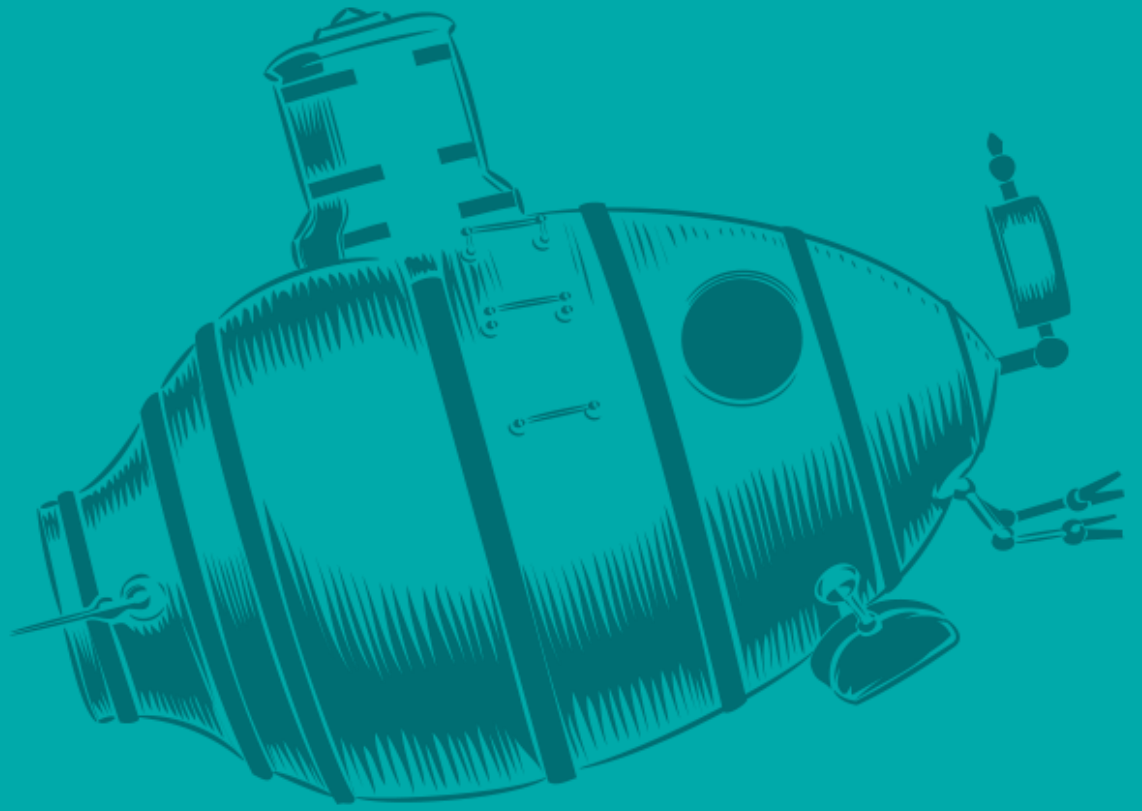
ALEF

ALEF Academy

online



Michal Motyčka
michal.motycka@alef.com

Lukáš Beňo
lukas.beno@alef.com

Co vás čeká?

BLOK 1

- F5 jako několik samostatných řešení
- Kampaně 2020

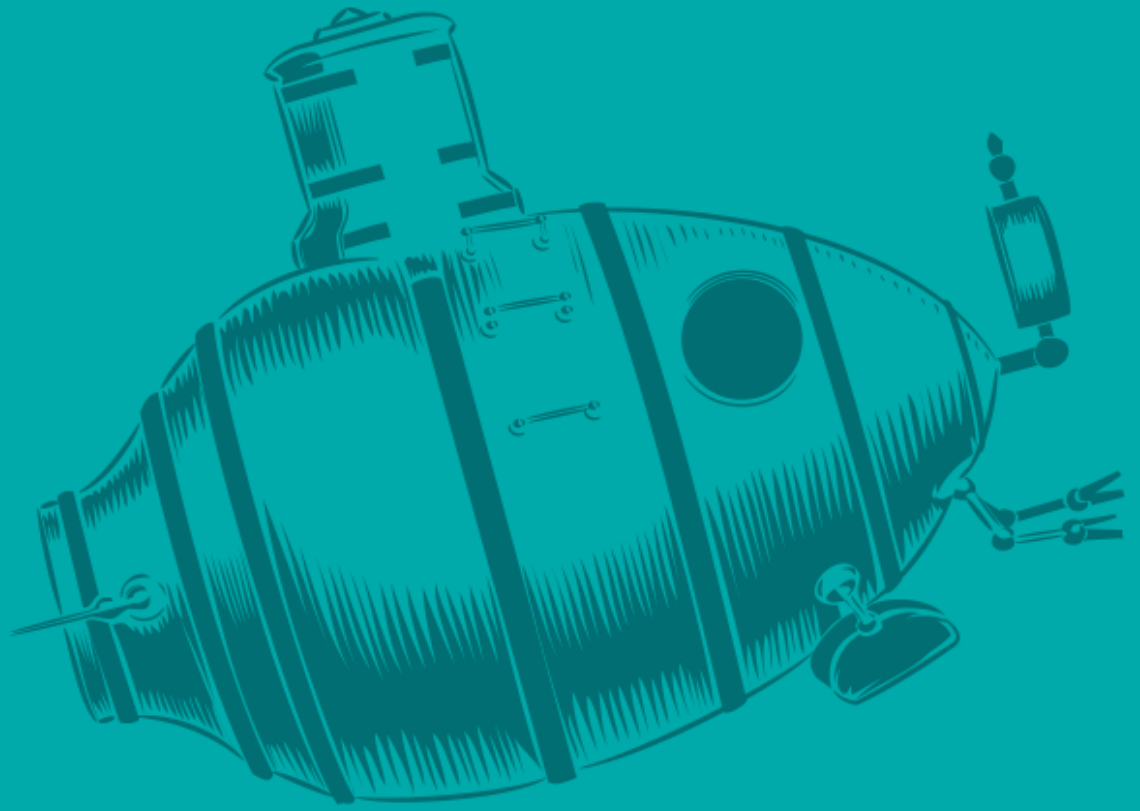
BLOK 2

- Vertikály zákazníků + use case

ALEF

ALEF

F5 jako několik samostatných řešení



Michal Motyčka
michal.motycka@alef.com

Lukáš Beňo
lukas.beno@alef.com

8,5 aplikace za dopoledne

Jak vypadá ideální aplikace?

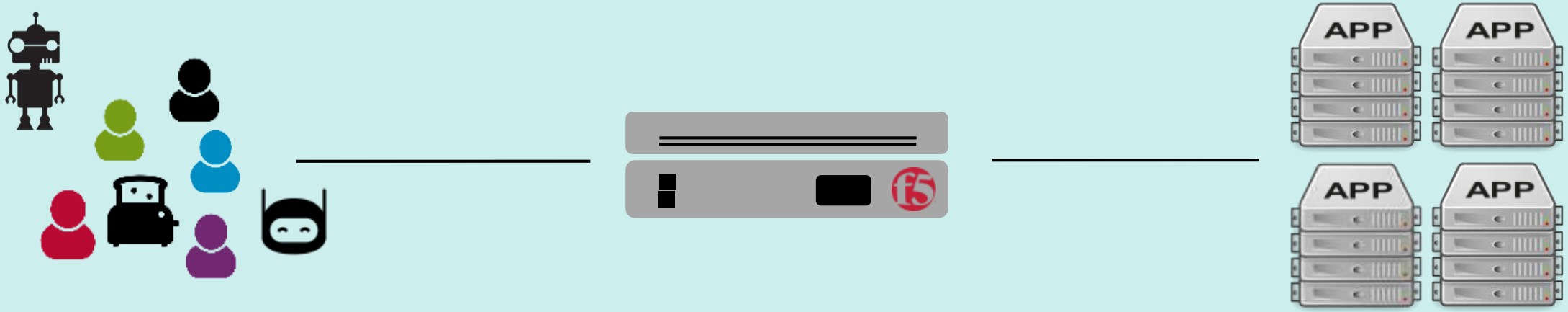
RYCHLÁ A SVIŽNÁ

VŽDY DOSTUPNÁ

BOHATÁ GRAFIKA

BEZPEČNÁ

PLNÁ FUNKCÍ

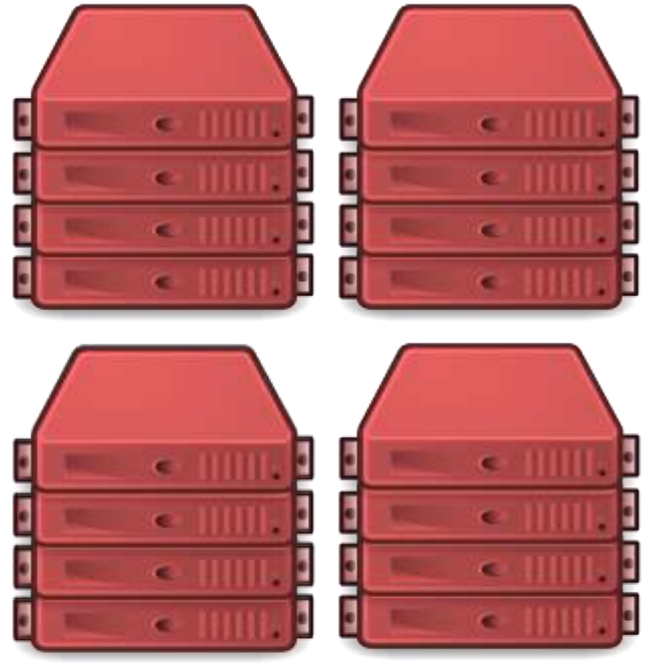

APP
APP
APP
APP

Řešení

Odezva aplikace, vysoká dostupnost

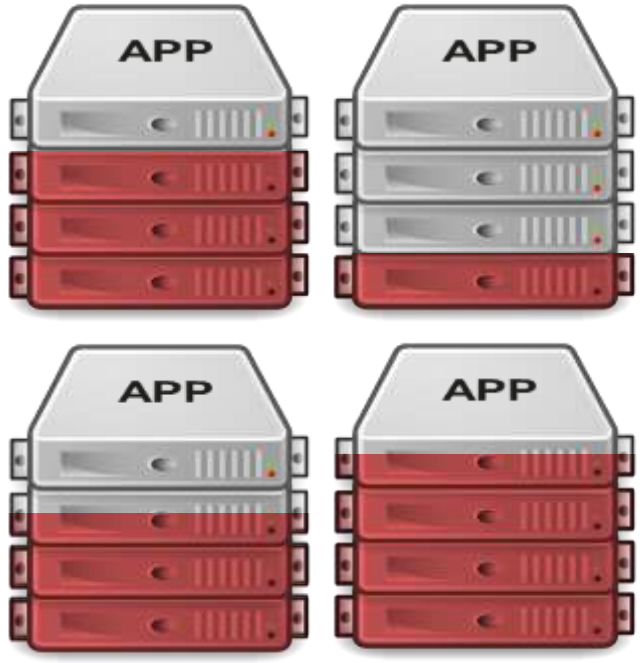
ALEF

TRAFFIC MANAGEMENT



ALEF

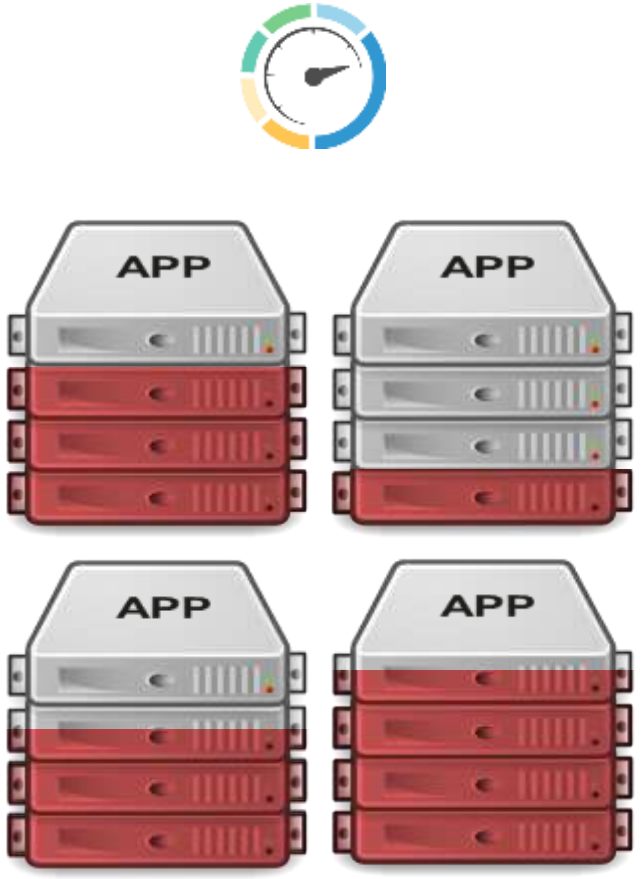
TRAFFIC MANAGEMENT



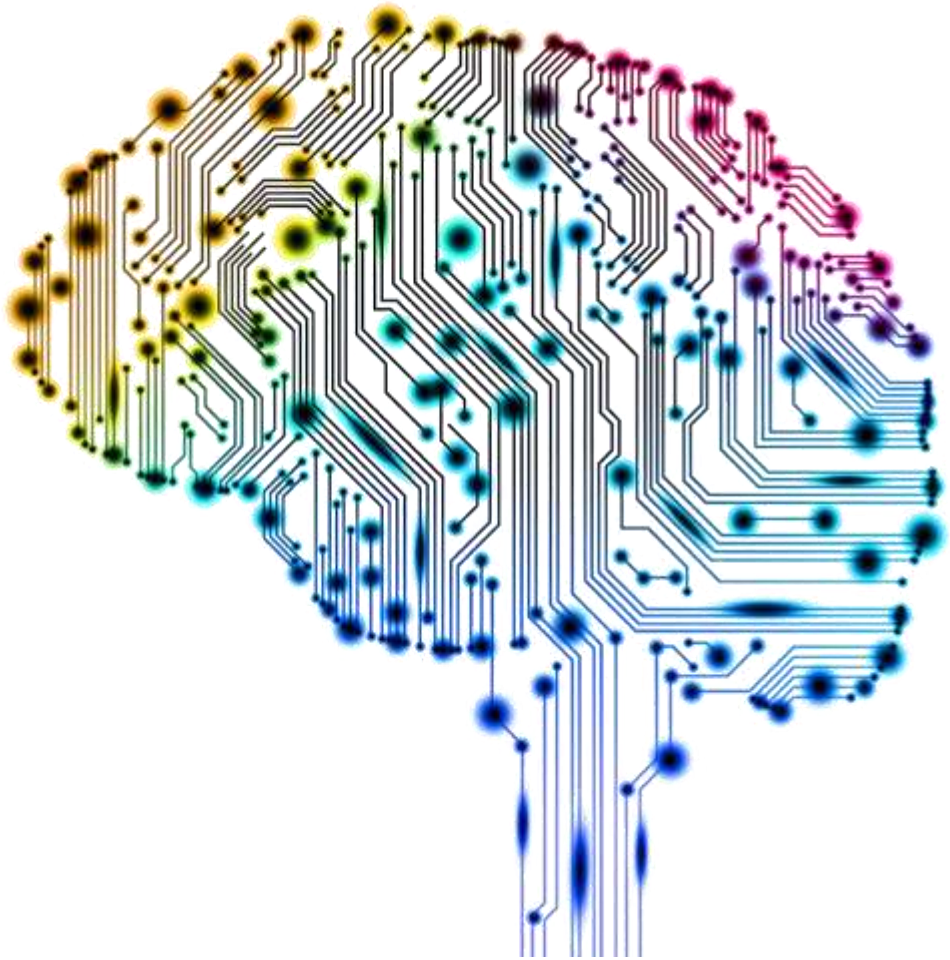
ALEF

V čem je tedy problém?

TRAFFIC MANAGEMENT



TRAFFIC MANAGEMENT



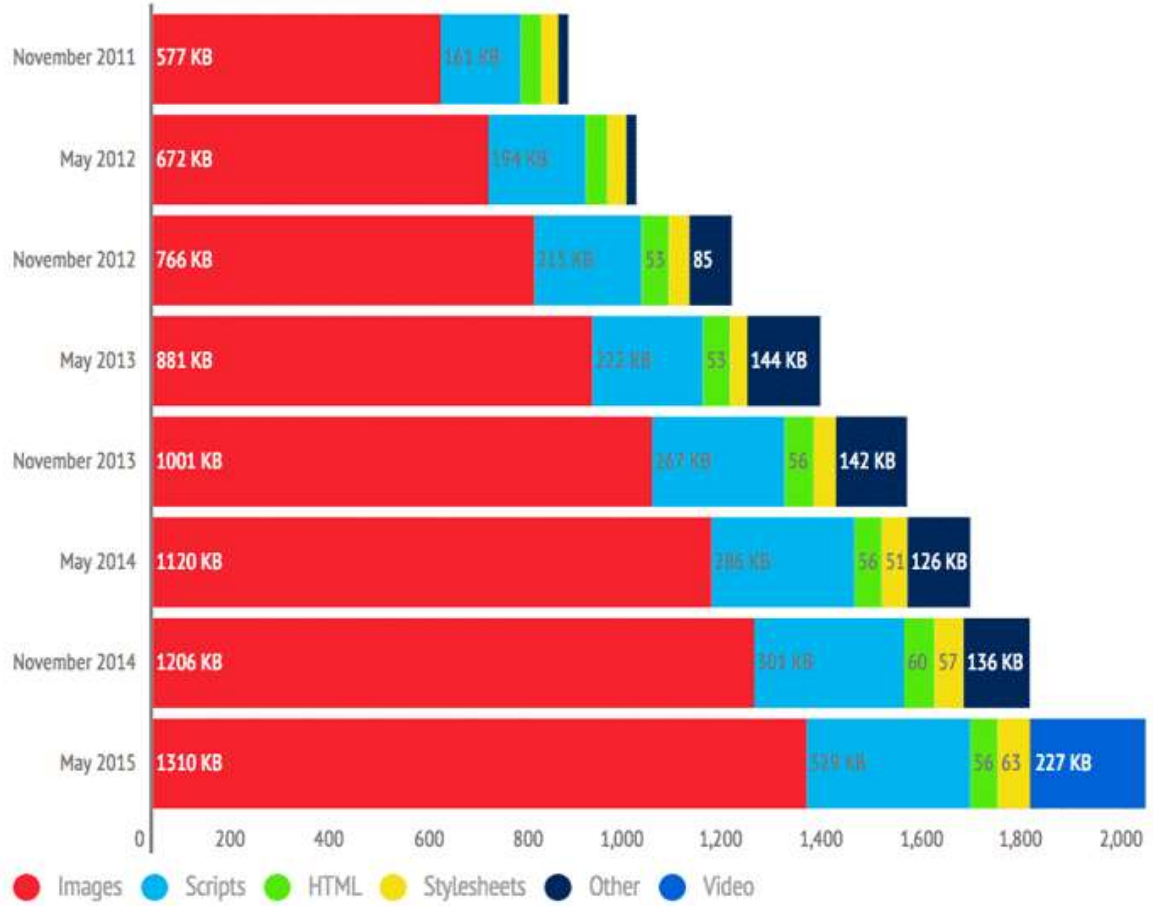
TRAFFIC MANAGEMENT

iRules

TRAFFIC MANAGEMENT


2014

TRAFFIC MANAGEMENT




309
AMMO
93%
HEALTH
2 3 4
5 6 7
ARMS
187%
ARMOR
BULL 309 / 400
SHEL 100 / 100
RCKT 15 / 100
CELL 20 / 600

Jak to budeme řešit?

TRAFFIC MANAGEMENT

- 40 %

Without Image Optimization

QUALITY: 90
SIZE: 102

Location	Label	Camera Date	Exposure Program
Copyright	Firmware	Digitized Date	Thumbnail
ISO	Flash Compensation	Modified Date	JPEG Quality
Shutter Speed	Image Number	File Date	Tags
Exposure Bias	Lens	Flash	Unique ID
Max Aperture	Lens ID	Focal Length	X Resolution
Focal Plane X Resolution	Serial Number	Focal Length in 35mm film	Y Resolution
Focal Plane Y Resolution	Software	CCD Width	Flash Function Not Present
Focal Plane Resolution Unit	Files size	Aperture	Flash Mode
Custom Rendered	Dimensions	F Number	Supports Red-Eye Reduction
Exposure Mode	Camera make	White balance	Flash Return
Scene Capture Type	Camera model	Metering Mode	

With Image Optimization

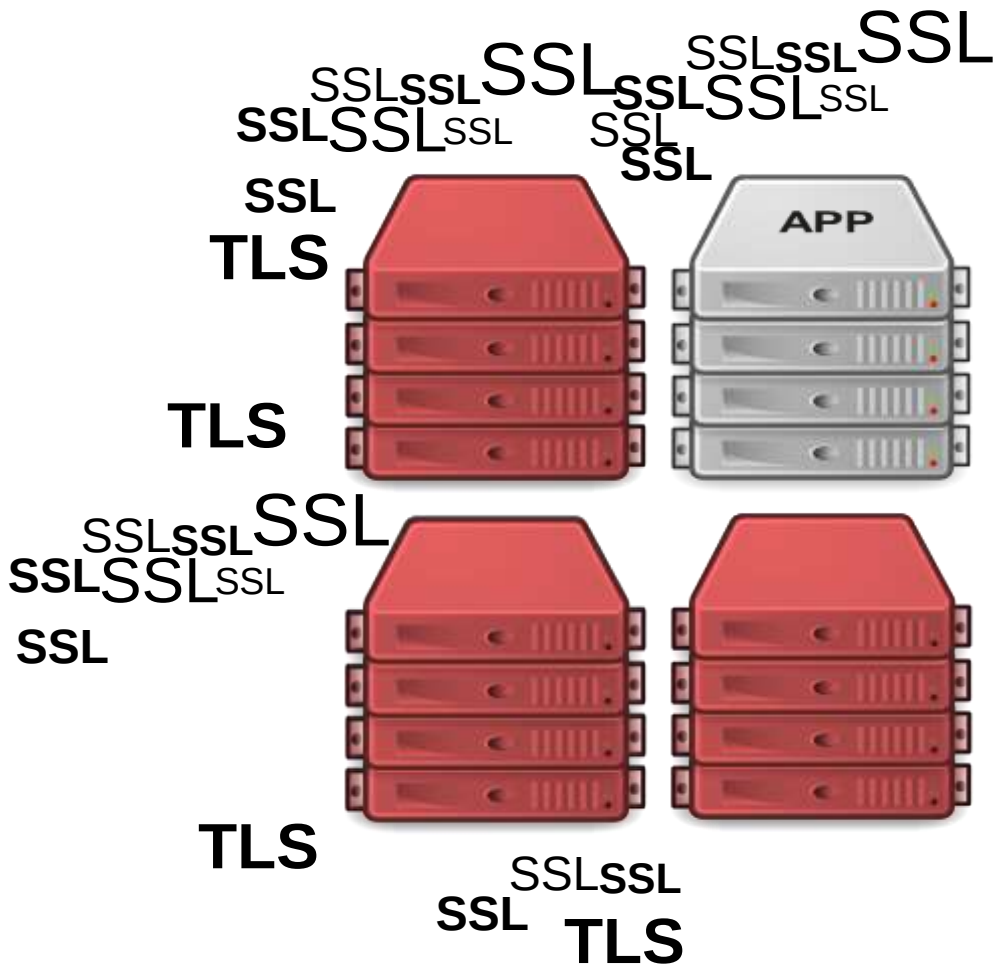
QUALITY: 70
SIZE: 50

Location	File Date
File Size	JPEG Quality
Dimensions	Unique ID

TRAFFIC MANAGEMENT

ALEF

TRAFFIC MANAGEMENT

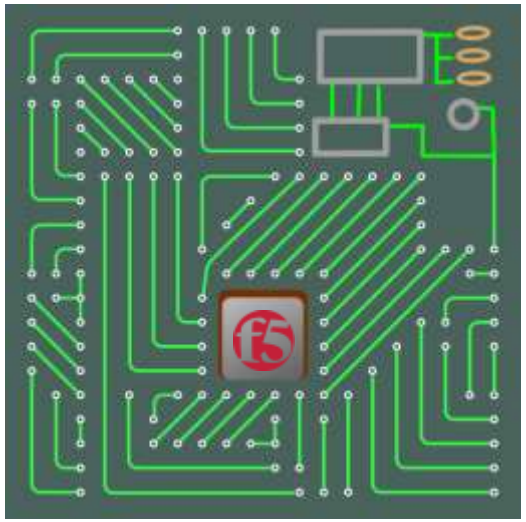


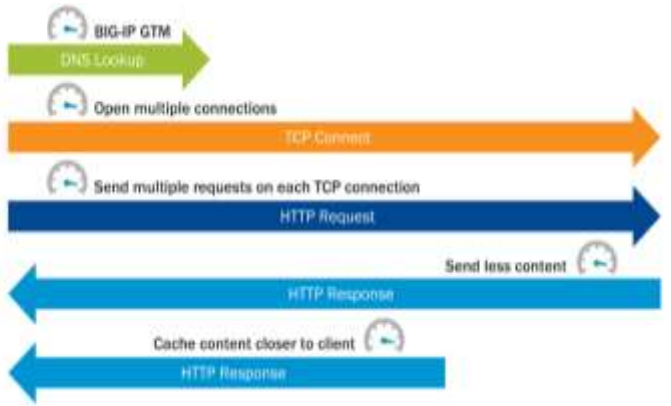
ALEF

TRAFFIC MANAGEMENT

ALEF

TRAFFIC MANAGEMENT





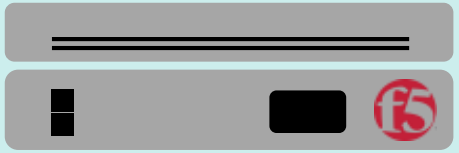
Zvýšení hodnoty současného HW

Nové možnosti správy provozu

Úspora/zvýšení výpočetního výkonu

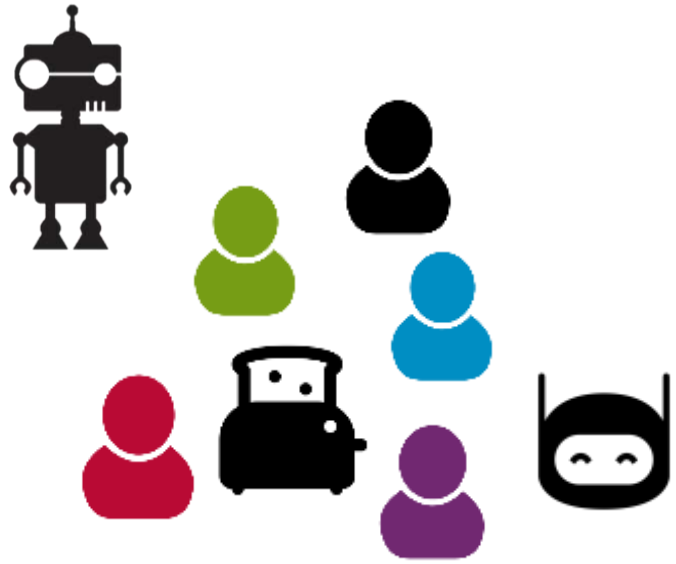
Zrychlení aplikace

LTM



Řešení

Bezpečná aplikace



SECURITY

1/3

aplikací

72 %

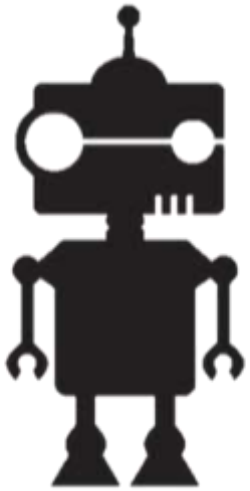
útoků

81 %

útoků

SECURITY

6 min
< 2 hodiny



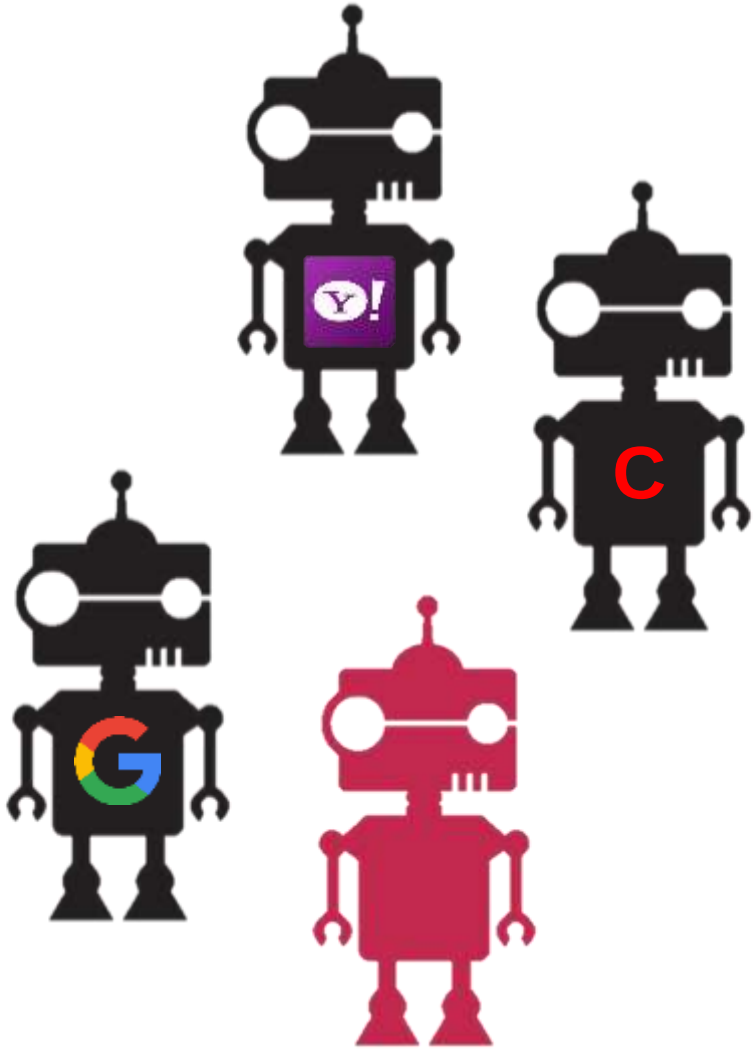
50 %

automatického provozu

ALEF

Proč nejde prostě blokovat komunikaci všech robotů?

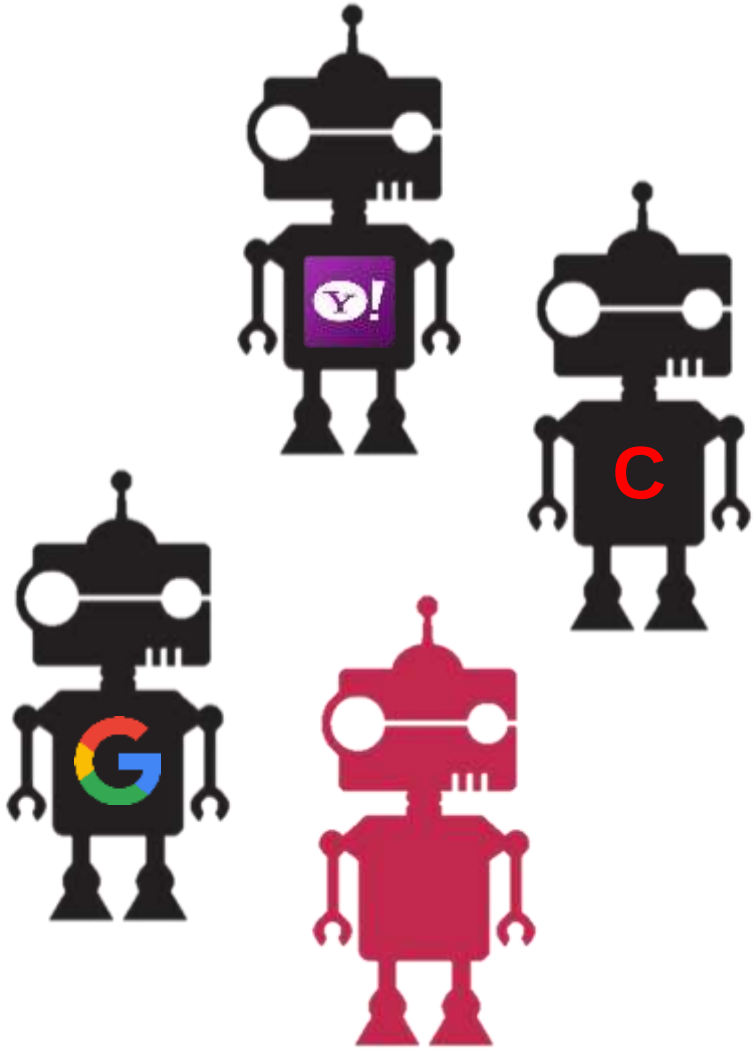
SECURITY



Nelze snadno poznat jejich záměr

ALEF

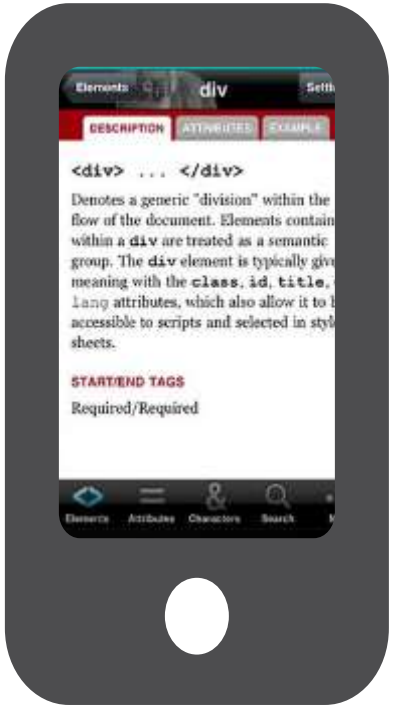
SECURITY



ALEF

SECURITY

Web



Hybrid

Native

SECURITY

OWASP

Open Web Application Security Project

ALEF

OWASP Top 10

#1: Injection

2013 OWASP Top 10

1. **Injection**
2. Broken authentication and session management
3. Cross-site scripting (XSS)
4. Insecure direct object references
5. Security misconfiguration
6. Sensitive data exposure
7. Missing function level access control
8. Cross-site request forgery (CSRF)
9. Using components with known vulnerabilities
10. Unvalidated redirects and forwards

2017 OWASP Top 10

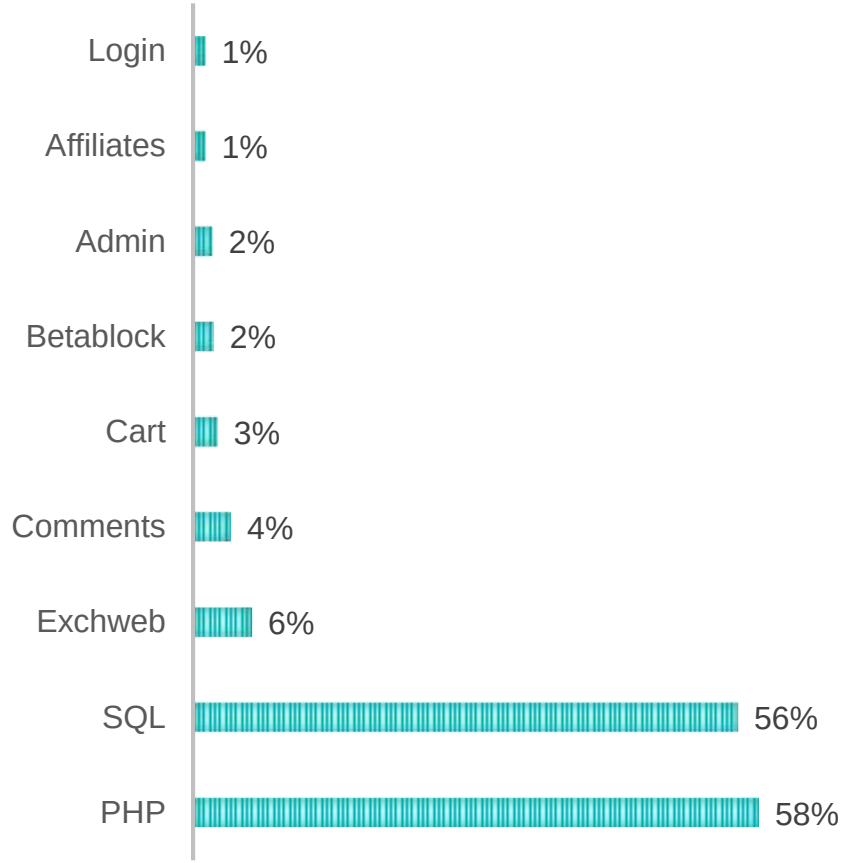
1. **Injection**
2. Broken authentication
3. Sensitive data exposure
4. XML external entities (XXE)
5. Broken access control
6. Security misconfiguration
7. Cross-site scripting (XSS)
8. Insecure deserialization
9. Using components with known vulnerabilities
10. Insufficient logging and monitoring

ALEF

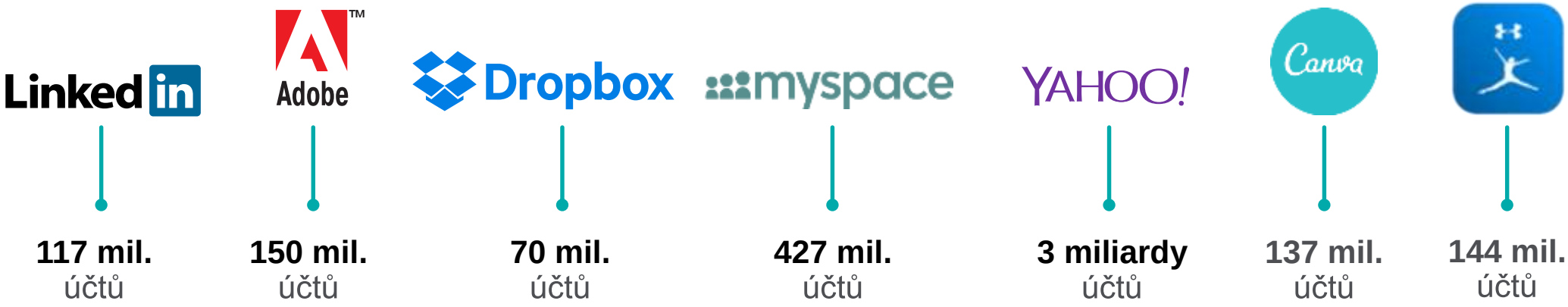
SECURITY


ZU 0666',0,0); DROP DATABASE TABLICE;--


'OR 1=1;--


Login 1%
Affiliates 1%
Admin 2%
Betablock 2%
Cart 3%
Comments 4%
Exchweb 6%
SQL 56%
PHP 58%

V posledních 8 letech bylo vyzrazeno více než 7.1 miliard identit

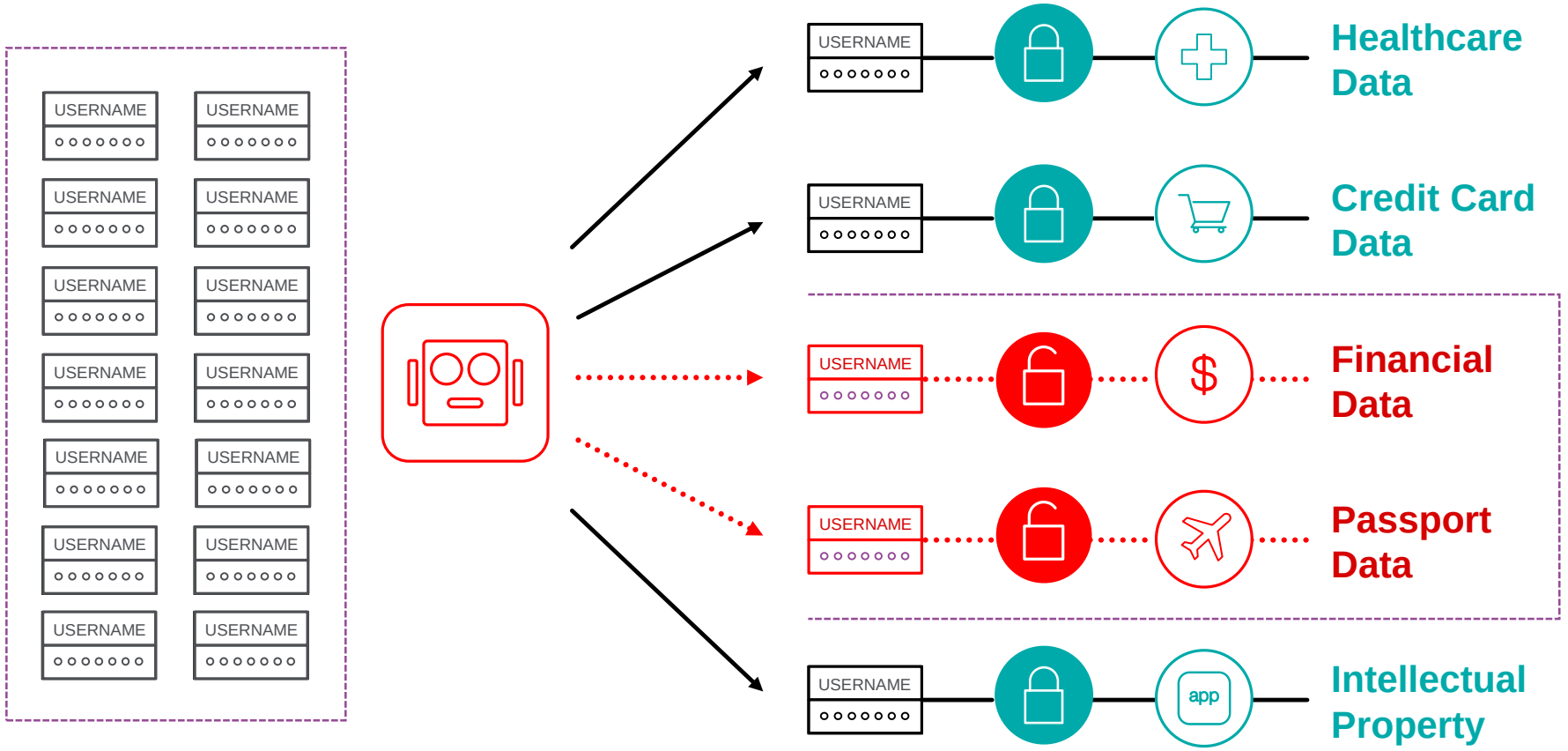


“Téměř 3 ze 4 uživatelů používají jedno heslo na více místech a nezměnili jej 5 a více let ”

ALEF

K čemu jsou útočníkům takové údaje?

SECURITY



Úspěšnost více než 7 %

SECURITY

aWAF

SECURITY

Behavioral DoS protection

ALEF

SECURITY

Slowloris

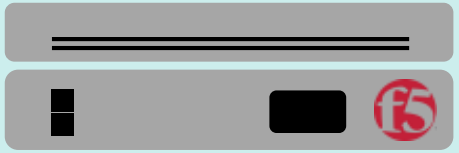
Redukce provozu o 30 %

Prevence násilného zastavení služby

Neznámé útoky, OWASP 10

Ochrana cenných dat

aWAF



Řešení

Čas na Shape!

About Shape

Protects web & mobile applications from automated attack and abuse

Customers include:

4 of the top 10 Global Airlines
3 of the top 5 US banks
2 of the top 10 Global Retailers
2 of the top 5 Global Hotel Chains
5 of the top 10 Credit Card Issuers
2 of the top 5 Insurers

Traffic Volume:

1B+ transactions/day
100M real human logins/day
125M mobile devices with Shape SDK

Founded:

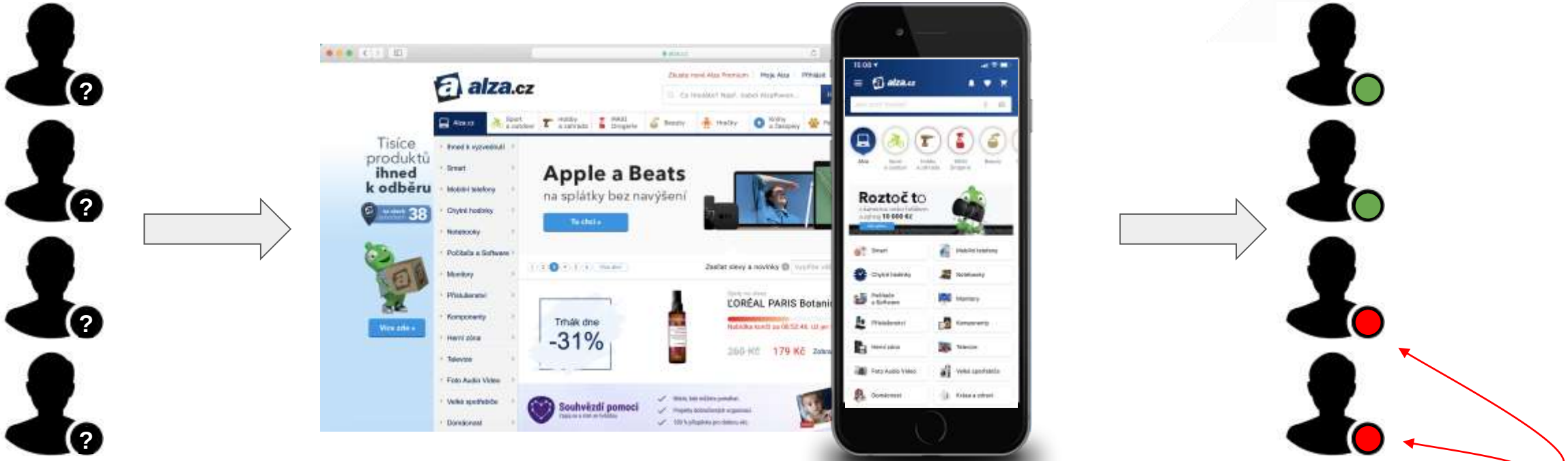
Mountain View, California 2011

Patents:

50+ Issued 130+ Pending

Recognised as the fastest growing company in Silicon Valley (Deloitte, 2018)

Fraud occurs when criminals act like legitimate users



Users
(criminals mixed in with good users)

Web & Mobile Apps
(serve good users & criminals alike)

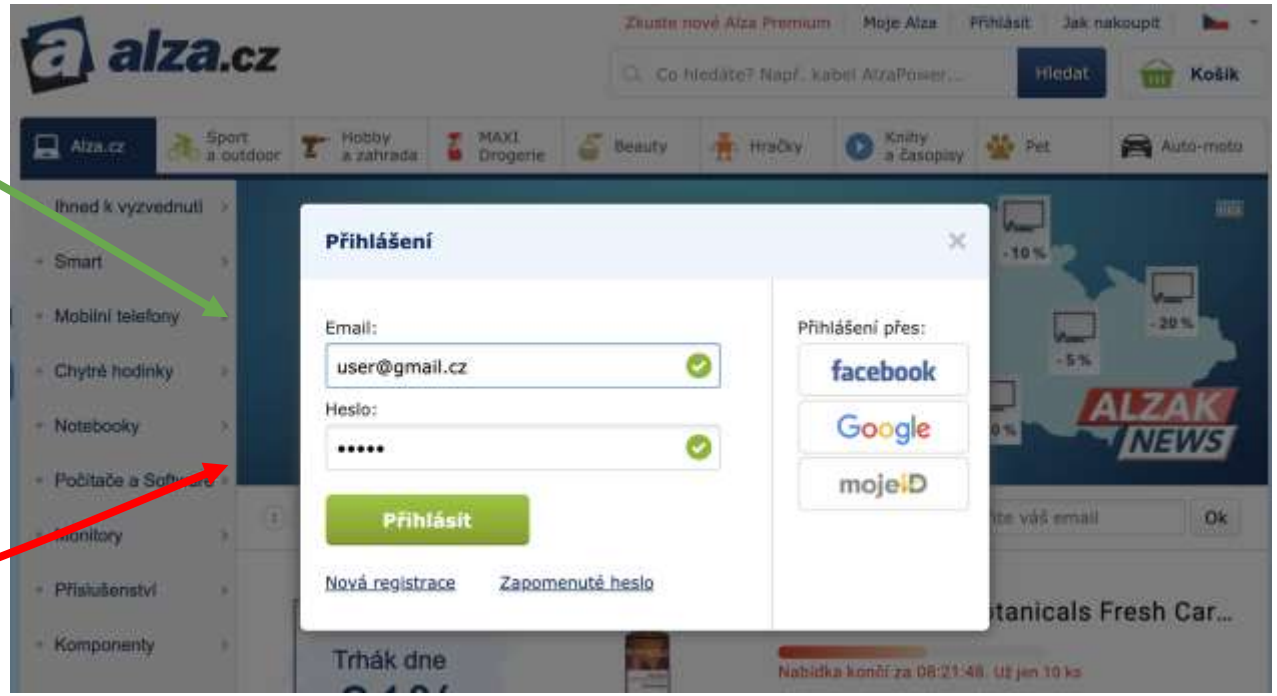
Criminals
(not evident until it's too late)

To compete today, enterprises must be open to anyone, anywhere, on any device. Web/Mobile Applications - significant source of fraud.

Challenge: criminals use apps as you intended (no flaws)

User: logs in with username & password

Attacker: logs in with username & password

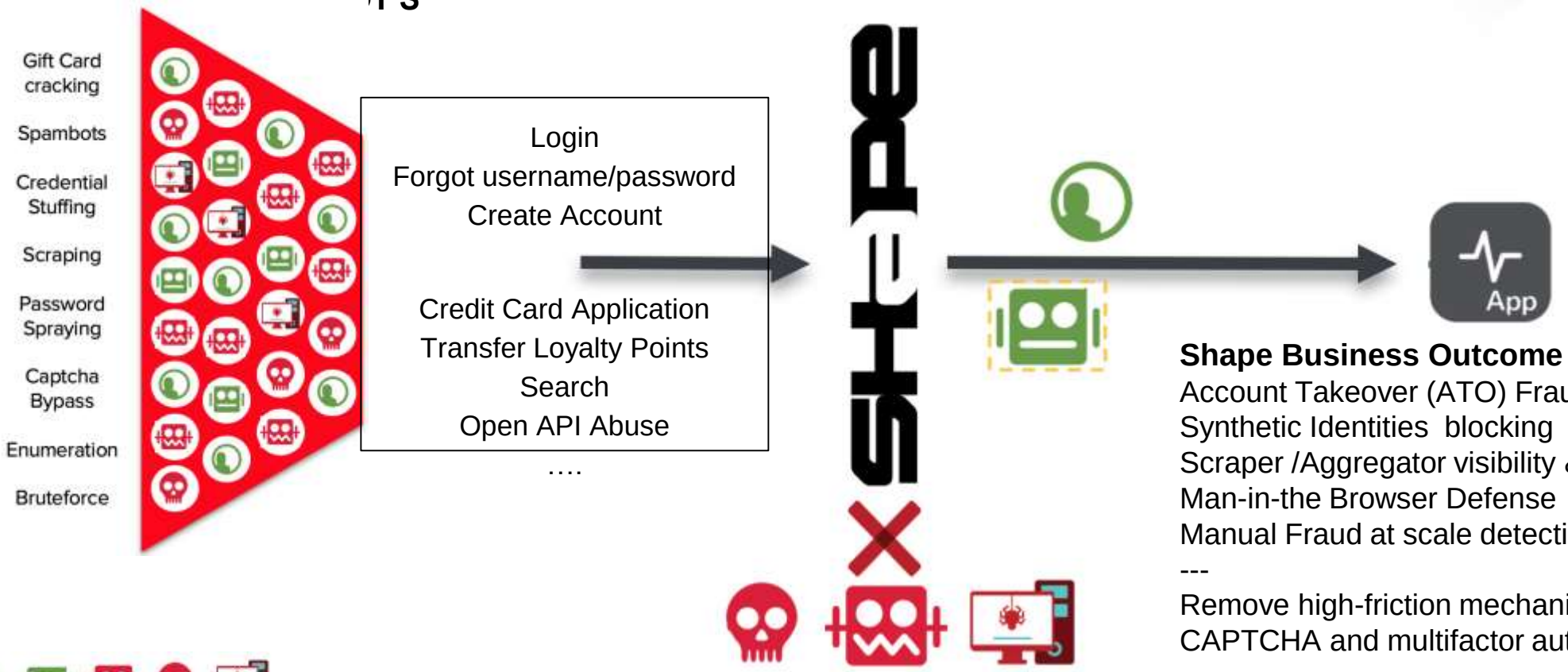


Criminals, armed with widely-available tools, can evade technologies like non-advanced WAF or ineffective techniques like CAPTCHA

Value Creation

Part of F5

WE SECURE THAT YOUR APPLICATION USED BY HUMAN AND NOT BAD BOT'S



Shape Business Outcome

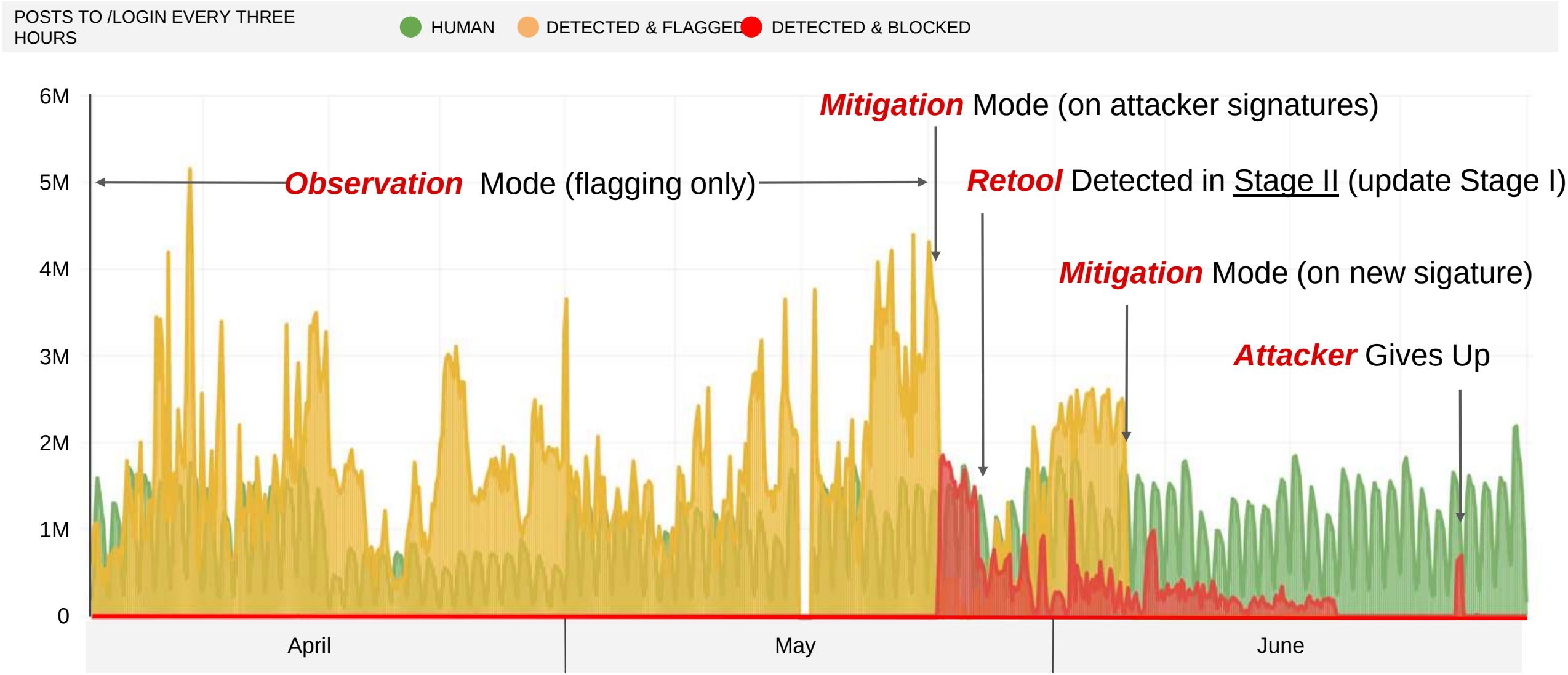
Account Takeover (ATO) Fraud Prevention
Synthetic Identities blocking
Scraper /Aggregator visibility & control
Man-in-the Browser Defense
Manual Fraud at scale detection/ blocking

Remove high-friction mechanisms, including CAPTCHA and multifactor authentication

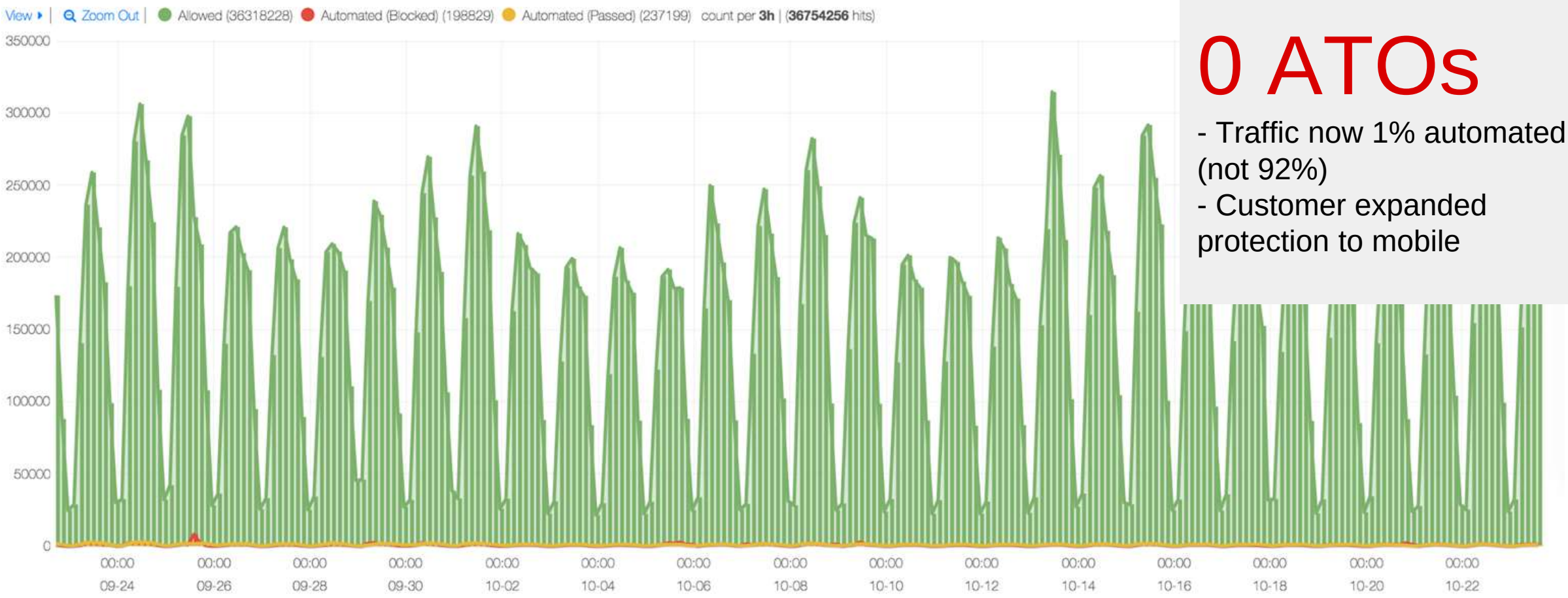
DETECTION-MONITORING-MITIGATION IN REALTIME

Legend: Customer, Friendly Bot, Malicious Bot, Manual Fraud, Threat Device

Major online retailer in Asia G2000 (Initial stages of mitigation)



Major online G2000 (Continued efficacy @ 18mo+)



0 ATOs

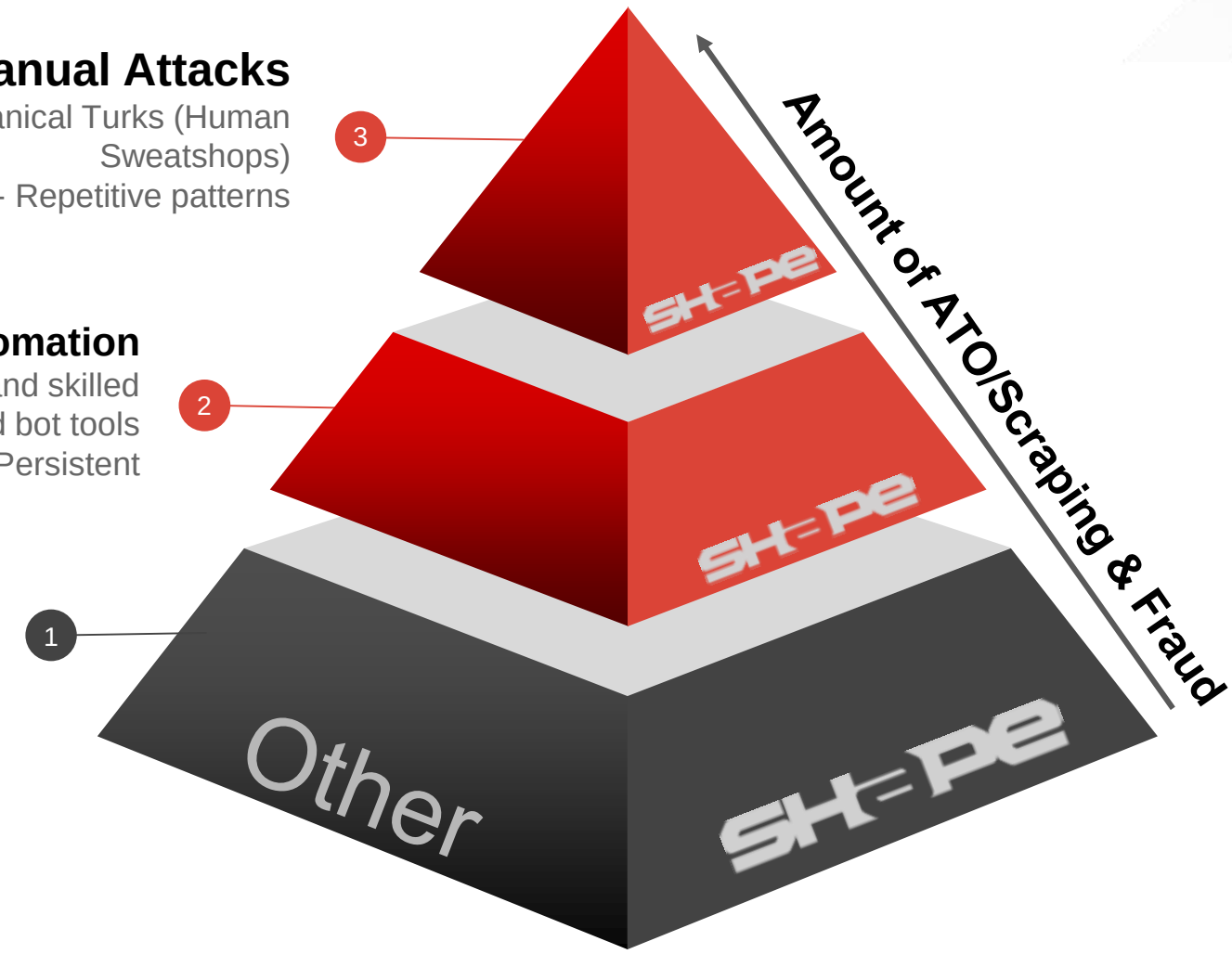
- Traffic now 1% automated (not 92%)
- Customer expanded protection to mobile

Shape is uniquely effective against sophisticated attacks

Scaled Manual Attacks
- Mechanical Turks (Human Sweatshops)
- Repetitive patterns

Professional Automation
- Highly motivated and skilled
- Customized bot tools
- Persistent

Amateur Automation
- Less motivated and skilled
- Off-the-shelf bot tools (Sentry MBA)
- Terminable



1 2 3 **Shape**

1 ○ ○ **Other Solutions**

Agenda

1. Evolution of Attacks – Why traditional security measures fail
2. Introduction Shape Enterprise Defense
3. Shape Deployment Options

Evolution of Attacks – Why traditional security measures fail

Criminals armed with widely-available tools and services to launch Imitation Attacks

WHAT ARE IMITATION ATTACKS?

Initation attacks occur when criminals simulate legitimate activity, like logging into an ccount, on your web and mobile applications.

These attacks result in ATO, stolen points, lost PII and fraud.

People reuse passwords
Up to 2% of all leaked credentials will work on any given site

Attackers use Automation to test credentials
-Penetrate sites that have not otherwise been breached

5+ Billion

Leaked credentials in 2016 to 2018 *alone*

>6M new creds leaked daily

FREE

Tools to imitate humans on any site

$50 per config

Botnets of real user machines

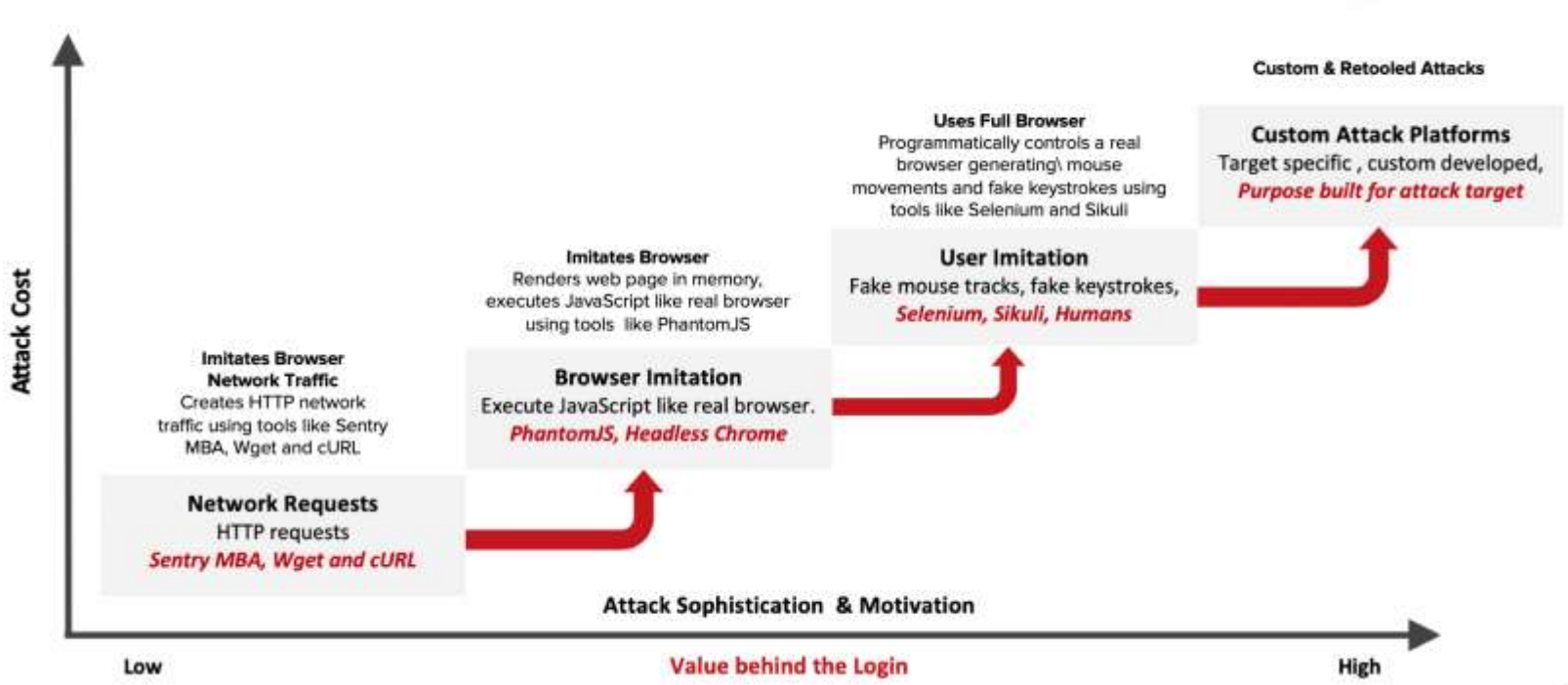
$2 per hour per 1,000 IPs

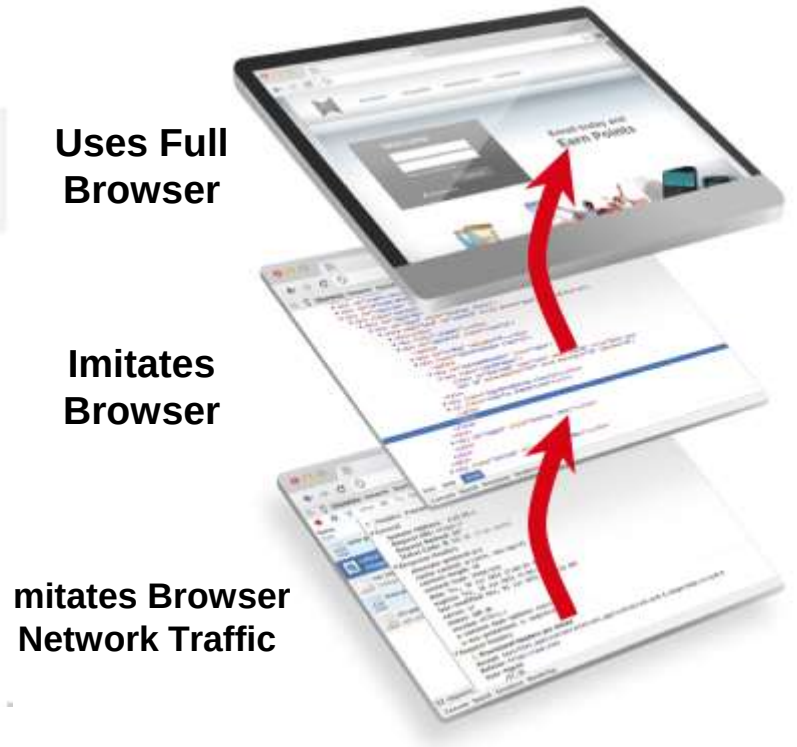
Speciality services to solve CAPTCHA

$1.39 per 1000

Evolution of Attacks – Why traditional security measures fail

Criminals armed with widely-available tools and services to launch Imitation Attacks

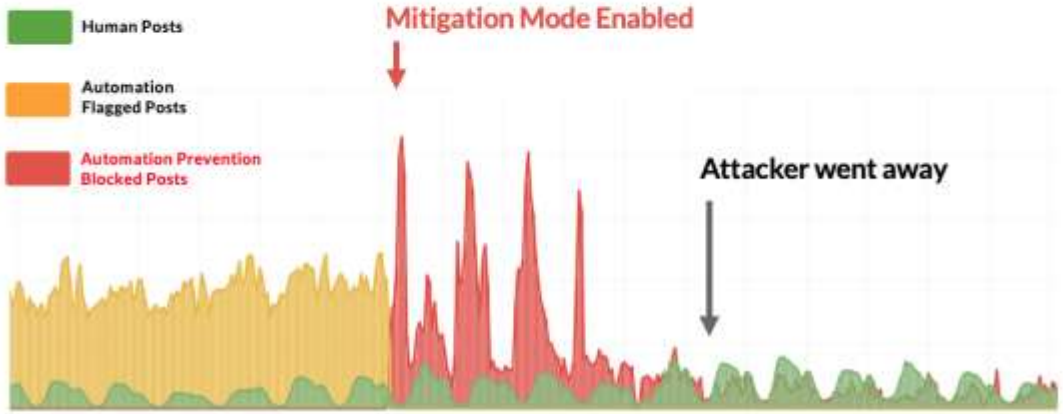




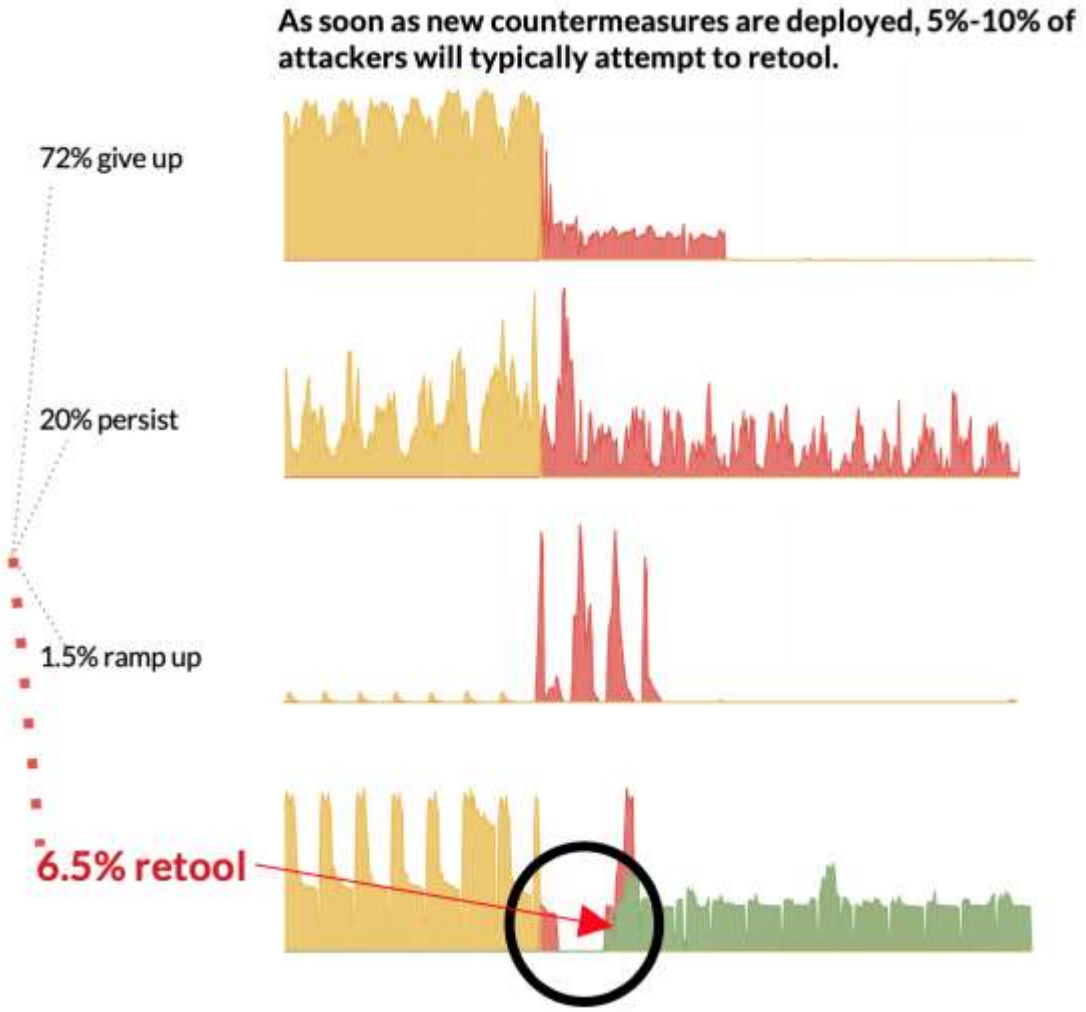
Traditional security measures (e.g. device ID, WAFs, IPS) are typically signature-based and can't defend against sophisticated, retooling attackers

What set us apart

Shape is designed to adaptand maintain full efficacy even as attackers evolve



Shape is designed to adapt and maintain full efficacy even as attackers evolve



A.I.
Shape
MACHINE LEARNING
ARTIFICIAL INTELLIGENCE

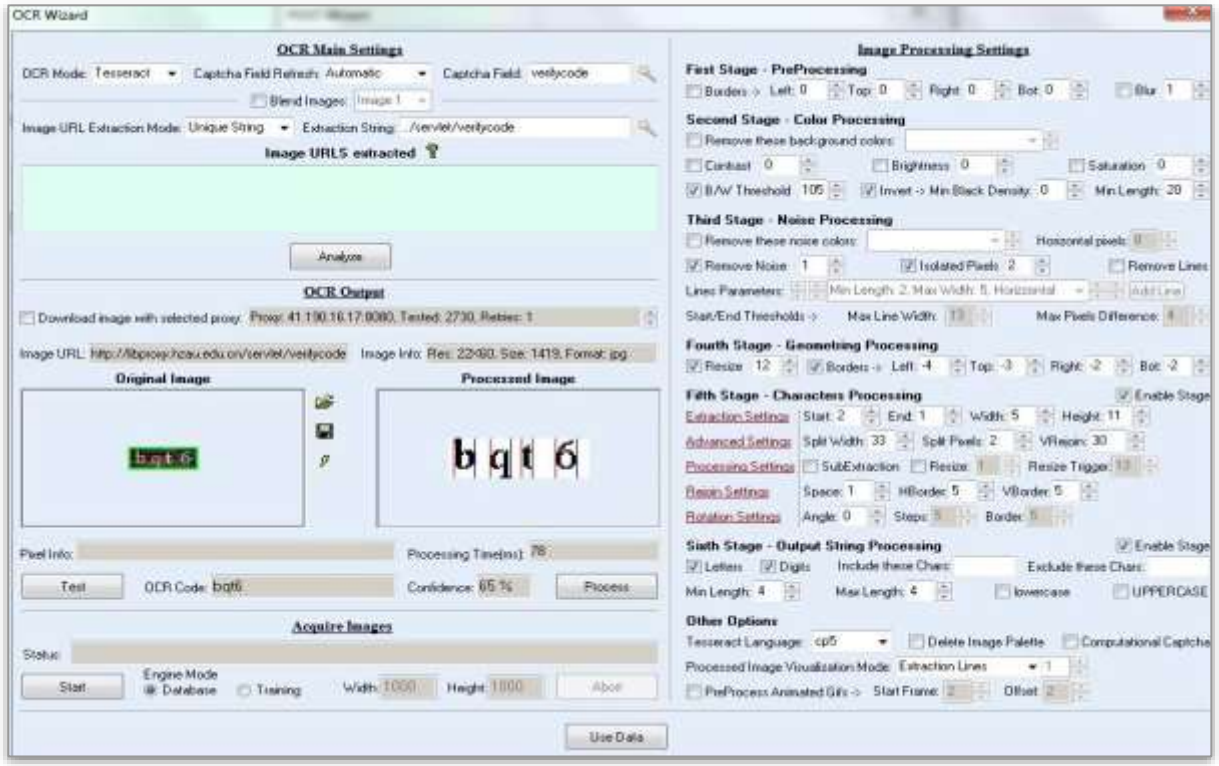
Shape Detect Advanced Attackers that Retool

Years of defending the largest brands has given Shape's machine learning models access to the most advanced attack data, allowing Shape to stop even the most sophisticated attackers.

Shape AI is trained on years of attack data from Fortune 500 companies

Tools and Services to launch Attacks

Sentry MBA - Credential stuffing / Brute-Force Login inclusive CAPTCHA solver



isentrymba.com › Forum › Tag ▾ Translate this page

timvision | iSentryMba - Italian Cracking Community

Oct 3, 2018 - 13 posts - 1 author

SentryMBA 2x Timvision Premium. Hidden content ... TimVision + Capture **Config** | Fast | Aggiornata 2018 Ecco a voi la **config** per TimVision, noto portale di streaming di telefilm e film creato da **Telecom Italia**. E' un buon ...

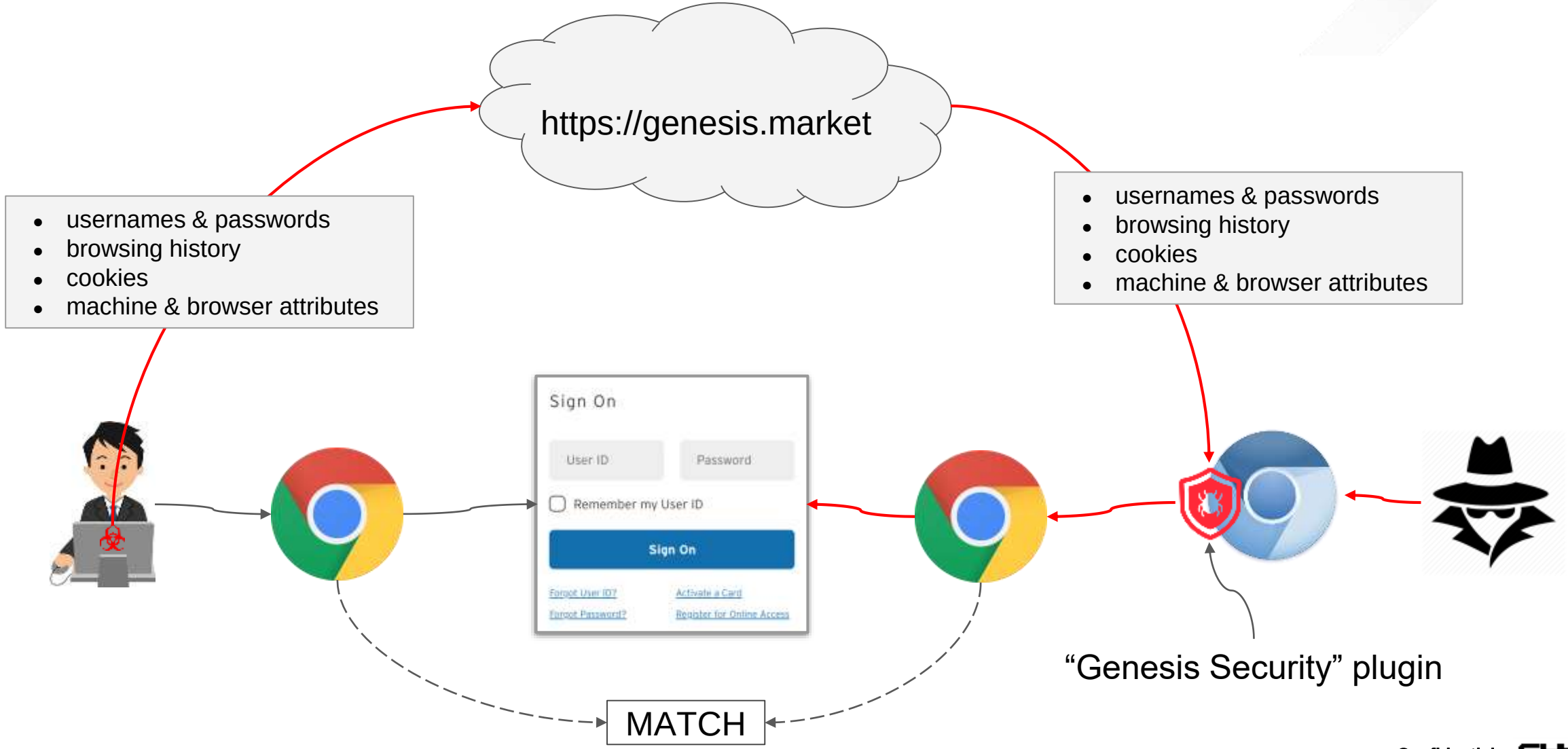
Sentry MBA Configuration Service [FROM $7.95] - Hack Forums

Premium Sellers Section-**Sentry MBA Configuration** Service [FROM $7.95] ... **Otto**.de. Transunion.ca. Mobilcom-debitel.de. Seatgeek.com. TOS

Sentry MBA leverage Data from data leaks for automated Credential stuffing / Brute-Force Login (Login, Password Reset, Account Registration, etc.)

Tools and Services to launch Attacks

Genesis Digital Fingerprint Marketplace



Evolution of Attacks – Business Impact

Increasing operational expenditure for the detection and defense against:

Scraping
(Price Comparisons, IP Theft, or Plagiarism)

Credential Stuffing / Brute-Force on Login Sites / Account Take Over
(Mass log in attempts used to verify the validity of stolen username/password pairs)

Fake Accounts Creation at Scale

Open API Abuse

Fraudulent Transactions
Arising from Man-in-the-Browser and malware

Business Problems

- Account Take Over Fraud
- Breach of personal information
- Multiple forms of fraud
- System Overhead
- Application DDoS
- Consume of Marketing KPI
- Block/Lock Online Inventory
- ….

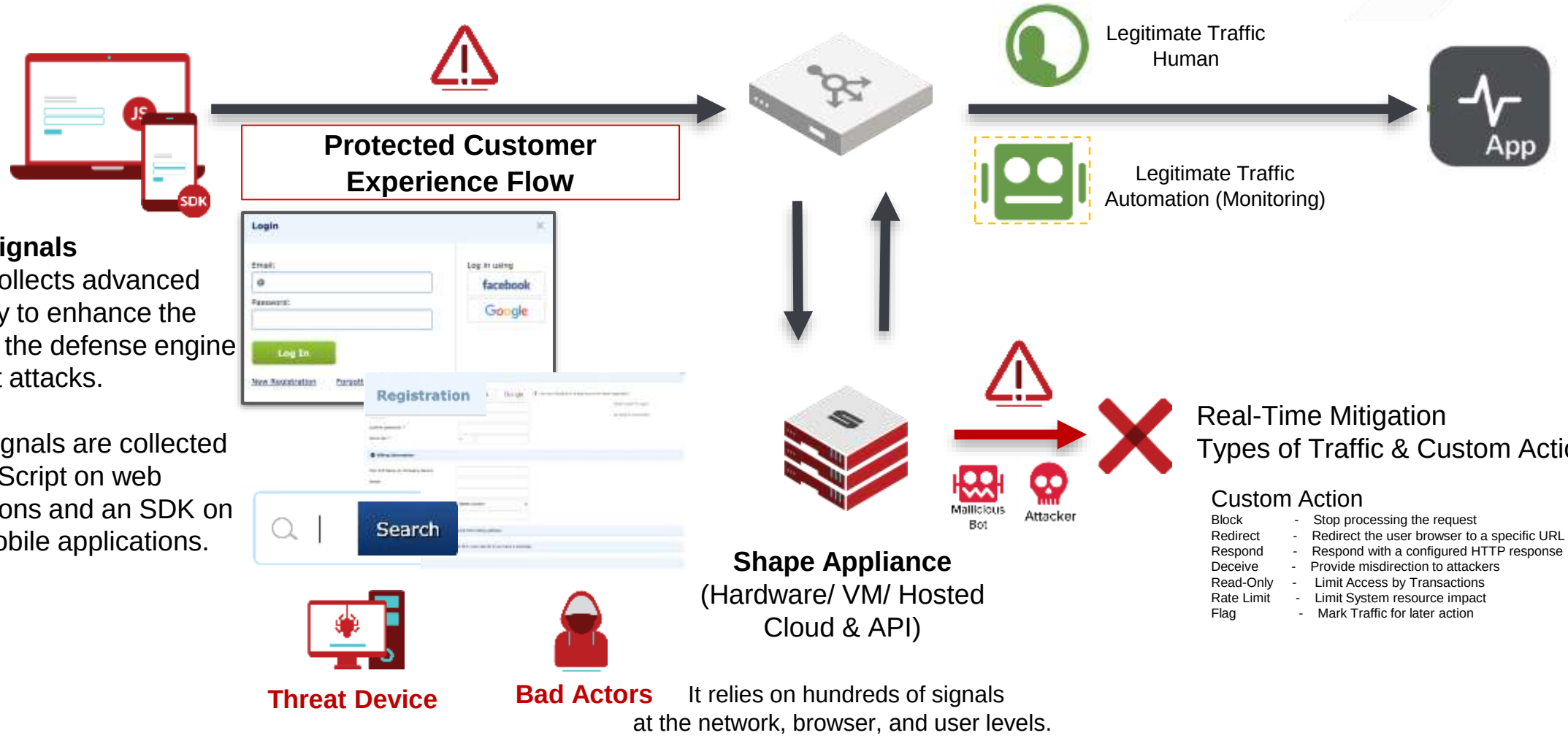
Agenda

1. Evolution of Attacks – Why traditional security measures fail
2. Introduction Shape Enterprise Defense
3. Shape Deployment Options

Shape Enterprise Defense

DETECTION-MONITORING-MITIGATION - enabling real-time fraud prevention

Shape Concept of Protected Customer Experience Flow (POST-GET Request)



Client Signals
Shape collects advanced telemetry to enhance the ability of the defense engine to detect attacks.

These signals are collected via JavaScript on web applications and an SDK on nativemobile applications.

Shape Appliance
(Hardware/ VM/ Hosted Cloud & API)

It relies on hundreds of signals at the network, browser, and user levels.

Real-Time Mitigation
Types of Traffic & Custom Action

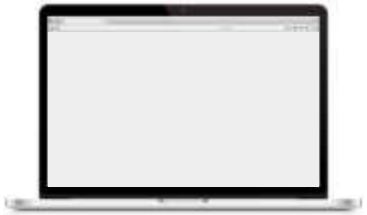
Custom Action

Block	-	Stop processing the request
Redirect	-	Redirect the user browser to a specific URL
Respond	-	Respond with a configured HTTP response
Deceive	-	Provide misdirection to attackers
Read-Only	-	Limit Access by Transactions
Rate Limit	-	Limit System resource impact
Flag	-	Mark Traffic for later action

Shape Enterprise Defense

Shape Signal Set

Protection is based on Fingerprints, Header Pattern, User Behavior Pattern and Signals –NOT IP‘s or User Agent



Interrogate Environment

Are you who you say you are? and more

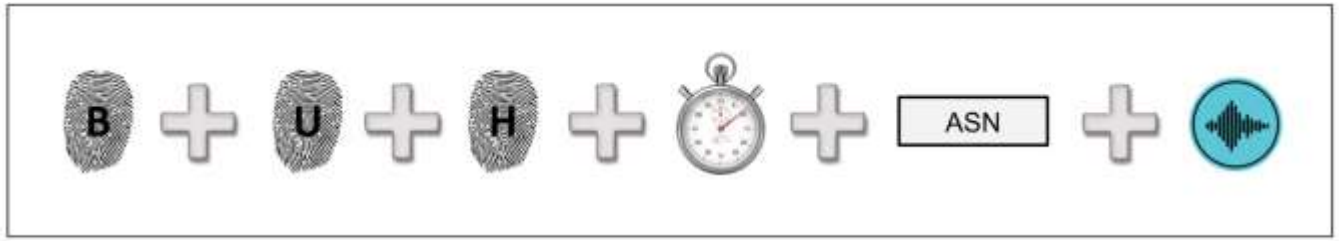
Client Detection

Are you even a browser? and more

Evaluate Behavior

Are you a human? and more

Proofs of hardware, proofs of environment, deception, user behavior collection, and much more

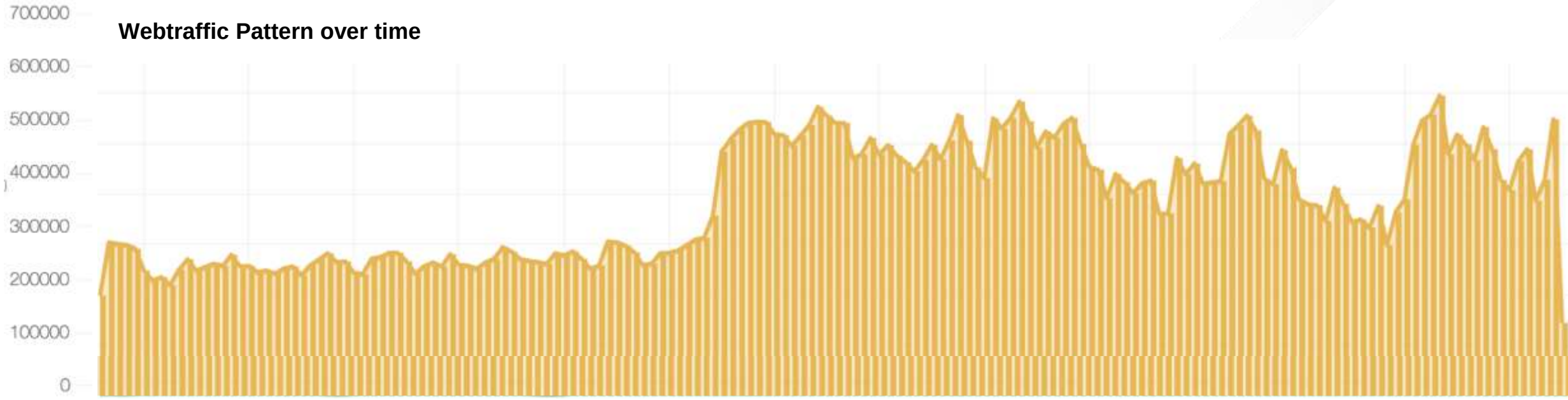


To find fraudulent transactions, we use one or more data points:

- Browser identifier based on unique interrogation
- User interaction pattern
- HTTP Header indicators
- Timing analysis (keystrokes and interaction)
- Traffic source analysis (Autonomous Systems)
- Custom signals and rules

Shape Enterprise Defense

Shape Signal Set – Real Example



68,6M

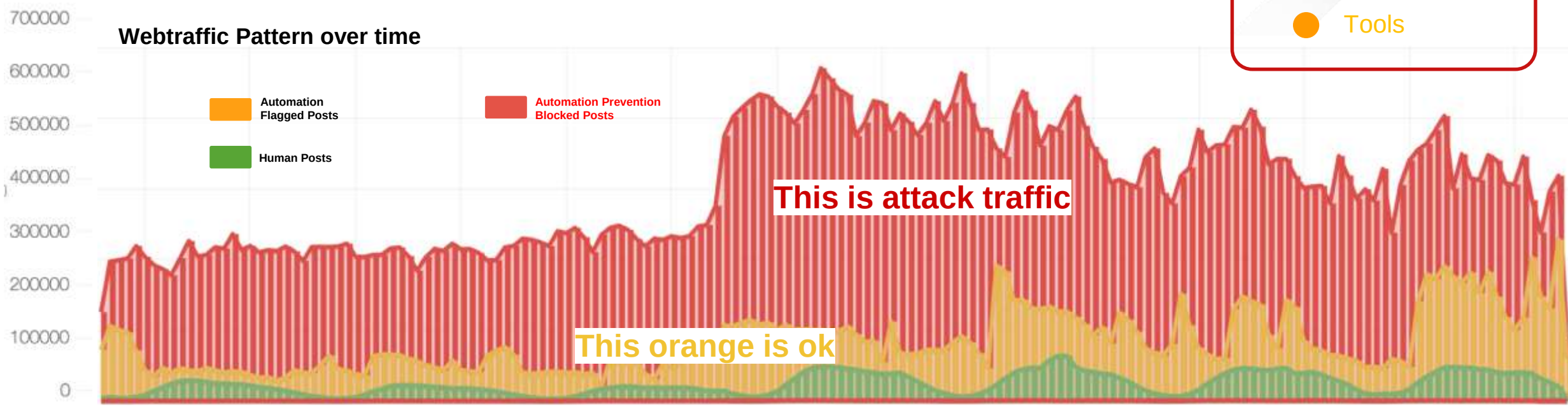
Total POSTs

Shape Enterprise Defense

Shape Signal Set – Real Example

5 Attackers

Tools



68,6M
Total POSTs

4,1 M
Human

64,6 M
Automated

94%
Automated

Shape Enterprise Defense

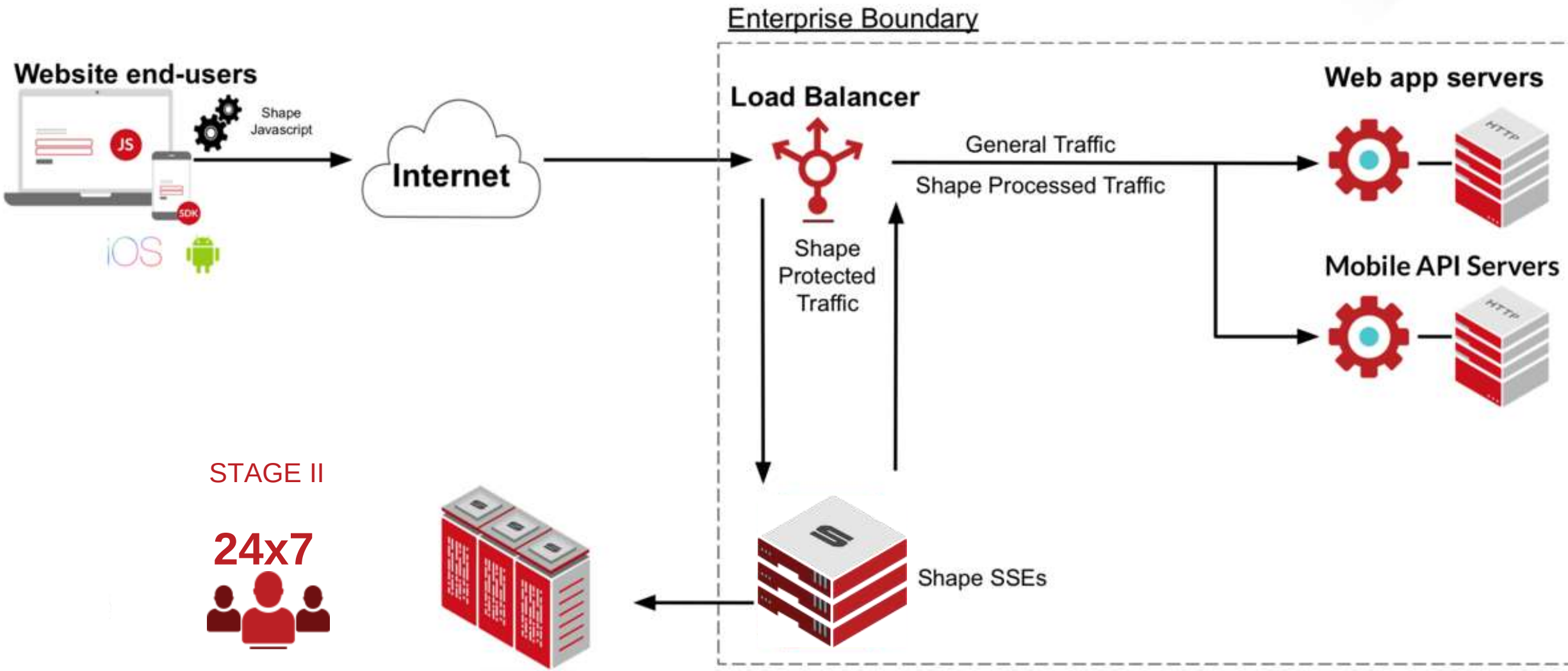
Shape Security includes a 24/7 traffic monitoring, threat intelligence analysis, and countermeasure deployment (if required) services

Part of F5

Agenda

1. Evolution of Attacks – Why traditional security measures fail
2. Introduction Shape Enterprise Defense
3. Shape Deployment Options

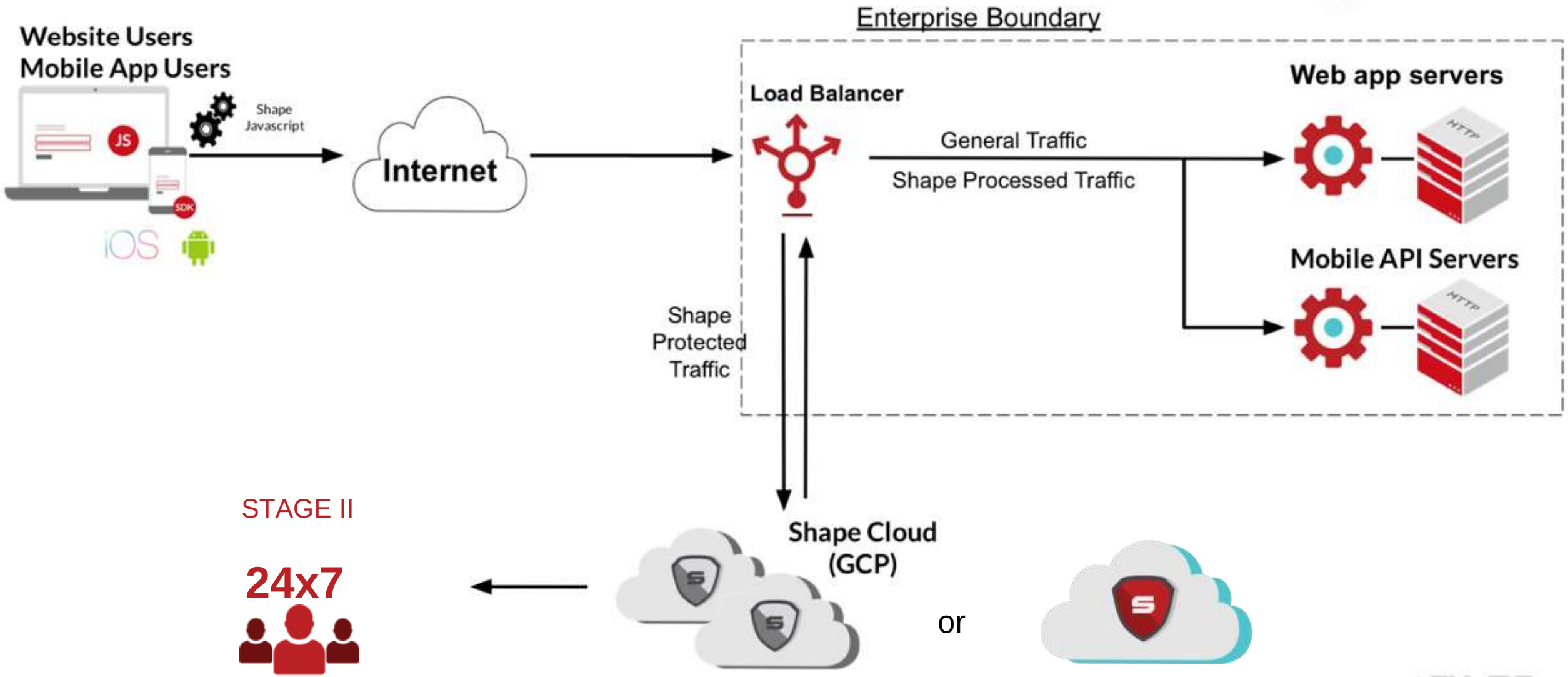
Shape Deployment On-Premise



STAGE II

24x7

Shape Deployment Cloud



Shape is CDN/Cloud/Load Balancer agnostic

Shape Security is compatible with all the leading CDN, Cloud, and Load Balancer providers, so you are not tied into any one technology stack.

Delivered as a Managed Services

Security Operations Center (24x7)

Threat Analysis & Reporting

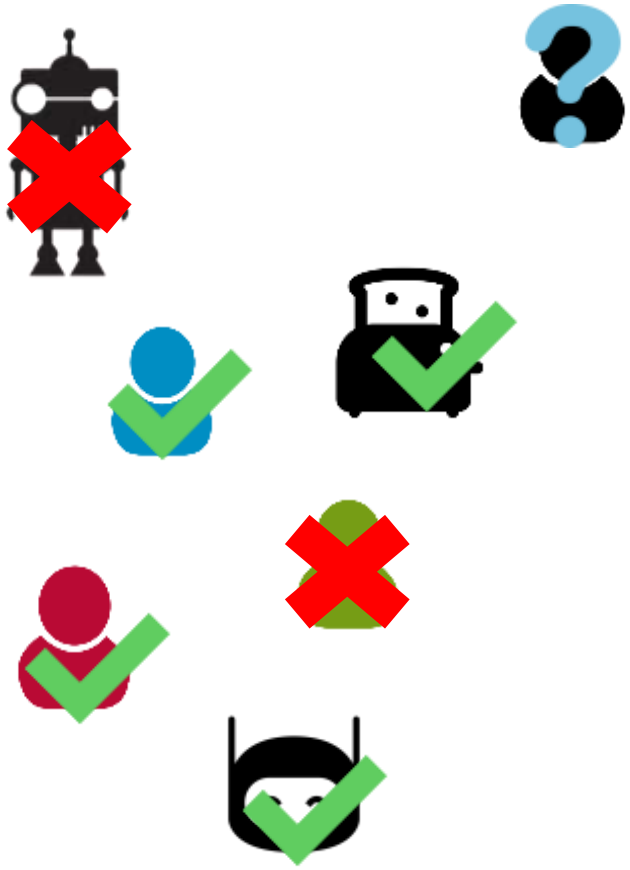
- Incident and Attack Reports
- Threat Summary Reports
- Raw Data Delivery

Threat Research

- Dark Web Reconnaissance (upon request)
- Attribution (upon request)

Přístup k aplikaci

ACCESS



- Co s novými příchozími?
- Jak zabránit úniku hesel zaměstnanců?
- Jak zvýšit zabezpečení přihlašování?

ALEF

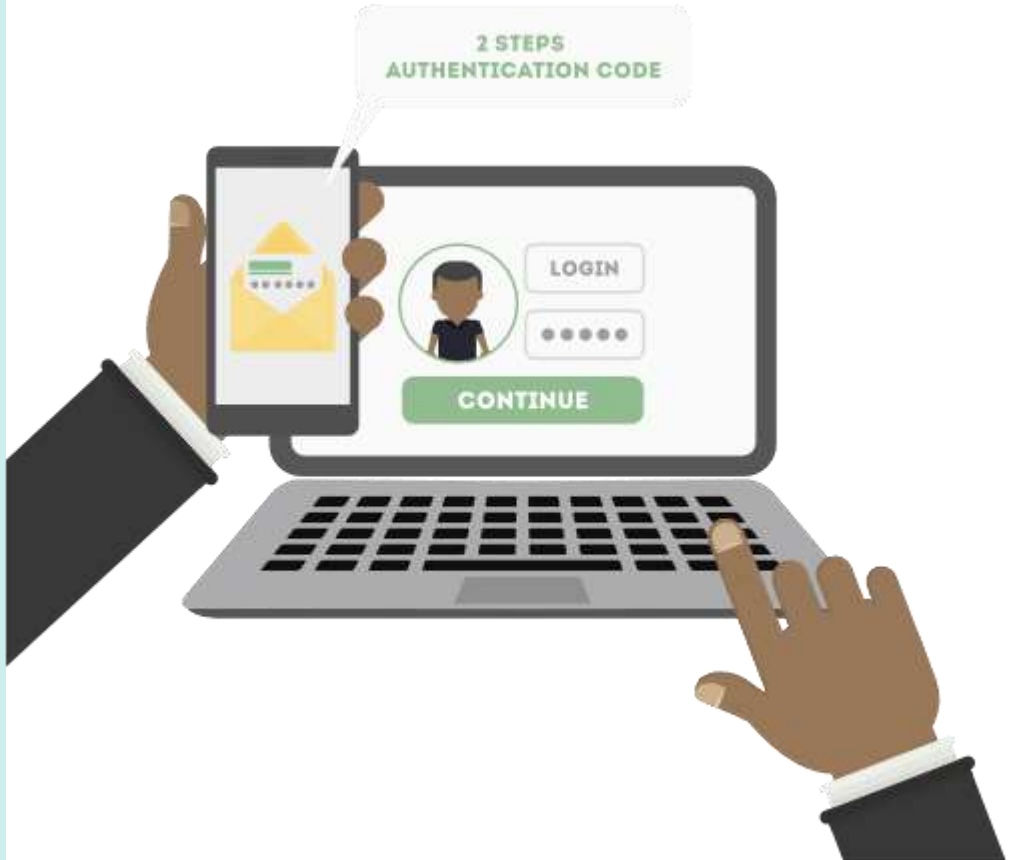
BYOD

ACCESS

SSO

ACCESS

Multifaktorová autentizace



ACCESS

ALEF

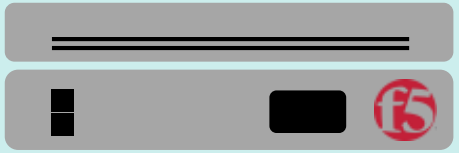
Na pár kliknutí

Multifaktorová autentizace

SSO

Bez hesla, jedním kliknutím

APM



Řešení

Univerzální dekrypce pro všechny security nástroje

ALEF

SSL/TLS Orchestrace

Nemohu zabezpečit, co nevidím…

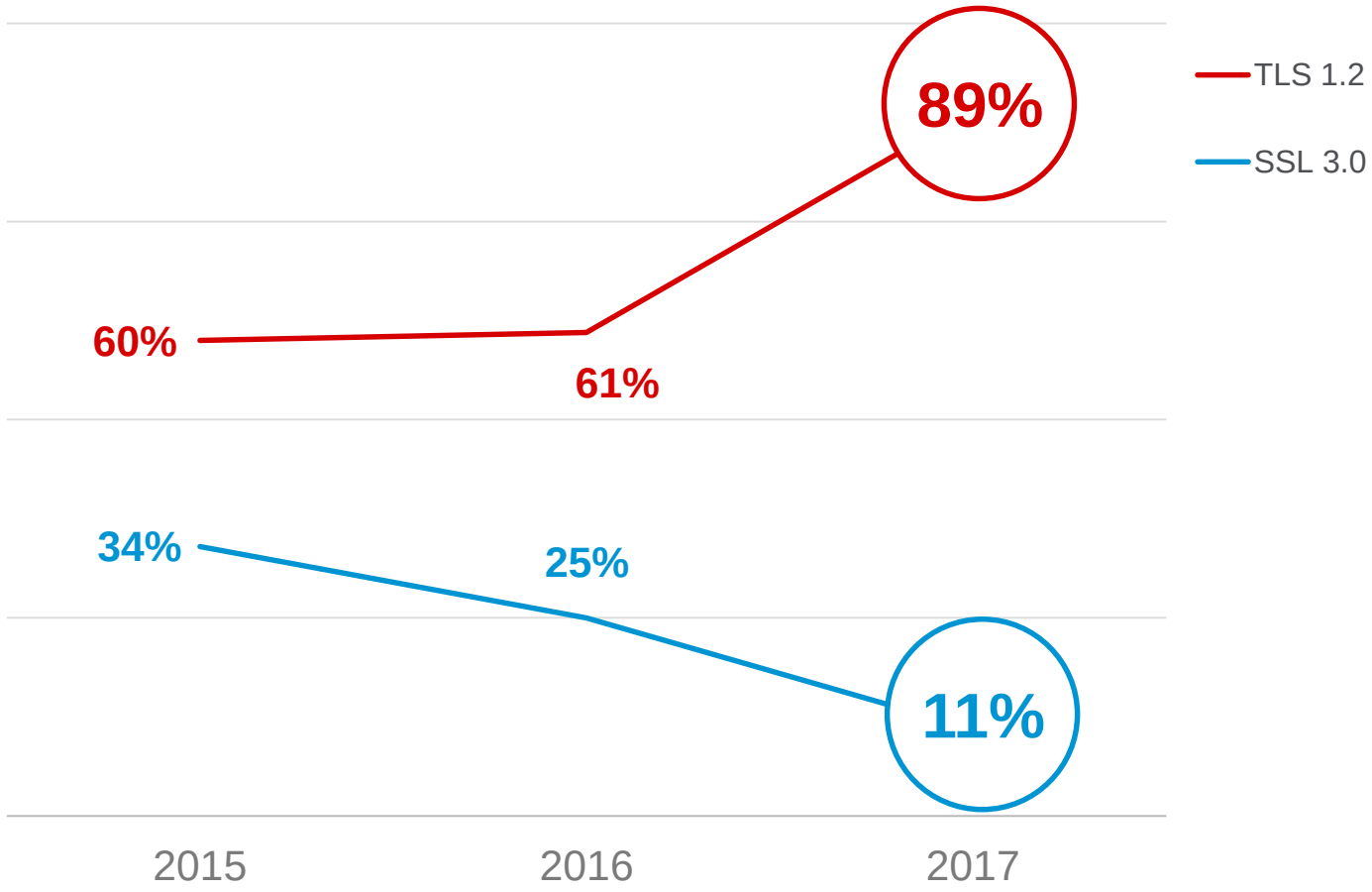
70% internetového provozu je šifrováno

80% webového obsahu je zabezpečeno SSL/TLS

ALEF

SSL/TLS narůstá

TLS 1.2 vs. SSL 3.0



SSL/TLS Orchestrace

ALEF

SSL/TLS Orchestrace

SSL/TLS šifrování Business Drivers

- Nárůst užívání sociálních sítí
- Vliv Microsoft Office 365
- Google Chrome upozornění na SSL/TLS
- Třídění výsledků vyhledávání
- GDPR
- Zvýšená snaha o zachování soukromí

ALEF

Tři výzvy SSL/TLS

SSL/TLS Orchestrace

Viditelnost

je zredukována kvůli užívání šifrování

Výkon

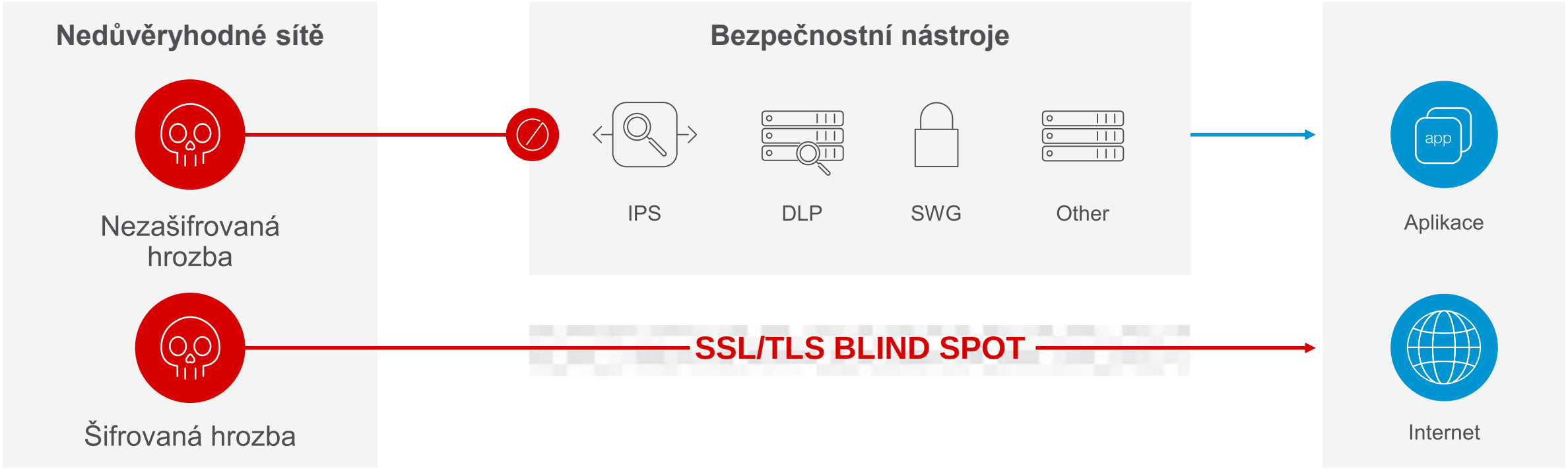
je degradován neustálou enkrypcí a dekrypcí

Složitost

zatěžuje celé IT organizace

ALEF

Požíváte šifrování? Útočníci také.

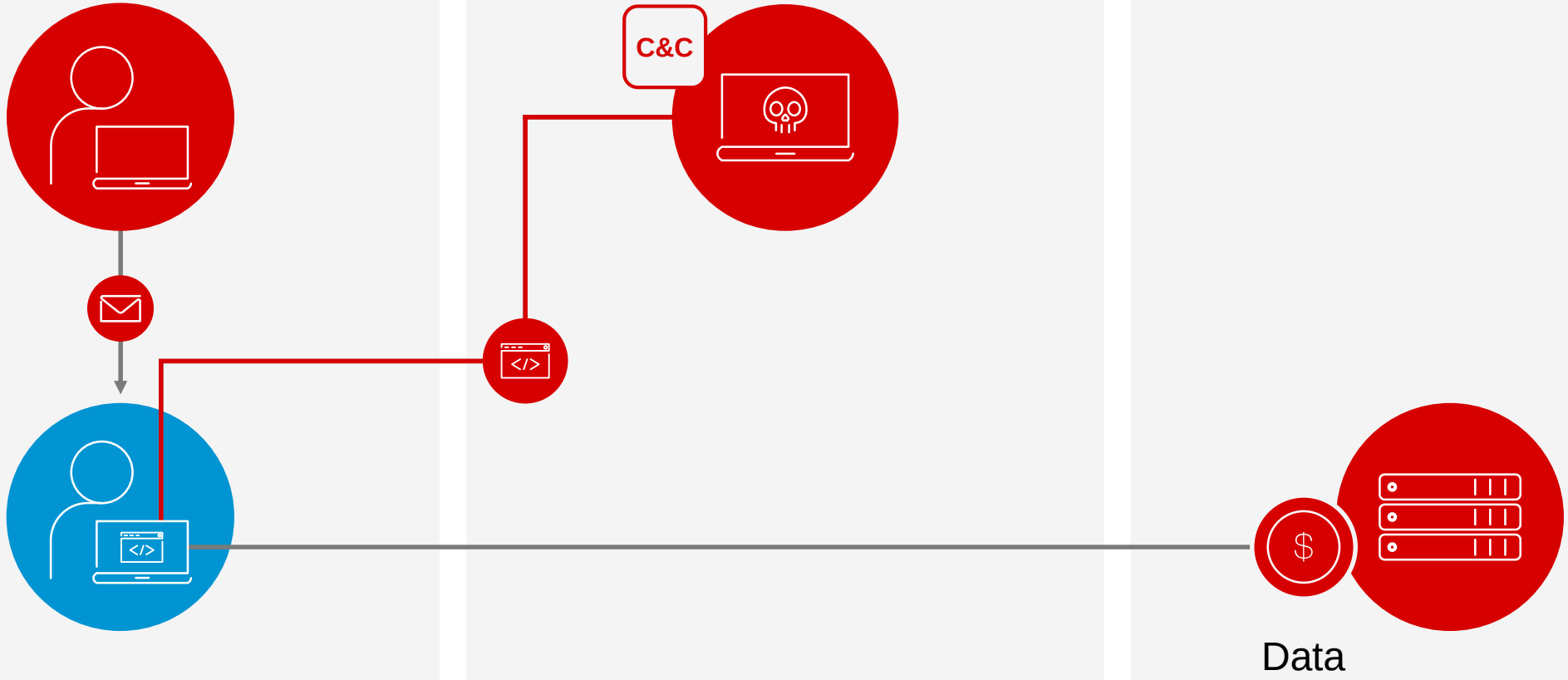


Získat data díky šifrování

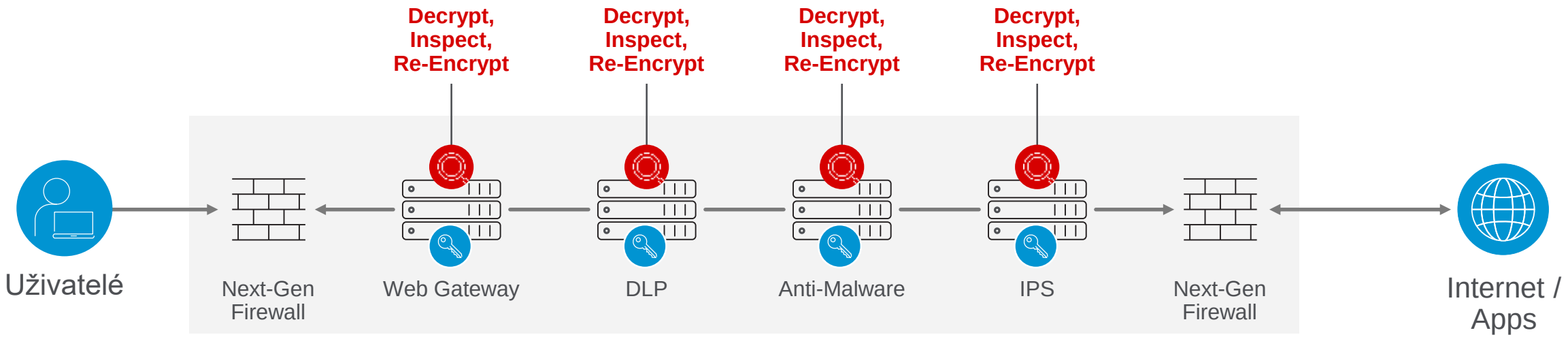
Využití uživatele

Command & Control

Exfiltrace dat



Jak to běžně vypadá s bezpečností a šifrováním?

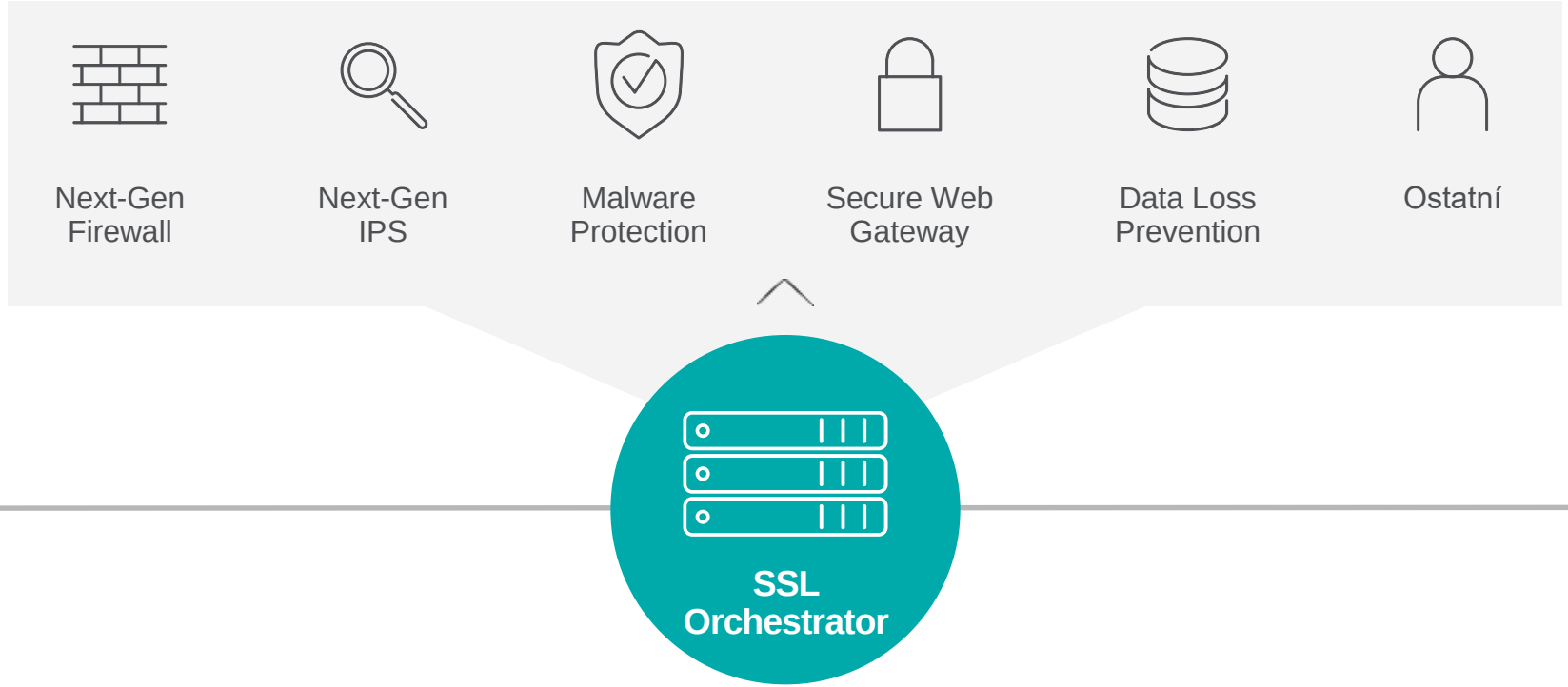


NNS Labs testovali Firewall v tomto scénáři

Čas odezvy narostl o **672%**

60% provozu bylo zahozeno/nezkontrolováno

SSL Orchestrator



Blind spot eliminován

Viditelnost nestačí

Stále potřebujeme jednoduchou správu, skupiny, pravidla…

ALEF

Akcelerace

Zrychlení přenosu

Úspora linky (o 40 %)

Chytré rozložení zátěže

Bezpečnost

Dobrý a špatný Bot

DDoS ochrana L3-L7

SQL Injection, …

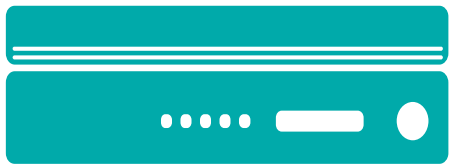
OWASP 10

BA

SSO

1 min

HOT FIX



BYOD

ALEF

Řešení

Něco pro vývojáře?


400M
sites run NGINX
WE HAVE TREMENDOUS INSIGHT INTO APPLICATION PATTERNS

Three challenges enterprises face in digital

CUSTOMER EXPERIENCE

BUSINESS AGILITY

DIGITAL ROI

Three mistakes customers make

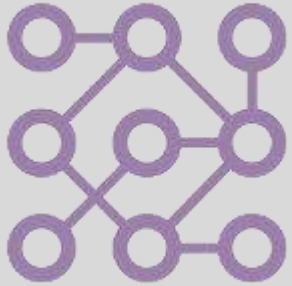
INFRASTRUCTURE LOCK-IN

Limits application portability across clouds

SECURITY & NETWORK BOTTLENECK

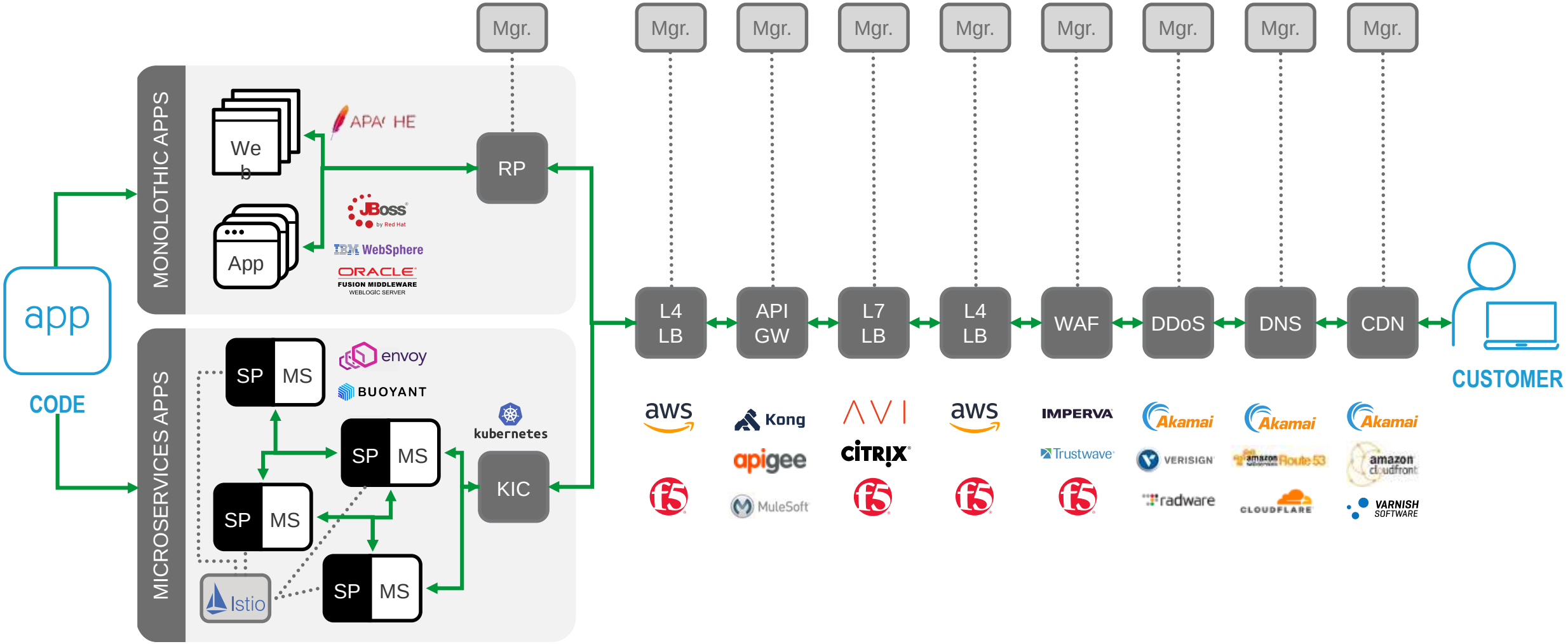
Prevents agility and collaboration among roles

TOOL SPRAWL

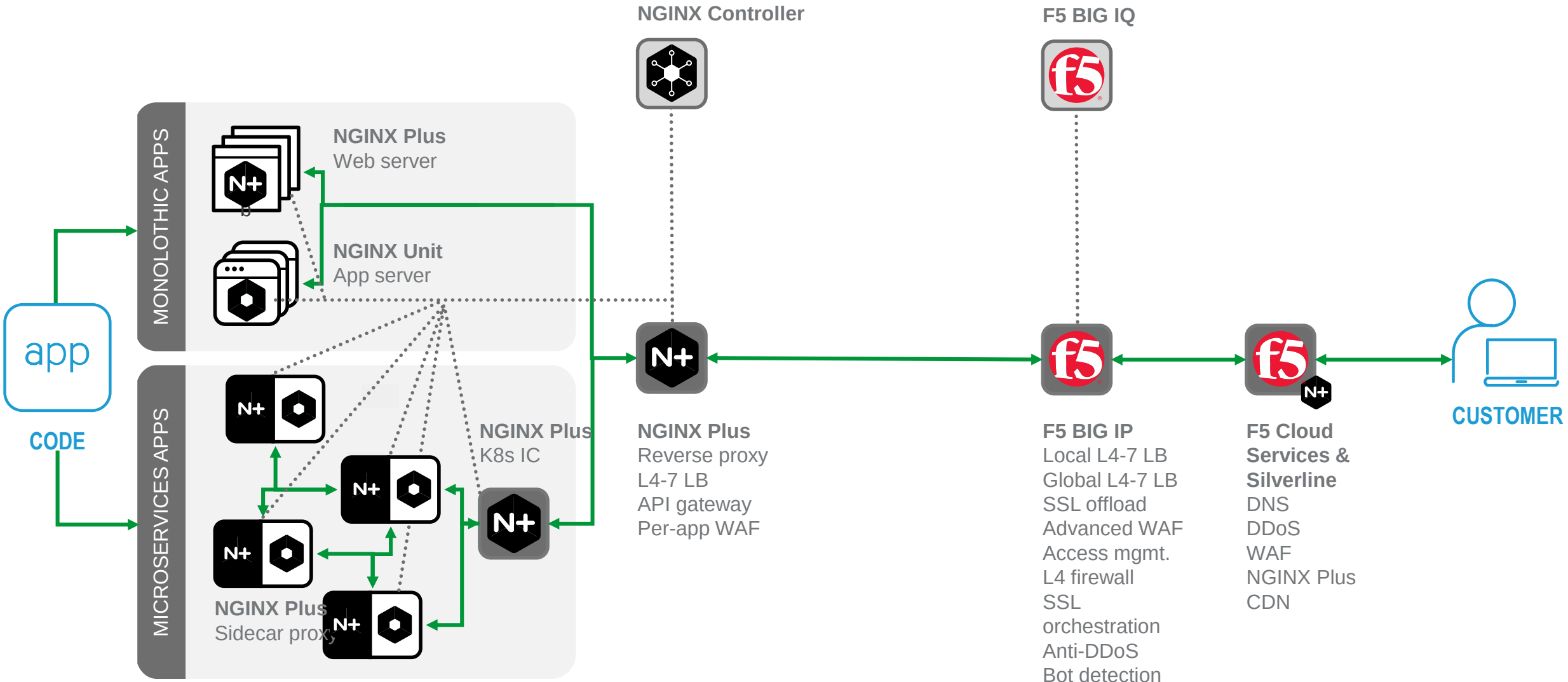


Leads to complexity and higher costs

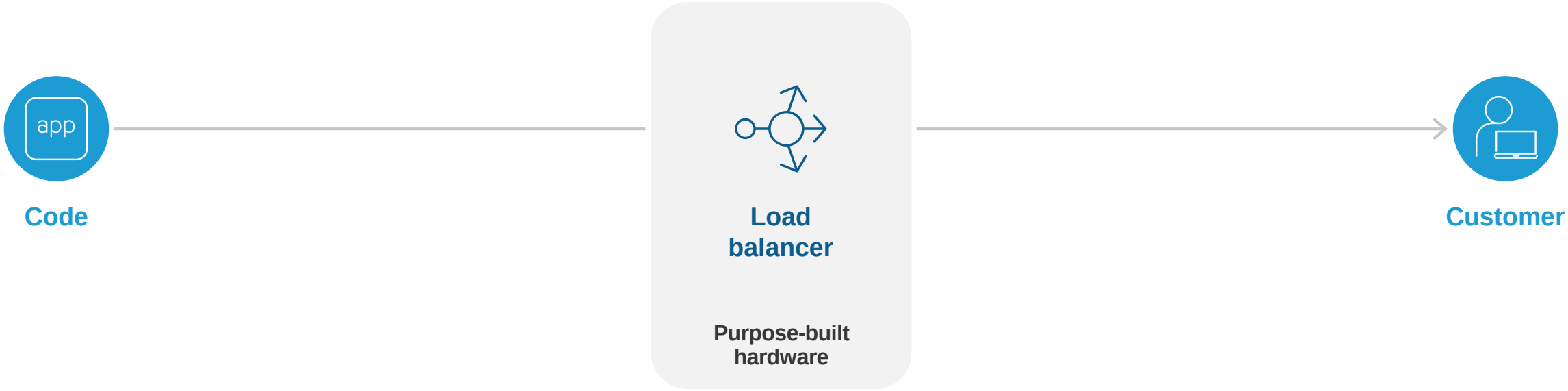
Today's architectures are a complex patchwork of tools spanning from code to customer



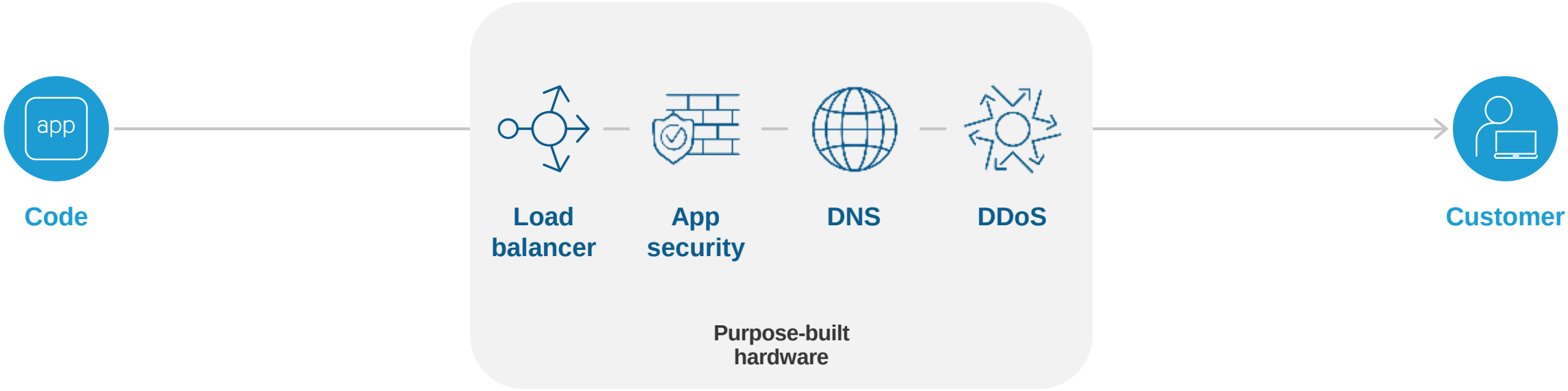
Complement F5 with a platform that simplifies your environment, reducing 13 platforms to 3



Early 2000's: Hardware load-balancers

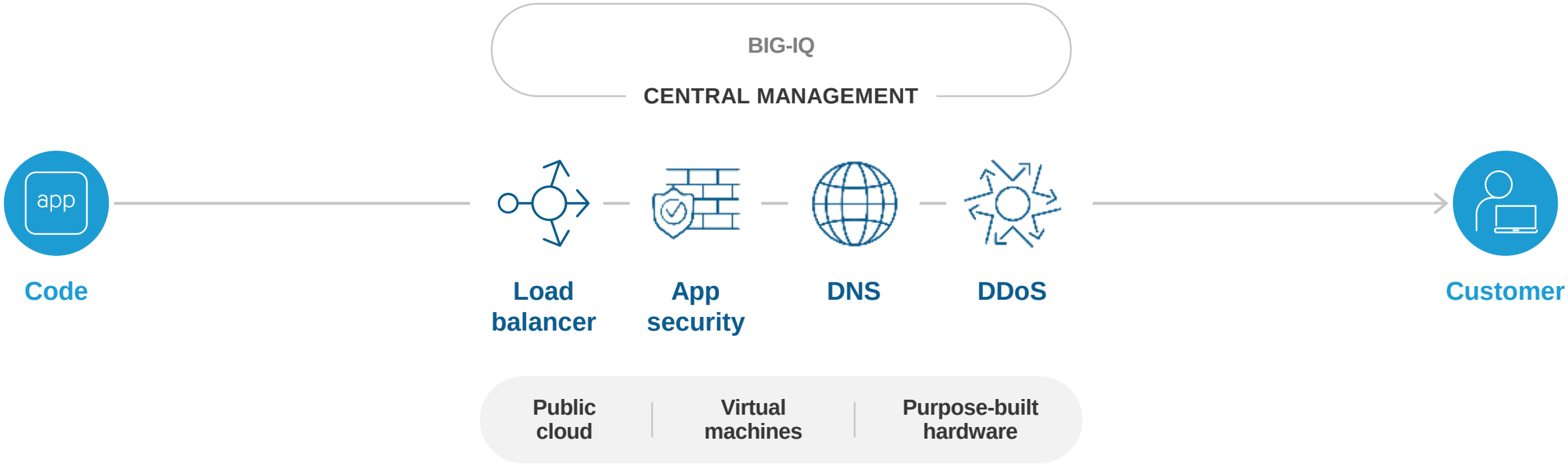


2005 to mid 2010's: Hardware ADCs

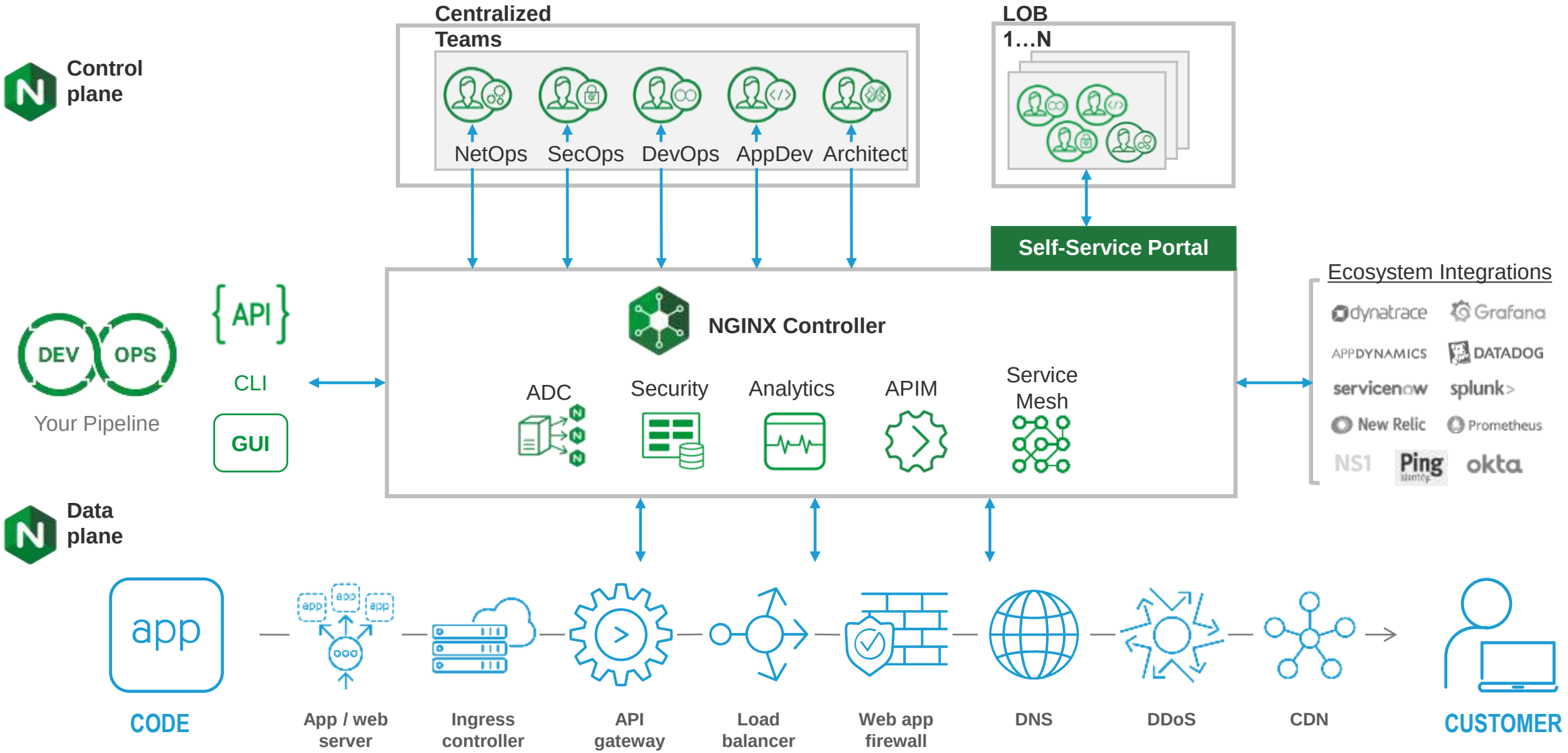


Mid 2010's: Services decoupled from the underlying infrastructure

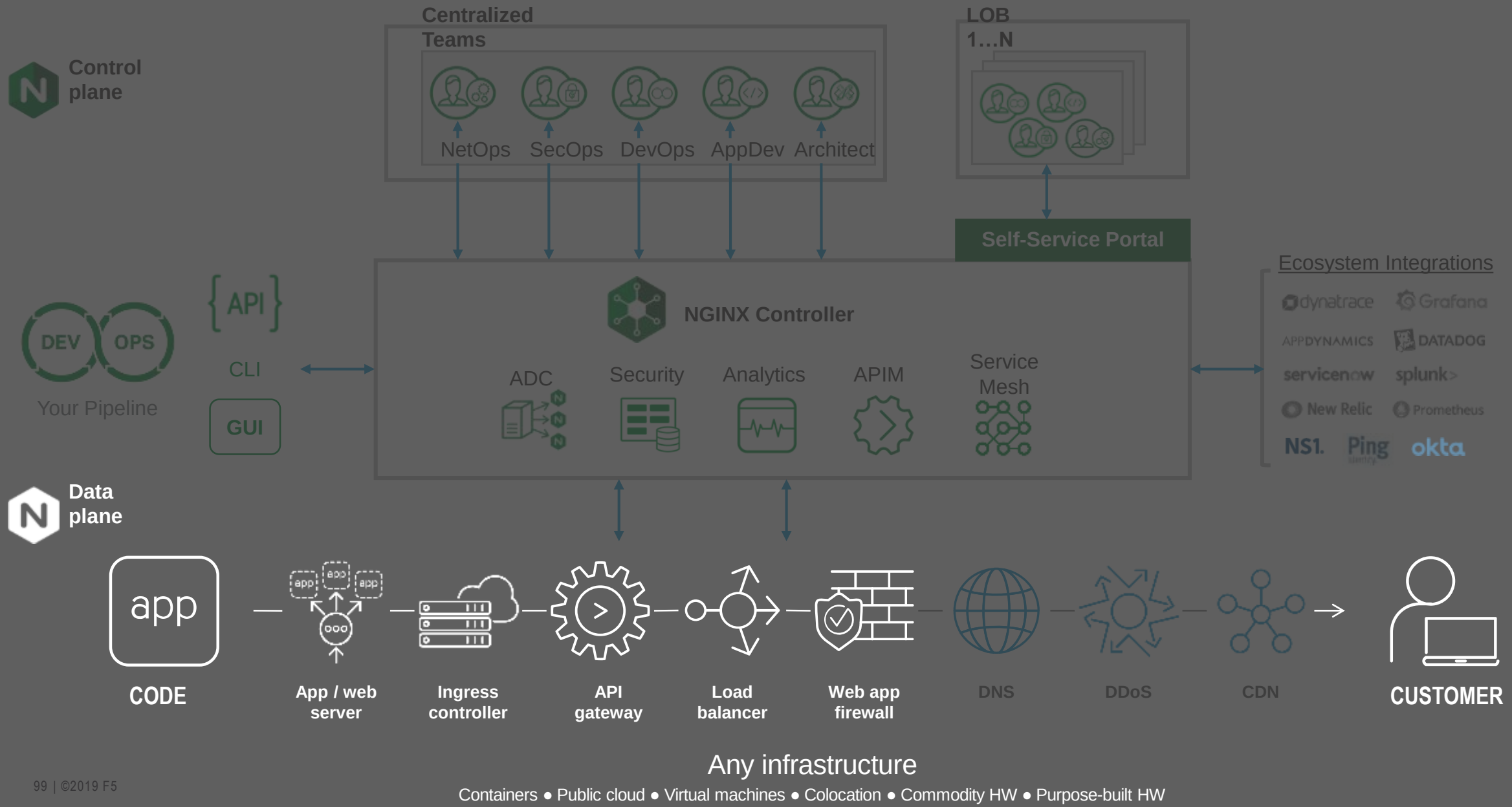
Mid 2010's: Central Management introduced to reduce operational overhead



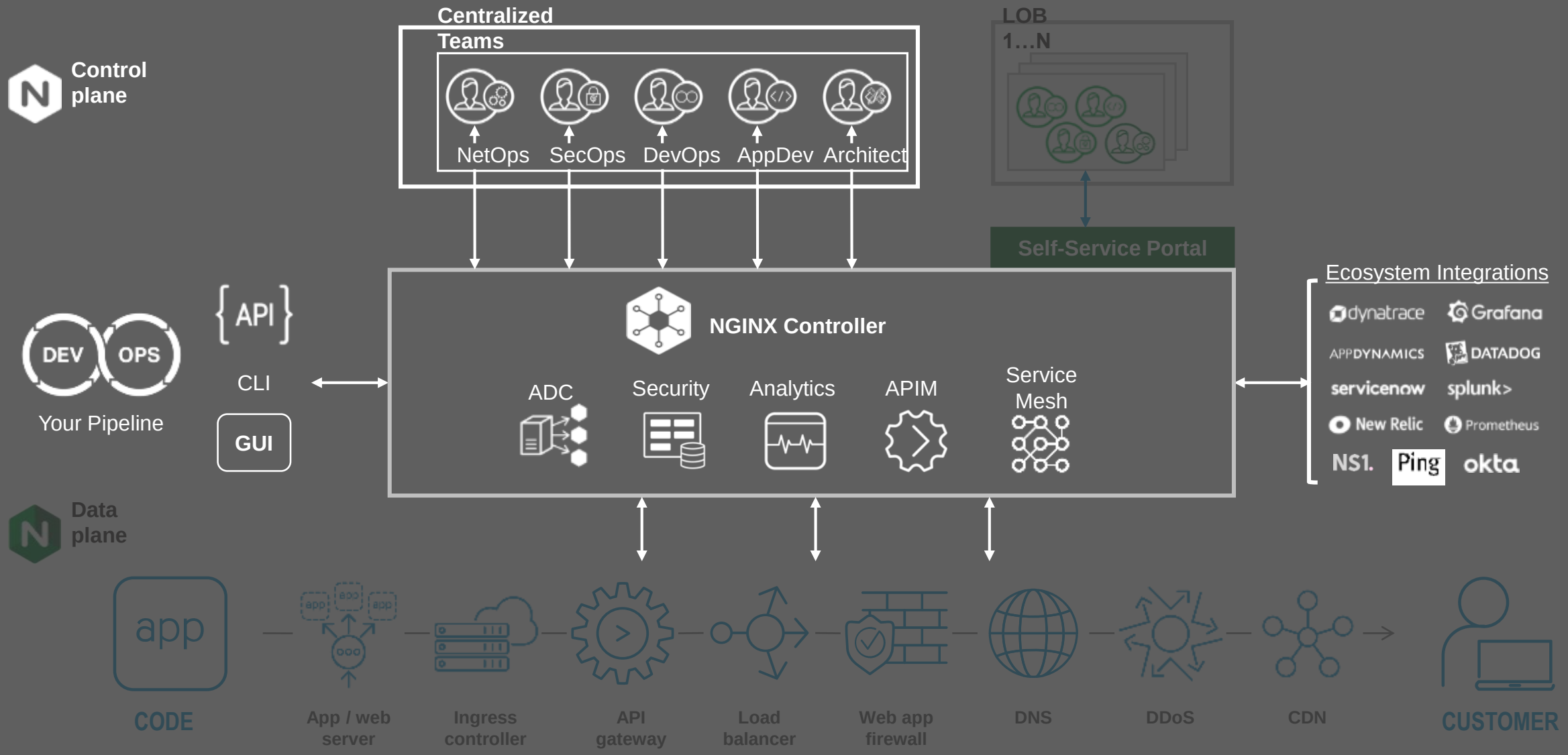
Let's dive into how NGINX Controller can help you today



Eliminate tool sprawl | Bake security in | Abstract underlying infrastructure

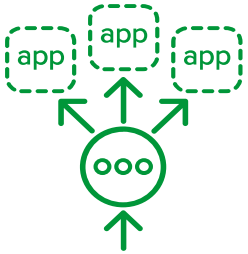


Give persona-specific views | Get end-to-end visibility | Automate intelligently | Integrate with ecosystem



Get Started with F5 and NGINX

FOUR WAYS TO USE NGINX TO DELIVER CODE TO CUSTOMERS

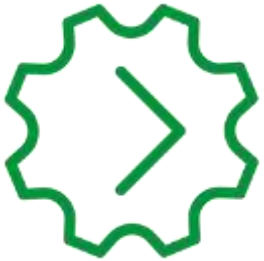


Migrate Hardware to Software ADC

Per-App and DevOps integrated load balancing

Scale ADCs Across Multi-Cloud

Secure and portable apps across multi-cloud

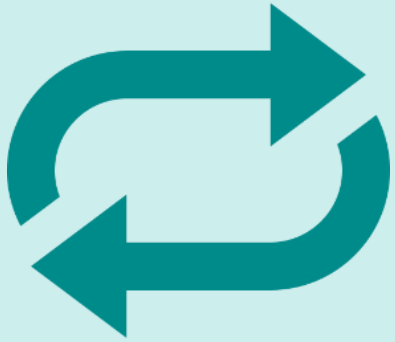


Deploy API Management

End-to-end API lifecycle services

Modernize Apps and Build New Apps

Lightweight, efficient service mesh and Kubernetes IC



LTM

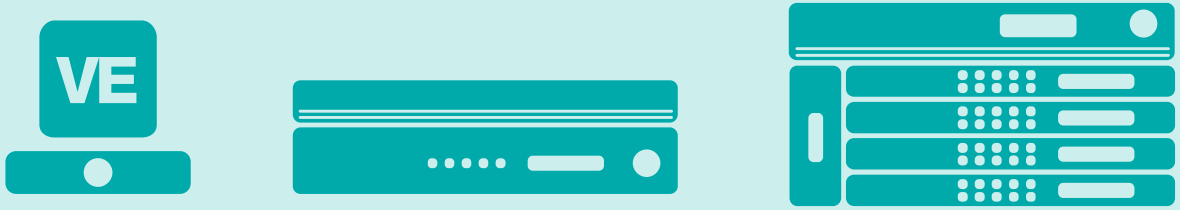
Local Traffic Management

aWAF

Advanced Web Application Firewall

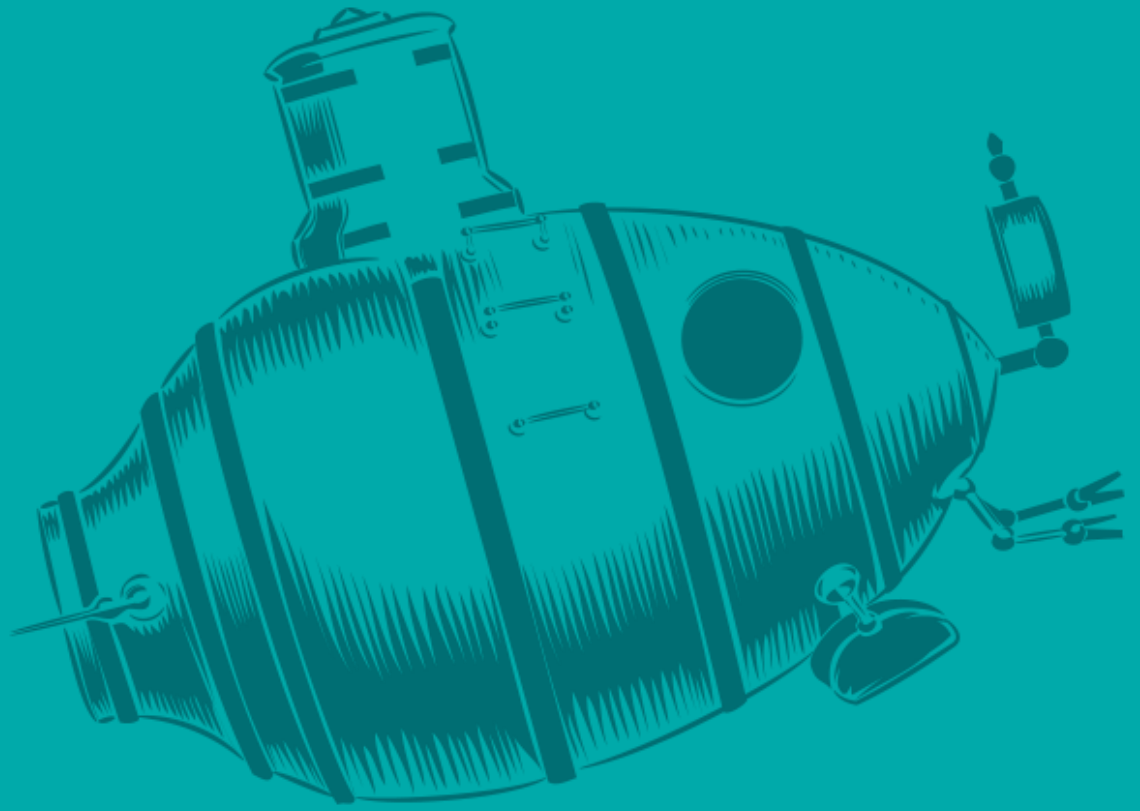
APM

Access Policy Manager



ALEF

kampaně FY 2020



Michal Motyčka
michal.motycka@alef.com

Lukáš Beňo
lukas.beno@alef.com

Kampaň č. 1

ASM > aWAF

ALEF

ASM to aWAF

ASM

- BOT protekce
- Limitovaná BDos detekce
- OWASP Top 10
- Několik LB metod

aWAF

- BOT protekce
- Plná BDos detekce
- OWASP Top 10 compliance
- Sada basic LB metod
- Credential Stuffing DB
- Datasafe
- AntiBot Mobile SDK *
- Threat Campaigns **

ASM to aWAF

ASM

aWAF

Threat Campaigns

ALEF

Kampaň č. 2

SSL O + Firepower

ALEF

Děkuji za pozornost!