

# Enabling Full Visibility for Zero Trust Networks

SSL Insight and DDoS Protection Solution Overview

17<sup>th</sup> of June 2020

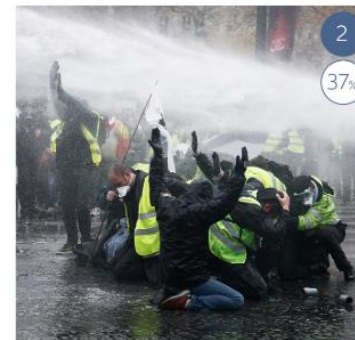
**A10**

Always Secure. Always Available.

# DIE WICHTIGSTEN GLOBALEN GESCHÄFTSRISIKEN 2020

Der Trend gibt die Änderung der Platzierung im Vergleich zum Vorjahr an.

Rang	Prozent	2019 rang	Trend
1 Cyber-Vorfälle (z.B. Cyberkriminalität, IT-Ausfall, Datenschutzverletzungen, Geldbußen und Strafen).	39%	2 (37%)	▲
2 Betriebsunterbrechung (inkl. Lieferkettenunterbrechung)	37%	1 (37%)	▼
3 Rechtliche Veränderungen (z.B. Handelskriege und Zölle, Wirtschaftssanktionen, Protektionismus, Brexit, Zerfall der Euro-Zone)	27%	4 (27%)	▲
4 Naturkatastrophen (z.B. Sturm, Überschwemmung, Erdbeben) <sup>1</sup>	21%	3 (28%)	▼
5 Marktentwicklungen (z. B. Volatilität, verstärkter Wettbewerb/neue Wettbewerber, M&A, stagnierende Märkte, Marktschwankungen)	21%	5 (23%)	◻
6 Feuer, Explosion	20%	6 (19%)	◻
7 Klimawandel/steigende Volatilität des Wetters	17%	8 (13%)	▲
8 Reputationsverlust oder Beeinträchtigung des Markenwerts	15%	9 (13%)	▲
9 Neue Technologien (z.B. Auswirkung der Vernetzung von Maschinen, Nanotechnologie, künstliche Intelligenz, 3D-Druck, autonome Fahrzeuge, Blockchain)	13%	7 (19%)	▼
10 Makroökonomische Entwicklungen (z.B. Sparprogramme, Anstieg der Rohstoffpreise, Deflation, Inflation)	11%	13 (8%)	▲
11 Politische Risiken (z.B. Krieg, Terrorismus, Aufruhr)	9%	11 (9%)	◻
12 Fachkräftemangel	9%	10 (9%)	▼
13 Stromausfälle bei kritischen Infrastrukturen (z.B. Unterbrechung der Stromleistungen) <sup>2</sup>	8%	17 (2%)	▲
14 Produktrückruf, Qualitätsmängel, Serienfehler	8%	12 (9%)	▼
15 Diebstahl, Betrug, Korruption <sup>3</sup>	7%	15 (7%)	◻
16 Umweltrisiken (z.B. Verschmutzung)	7%	14 (7%)	▼
17 Gesundheitsthemen (z. B. Pandemien)	3%	16 (3%)	▼
Andere	3%	-	-



- 1 Naturkatastrophen rangieren aufgrund der höheren Anzahl der Antworten höher als Marktentwicklungen (Prozentsatz ist gerundet).
- 2 Stromausfälle bei kritischer Infrastruktur rangieren aufgrund der höheren Anzahl der Antworten höher als Produktrückrufe (Prozentsatz ist gerundet).
- 3 Diebstahl, Betrug und Korruption rangieren aufgrund der höheren Anzahl der Antworten höher als Umweltrisiken (Prozentsatz ist gerundet).

Everything

heise online - IT-News, Nachrichten



vThunder1 VIP-S



heise o

VET

Aus e  
Jahr  
von L  
Servic

Home - dakoServ GmbH

https://www.dakoserv.de

Seiteninformationen - https://www.dakoserv.de/

Allgemein Medien Berechtigungen Sicherheit

### Website-Identität

Website: www.dakoserv.de

Besitzer: Diese Website stellt keine Informationen über den Besitzer zur Verfügung.

Validiert von: DigiCert Inc

Zertifikat anzeigen

Gültig bis: 16. April 2020

### Datenschutz & Chronik

Habe ich diese Website früher schon einmal besucht? Ja, 15 Mal

Speichert diese Website Daten auf meinem Computer? Ja, Cookies

Cookies und Website-Daten löschen

Habe ich Passwörter für diese Website gespeichert? Nein

Gespeicherte Passwörter anzeigen

### Technische Details

Verbindung verschlüsselt (TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, 128-Bit-Schlüssel, TLS 1.2)

Die Seite, die Sie ansehen, wurde verschlüsselt, bevor sie über das Internet übermittelt wurde.

Verschlüsselung macht es für unberechtigte Personen schwierig, zwischen Computern übertragene Informationen anzusehen. Daher ist es unwahrscheinlich, dass jemand diese Seite gelesen hat, als sie über das Internet übertragen wurde.



# Allgemeine

FAZ.NET

Gesellschaft Stil Rhein-Main

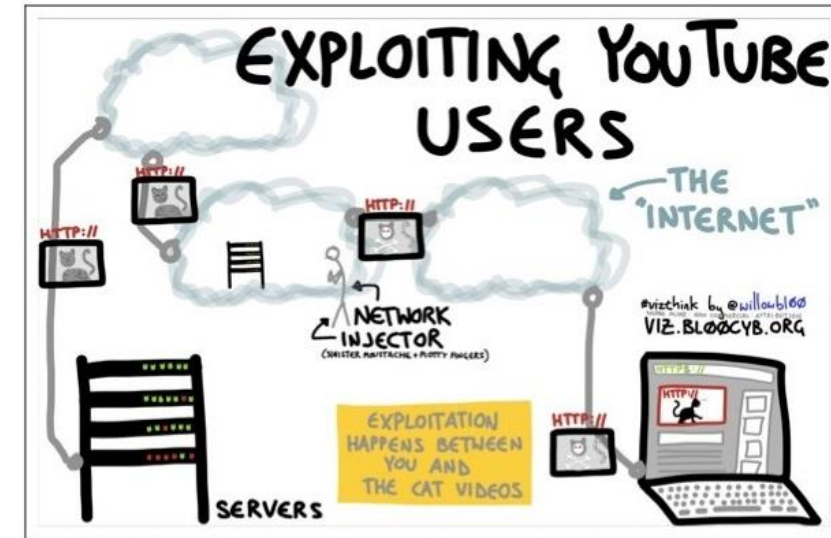
al | Do Not Distribute

3

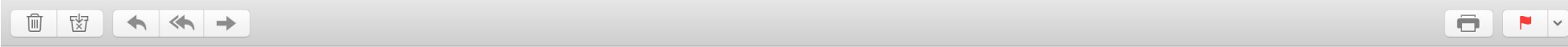


# Reason for SSL

- Snowden revelations of NSA snooping
- Disclosures in 2014 that governments were injecting surveillance software in web traffic
  - YouTube and Microsoft Live used as conduits to inject malware
  - Both now encrypt traffic
- Google ranks SSL sites higher for SEO
- RFC 8446 TLS 1.3 introduced by Mozilla



# Increasing Threats



G.M.X

GMX-Sie wurden ausgewählt {heiko.frank} !

An: Heiko Frank

Eingang - Gmx    Vorgestern um 10:37



**Sehr geehrter GMX-Kunde,**

**Sie wurden für eine exklusive Belohnung ausgewählt**

Haben Sie 30 Sekunden Zeit, um uns Feedback zu geben?

Als geschätzter Kunde möchten wir unseren Service in diesem Jahr weiter verbessern! Wir bieten eine tolle und exklusive Belohnung! Um sich für dieses Sonderangebot zu qualifizieren, müssen Sie lediglich unsere 30-Sekunden-Marketingumfrage über Ihr Sparerlebnis ausfüllen

**NEHMEN SIE DIE UMFRAGE JETZT**

<http://korturl.dk/03rp>

Um diese zu stoppen, gehen Sie bitte [hier](#)

# Cyber Crimes are on the Rise!



**\$3.92 M**

Average cost of a  
Data Breach



**650%**

Increase in  
Trojan-based  
malware threats



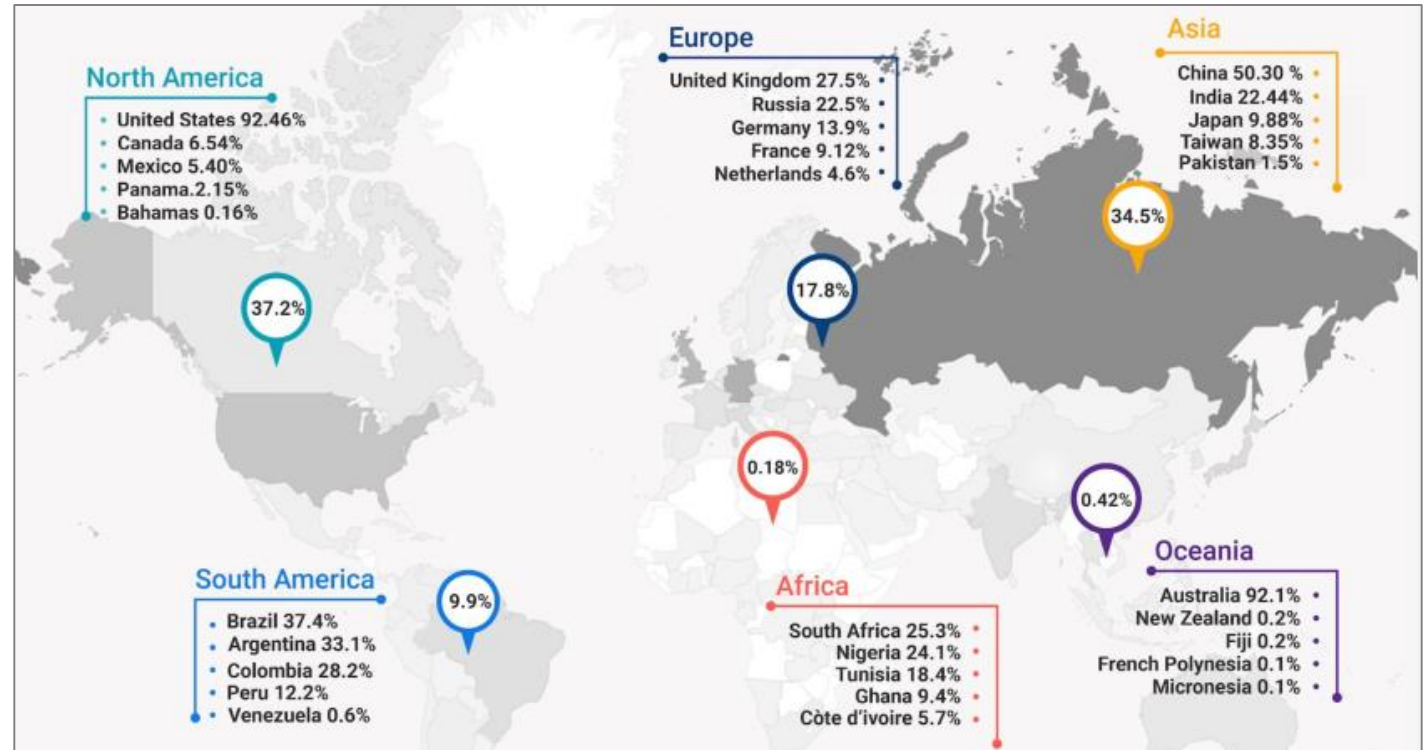
**90%**

Breaches caused by  
Phishing

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

# Impact of Data Breaches

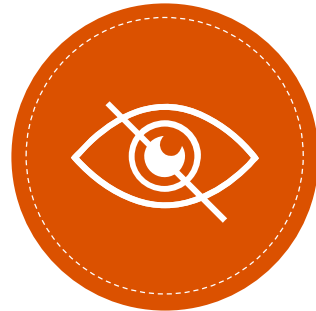
- Ransom
- Lost revenue
- Brand damage
- Regulatory fines e.g. GDPR
- Investigation costs
- Lawsuits



*Data Breaches can happen anywhere, at any time*

# Encryption Introduces New Challenges & Complexity

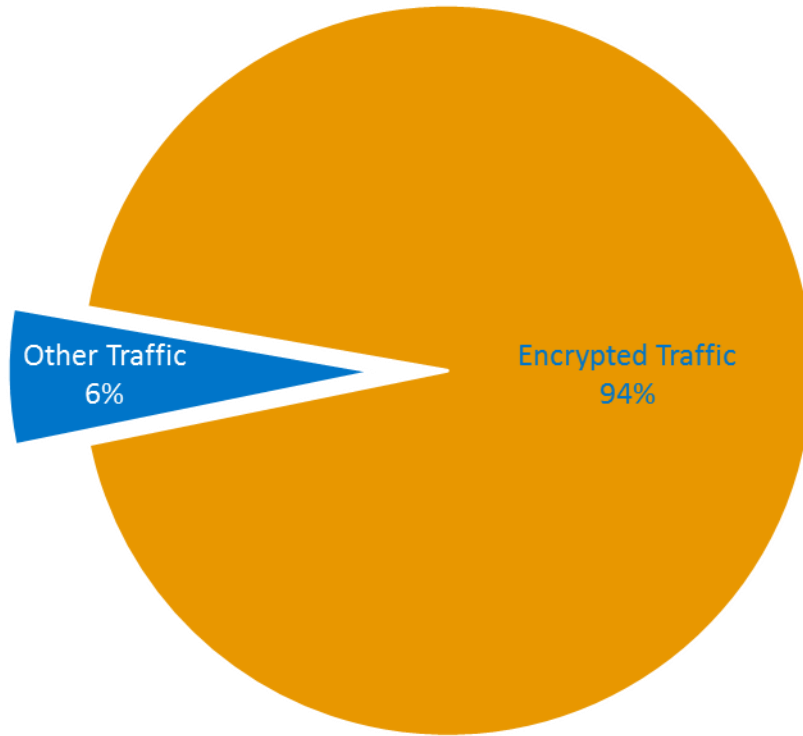
*Encryption gives you **Privacy***



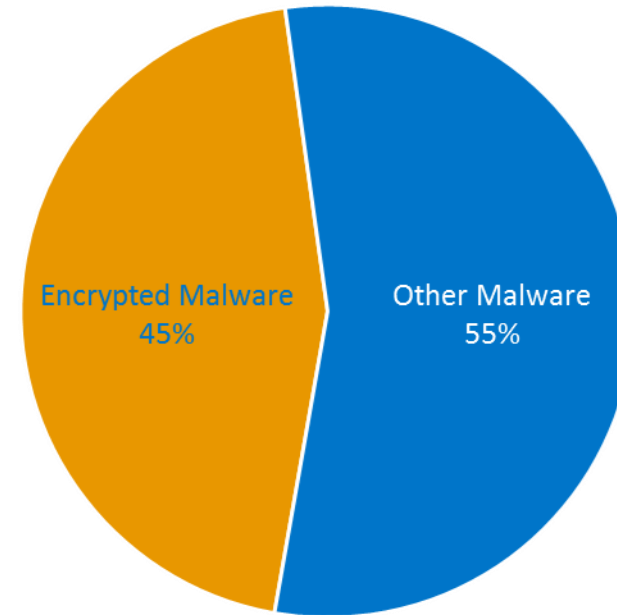
*But it can hurt your **Security***



# Exploiting The Growing Encrypted Blind Spot



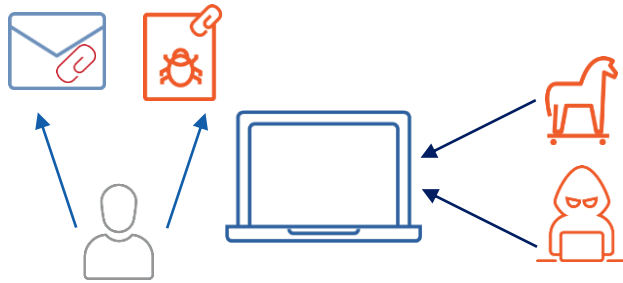
94% of all internet traffic is encrypted



Almost half of cyber attacks use encryption to evade security

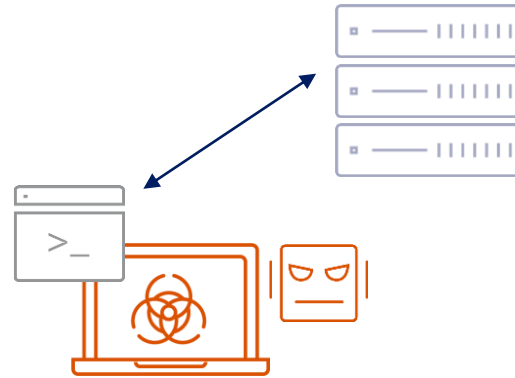
# Encryption Makes Traditional Defenses Ineffective

## 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*

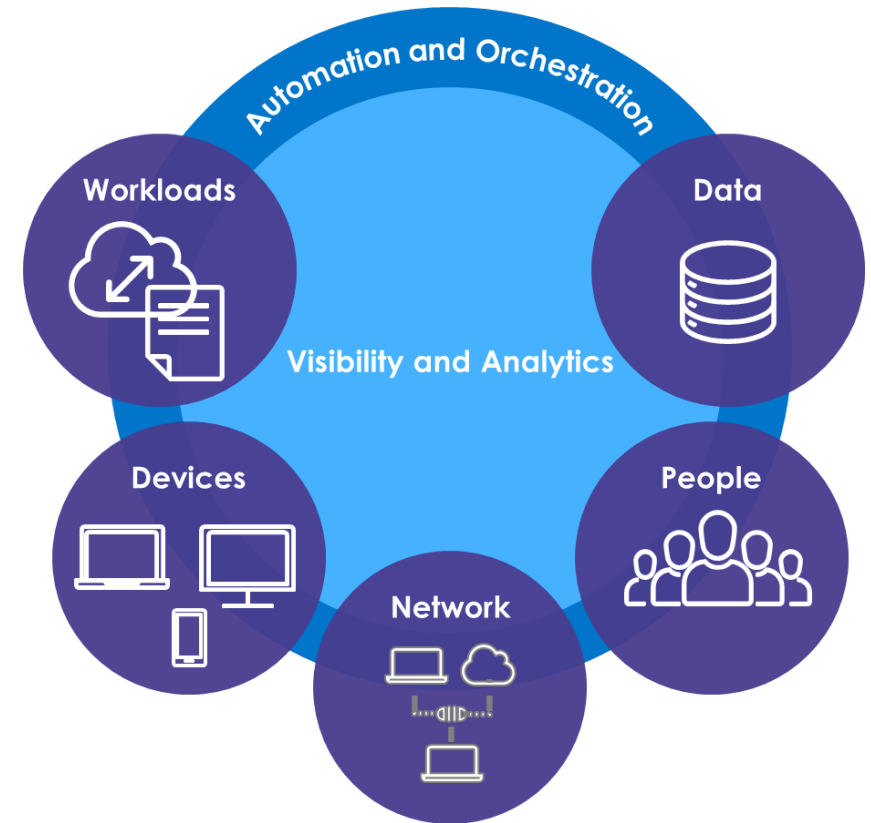
# Zero Trust Aims to Solve These Security Issues

- 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

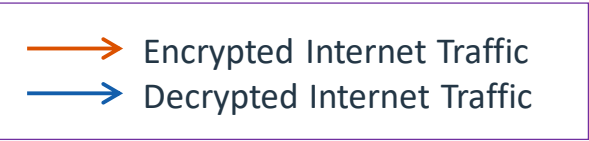
- “Trust Nobody”
  - Redesign networks into secure **micro-perimeters**
  - Limit **excessive user privileges**
  - Improve detection and response times through **analytics and automation**
  - Enable **compliance**
  - Improve security detection and response with **centralized visibility & control**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



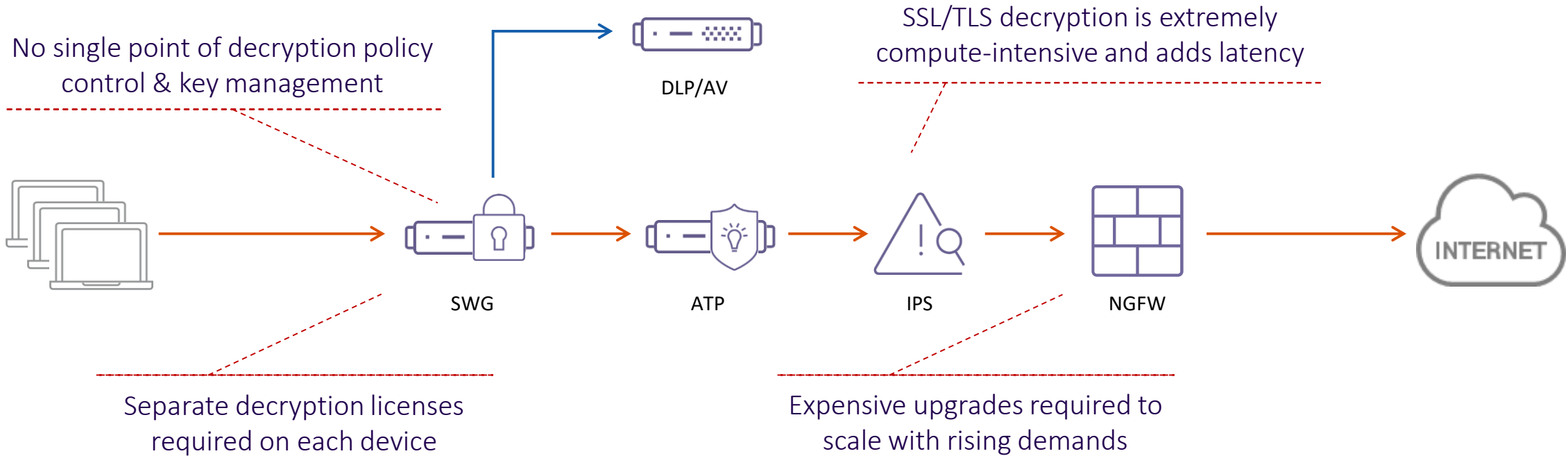
Zero Trust Model Will Also Fail Without Decryption Because

**Visibility Is Key**

# Decryption Scale and Security Problems



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?*

# “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<sup>®</sup>

**A10**

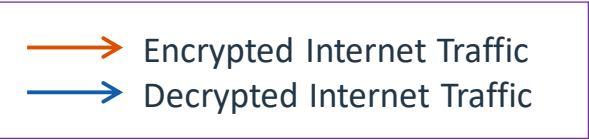
Always Secure. Always Available.

# SSL Insight is at the Core of the Zero Trust Model

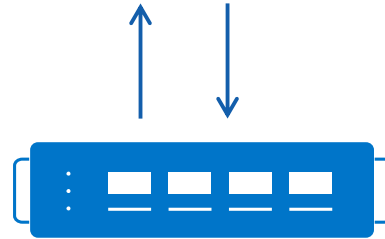
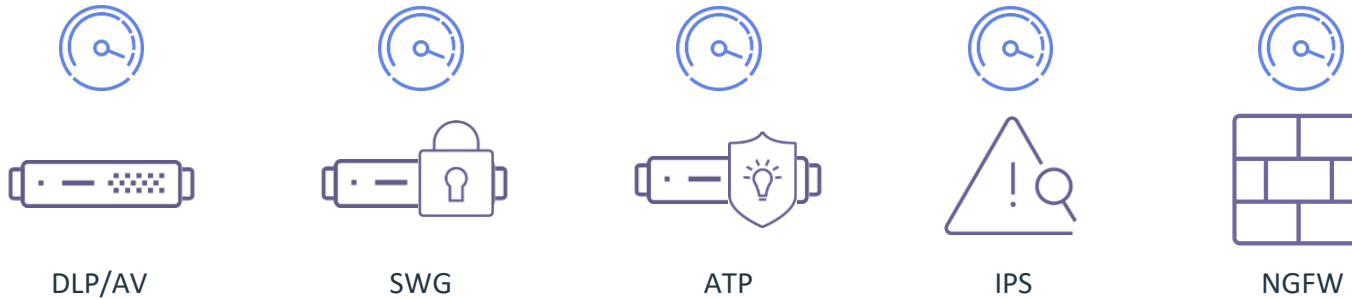
- With most of internet traffic being encrypted, SSL Insight enables other Zero Trust security devices and improves their efficacy
- Multi-Layered Security Services:
  - Enable compliance
  - Restrict and scrutinize user access
  - Provide consolidation of multiple security services in one platform
- “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

Enhanced performance due to  
Decryption/Re-encryption offload



## SECURE DECRYPT ZONE



Improved user experience due to  
reduced latency

Centralized decryption, policy control  
and key management

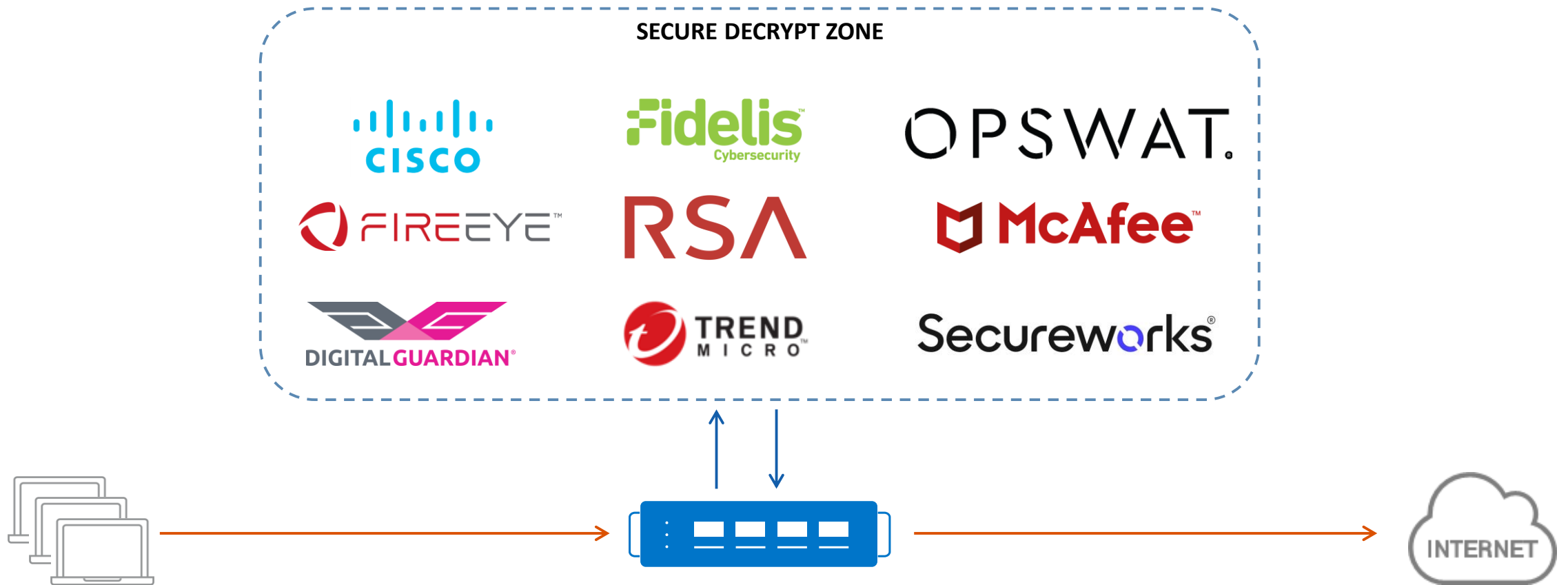
# Full Traffic Visibility

- 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*

# Multi-Layered Security Services



*Application  
Firewall*

*Threat  
Investigator*

*URL & Web  
Filtering*

*ICAP  
Integration*

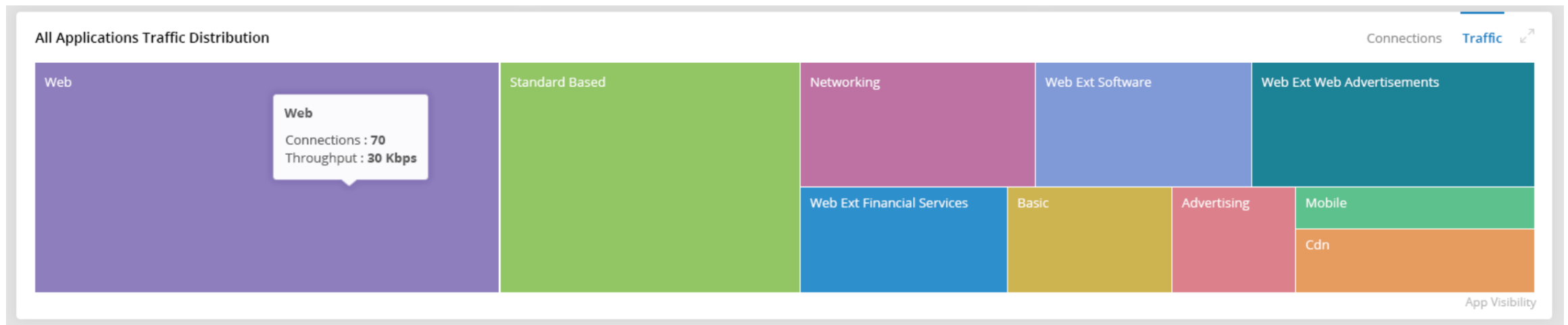
*Threat  
Intelligence*

*User ID Based  
Traffic Filtering*

*...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





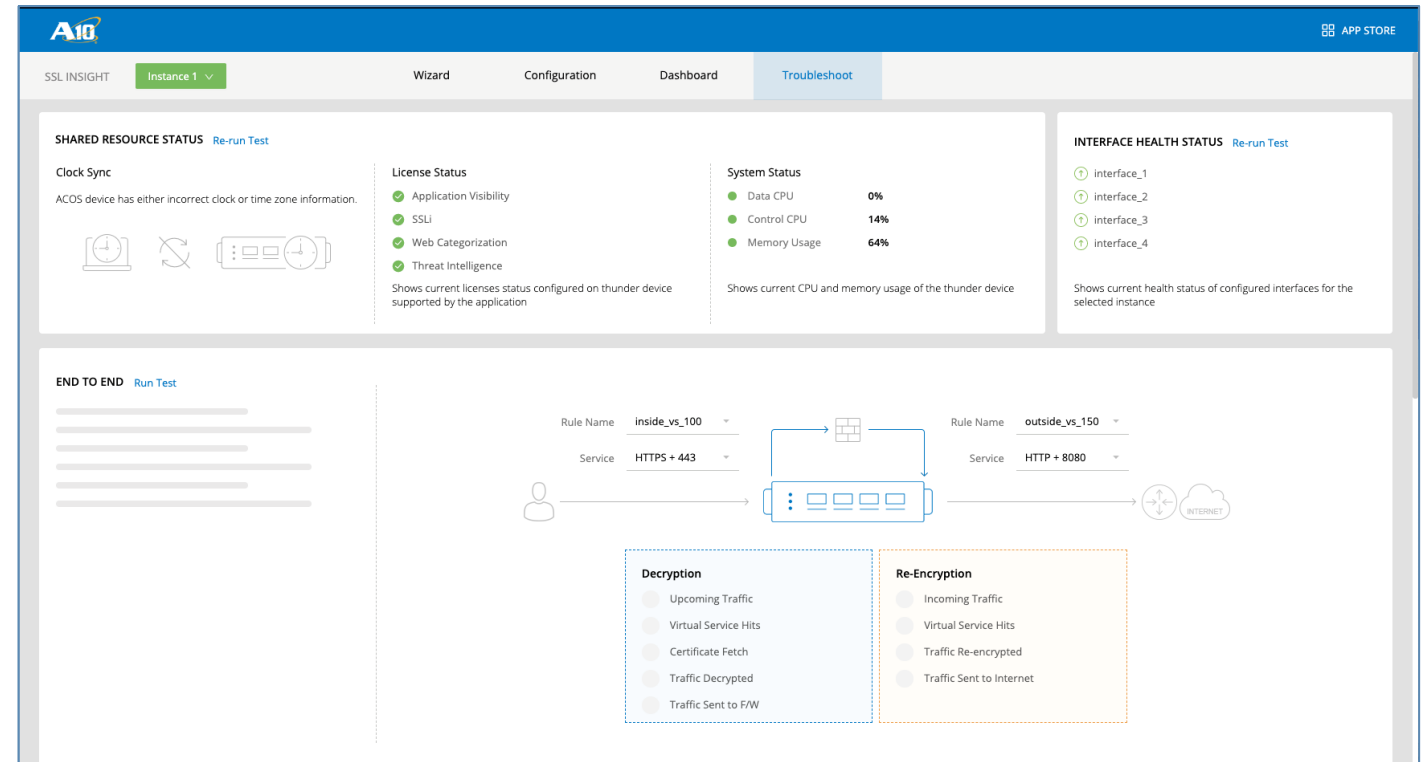
# Analytics & Ease of Use

**A10**

Always Secure. Always Available.

# Simple and Easy to Use

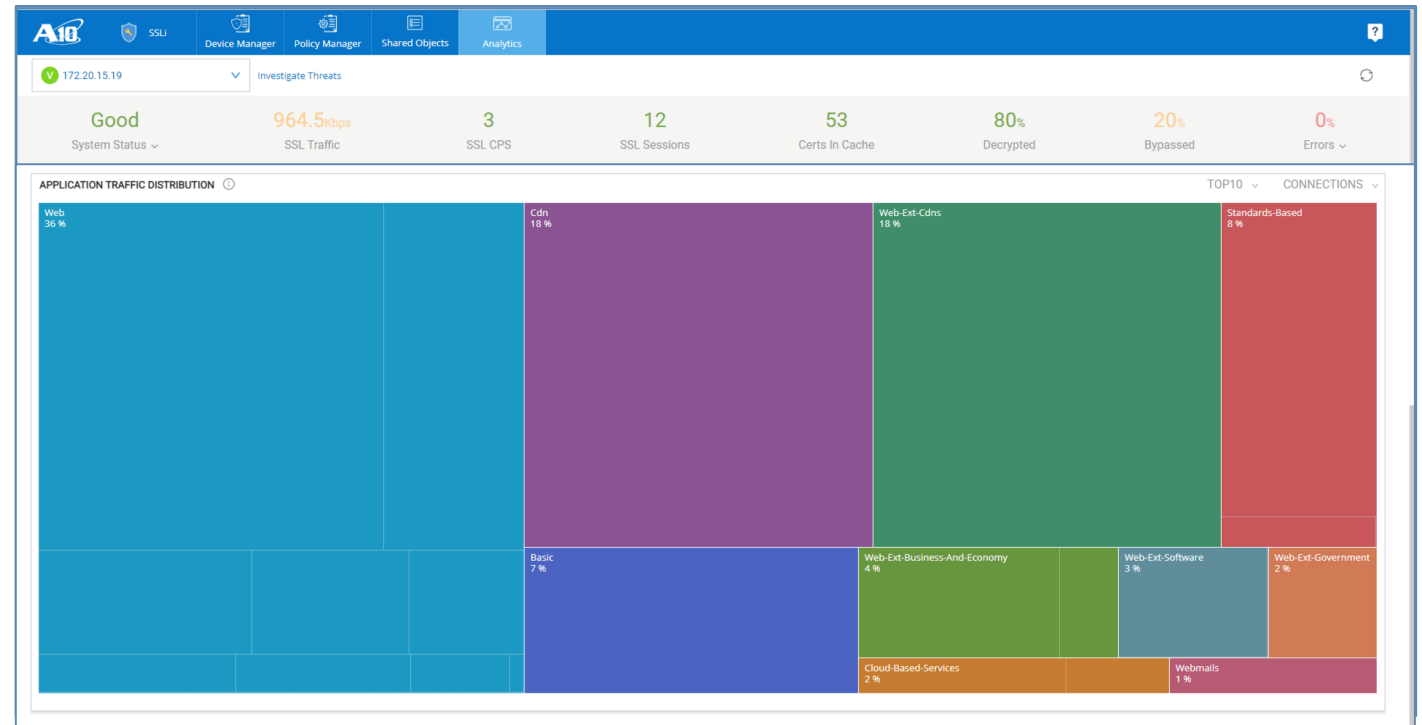
- AppCentric Templates
  - Streamlined Wizards
  - Wider coverage of use cases
  - Configuration Dashboard
- 3-step configuration
- Streamlined, single device deployments
- Simplified, wizard-based troubleshooting



Configuration Dashboard Help step wizard for selecting configuration before making edits

# Centralized Management and Visibility

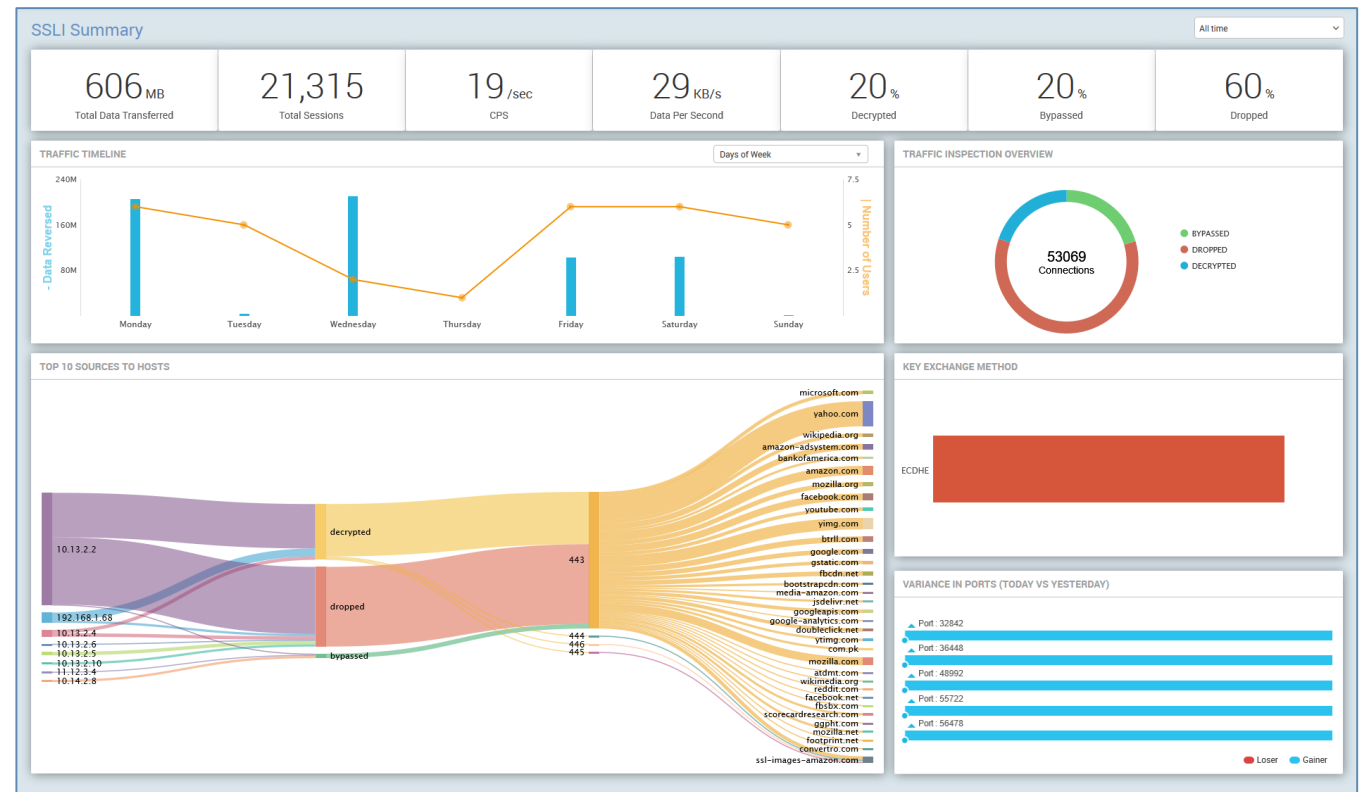
- Harmony Controller SSLi App
  - Streamlined Wizards
  - Device and Policy Manager
  - Wider coverage of use cases with shared objects
- Multi-device, Multi-site deployments
- Enhanced operational efficiency



The dashboard can be used to monitor and manage SSL traffic across multiple devices and device groups, providing a centralized view of SSL traffic and allowing for the application of policies to 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



# ...but back to the Risk

The screenshot shows the ALDI SUISSE website interface. At the top left is the ALDI SUISSE logo. The main navigation bar includes links for 'Aktionen', 'Sortiment', 'Rezepte', 'Infos', 'Services', 'Über uns', and 'Nachhaltigkeit'. The 'Services' link is highlighted in yellow. In the top right corner, there are buttons for 'Deutsch' and 'Einkaufsliste'. Below the navigation bar, a breadcrumb trail reads: 'Sie befinden sich hier: ALDI SUISSE - Start → Services → Serviceportal → IP Überwachungskamera'. A secondary navigation bar contains buttons for 'letter', 'ALDI SUISSE App', 'Erinnerungsservice', 'Geld-zurück-Garantie', 'Apple Pay', 'Serviceportal', and 'Schweizweite Heimlieferung'. The main content area features an advertisement for 'IP Überwachungskamera' (IP surveillance camera). The ad includes the text 'Neueste Updates zum Schutz vor fremden Zugriff verfügbar!' (Latest updates for protection against unauthorized access available!) and an image of a black camera on a desk next to a laptop displaying a multi-camera feed and a smartphone. A dark blue box on the right side of the ad contains the text 'IP Überwachungskamera'. At the bottom of the ad, there is a blue button labeled 'Beschreibung' (Description).

# World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices

Tuesday, September 27, 2016 Swati Khandelwal

G+1 123 Like 11K Share 9757 Tweet 1137 in Share 639 Share 11.9K



Do you know — Your Smart Devices may have inadvertently participated in a record-breaking largest cyber attack that Internet has just witnessed.

ALLEN VAULT  
Beginner's Guide to Hybrid Cloud Security: From the Data Center to the Cloud  
DOWNLOAD NOW >

Lernen Sie Ihr neues WebEx kennen.  
cisco WebEx  
Kostenlos registrieren

Cookies erleichtern die Bereitstellung unserer Dienste. Mit der Nutzung unserer Dienste erklären Sie sich damit einverstanden, dass wir Cookies verwenden. [\[mehr Informationen\]](#) [OK](#)



YOUR READING LIST



Here's How Allegedly F Samsung S -- And How Protect Yo

Workday V The Innov The Cataly Driving Di Transform

LISTEN N Creative B And Badas In STEM



# CIA macht Samsung Smart TV zu Wanzen

BASTIAN EBERT am Mittwoch, 8. März 2017

Advertisement for freenetmobile: freeFlat ab 13,95 € freeFLAT 2000: 2 GB LTE im D-Netz und Allnet-Flat\* freenetmobile.de

DAS NEUE IPHONE 7 UND 7 PLUS



Das neue iPhone 7 (plus) mit und ohne Vertrag im Überblick:

# What is the Problem?

**A10**

Always Secure. Always Available.





PEW!  
PEW!

VS.



DDoS 2015  
100 Gbps

DDoS 2018  
Billion/IoT

# The World We Live In

**DO YOU KNOW THIS MAN?**



John Kelsey Gammell

“FBI convicted a Minnesota man for launching hundreds of DDoS attacks ... former employers and business partners”

vDOS

<- Paid: **\$652.87**

-> “30Gbps of Dedicated Bandwidth” and “Unlimited Boots.”

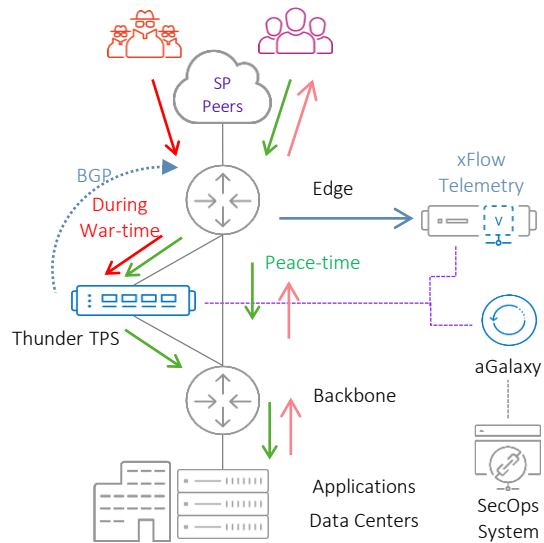
Source: [bleepingcomputer.com](http://bleepingcomputer.com) and Minnesota Star Tribune, Nov 6, 2017  
<https://www.bleepingcomputer.com/news/security/man-uses-ddos-for-hire-services-to-attack-former-employer-taunts-firm-via-email/>  
<http://www.startribune.com/hacker-for-hire-cases-going-federal-in-minnesota/455624163/>

## BUSINESSES ATTACKED:



# Most Common Use Cases

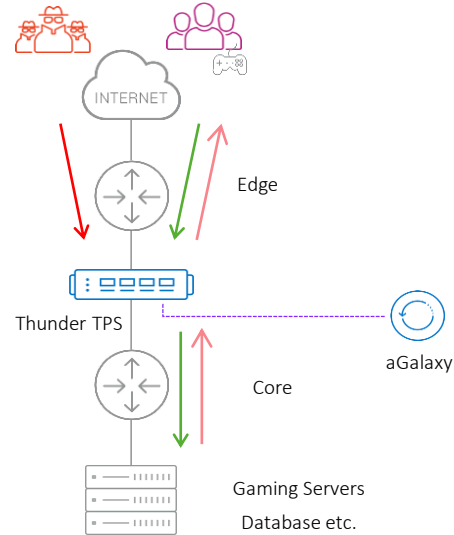
## Service Provider



- Reactive infrastructure protection
- Proactive DNS, SIP, HTTP/S, GRE protection
- Automatic BGP announcements
- REST API SecOps system integration

Infrastructure & Critical App. Protection

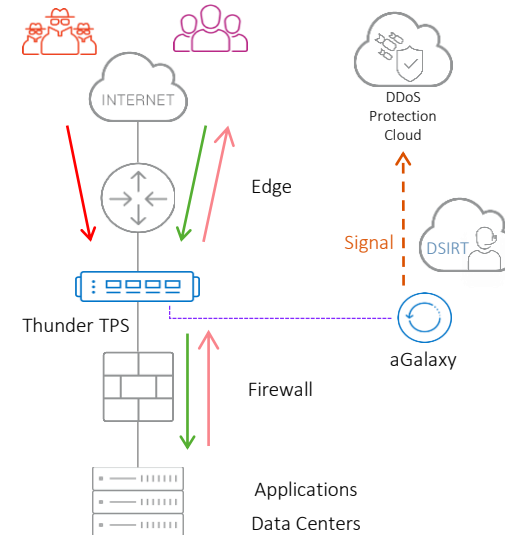
## Gaming



- Real-time proactive protection
- Full spectrum, sub-second mitigation
- Zero-trust security posture
- DDoS and Cheater blocking

Player Experience Protection

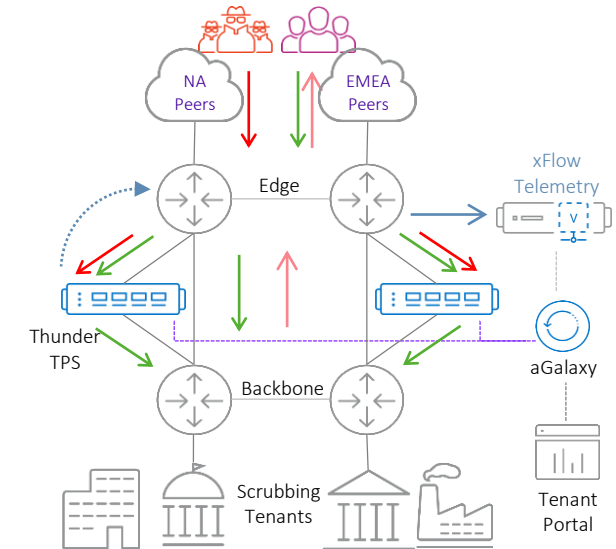
## Enterprise



- Always-on protection
- Multi-vector protection
- DDoS Protection Cloud integration
- Application availability assurance

Hybrid Application Protection

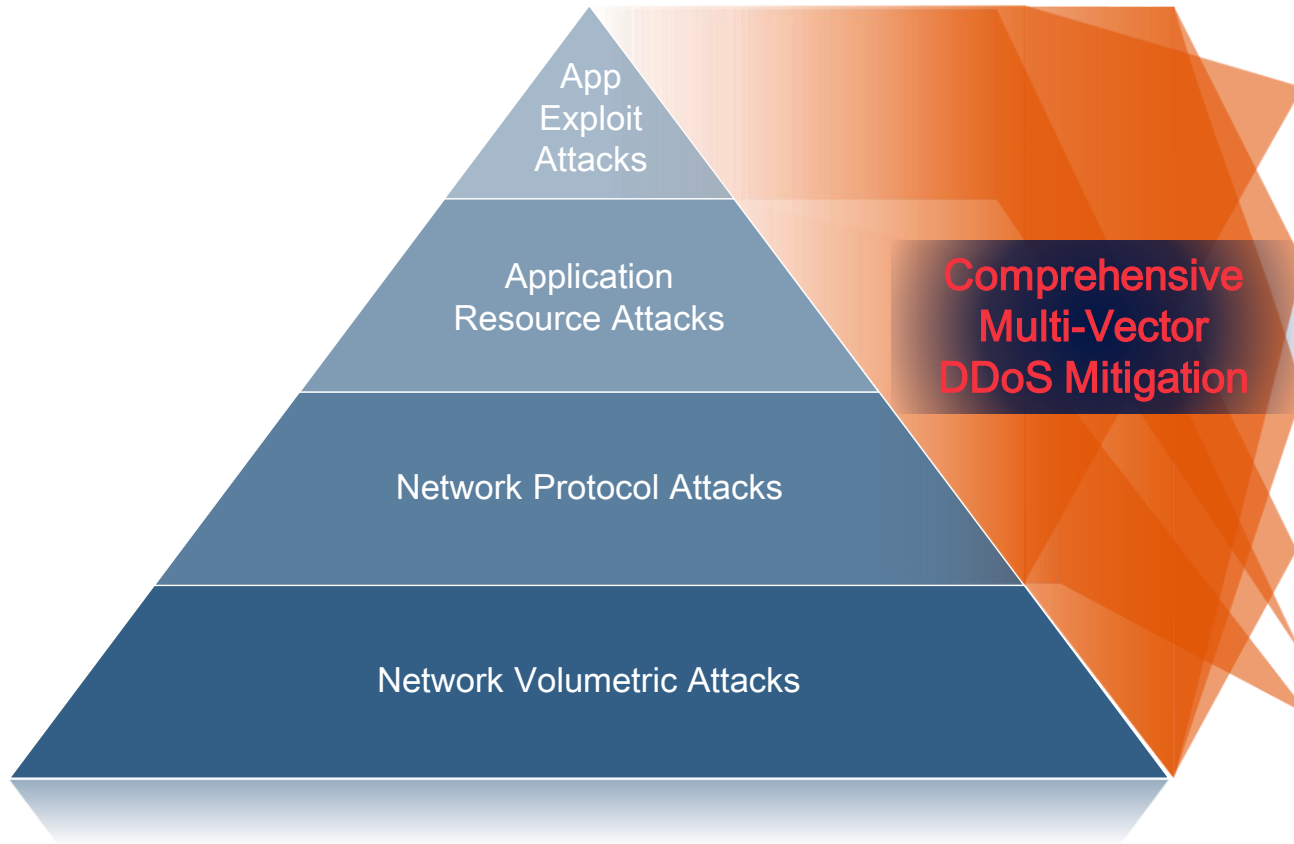
## MSSP



- Highly scalable tenant protection
- Profit driven on-demand, auto-reactive, and always-on services
- Robust tenant reporting

Multi-tenant Protection

# Mitigating DDoS Attacks Using Thunder TPS Series



**Behavioral Policies & Content Signatures**  
Thwart malicious behavior and surgically target content patterns

**Challenge-Based Authentication**  
Identify malicious from legitimate clients

**Black and White Lists**  
High-scale source-based admission control

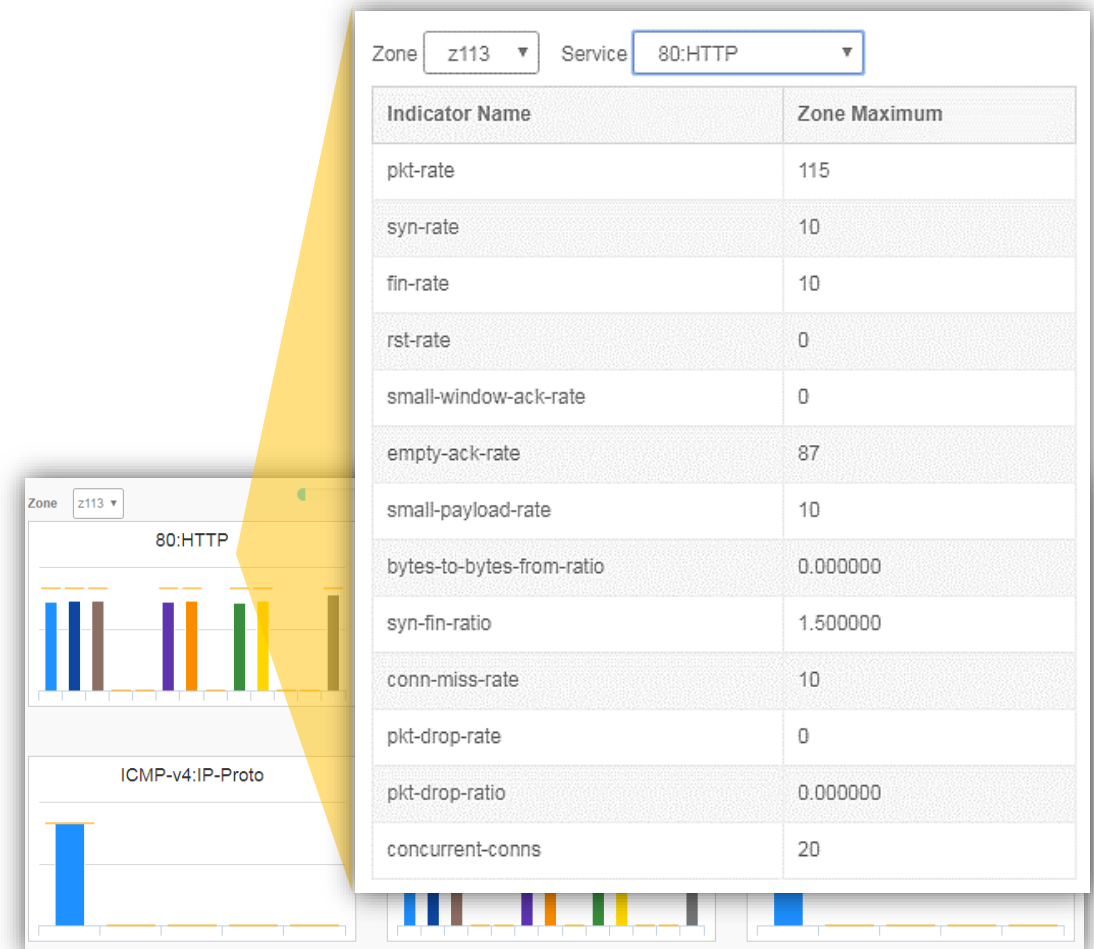
**Traffic Rate Control**  
High-granularity traffic rate enforcement

**Packet/Request Anomaly Check**  
Validate incoming packets & requests

# Precise DDoS Detection

- Understanding traffic characteristics better is the key
- Baseline for individual protected service-port
  - Automatically builds behavioral traffic profile in learning mode, or manual entry
  - Traffic profile = detection threshold
- Monitoring multiple protocol indicators in addition to typical packet or bit indicators (pps or bps)
  - Protocol indicators provide better visibility to traffic characteristics and improve detection precision

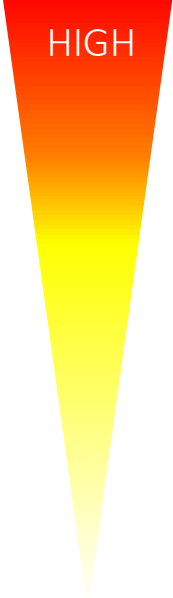

*Baselining for HTTP service port  
(13 indicators)*



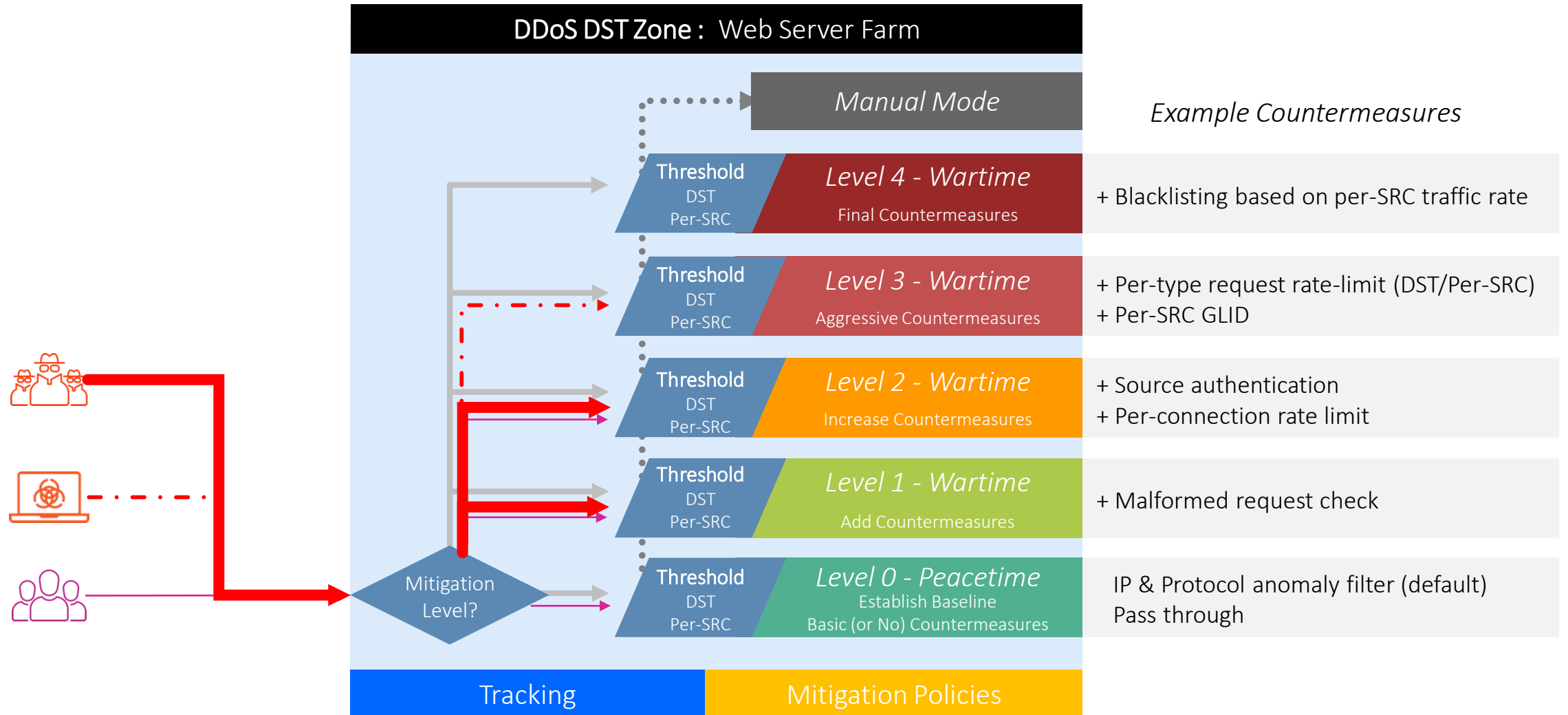
Baselining & Anomaly Detection



# DDoS Attack Mitigation Strategies

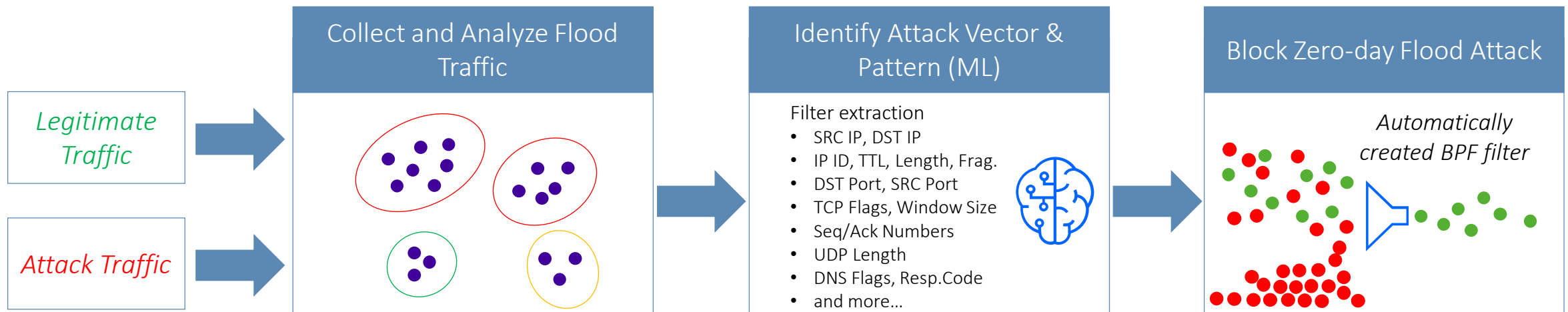
Potential impact on valid users	Commonly used countermeasures	Technical complexity	A10's Surgical Mitigation
 <p>HIGH</p>	Blackholing / RTBH Destination rate limit/ traffic shaping IP reputation/Geo-based blacklist		<i>Precise tracking &amp; anomaly detection using extensive indicators</i> <ul style="list-style-type: none"> <li>Catch any type of traffic anomaly</li> <li>Monitor destination or per-source basis</li> </ul>
None	<div style="background-color: #0056b3; color: white; padding: 5px;">             A10's Strength           </div> IPS attack pattern filter Per-SRC rate limit/ traffic shaping L4-7 behavioral policy violation with rate limit L4-7 behavioral policy violation with SRC blacklist Application malformed request check Advance L7 challenge authentication Automatic attack pattern recognition L4 source (SRC) authentication		<i>Breadth &amp; cutting edge L4-7 countermeasures</i> <ul style="list-style-type: none"> <li>Distinguish users and attackers</li> <li>Verify application/ protocol behavior</li> <li>Limit/ drop only attack traffic</li> </ul>
	Protocol misuse & anomaly check Block/rate limit amplification attacks Packet anomaly check		<i>Machine-learning, zero-day automated protection</i> <ul style="list-style-type: none"> <li>Precise pattern filter</li> <li>Increase mitigation accuracy</li> </ul>
<b>How To Apply Those Countermeasures?</b>			<i>Auto-escalation, multi-stage mitigation rules</i> <ul style="list-style-type: none"> <li>Minimize false-positive by applying basic through aggressive countermeasures progressively</li> </ul>

# Zone: Auto-Mitigation & Managing Threat Levels



# Zero-day Automated Protection - ZAPR filter

- Zero-day protection powered by **Unsupervised Machine Learning**
  - Dynamic DDoS attack pattern recognition
  - **Automatic** BPF filter creation\*
  - No SecOps admin input required
- Capable of **extracting filters** from zero-day attack and emerging attack
- Best suited for **blocking volumetric DDoS attack**, such as SYN-ACK flood
- Easy setup and operation via aGalaxy-TPS
- Combining other countermeasures to enforce precise surgical mitigation



\*BPF filter is also presented in human readable lexical format.



# COLOSSAL

DDoS Attacks Loom

Defeating DDoS Needs a Precision Strategy





# Thank You

**A10**

Always Secure. Always Available.