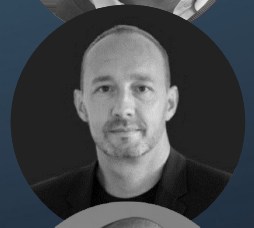
ANECT | F5 | SPCSS

Moderní technologie F5 v cloudových prostředích

ANECT | F5 | SPCSS

Eduard Lorenc
Vedoucí oddělení správy komunikačních technologií/Network Architect, Státní pokladna Centrum sdílených služeb, s. p.



Filip Kolář
Territory Account Manager, F5

Petr Panec
Head of Enterprise Sales, ANECT

ANECT | f5 | SPCSS

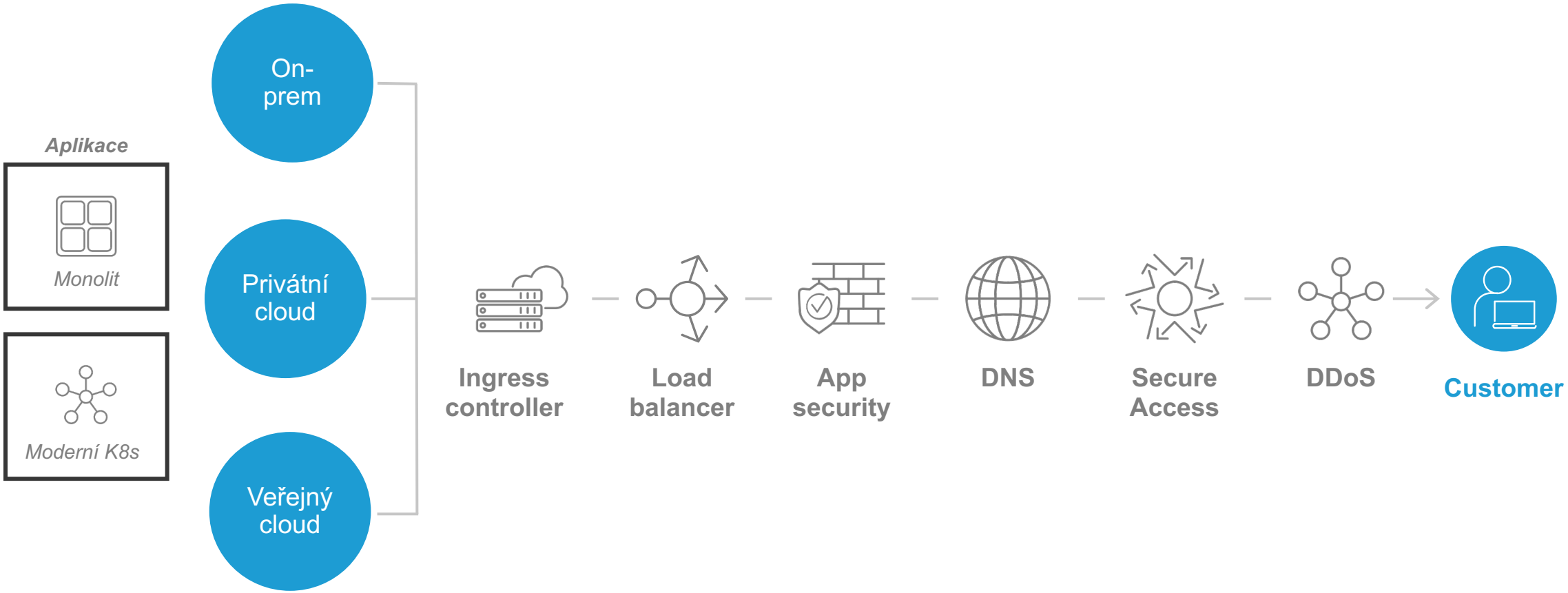
Technologie potřebné pro doručování aplikací (nejen) v cloudu

Filip Kolář
Territory Account Manager, F5

Na úvod kdo nás používá v ČR

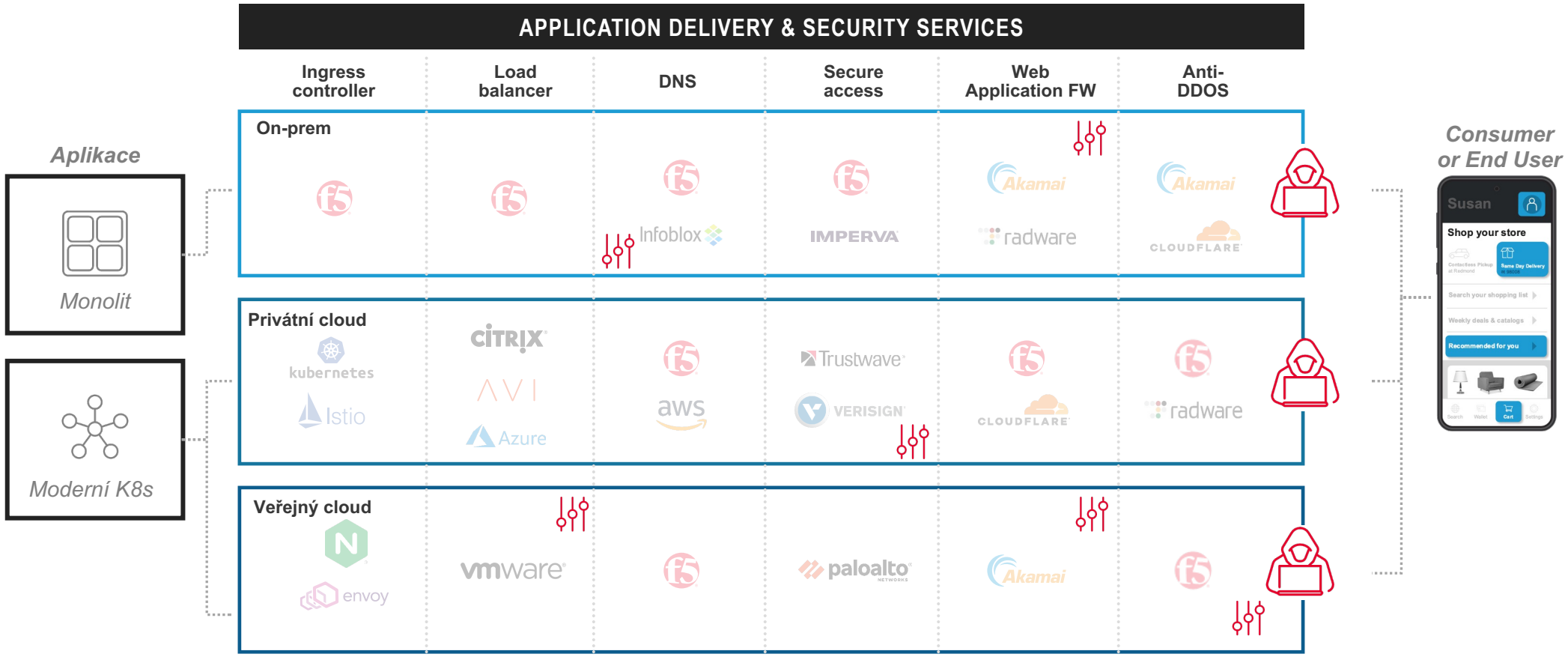
- Finance – Banky, nebankovní instituce, platební brány
- Komerční sektor – Sázkové kanceláře, utility, …
- Operátoři – Telco, ISP, poskytovatelé „manageovaných“ služeb
- Státní správa a podniky - Ministerstva, kraje, velké státní podniky

Jaké aplikační služby jsou dnes nezbytné pro doručování a zabezpečení tradičních a moderních aplikací?

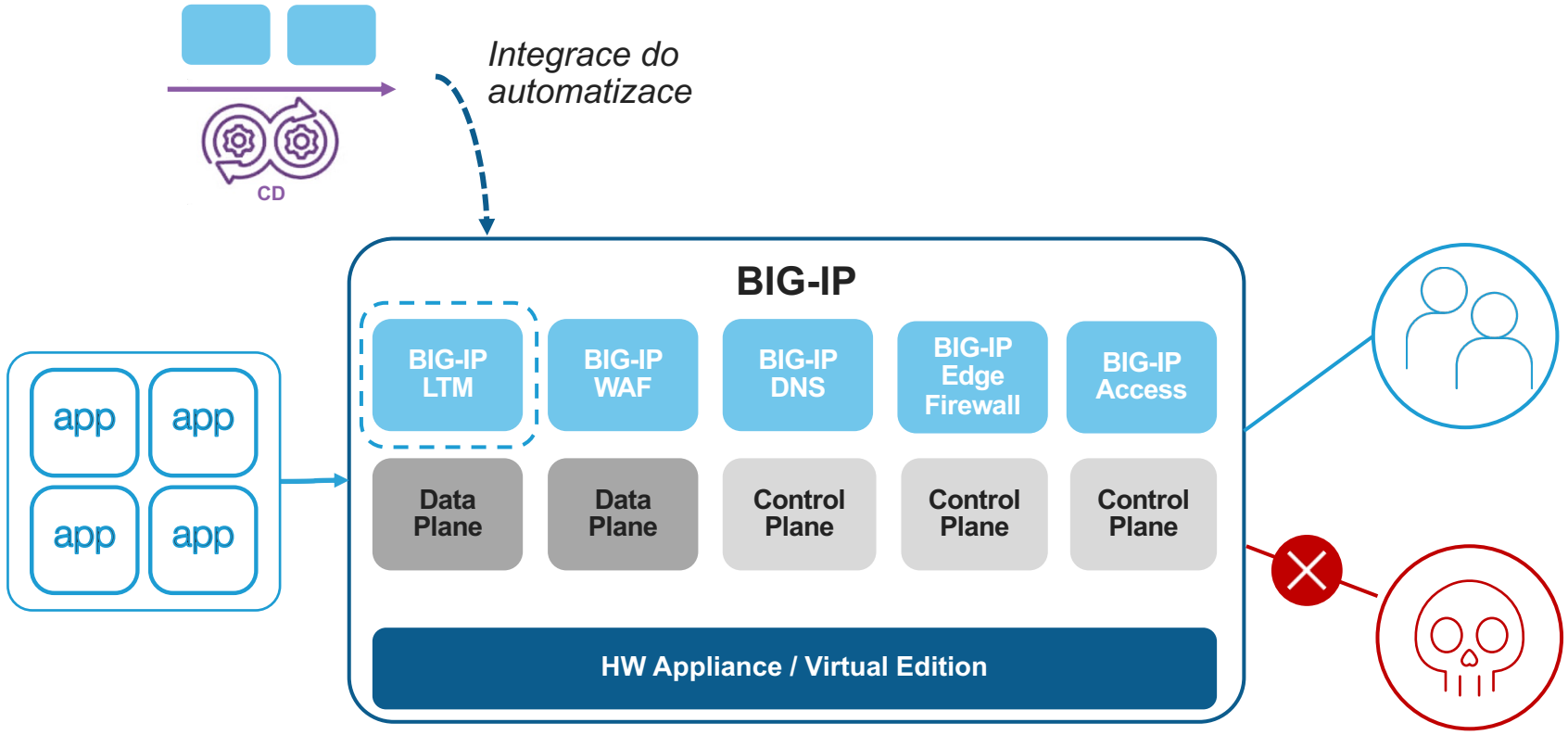


Kombinace více prostředí, typů aplikací a různých dodavatelských řešení znamená komplexitu a příležitost pro útočníky

Fragmented | Inconsistent | Difficult to scale | Trapped data | Vulnerable to attack



Technologie F5 BIG-IP konsoliduje aplikační služby v multi-cloudu pro tradiční i moderní aplikace



Podporuje všechny klíčové platformy a cloudy

Flexibilní licencování umožňuje doručit jakoukoli velikost projektů

Virtual – Private / Public Clouds

F5 Virtual Editions

Provide flexible deployment options for virtual environments and the cloud, both private and public

HighPerf VE supporting addon's:

- HW accelerated SSL
- HW accelerated DDoS/FastL4/NAT

Physical

F5 physical ADCs

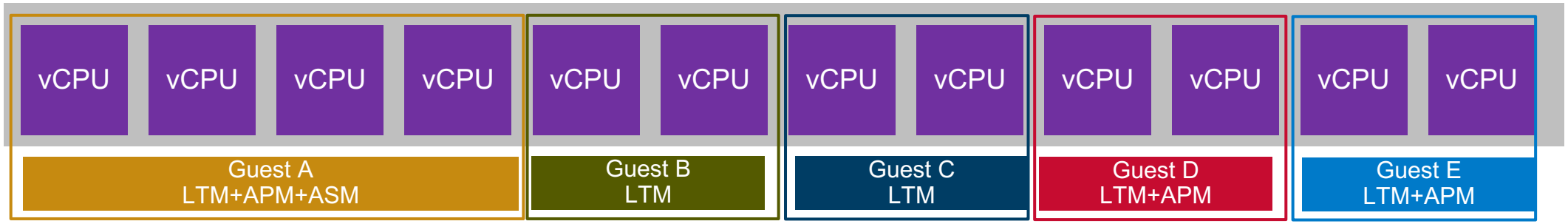
High-performance purpose-built hardware
All in one HW+SW

Best for:

- HIGH Performance / Scale
- Edge and Front Door Services

F5 BIG-IP umožňují separaci zdrojů pomocí Partitions, Routing Domén a per vCPU

SEPARACE ZDROJŮ NA FYZICKÝCH ZAŘÍZENÍCH



Externí aplikace

Interní Aplikace

Kritické aplikace

Předprodukce

Test

ANECT | f5 | SPCSS

Ingress controller

Load balancer

Vysoká dostupnost aplikací (LTM, Container Ingress)

BIG-IP LTM je na trhu synonymum pro řešení vysoké dostupnosti aplikací

Load-Balancing

Distribute application load across multiple servers and multi-cloud to increase availability

Health Monitory

Verify health and performance to check the status of applications and resources

Řízení provozu

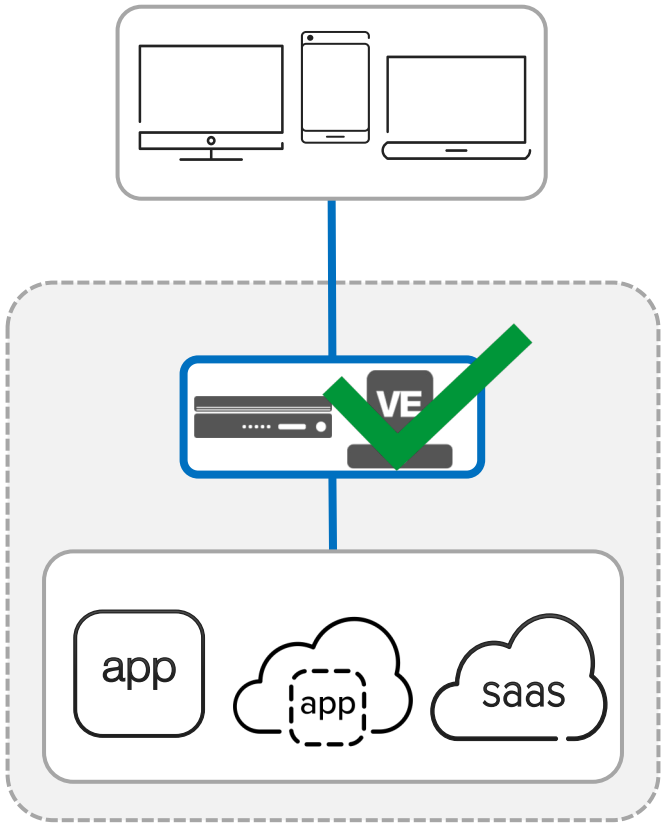
Direct a particular type of traffic to resources designed to handle that type of workload

Řízení Spojení

Mirror connection and persistence information to prevent interruption in service

Ochrana Klíčů

Protect and manage keys with hardware security modules for physical, virtual, and multi-cloud



Perfect Forward Secrecy

Protect customer privacy from future decryption with a unique key for each session

Caching

Offload repetitive traffic from application servers to improve performance and scale

SSL Offload

Decrypt inbound traffic before it hits the server to decrease demand on server resources

Komprese

Compress data from applications to reduce traffic and overcome latency

Podpora Nových Protokolů

Leverage new technologies like HTTP/3, QUIC and WebSockets without re-architecting

Vizibilita a Kontrola

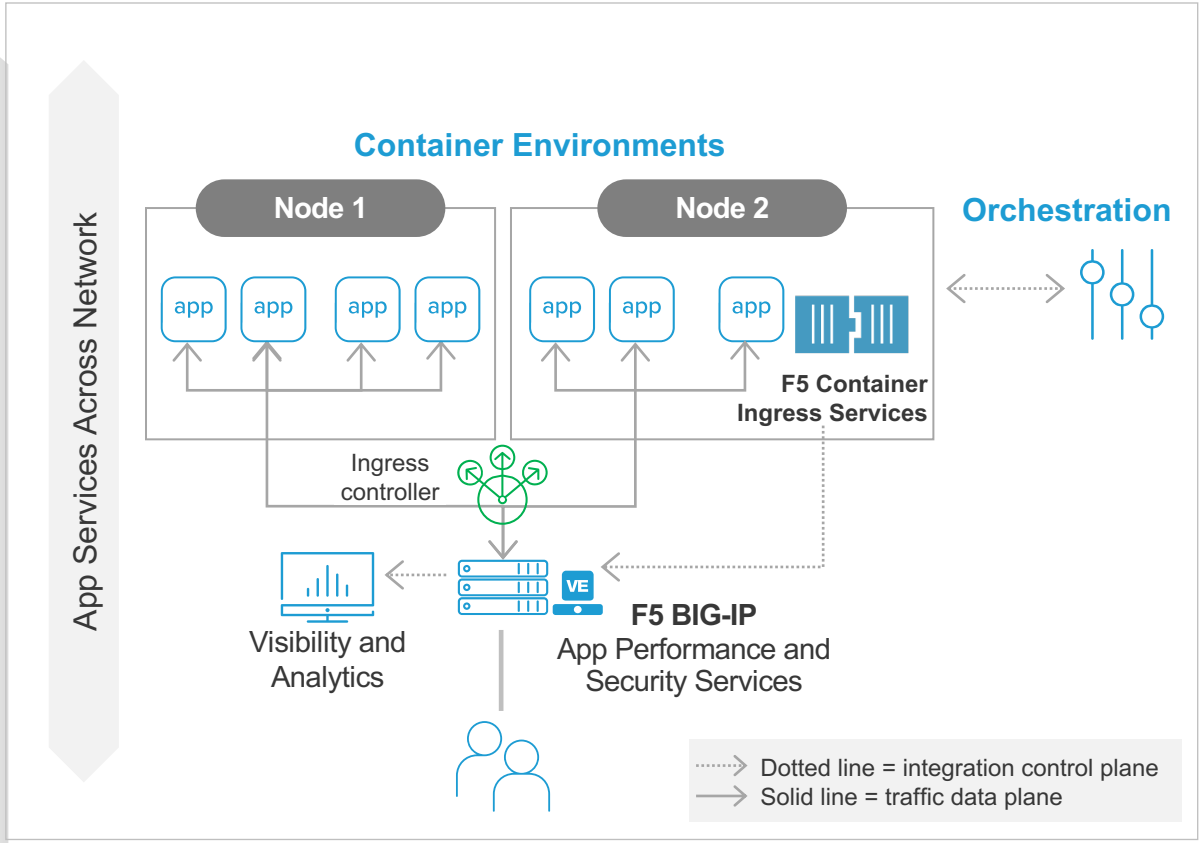
Remove the blind spot that is created by encryption for inbound and outbound traffic

A dále konsoliduje balancing pro K8s aplikace

F5 Container Ingress Services (CIS)

Best-in-class app services for containerized applications

- Control Ingress into container and PaaS environments via native, open-source, **enterprise-grade** F5 BIG-IP integrations
- Ensure performance, security, and availability of container apps **and** ingress controllers
- Enable self-service selection in orchestration for app services
- Scale and secure apps through automated event discovery and service insertion
- Inject automation into CIS and ecosystems with F5 Application Services 3 (AS3) extension and declarative APIs
- Increases flexibility of F5 application delivery and security services via K8s Custom Resource Definitions integration

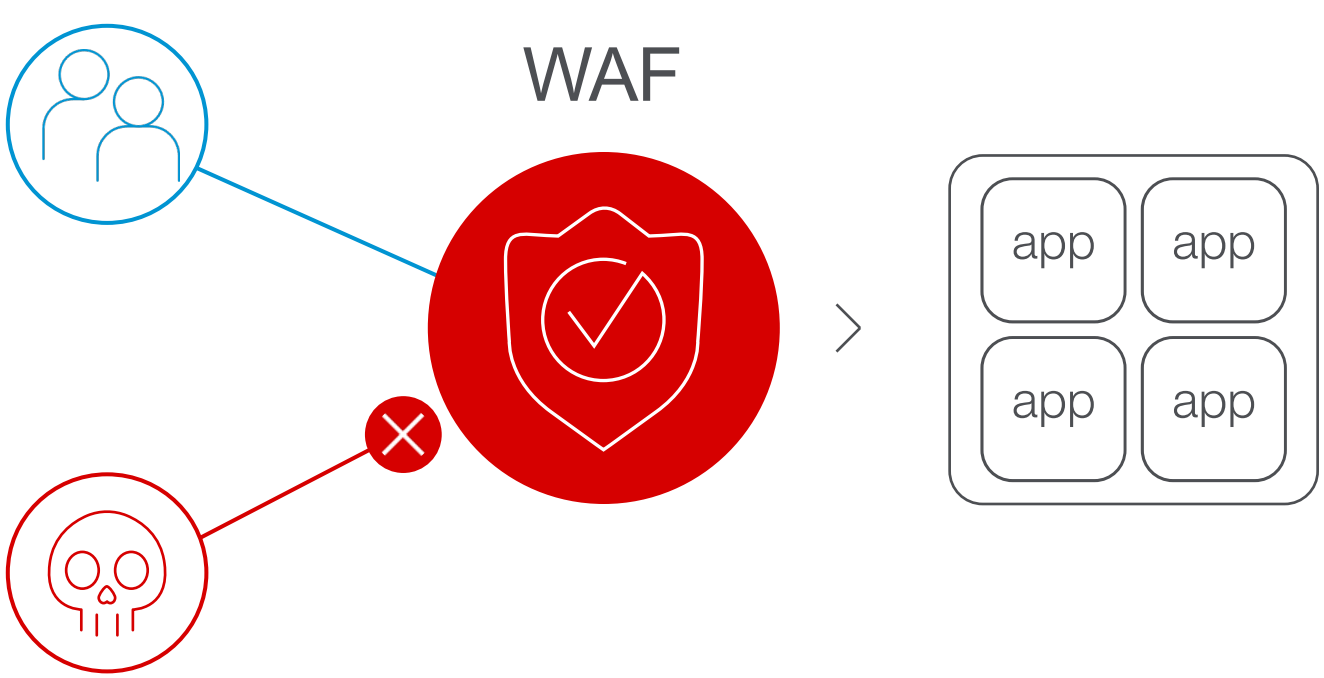


ANECT | f5 | SPCSS

App security

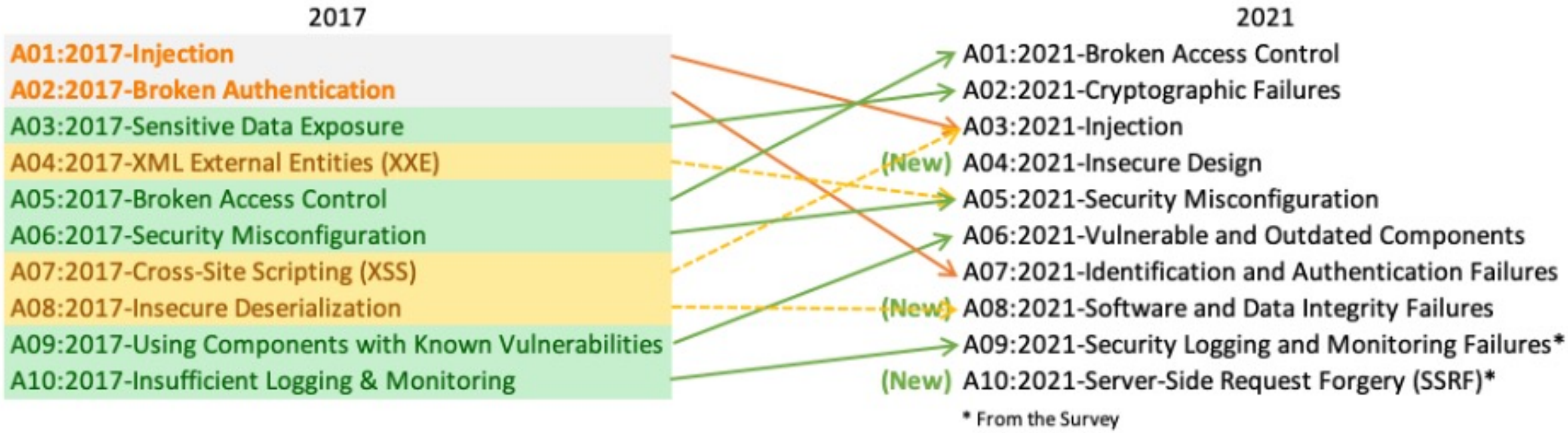
Web aplikační FW (Advanced WAF)

Web Aplikační FW (WAF) není FW :-)

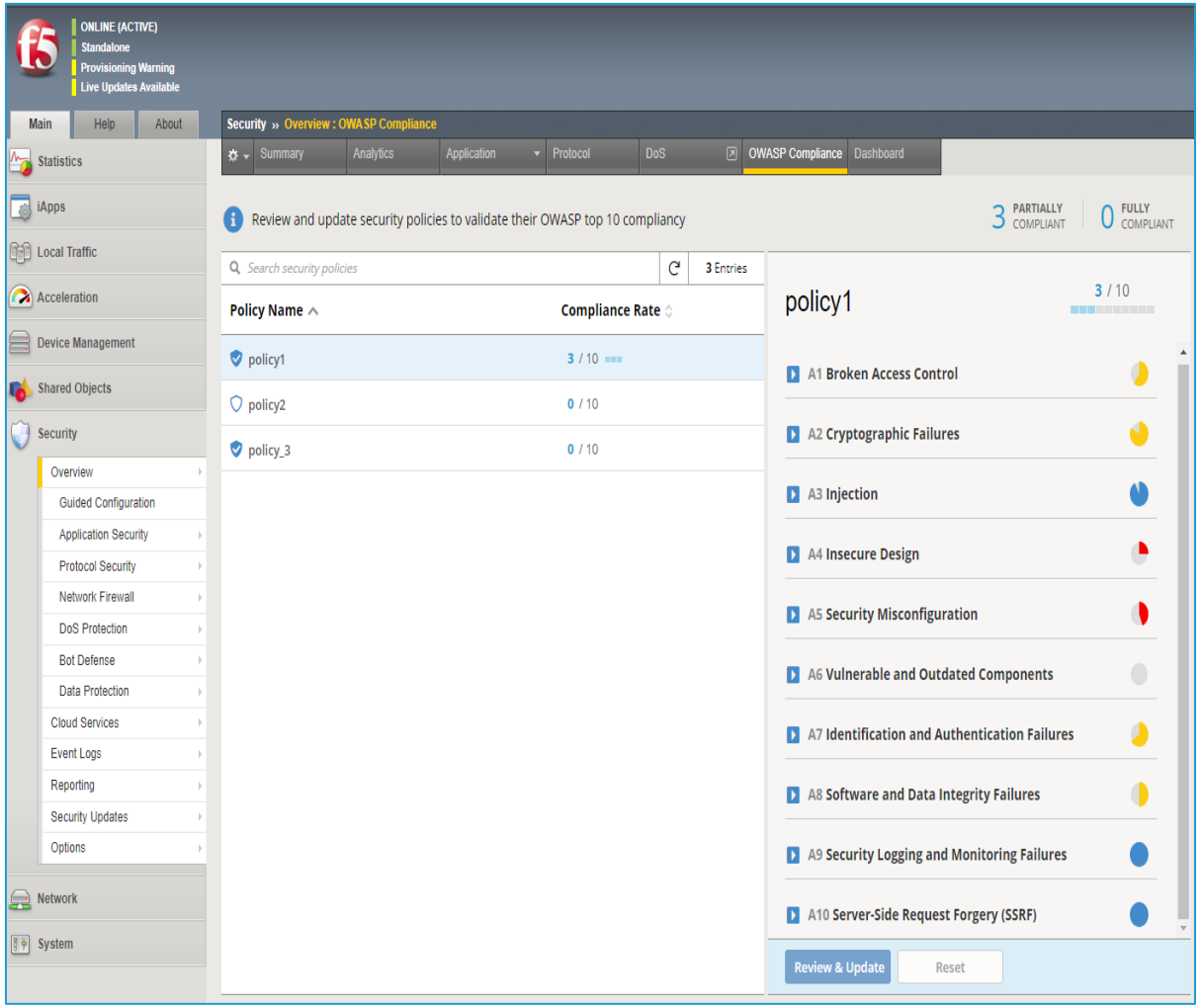


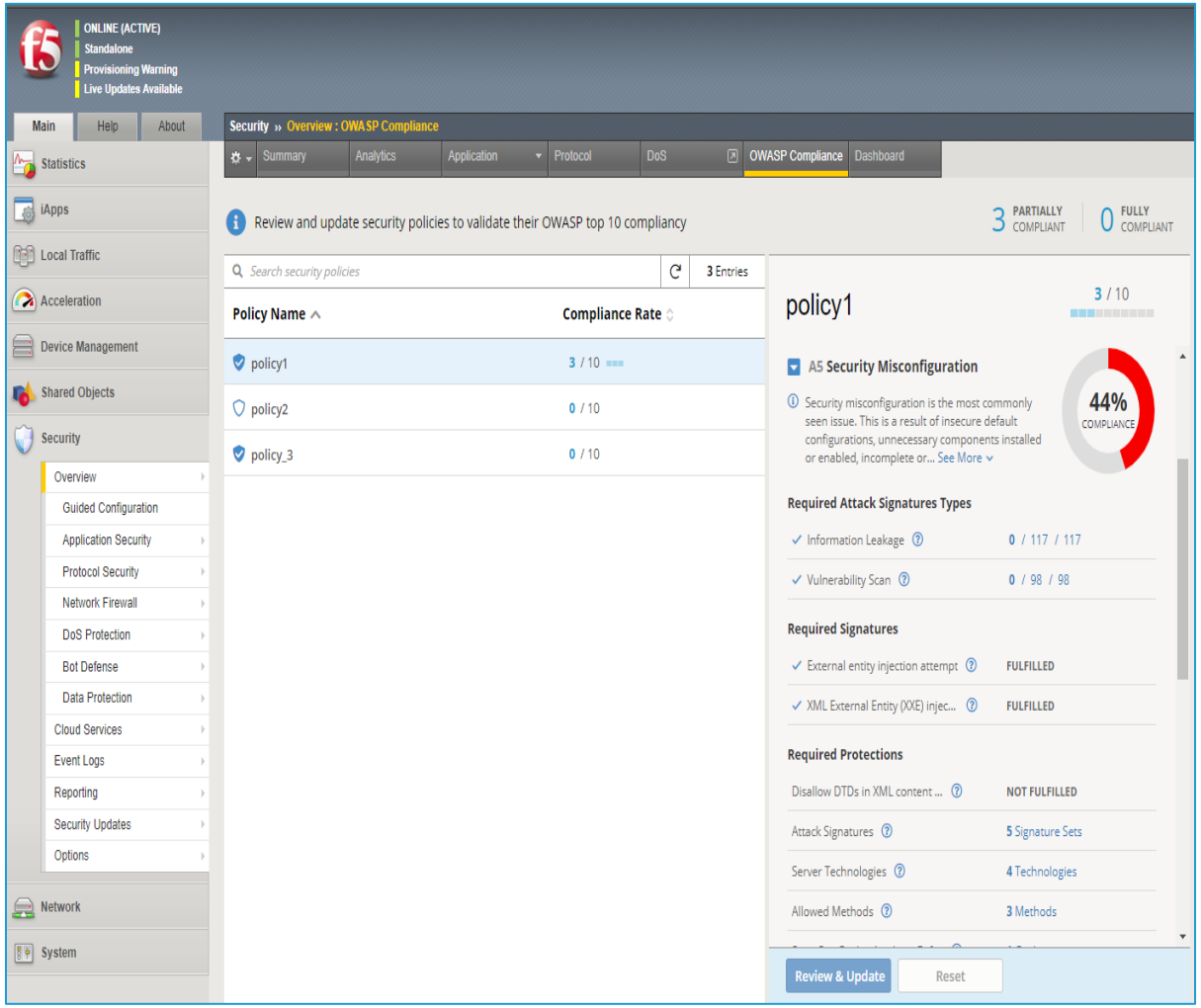
- Zranitelnosti
- Aktivní útoky
- Compliance

WAF by měla umět čelit zranitelnostem, které analyzuje a popisuje združení OWASP



F5 WAF grafický dashboard ”OWASP Top 10 2021” umožňuje zobrazit úroveň nasazené ochrany





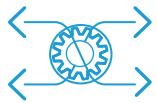
Klíčové vlastnosti, které musí dnešní WAF mít pro účinnou ochranu kritických aplikací

Common WAF security

Layer 7 DoS mitigation

Credential protection

API security



DevOps and security automation

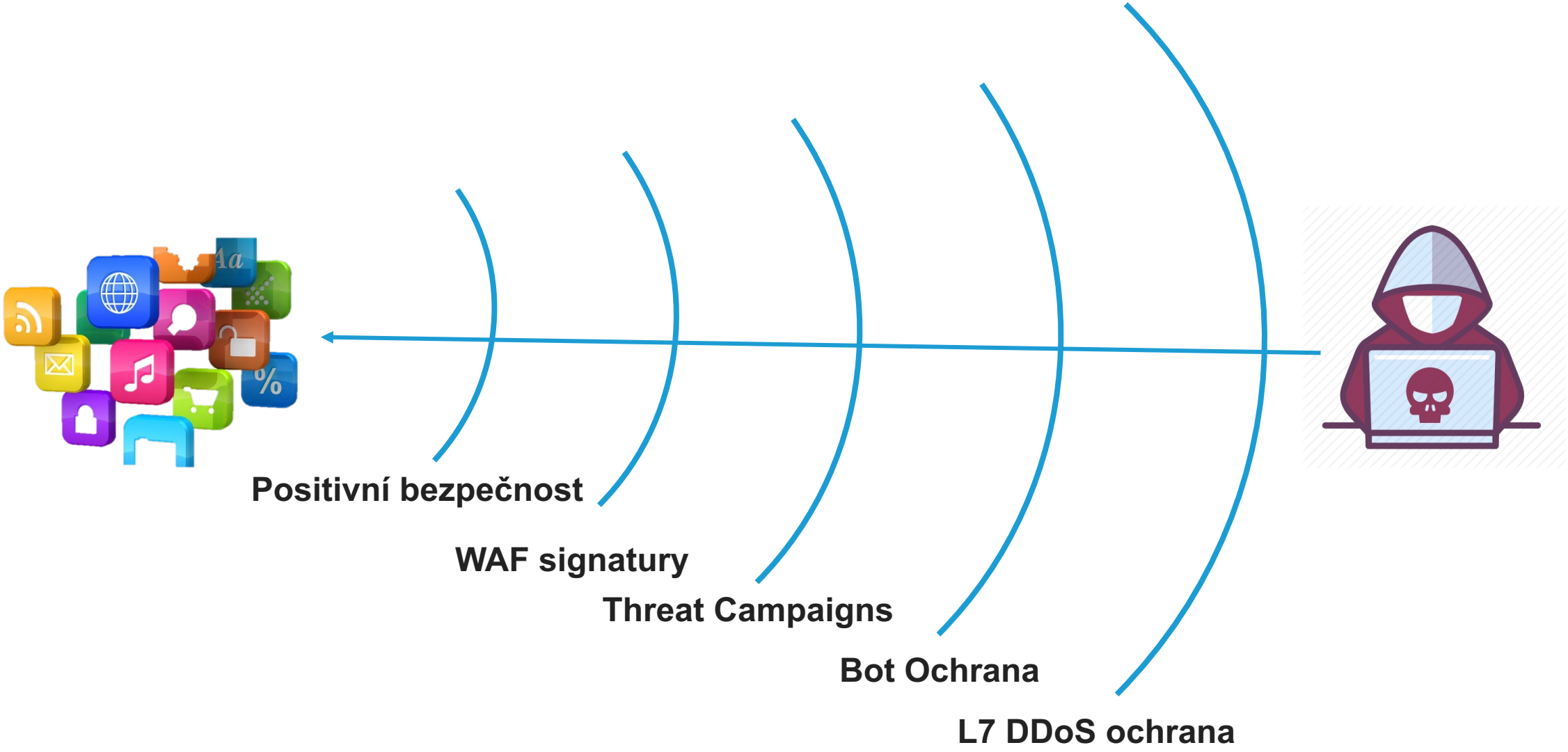
Integrated LTM

Threat campaigns

Leaked credential protection

Bot defenses

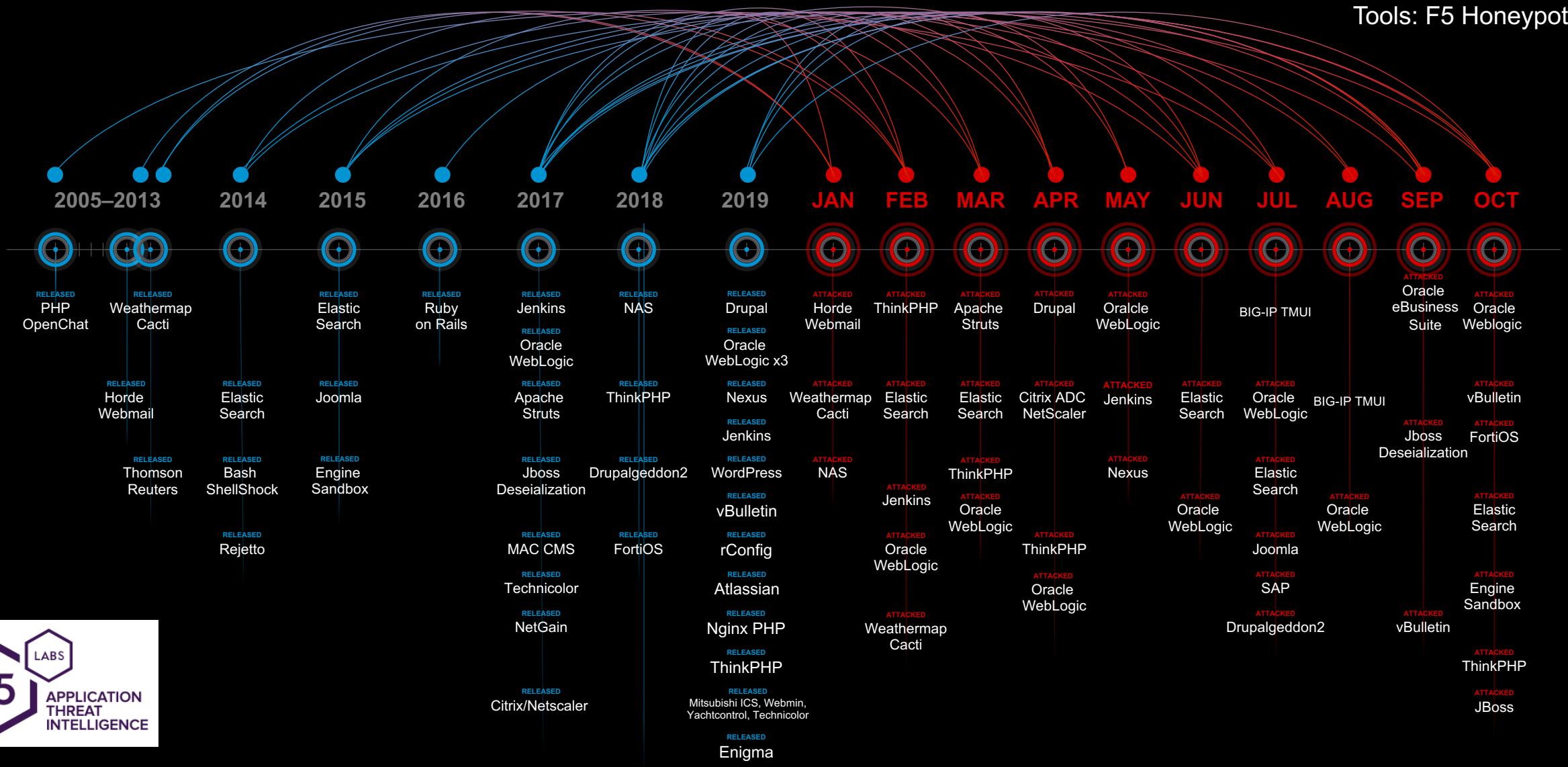
Komplexní vícevrstvá aplikační ochrana v F5 WAF



18

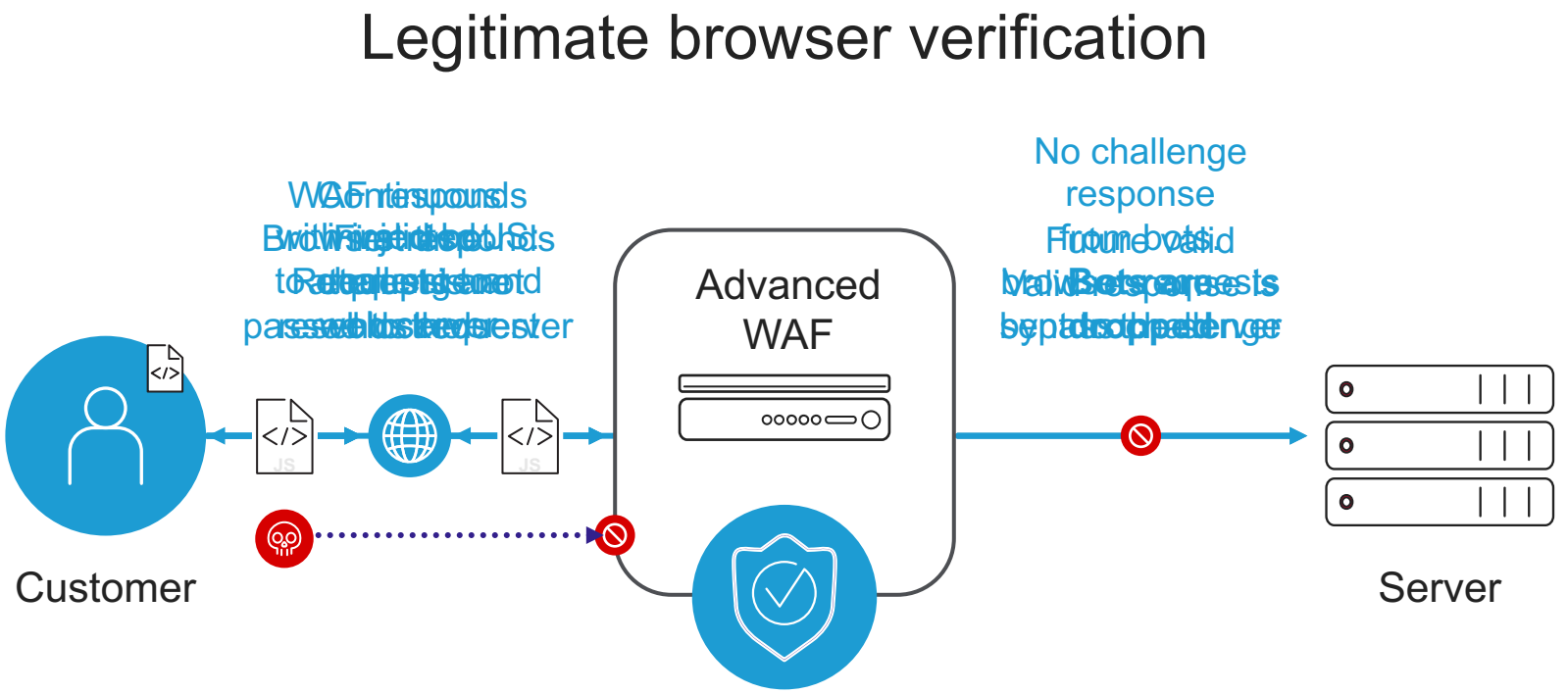
Kampaně na známá CVE – 15 let staré zranitelnosti v útocích a skenech

Source: F5 Labs
Tools: F5 Honeypots



F5 LABS APPLICATION THREAT INTELLIGENCE

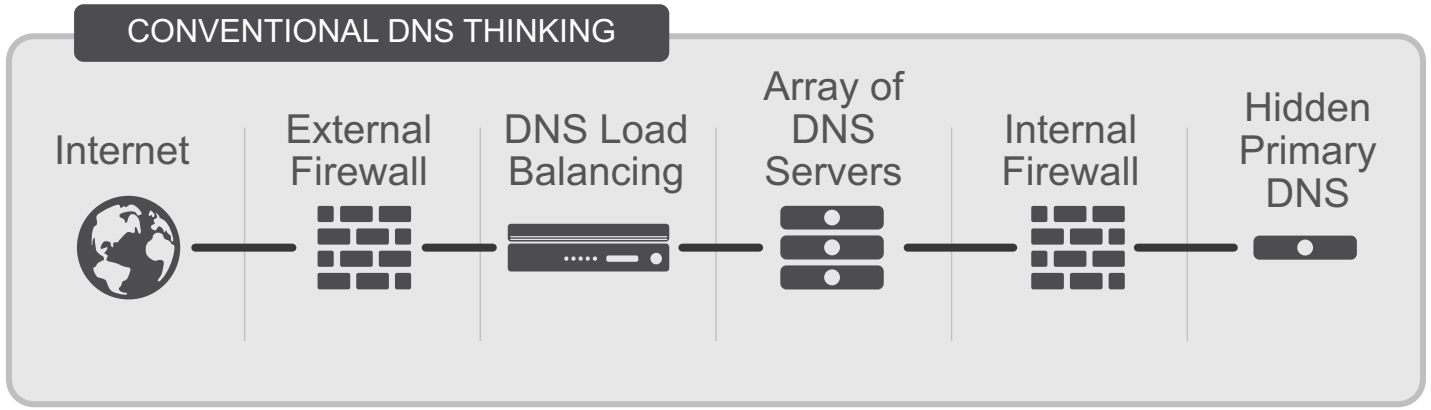
Nad rámec signaturní ochrany, F5 WAF umožňuje pokročilou detekci botů pomocí JS challenge



ANECT | f5 | SPCSS

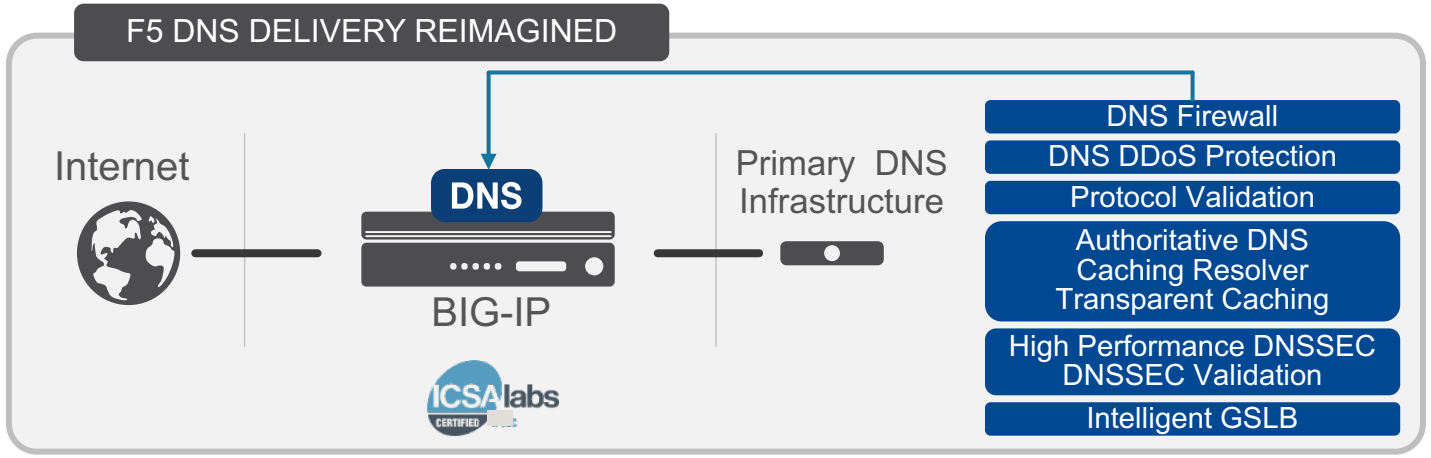
DNS

F5 DNS konsoliduje DNS infrastrukturu, pomáhá a chrání



- Performance = Add DNS boxes
- Weak DoS/DDoS Protection
- Firewall is THE bottleneck

F5 PARADIGM SHIFT

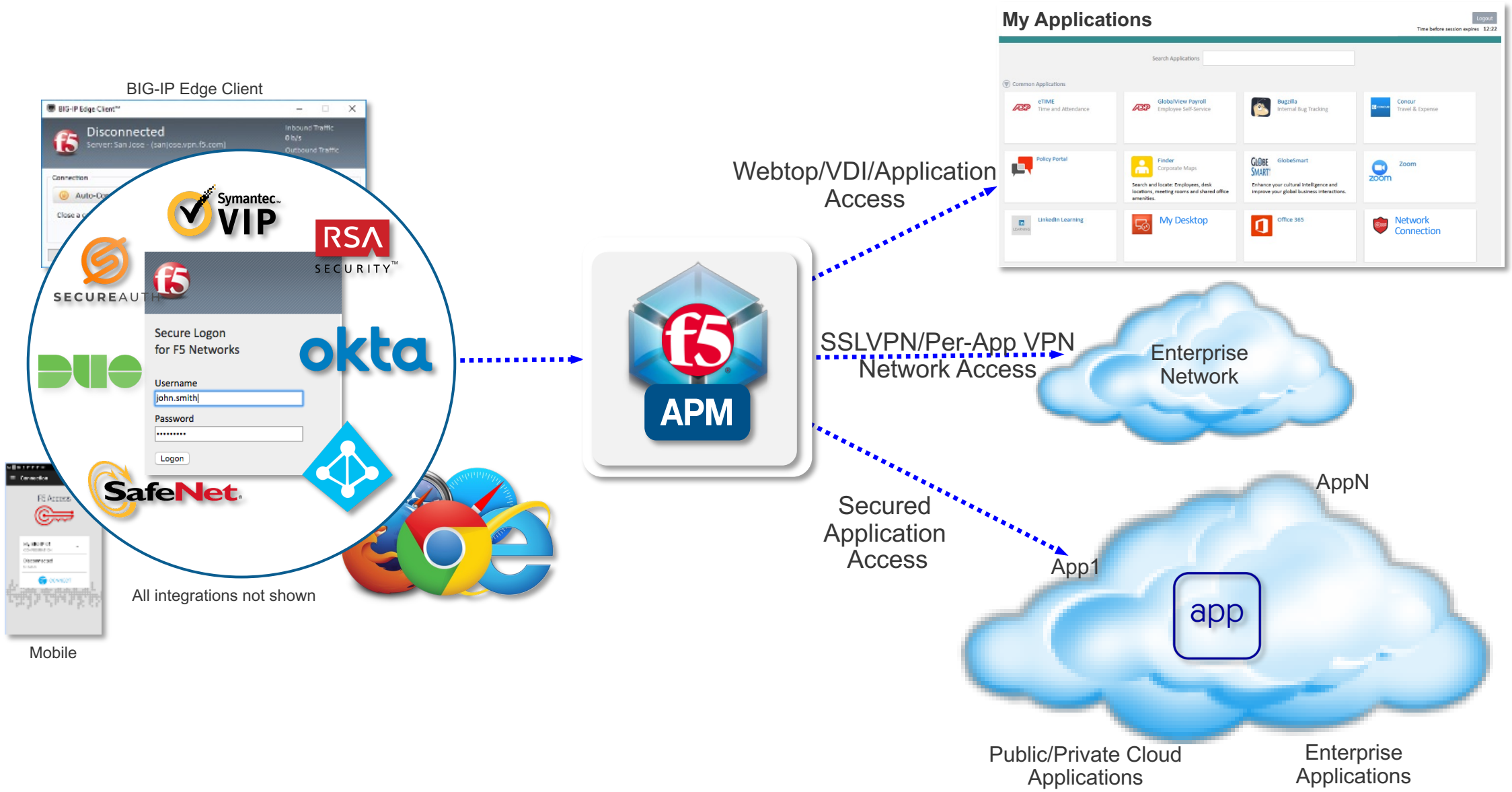


- Scalable performance up to 50M RPS!
- Strong DoS/DDoS protection
- Lower CapEx and OpEx

ANECT | f5 | SPCSS

Zabezpečený přístup k aplikacím (APM)

F5 APM umožňuje doručit jak SSL VPN, tak koncept Zero Trust



ANECT | F5 | SPCSS

CZECH BEST MANAGED COMPANIES 2023

„Digitalizujeme a automatizujeme vaši infrastrukturu & bezpečnost“

Inovace – Zjednodušení – Užitek

WAFaaS – kontinuální proces

Petr Panec
Head of Enterprise Sales, ANECT

ANECT | f5 | SPCSS

Varianta umístění WAF

SÍŤOVÝ

HOSTITELSKÝ

CLOUDOVÝ

ANECT | f5 | SPCSS

Filtrace provozu

Univerzální

- Na základě univerzální sady pravidel (seznamy zranitelností, pozitivní / negativní list).

Specificky dle aplikace

- Nutná komunikace s autory aplikace.
- Nastavení pravidel v souladu s návrhem aplikace (včetně API).
- Zajištění souladu se změnami aplikace.

ANECT | f5 | SPCSS

Rozsah činností

Servis a správa WAF

Realizace provozních změn

Bezpečnostní analytika

Proaktivní monitoring, vyhodnocování bezpečnostních incidentů

ANECT | f5 | SPCSS

Update signatur

Nahrání nových signatur

Staging mode

monitoring zda nová pravidla nelimitují legitimní provoz

Blocking mode

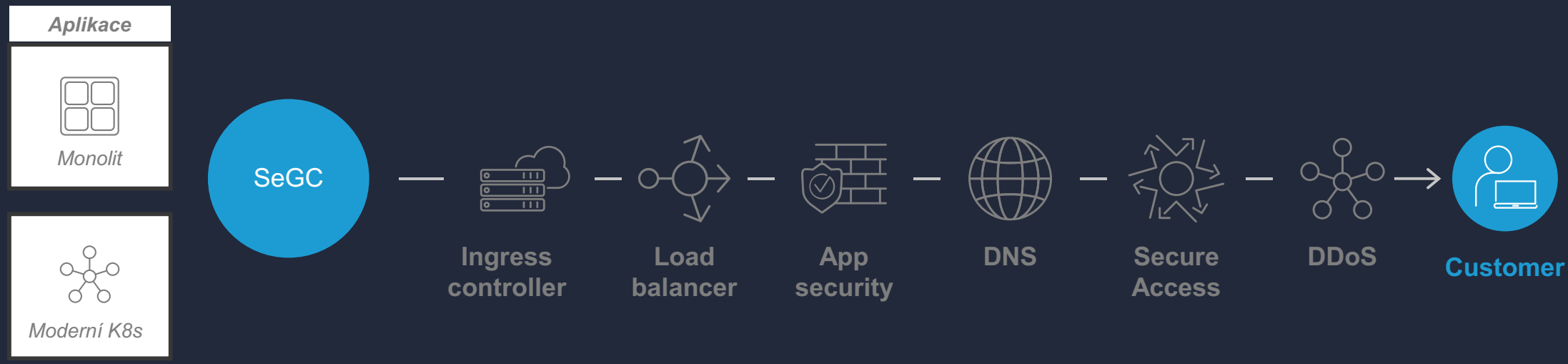
dočasně finální nastavení


SPCSS
Státní pokladna
Centrum sdílených služeb
Spolu tvoříme digitální budoucnost

Technologie F5 v SeGC

Eduard Lorenc
Vedoucí oddělení správy komunikačních technologií/Network Architect, Státní pokladna Centrum sdílených služeb, s. p.

Služby SeGC stavíme na technologii F5



ANECT | f5 | SPCSS

Služby SPCSS

Řešení dle potřeb zákazníka

Sdílená správa

SLA

ANECT | f5 | SPCSS

Eduard Lorenc
Vedoucí oddělení správy komunikačních technologií/Network Architect, Státní pokladna Centrum sdílených služeb, s. p.