Limity tradičního Security Perimetru: Jak s nástupem Cloudu ochránit poskytované služby (aplikace)?

PRESENTED BY:

Filip Kolář, F5 Networks

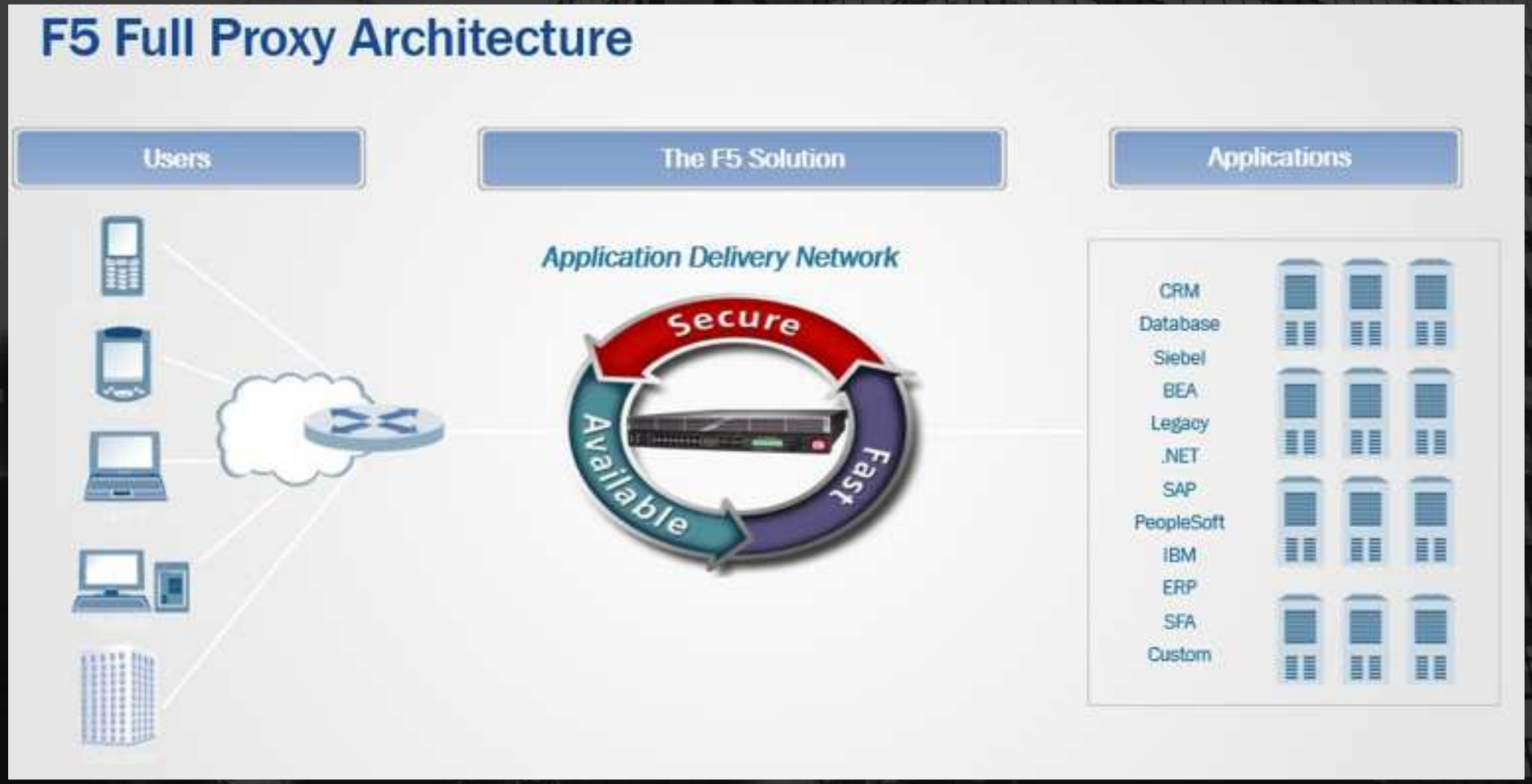
2. Dubna 2017

WE MAKE APPS GO FASTER. SMARTER. SAFER.

Nejstrašidelnější maska na Haloween…

KDO JE F5 NETWORKS?

F5 = “Application Delivery”
Dostupné, rychlé a bezpečné aplikace



20 let na trhu, 9 let leaderem dle Gartnerova MQ

Gartner Magic Quadrant for Application Delivery Controllers, 2016

Jsme u těch největších…

F5 je součástí všech klíčových Cloudových platforem

Cloud Service Providers

amazon web services™
Windows Azure
SOFTLAYER an IBM Company
Google Cloud Platform Live

Managed Service Providers

rackspace the #1 managed cloud company
DATAPIPE
CenturyLink
ColoSpace
Joyent Cloud Computing
CSC

Traditional Providers

verizon
at&t
NTT
BT
Telefónica
SingTel
中華電信 Chunghwa Telecom

Integrated Players

CISCO Intercloud
hp Cloud
vmware vCloud Air™ Network
WIPRO Applying Thought
IBM
ORACLE CLOUD

REDUCED COSTS
FLEXIBILITY
SERVICS RICH
MORE MOBILITY
HIGHLY AUTOMATED
EASY TO IMPLEMENT
END USER PRODUCTIVITY

JAKÉ JSOU DNEŠNÍ VÝZVY S POSKYTOVÁNÍM APLIKACÍ?

Tradiční Datové Centrum

VÝHODY

- Jednoduchost
- Kontrola zařízení
- Bezpečnost

NEVÝHODY

- Statické
- Omezená škálovatelnost
- Vstupní investice

Budoucnost: Cloud

Zvýšení produktivity

Zrychlit inovace

Snížit náklady na IT

Díky Cloudu zažíváme obrovský rozmach využívání business aplikací

715
Average number of apps per enterprise[1]

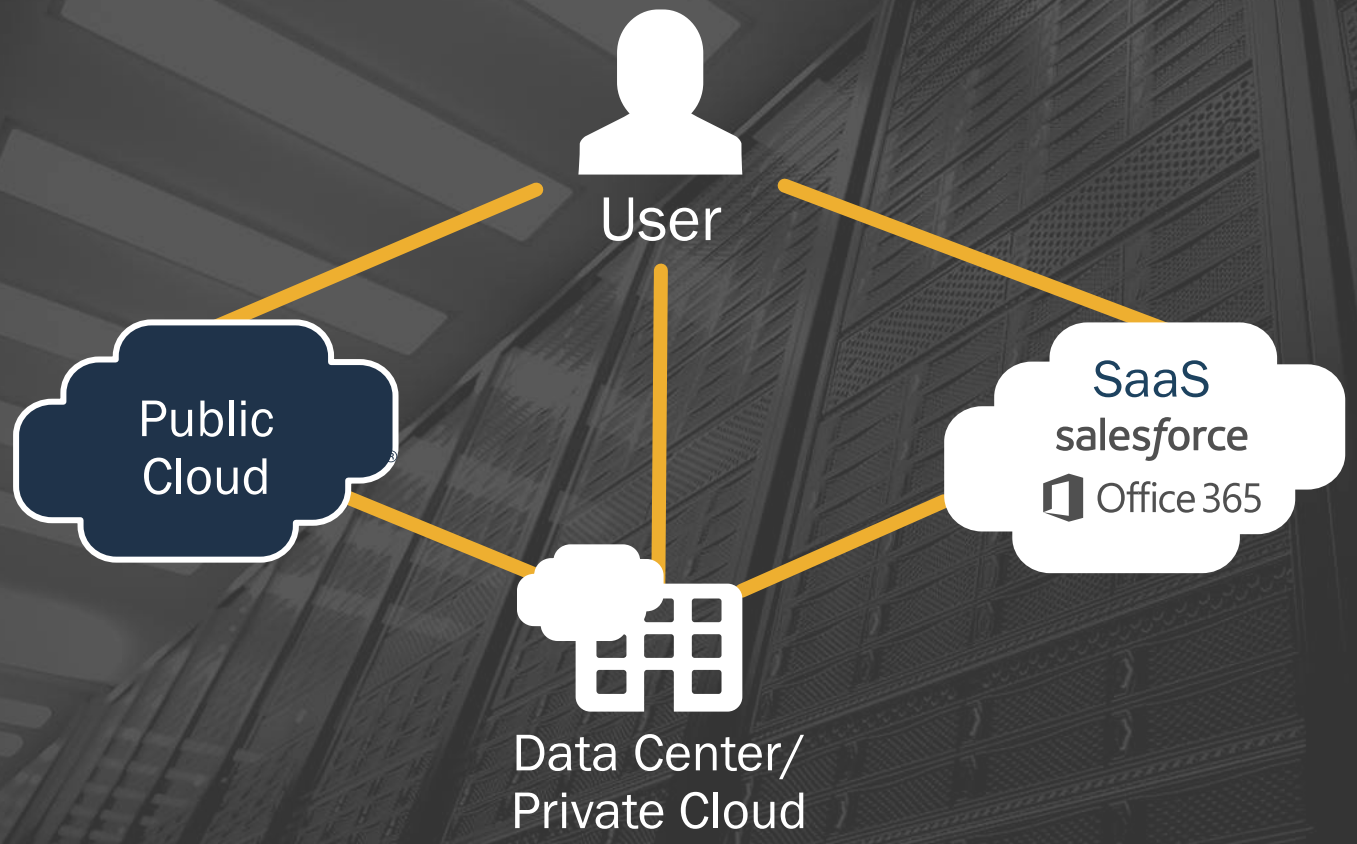
26.8
Average number of apps per worker[2]

82%
Enterprises with a hybrid cloud strategy, up from 74% in 2014[3]

90%
of organizations concerned about public cloud security[4]

Sources: [1]NetScope, [2]F5 State of Application Delivery Survey, 2015, [3]Cloud Security Spotlight Report, [4]Information Security Linkedin Group, 2015

Dnešní typická architektura přechodu do Cloudu



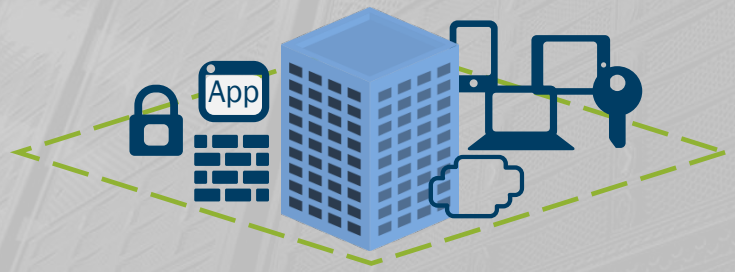
- Heterogenní prostředí
- Různá úroveň bezpečnosti
- Nesourodá SLA vůči koncovým uživatelům
- Omezená flexibilita dalšího IT rozvoje

Vzniká “Security gap” v důsledku heterogenních ostrůvků

Regional DC

Cloud A

Cloud B



Primary DC

Nekonzistentní bezpečnostní a přístupové politiky jsou příležitostí pro narušení kybernetické bezpečnosti

V tradiční modelu jsou data a uživatelé chráněni v rámci bezpečnostního perimetru

Cloudové aplikace ale mění pravidla hry…

3.2 billion unknown users 7.4 billion unsecured devices	1 Billion Applications	44 ZB of Data by 2020

Dnešní hlavní cíl:
Ochránit uživatelskou identitu, aplikace a data

JAKÁ JE POVAHA DNEŠNÍCH ÚTOKŮ?

Útoky se přesouvají ze síťové na aplikační vrstvu …ovšem investice směřují do síťové…

Network Threats

28%
of attacks are focused here

90%
of security investment

Application Threats

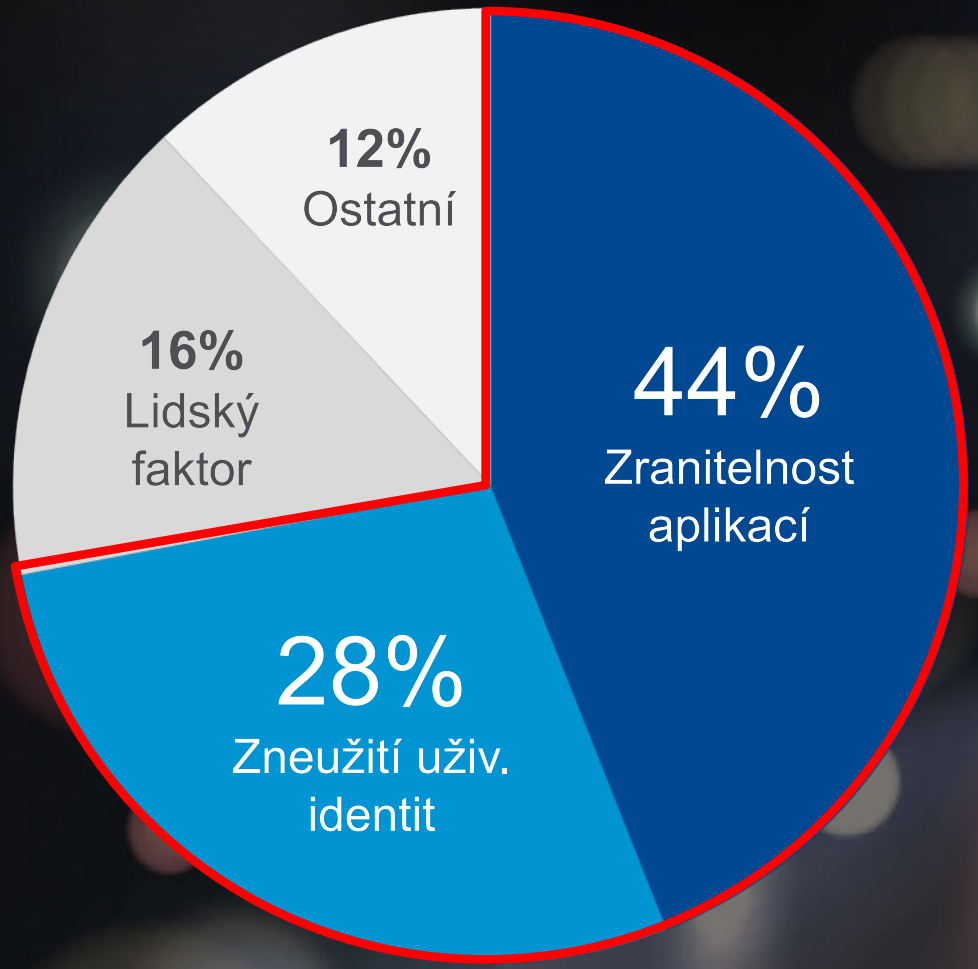
72%
of attacks are focused here

10%
of security investment

Source: Gartner. 2016

72% narušení kyber bezpečnosti je způsobeno zranitelností aplikací a zcizením uživatelských identit

Source of data breaches



1.2B
Compromised records since 2014

$15M
Average cost of an attack

46
Average days to resolve an attack

514M
Personal Profiles Stolen

$210M
Credit Card Fraud in 2015

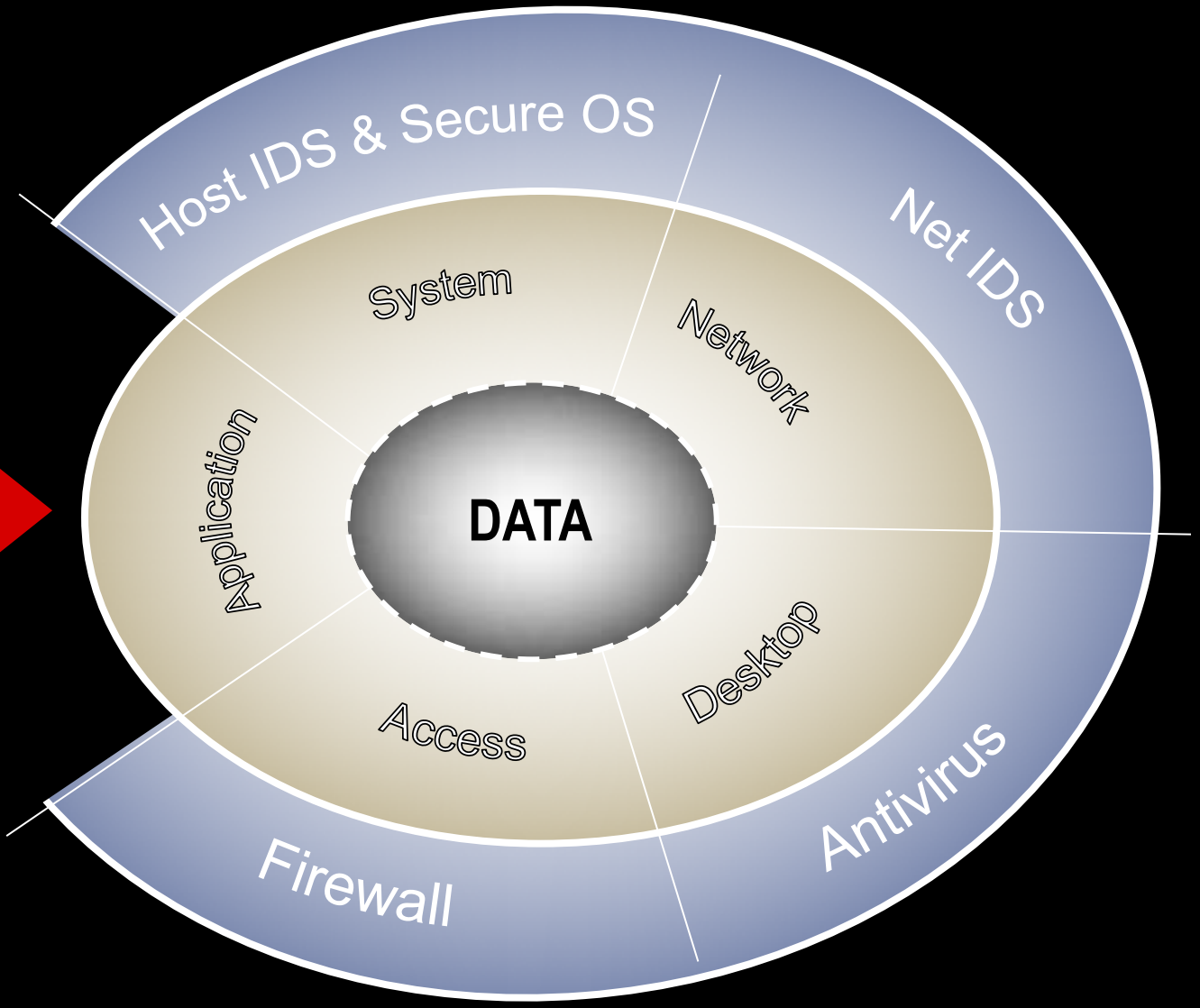
Source: Based on aggregated data from IT Business Edge, Krebs on Security, Security Week, and CSO Online

Protože právě data/aplikace mají hodnotu…

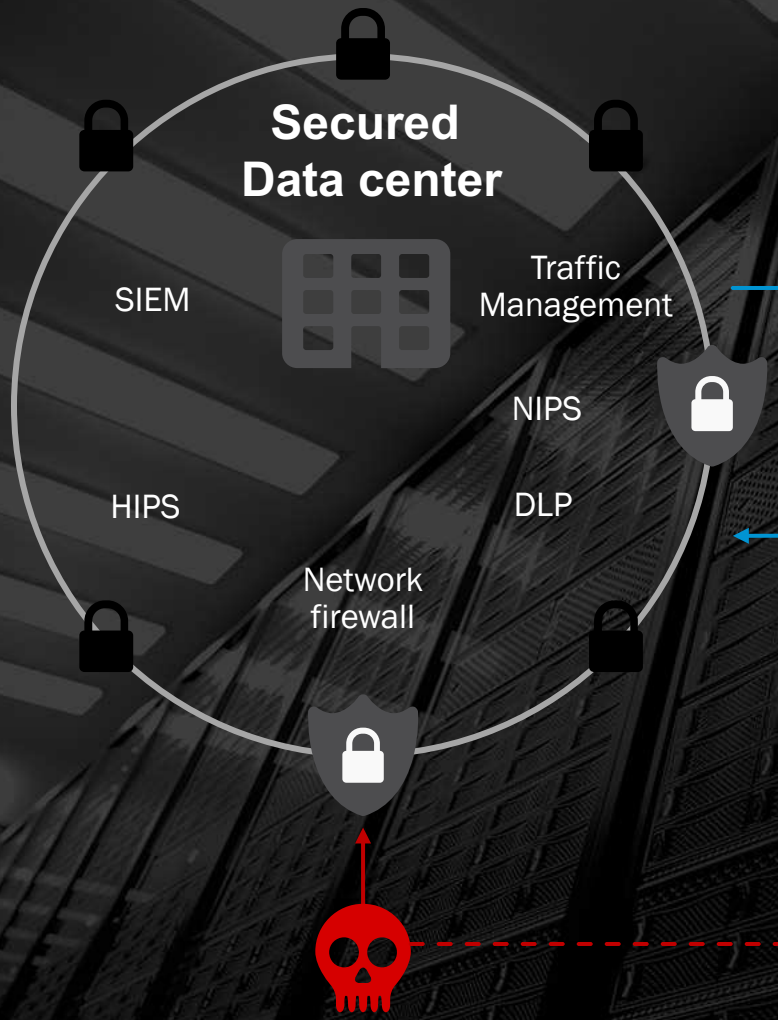
Kde je tedy ten ”Security Gap”?

“64% of the 10 million security incidents tracked targeted port 80.”

Information Week



Prohlížeč je nejslabší článek řetězce…



HTTP/HTTPS

Customer Browser

Leveraging Browser application behavior

- Caching content, disk cookies, history
- Add-ons, Plug-ins

Manipulating user actions:

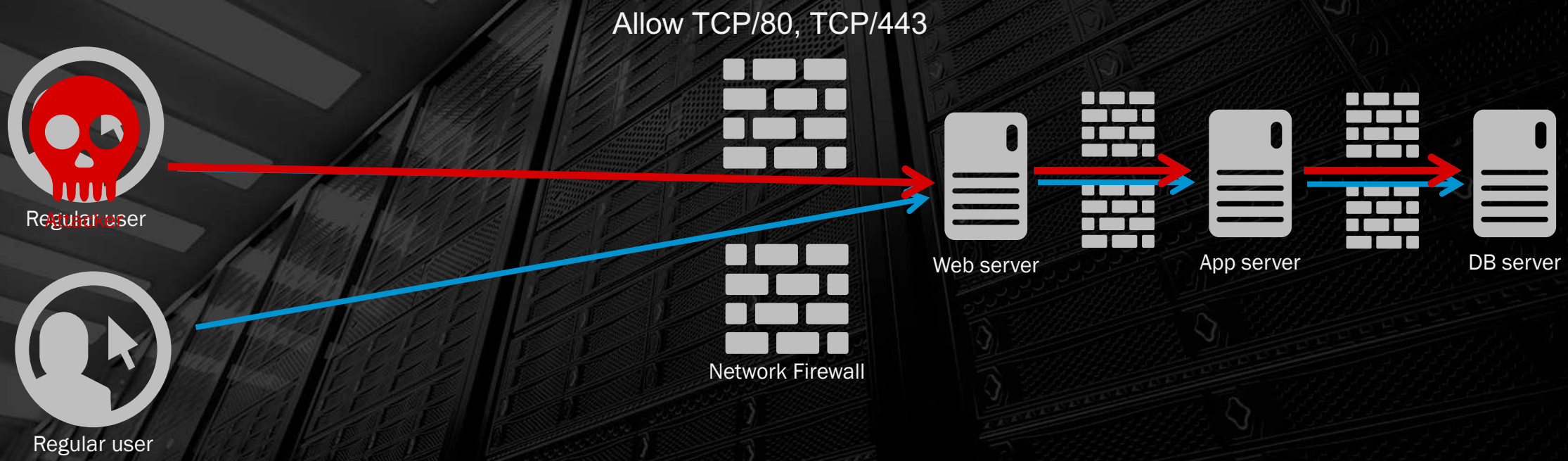
- Social engineering
- Weak browser settings
- Malicious data theft
- Inadvertent data loss

Embedding malware:

- Keyloggers
- Framegrabbers
- Data miners
- MITB / MITM
- Phishers / Pharmers

Proč?

Současný perimetr se zaměřuje na útoky na síťové vrstvě…



DŮLEŽITOST APLIKAČNÍ OCHRANY

Jaké jsou dnes typické útoky na aplikace?

CSRF
OWASP top 10
Forceful browsing
Web scraping
SQL injections
Field manipulation
Cross-site scripting
Command injection
Bots

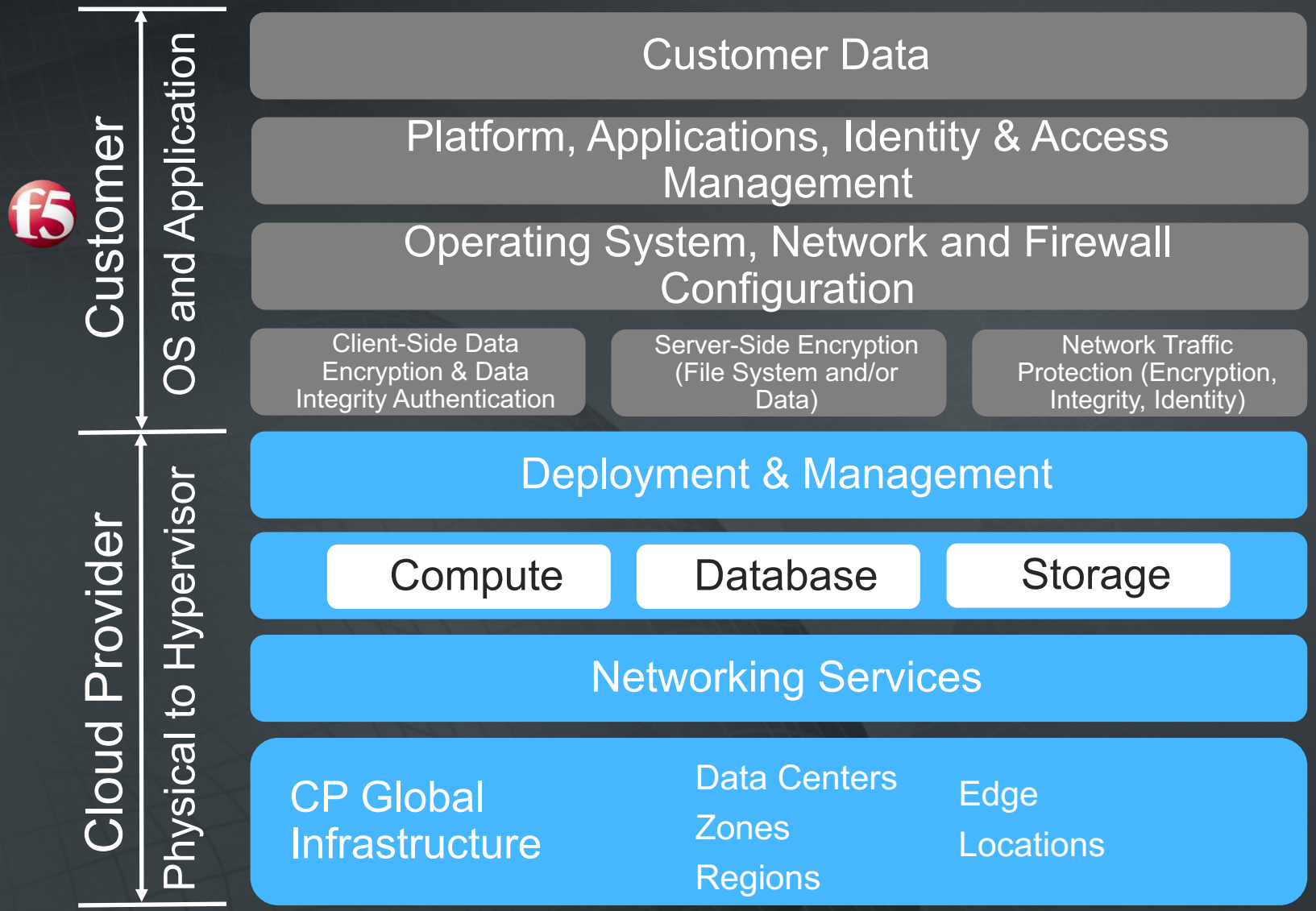
Cookie manipulation
Brute force attacks
Buffer overflows
Parameter tampering
Information leakage
Session high jacking
Zero-day attacks
ClickJacking
Business logic flaws

Jaký je nejvhodnější nástroj pro ochranu aplikací?

	Network / Next Gen Firewall	*IPS*	*Web Application FW*
Known Web Worms	Limited	✓	✓
Unknown Web Worms	X	Limited	✓
Known Web Vulnerabilities	Limited	Partial	✓
Unknown Web Vulnerabilities	X	Limited	✓
Illegal Access to Web-server files	Limited	X	✓
Forceful Browsing	X	X	✓
File/Directory Enumerations	X	Limited	✓
Buffer Overflow	Limited	Limited	✓
Cross-Site Scripting	Limited	Limited	✓
SQL/OS Injection	X	Limited	✓
Cookie Poisoning	X	X	✓
Hidden-Field Manipulation	X	X	✓
Parameter Tampering	X	X	✓
Layer 7 DoS Attacks	X	X	✓
Brute Force Login Attacks	X	X	✓
App. Security and Acceleration	X	X	✓

Útoky jsou tak jednoduché…

Public Cloud – Sdílená odpovědnost ohledně zabezpečení infrastruktury



Customer's responsibility

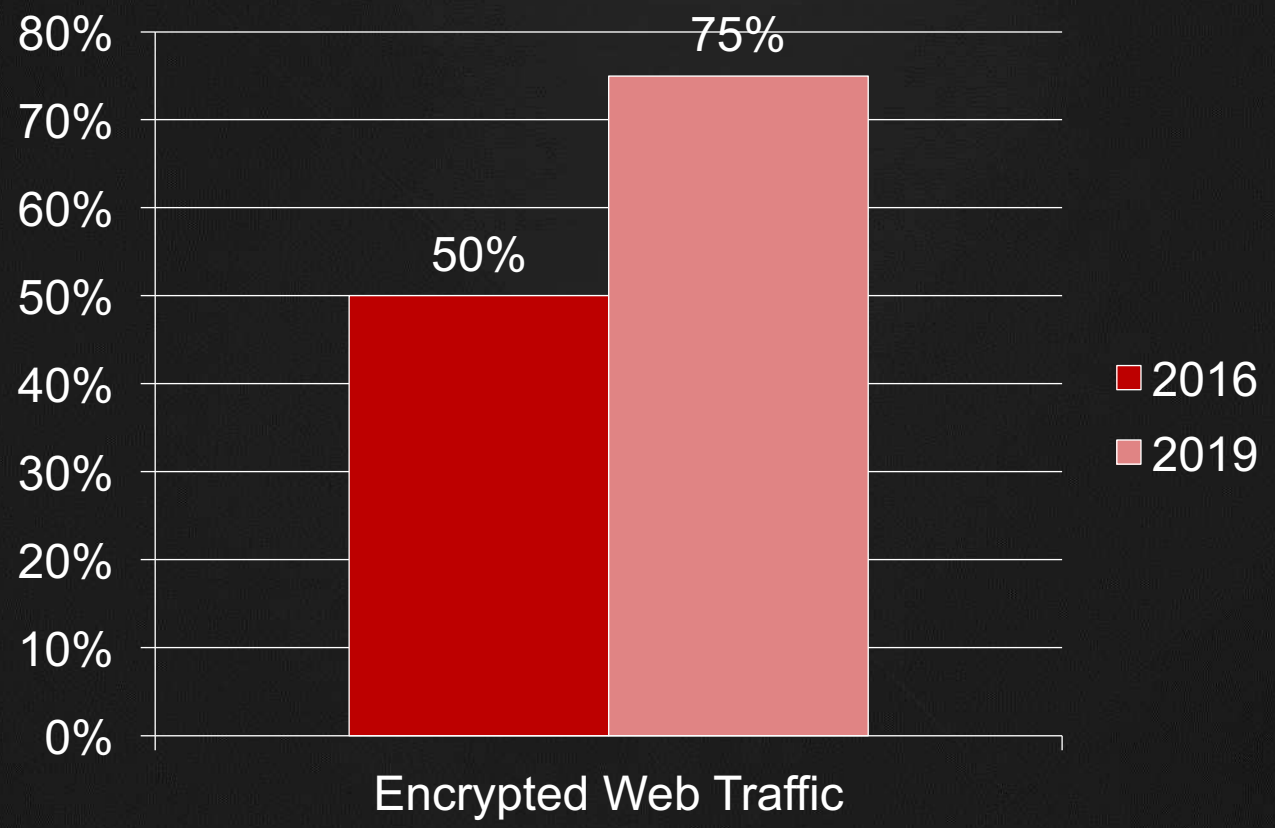
- Protecting the confidentiality, integrity, and availability of their data in the cloud
- OS and application-level security

Cloud Provider responsibility

- Providing a global secure infrastructure and services

VIDÍTE TYTO ÚTOKY?

HTTPS (SSL/TLS) provoz roste meziročně 20%



Source: "TLS/SSL: Where Are We Today?", NSS Labs, October 2016

A jsme zpět u security perimetru – pracujete s SSL?

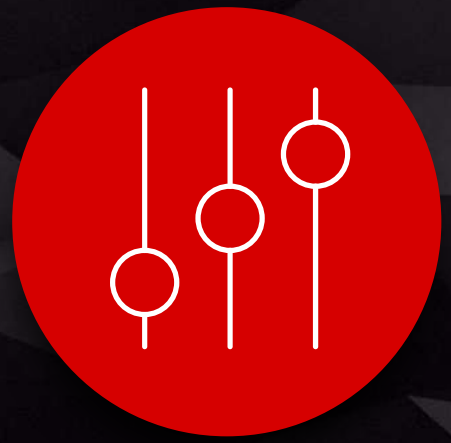
ŘEŠENÍ?

JE MOŽNÉ ZABEZPEČIT DATA NEHLEDĚ NA TO, ZDA JSOU V ”DOMA” NEBO V CLOUDU?

Základy dnešní bezpečnosti:

Visibilita

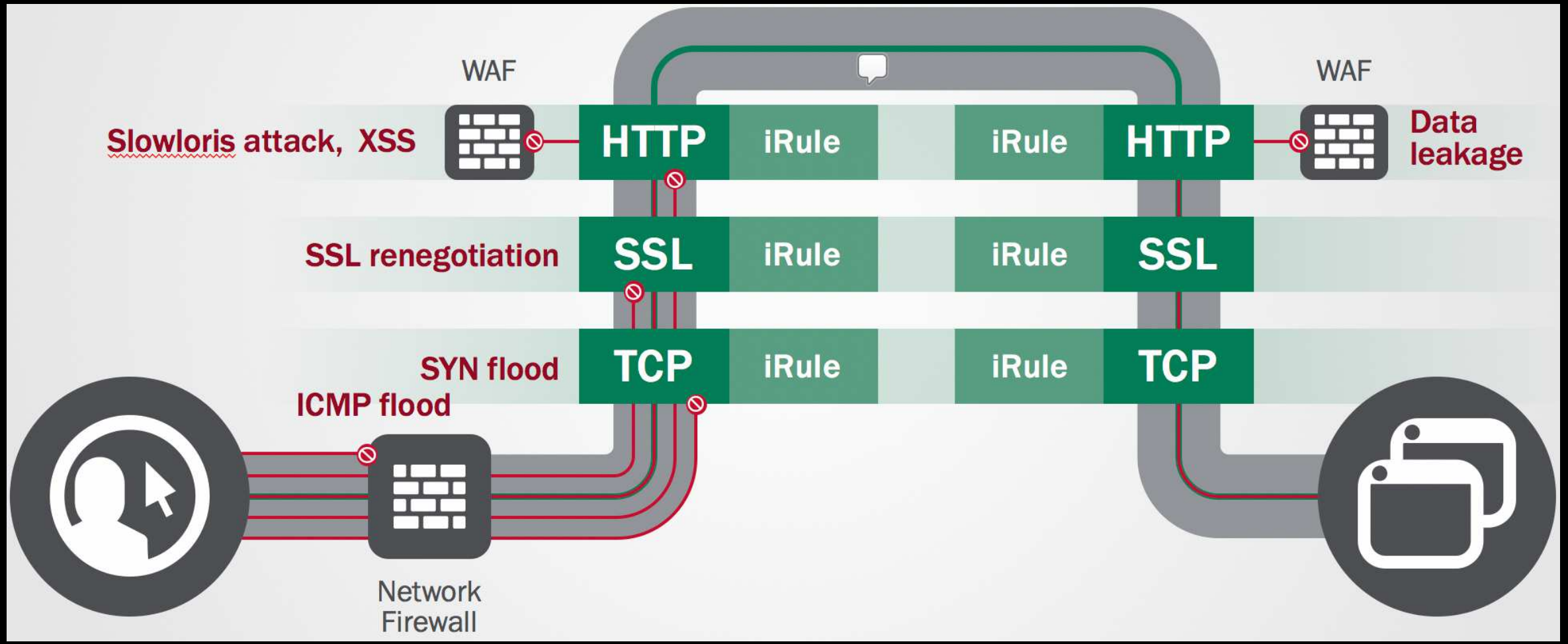
Kontext



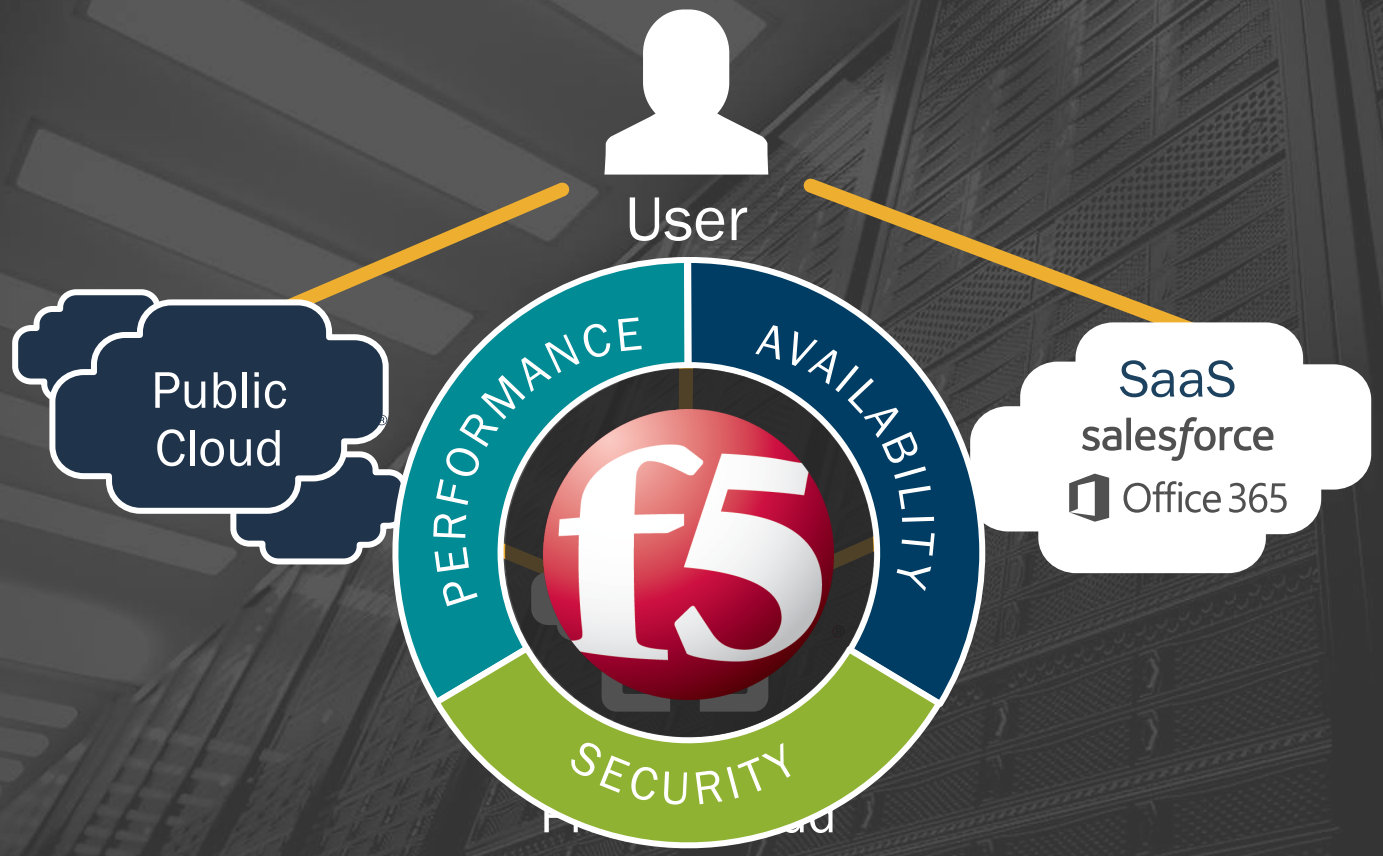
Kontrola

F5 umí zkombinovat všechny 3…

Proxování aplikací – klíčový bezpečnostní koncept



Cílový stav: Aplikačně orientovaná architektura



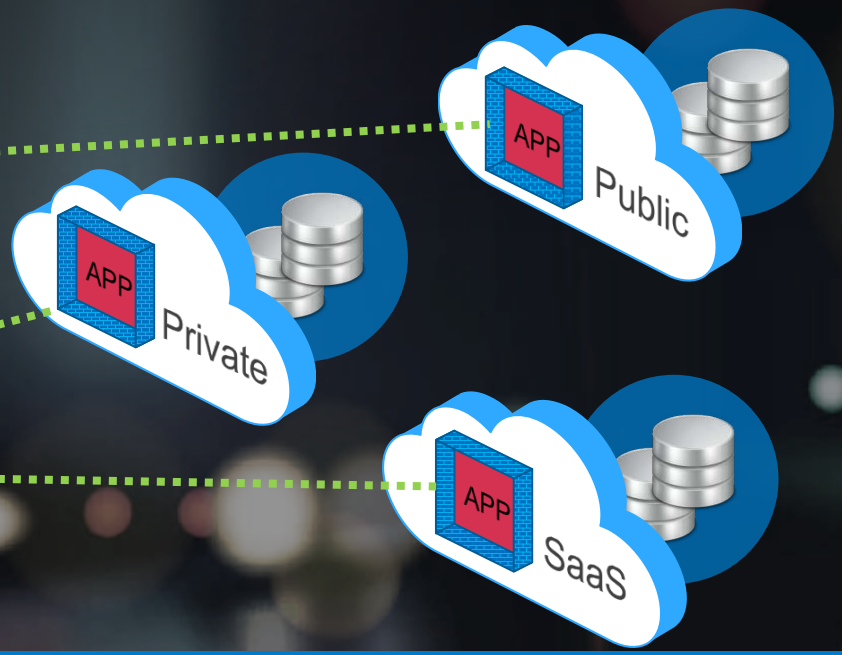
- Konzistentní a škálovatelné prostředí
- Visibilita do SSL provozu
- Aplikační ochrana
- Jednotný přístup

F5 Networks: Komplexní řešení ochrany aplikací a uživatelských dat/přístupů

F5: PŘÍSTUP K APLIKACÍM

- Secure Web Gateway
- Identity Federation
- Remote Access
- App Access Mgmt
- Enterprise Mobility Gateway

F5: OCHRANA APLIKACÍ



- WAF
- DDoS Protection
- Web Fraud Protection
- Carrier Class Firewall
- IP Intelligence
- DNS Security

SSL Inspection & Interception

PARTNER ECOSYSTEM

NGFW	IDS	Data Loss Prevention	APT Scanning
Vulnerability Scanning	Packet / Forensics	HSM	IPS

F5 Synthesis	https://synthesis.f5.com/
DevCentral	https://devcentral.f5.com/
AskF5/Support	https://ask.f5.com/
iHealth	https://ihealth.f5.com/
University	https://university.f5.com/

Děkuji