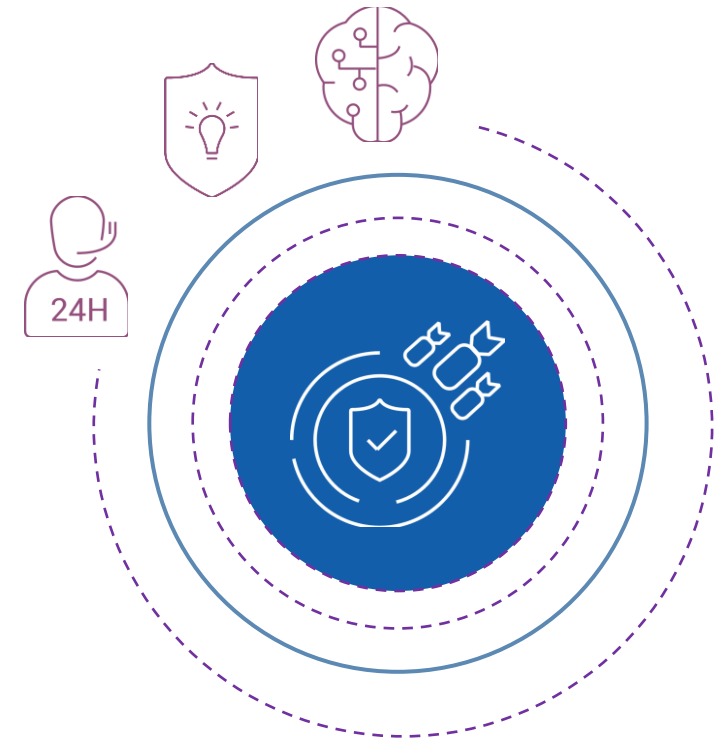


WHY A10

- A10's "secure decrypt zone" with the decrypt once and inspect many times approach
- A10's superior SSLi performance at an affordable price
- Simplicity and ease of use with AppCentric Templates (ACT)
- Centralized management and visibility with Harmony Controller

A10 Networks – Ensuring Your Success

- **A10 Professional Services**
 - With multiple service packages
- **24x7 Support**
- SSL Insight education and **training**
- Product Security Incident Response Team (**PSIRT**)



Next Steps

- **Learn** how Thunder SSLi can be deployed to enhance the efficiency of your security infrastructure
- **Read** our Solution Briefs for an overview of our solution components
- **Watch** our videos to learn more about the common threats hiding behind SSL encryption



Solution Briefs and Deployment Guides



Learn more about Thunder SSLi – Watch our videos



```
if ($?DEBUG >= 2) { log "not_valid_after [SSL:cert  
not_valid_after_cert"]  
set not_valid_after [TIME:clock scan  
not_valid_after_cert]  
if ($?DEBUG >= 3) { log "DEBUG3 not_valid_after:  
not_valid_after"]  
set expire [TIME:clock format $not_valid_after -format  
"%a %b %d %H:%M:%S" -gmt 1]  
if ($?DEBUG >= 1) { log "Certificate Name: $cn"  
if (current_time > $not_valid_after) {  
add_certs_expired $client_ip $cn 600 600  
if ($?DEBUG >= 1) { log "Certificate Expired - $cn from  
$client_ip $client_port"  
close  
if ($?DEBUG >= 2) { log "Certificate NOT Expired -  
$cn expire from $client_ip:$client_port"  
if ([CLASS:match $cn equals CertMAP] == 1) {  
set pool [CLASS:match $cn equals CertMAP value]  
if ($?DEBUG >= 1) { log "Certificate Mapped  
$cn from $client_ip $client_port - pool $pool (selected)"  
if ($?DEBUG >= 1) { log "Certificate NOT Mapped - $cn  
if ($?DEBUG >= 1) { log "Certificate NOT Mapped - $cn
```

Thank You

A10

Always Secure. Always Available.

Appendix

A10

Always Secure. Always Available.

Setup Slides

A10


Always Secure. Always Available.

Zero Trust is Endorsed by Many

FORRESTER

FOR SECURITY & RISK PROFESSIONALS

The Zero Trust eXtended (ZTX) Ecosystem
Strategic Plan: The Zero Trust Security Playbook
July 11, 2019

 This is the **Strategic Plan** report in **The Zero Trust Security Playbook For 2020**.

Why Read This Report

In the past two years, Forrester's Zero Trust security has exploded in awareness and plans for adoption. We've reached this market inflection thanks to the categorical realization from both security vendors and security pros that perimeter-based security has failed. However, with market hype comes the need for security pros to closely discern between real capabilities and technology alignment to their Zero Trust strategy and vendor marketing. In this report, we help security pros understand and develop a road map to implement a Zero Trust eXtended (ZTX) ecosystem.

Tags: Business & IT Alignment, Digital Business, Information Security, Technology, Zero Trust

Gartner Research

Market Guide for Zero Trust Network Access

Published: 29 April 2019

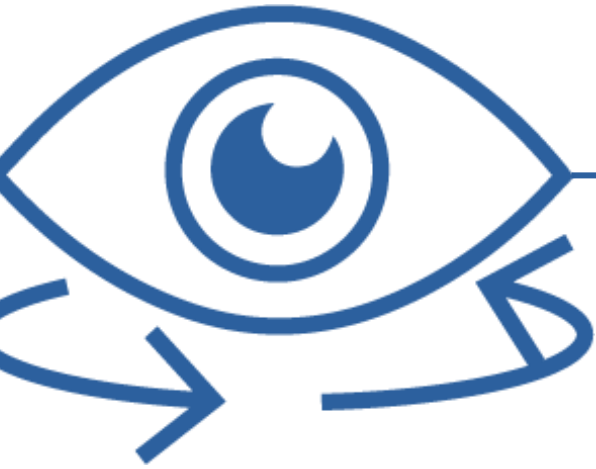
ID: G00386774

Analyst(s): Lawrence Orans , Neil MacDonald , Steve Riley

Summary

Zero trust network access replaces traditional technologies, which require companies to extend excessive trust to employees and partners to connect and collaborate. Security and risk management leaders should plan pilot ZTNA projects for employee/partner-facing applications.

The A10 Advantage



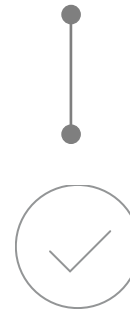
Visibility, Versatility with Performance

Highly Efficient &
Flexible



High Performance &
Versatility

Multi-Layered
Security Services



Added Security &
Control

Simple and
Easy to Use



Streamlined Configuration &
Detailed Analytics

Validated Security Partner Solutions



Cisco Firepower and
WSA



RSA Netwitness



Trend Micro
Deep Discovery



Fidelis Network



FireEye NX and EX series



Digital Guardian
Network DLP



OPSWAT
MetaDefender



McAfee Network
Security Platform (NSP)



Secureworks iSensor



IBM QRadar



Interface Masters
Network Bypass Switch



Check Point®
SOFTWARE TECHNOLOGIES LTD.

Check Point NGFW

Examples of Internal Threat Actors Enabling Attacks

A10

Always Secure. Always Available.

Example – Employee Data Exfiltration

- Anthem's Data Breach
- Employee had been stealing and misusing Medicaid member data for almost a year
 - Emailed files containing Anthem member data to personal email account
 - Included information like:
 - Medicare IDs
 - Social Security Numbers (SSN)
 - Health Plan IDs
 - Names
 - Dates of enrollment etc.

Example – Multi-Staged Attacks

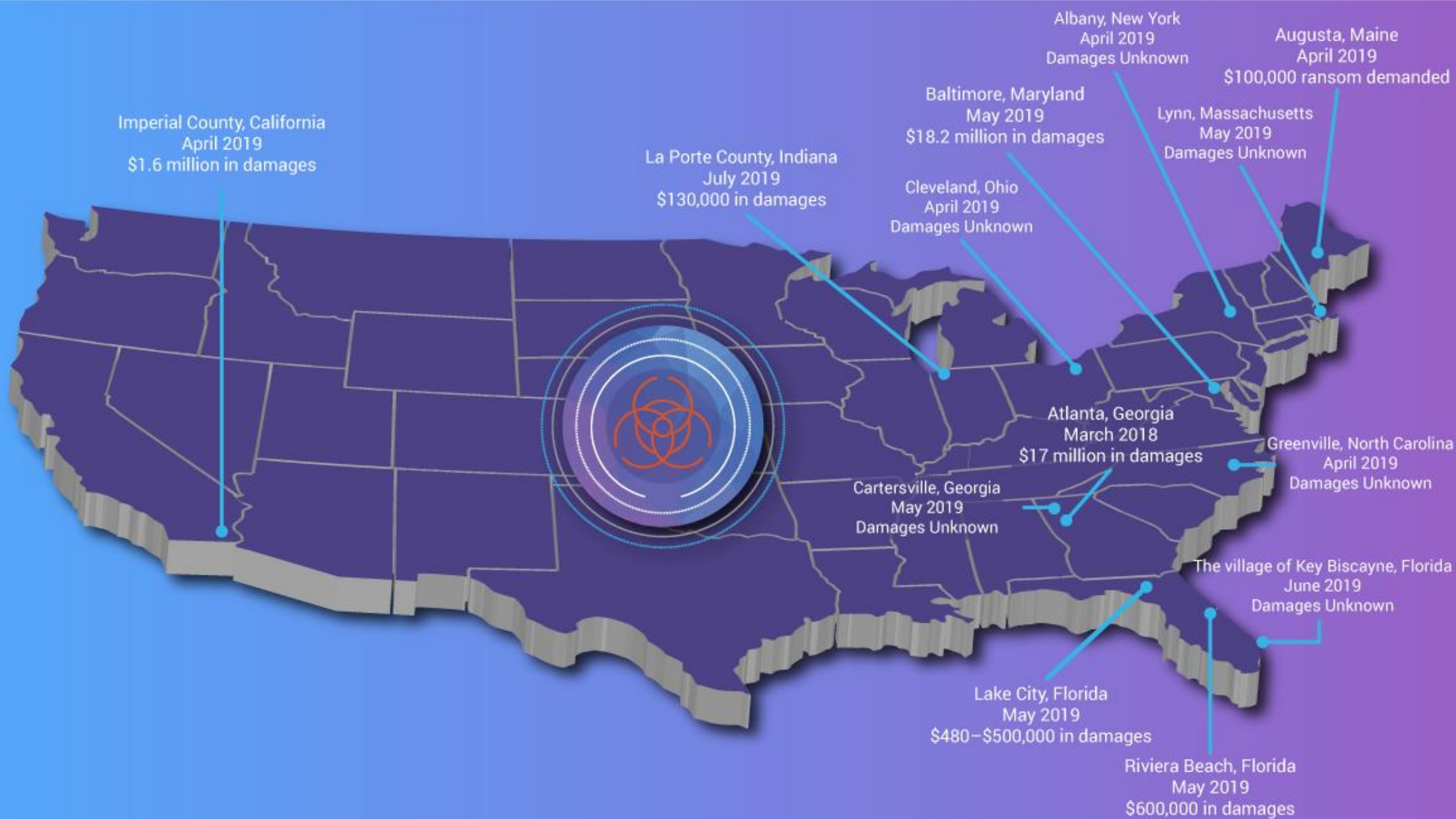
- Lake City, Florida Ransomware Attack
- City employee downloaded infected file via email
- Multi-staged attack which included:
 - **Emotet** Trojan which started the attack & downloaded,
 - **TrickBot** Trojan which downloaded and installed,
 - **Ryuk** Ransomware which encrypted critical files
- City paid a ransom of 42 bitcoins (\$500,000)

Example – Phishing Attacks

- RSA's Breach
- Employees fell for a targeted phishing attack
- Multiple hacker groups involved
 - Pretended to be trusted co-workers and contacts
- Led to a successful Advanced Persistent Threat (APT) attack
 - 40 million employee records were compromised

Example – Ransomware Attacks

- Riviera Beach, Florida Ransomware Attack
 - Employee of Police Department opened an infected email
 - Infected computers across the city's network
 - City government held a vote and paid a hefty ransom of 65 bitcoins (\$600,000)



Encryption Introduces a New Layer of *Complexity & Challenges*

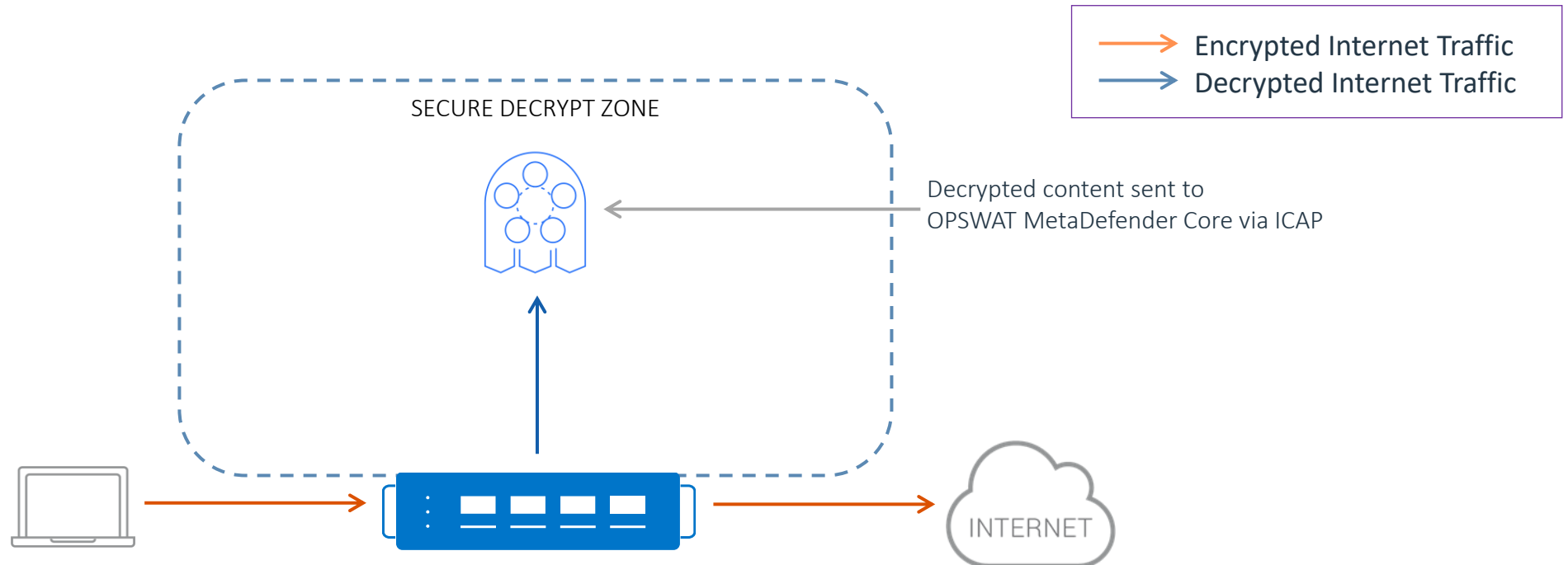
Multi-Layered Security Services

A10

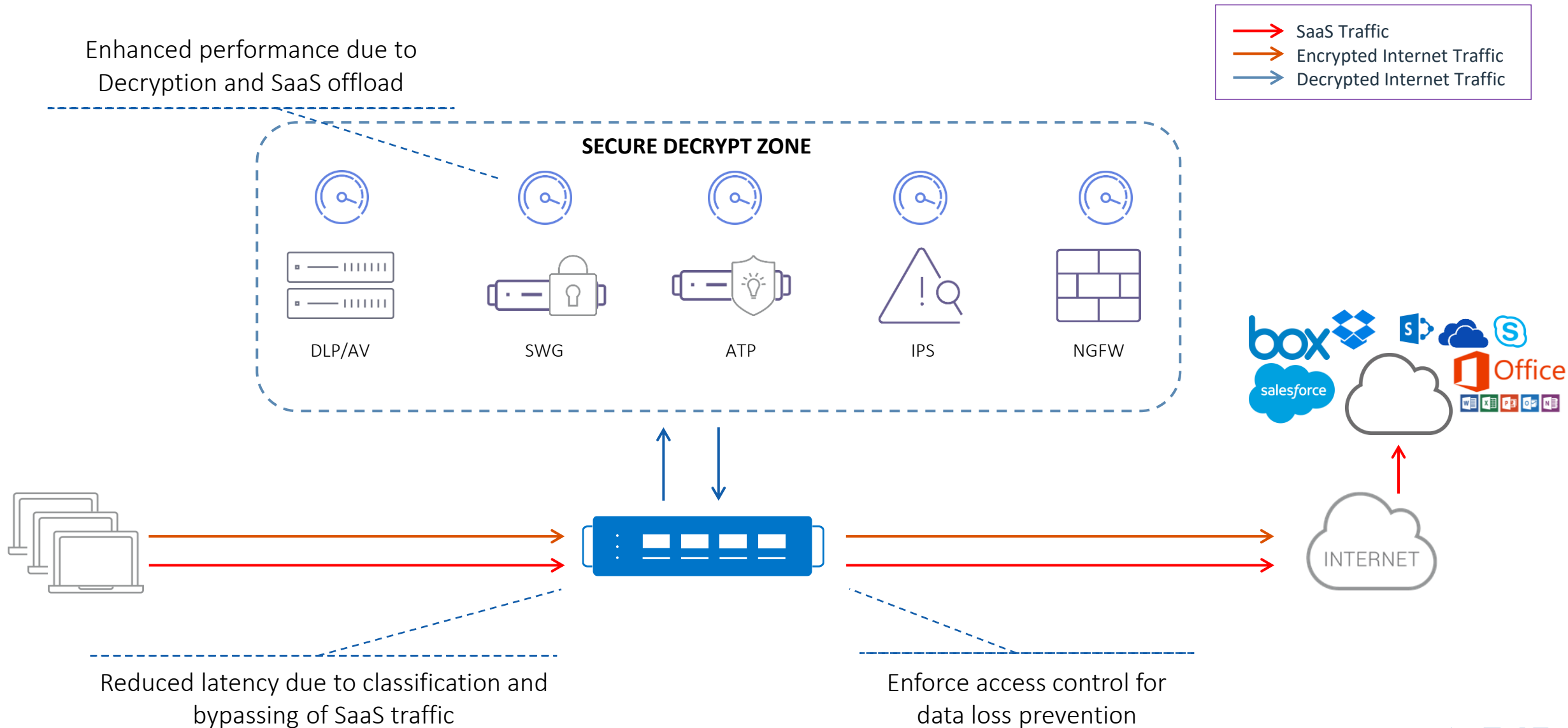
Always Secure. Always Available.

OPSWAT Integration for Malware Protection

- OPSWAT MetaDefender offers protection from content-based threats using:
 - Multi-scanning
 - Data Sanitization
 - Vulnerability Assessment and,
 - Data Loss Prevention



Local Breakout & Access Control for SaaS



Additional Case Studies

A10

Always Secure. Always Available.

Case Study – Reduced Traffic to DLP

Large, Integrated Health Care Organization

Challenges

- Required visibility for outbound traffic
- Moving from Cisco ASA, & WSA to PAN
- ICAP load balancing to 15 Symantec DLP sensors
- Issues with F5 (SSL Orchestrator, Herculon Version 13)
 - Orchestrator creates 14 separate iRules with 4,789 lines of logic
 - Config output for Orchestrator is 657 lines
 - Costly to upgrade HW, customer needs LIFETIME F5 PS

Business Impact

- Reduced traffic to DLP
- Reduced CapEx/OpEx
- Reduced risk and exposure to online threats
- Ease of use of URL bypass for operational transparency and regulatory compliance

Solution

- Thunder CFW
 - SSL Insight
 - URL Classification service

WHY A10

- Product maturity & go-to-market confidence (4+ years of product development)
- Market expertise deploying SSLi in complex environments
- Quick PoC response, set up in less than 10 days from initial meeting
- A10 Executive team participated early in the sales cycle, sharing the product roadmap, giving the customer additional confidence in A10 Networks

Case Study – Streamlined Security for Industrial Group

Customer – Borusan Holding

- EMEA, Turkey (Industrial Group)
- Borusan Holding, a \$4.8 billion company, is a leading industrial group based in Turkey and operates in 10 countries on three continents.

Challenges

- With web traffic volumes growing rapidly (+9000 users and 2,000 servers), the company needed better visibility into attacks hiding in encrypted traffic

Business Impact

- Gained complete visibility into encrypted web traffic across global operations
- Eliminated blind spots so security infrastructure could detect and stop hidden threats
- Streamlined security infrastructure
- Improved performance of security infrastructure by offloading compute-intensive decryption

Solution

- Thunder SSLi
 - TLS/SSL Decryption
 - Load Balancing



WHY A10

- Thunder SSLi decrypts traffic across all ports and multiple protocols, enabling third-party security devices to analyze traffic without degrading performance
- Leading interception technology, source-side NAT support, and provides integrated load balancing to help distribute Internet traffic between proxy appliances
- SSL traffic is centralized and can be managed from one device
- Integration of Thunder SSLi into the IT infrastructure was a smooth process

Case Study – Optimized SaaS for Better User Experience

Customer – Siam Commercial Bank (SCB)

- APAC, Thailand (Financial, Banking)
- SCB is Thailand's largest commercial bank (in total assets). They are also listed in the Forbes G2000.

Challenges

- Traditional proxies are neither designed nor optimized to address Office 365 traffic and can quickly become a bottleneck
- SCB had 3 Proxies, but with Office 365, they increased to 12 Proxies and the load continued to increase

Business Impact

- User experience is better and faster
- Optimized proxies

Solution

- Thunder CFW
- Cloud Access Proxy
- SaaS Traffic Optimization
- Tenant Access Control



WHY A10

- Easy to scale
- Network functions consolidation
- Better user experience and lower latency
- Auto update Office365 end-point
- Completed successful POC to prove capabilities

Differences Between Thunder SSLi and CFW (SWG)

A10

Always Secure. Always Available.

Definitions

- **SSL Insight**

- A10 Networks' outbound SSL/TLS decryption technology that is available on two separate product lines i.e. Thunder SSLi and Thunder CFW.

- **Thunder SSLi**

- A10 Networks' dedicated decryption product for enterprises, primarily focused on the SSL Insight technology.

- **Thunder CFW**

- A10 Networks' Convergent Firewall product. This product line also contains the SSL Insight technology for outbound decryption in an enterprise perimeter use case.
- Thunder CFW can loosely be defined as a super set of most of our other products including Thunder SSLi, ADC, and CGN.

Feature Comparison

Feature	Thunder SSLi	Thunder CFW
SSL Insight (Forward Proxy)	✓	✓
ADC	✗	✓
CGNAT	✗	✓
Integrated DDoS Protection	✗	✓
Firewall/DC Firewall	✗	✓
Gi/SGi Firewall	✗	✓
GTP Firewall	✗	✓
Site to Site IPsec VPN	✗	✓
Inbound SSL Decryption	✓	✓
WAF	✗	✓
DAF	✗	✓

Feature Comparison

Feature	Thunder SSLi	Thunder CFW
GSLB	✗	✓
RAM Caching	✗	✓
User Authentication (AAM)	✓	✓
aFlex Scripting	✓	✓
Dynamic Port Inspection	✓	✓
SSH, SCP, sFTP STARTTLS, SMTP, XMPP Decryption	✓	✓
Onboard HSM (FIPS 140-2 Level 3)	✓	✓

Services & Add-ons

Services / Add-ons	Thunder SSLi	Thunder CFW
URL Bypassing (Webroot)	✓	✓
URL Filtering (Webroot)	✓	✓
Application Visibility (Qosmos)	✗	✓
Threat Intelligence (Webroot)	✗	✓
Threat Intelligence (ThreatSTOP)	✓	✓
Threat Investigator (included with Webroot)	✓	✓

Deployment Options

Deployment Option	Thunder SSLi	Thunder CFW
Decrypt Once, Inspect Many Times	✓	✓
ICAP Support	✓	✓
Transparent Proxy Deployment	✓	✓
Explicit Proxy Deployment	✓	✓
Proxy Chaining	✓	✓
IP-less (Bump-in-the-Wire) Deployment	✓	✓
Layer 2 (Routed) Deployment	✓	✓
Layer 3 (Routed) Deployment	✓	✓
Firewall Load Balancing*	✓	✓

*Load Balancing up to 16 security devices in the secure decrypt zone

Management & Analytics Options

Management Options	Thunder SSLi	Thunder CFW
CLI	✓	✓
ACOS GUI	✓	✓
AppCentric Templates	✓	✓
Harmony Controller Apps	✓ (SSL Insight)	✓ (SSL Insight, CGNAT, GiFW and ADC)
Splunk App	✓ (SSL Insight)	✓ (SSL Insight, L4 FW and AppFW)