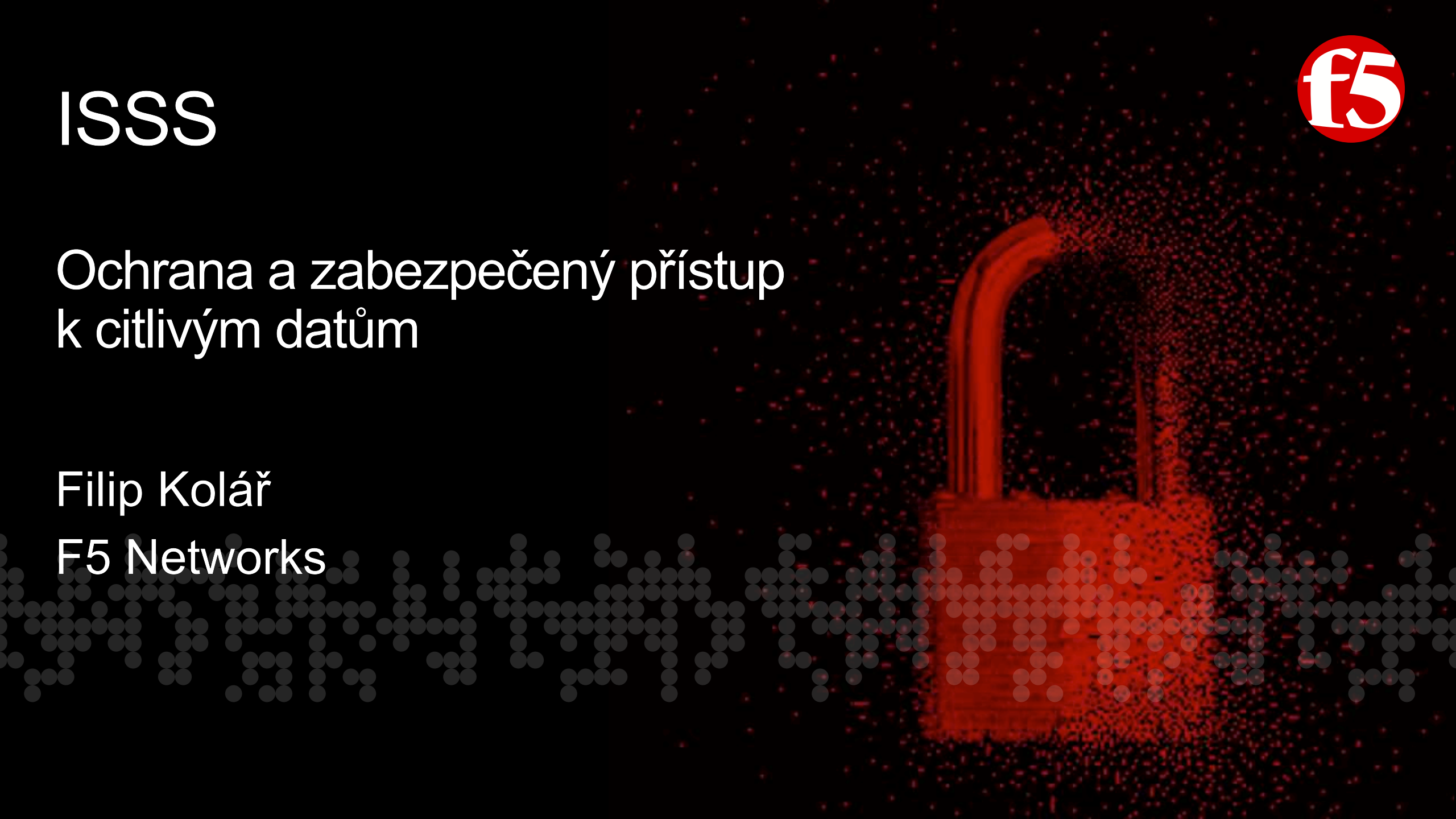
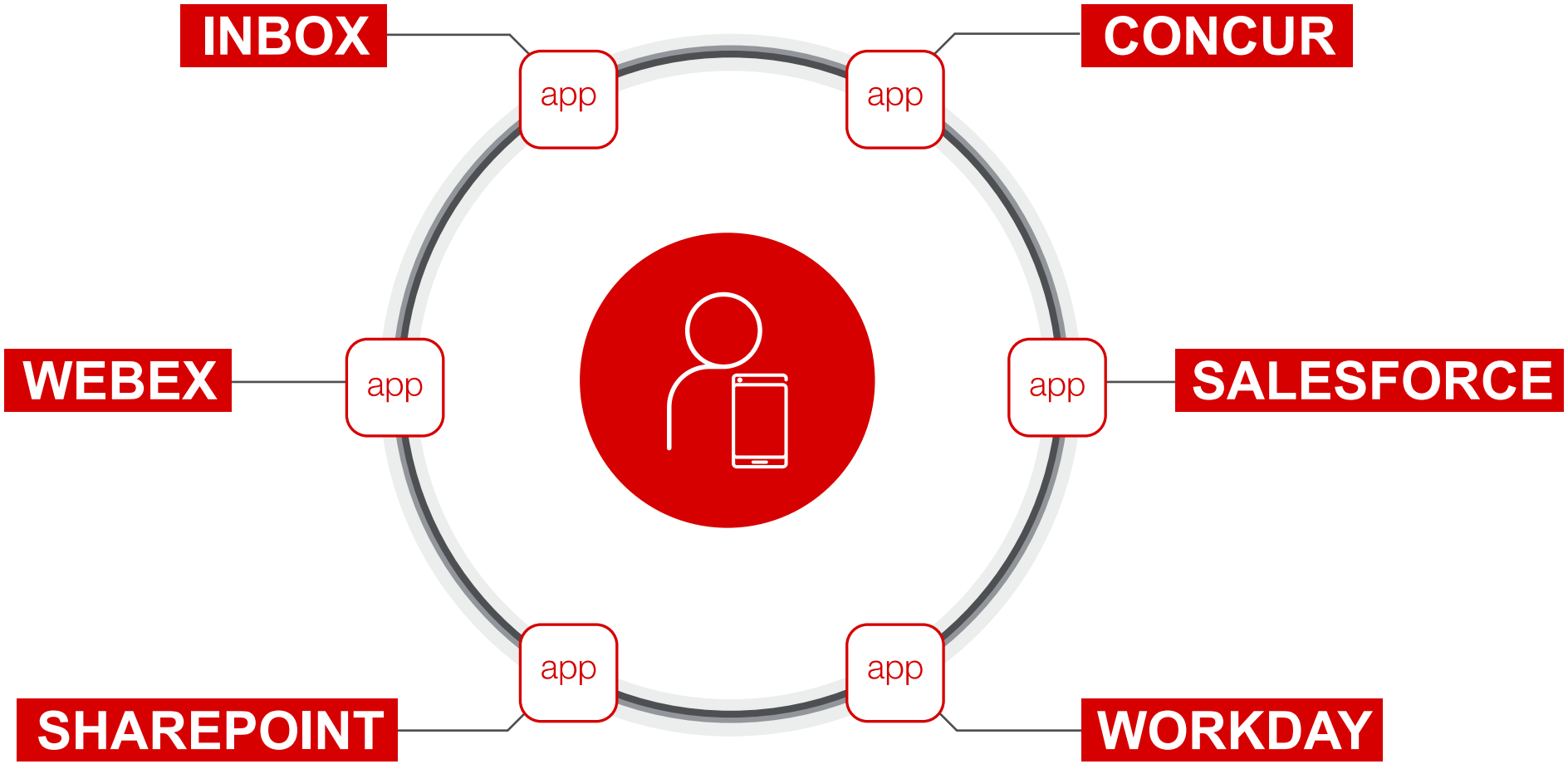
ISSS

Ochrana a zabezpečený přístup k citlivým datům

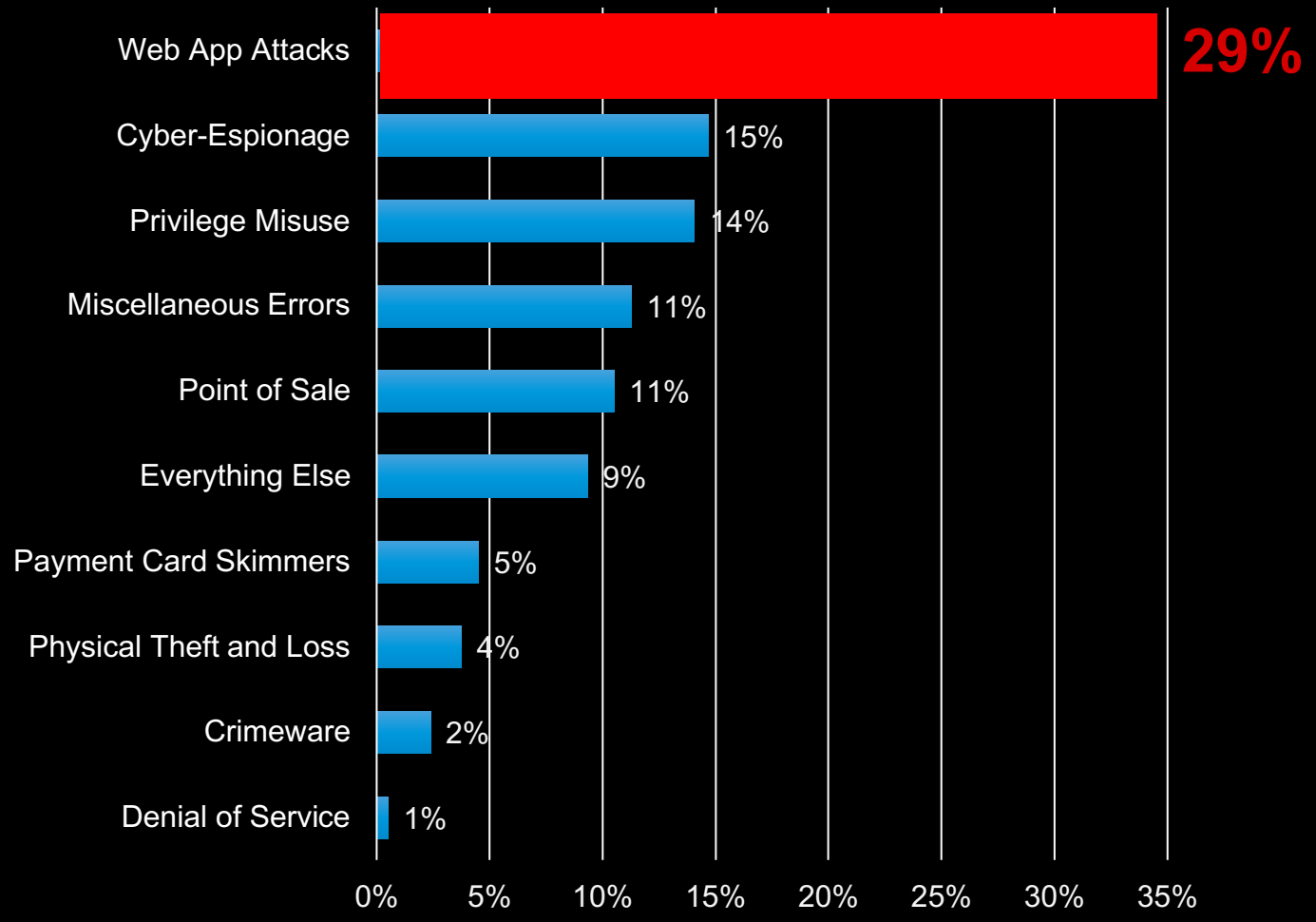


Filip Kolář

F5 Networks



Web App Attacks are the #1 Source of Data Breaches



2017 Verizon Data Breach Investigations Report

”Web Application Attacks remains the most prevalent”

“Use of stolen credentials against web applications was the dominant hacking tactic“

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Attackers Follow the Money

“Ransomware Surges Again As Cybercrime-as-Service Becomes Mainstream for Crooks”

ZD Net

“Russian Hackers Selling Login Credentials of UK Politicians, Diplomats – Report”

The Register

“Rent-a-Botnet Services Making Massive DDoS Attacks More Common Than Ever Before”

PC World

“IoT Botnets Are Growing – and Up for Hire”

MIT Technology Review

“Attacker Demands Ransom After Series of DDoS Attacks on Poker Site”

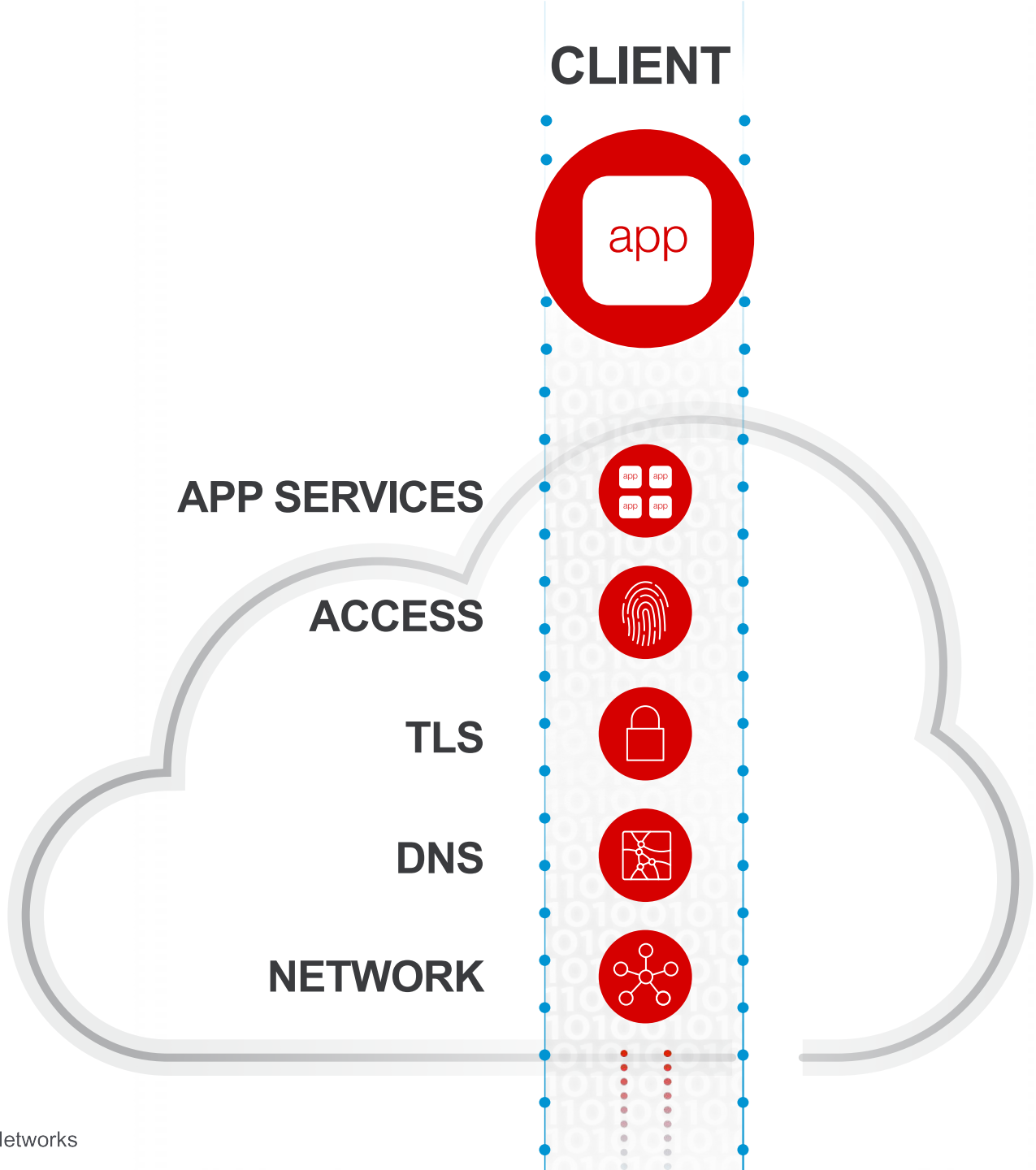
Hack Read

“Hacked Yahoo Data Is for Sale on Dark Web”

New York Times

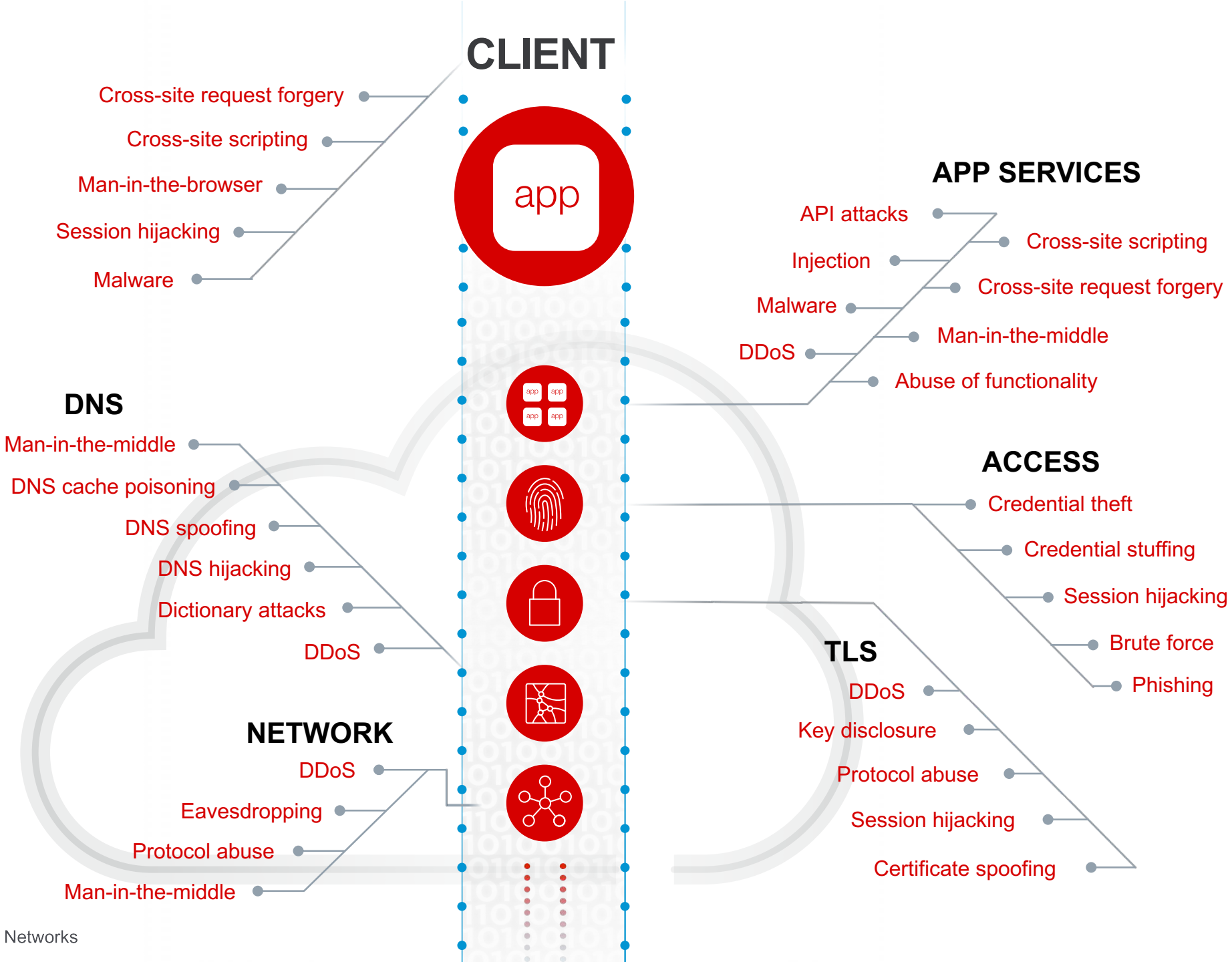
“93% of breaches in 2016 involved organised crime”

Source: Verizon 2017 Data Breach Investigations Report



THE APPLICATION IS THE GATEWAY TO DATA

Understand the application



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	✓

*F5 Networks Positioned as a Leader in 2017 Gartner Magic Quadrant for Web Application Firewalls**

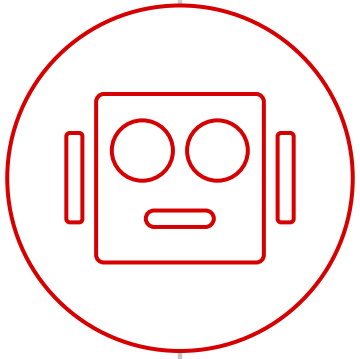
F5 is highest in execution within the Leaders Quadrant.

* Gartner, Magic Quadrant for Web Application Firewalls, Jeremy D'Hoinne, Adam Hils, Claudio Neiva, 7 August 2017

Bots, Bots, and More Bots

50%

of Internet traffic is automated



77%

of 2016 web application breaches involved the use of bots

98.6M bots observed

Source: Internet Security Threat Report, Symantec, April 2017

Bots

A common source of many threat vectors

Client-Side Attacks

- Malware
- Ransomware
- Man-in-the-browser
- Session hijacking
- Cross-site request forgery
- Cross-site scripting

App Infrastructure Attacks

- Man-in-the-middle
- Key disclosure
- Eavesdropping
- DNS cache poisoning
- DNS spoofing
- DNS hijacking
- Protocol abuse
- Dictionary attacks

DDoS Attacks

- SYN, UDP, and HTTP floods
- SSL renegotiation
- DNS amplication
- Heavy URL

Web Application Attacks

- API attacks
- Cross-site scripting
- Injection
- Cross-site request forgery
- Malware
- Abuse of functionality
- Man-in-the-middle
- Credential theft
- Credential stuffing
- Phishing
- Certificate spoofing
- Protocol abuse

Proactive Bot Defense

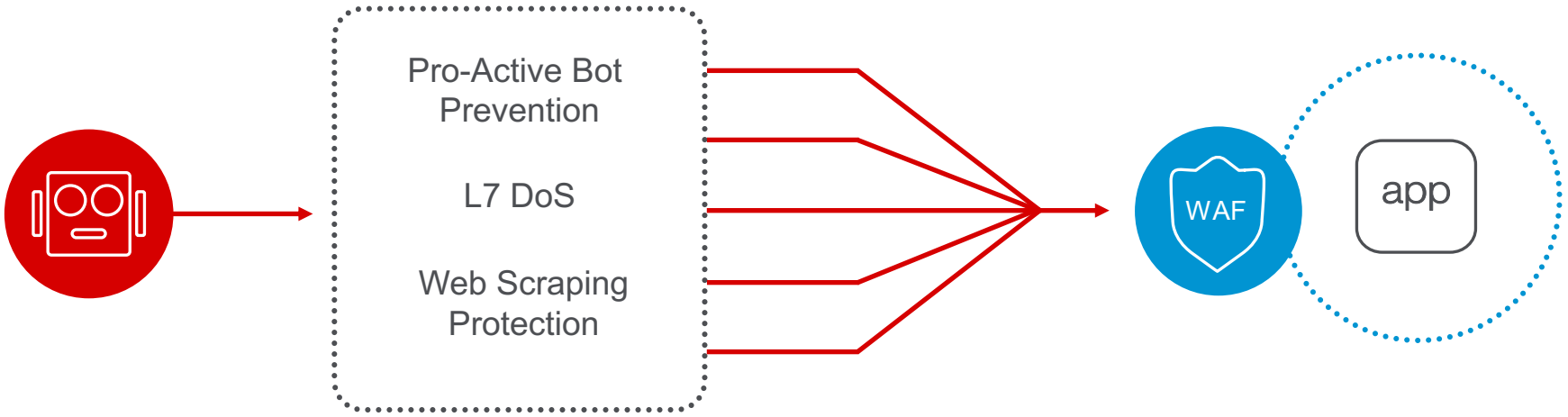
PROBLEM

Malicious bots

SOLUTION

Web Application Firewall (WAF)

Behavioural analysis to identify malicious bots

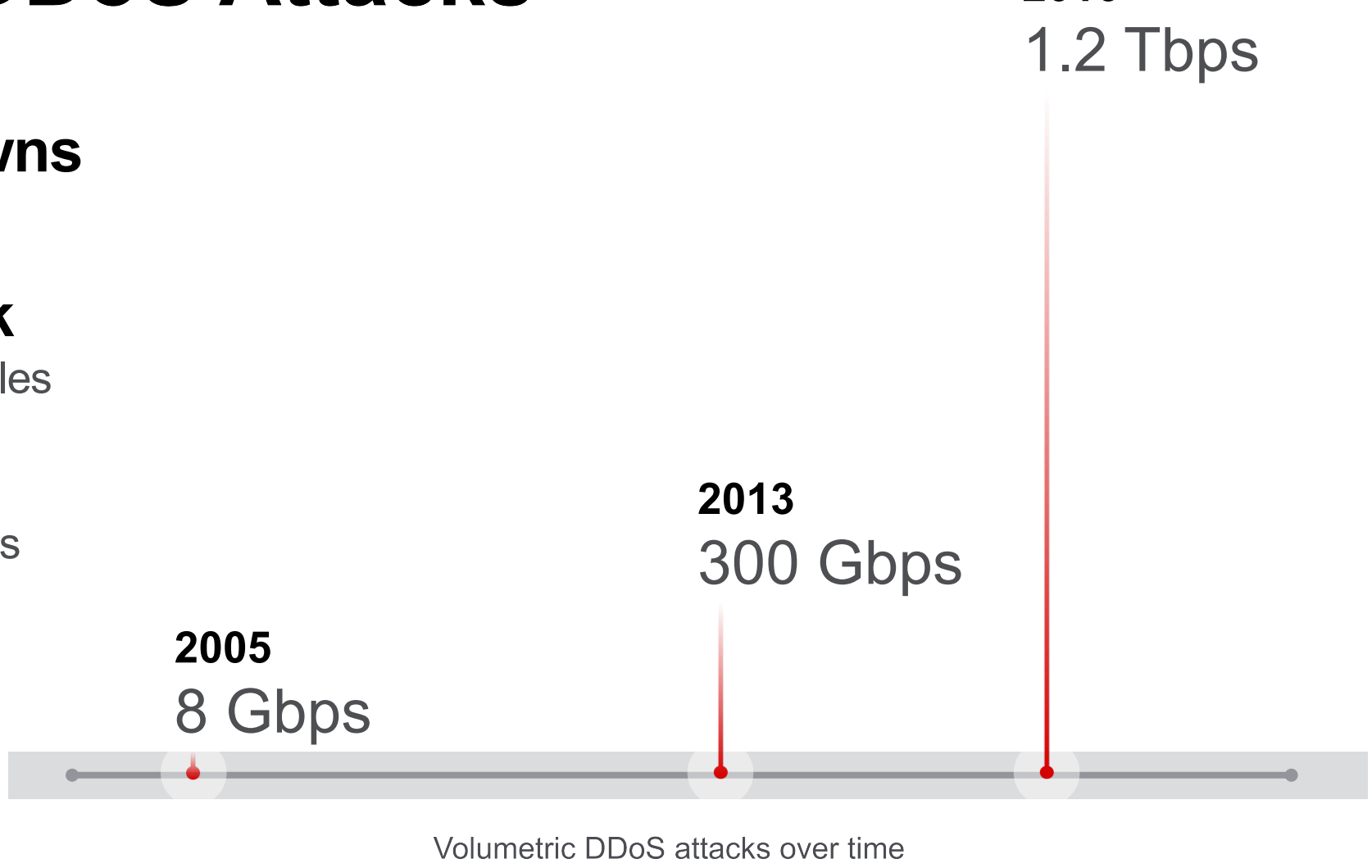


Evolution of DDoS Attacks

Volumetric take-downs
Consume bandwidth of target

Network layer attack
Consume connection state tables

Application layer
Consume application resources



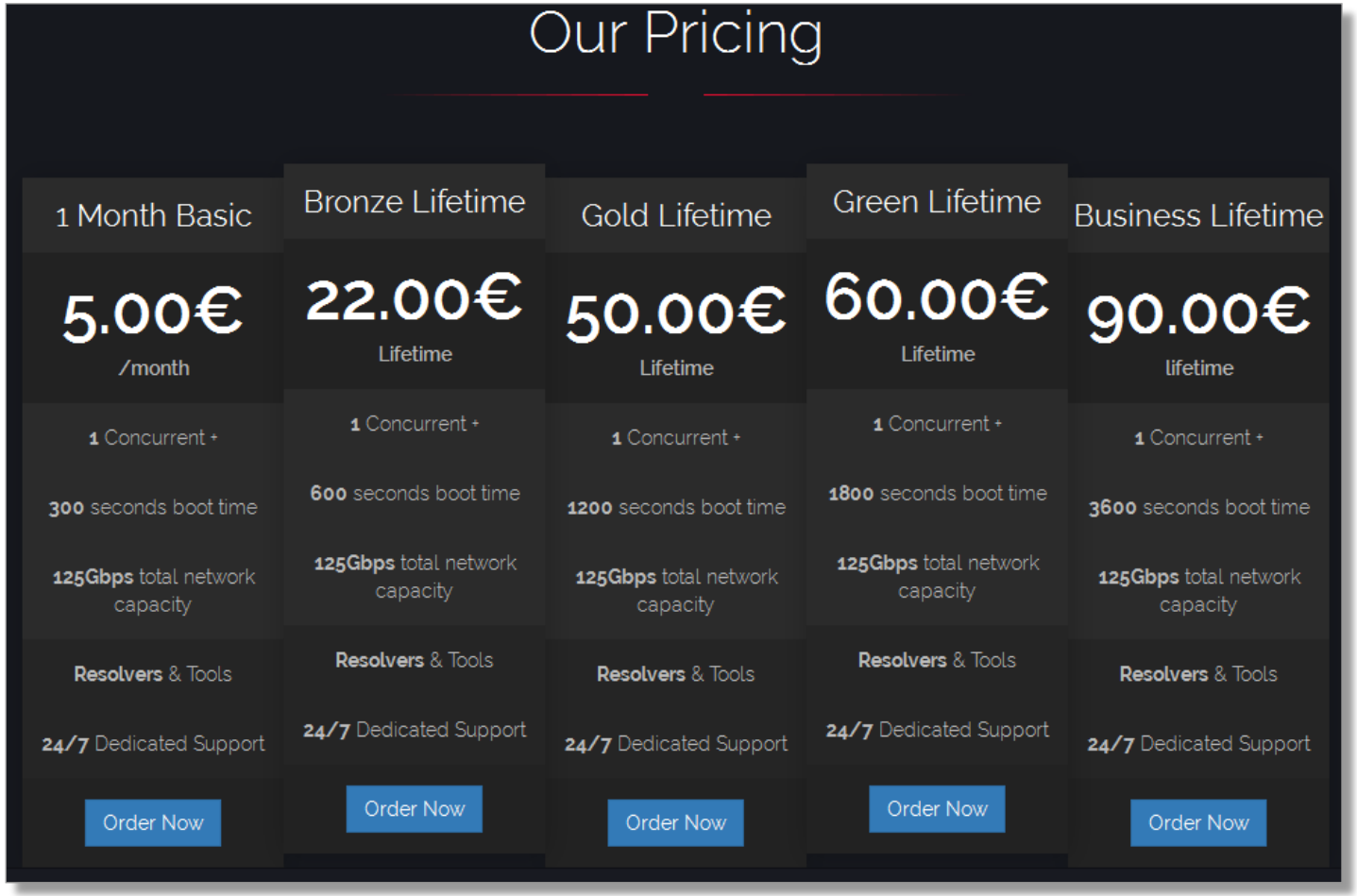
Volumetric DDoS attacks over time

Source: How DDoS attacks evolved in the past 20 years, BetaNews

DDoS for Hire

Low sophistication, high accessibility

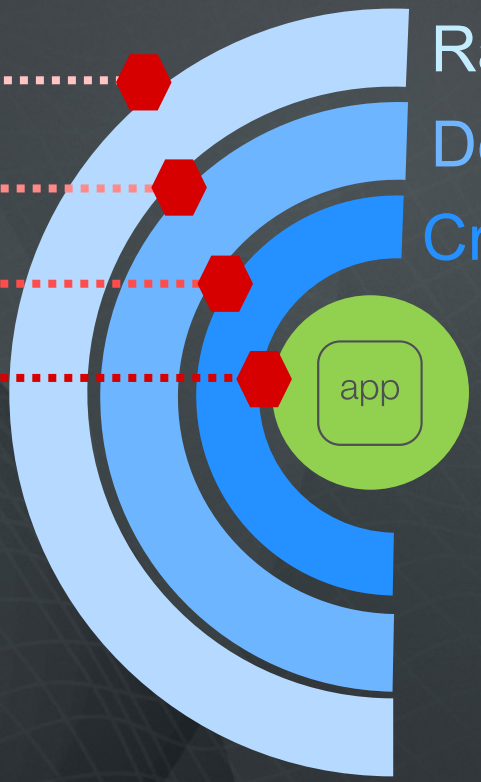
- **Accessible**
  Booters/stressers easy to find
- **Lucrative**
  Profit margins of up to 95%
- **Effective**
  Many DDoS victims pay up



Source: Securelist, Kaspersky Lab, March 2017

L7 Behavioral DDOS Protection: an advanced, phased approach

Multiple Layers of Protection



Start of Attack

Identify Attackers

Advanced Attacks

Persistent Attacks

Rate Limit to Protect the Server

Detect and Block Bots and Bad Actors

Create and Enforce Dynamic Signatures

Even basic attacks can take an unprotected server down quickly.

Persistent attackers will adjust tools, targets, sources and attack volume to defeat static DOS defenses.

Analyze Application Stress and Continually Tune Mitigations.

Malware Trends

In the first quarter of 2017, a new specimen of malware emerged every 4.2 seconds

1 in every 131 emails included malware in 2016

Over half (51%) of all breaches in 2016 involved some form of malware

Sources:
1) Malware trends 2017, G DATA Software
2) Symantec Internet Security Threat Report, April 2017
3) WannaCry Update, Rapid7 Blog, May 2017

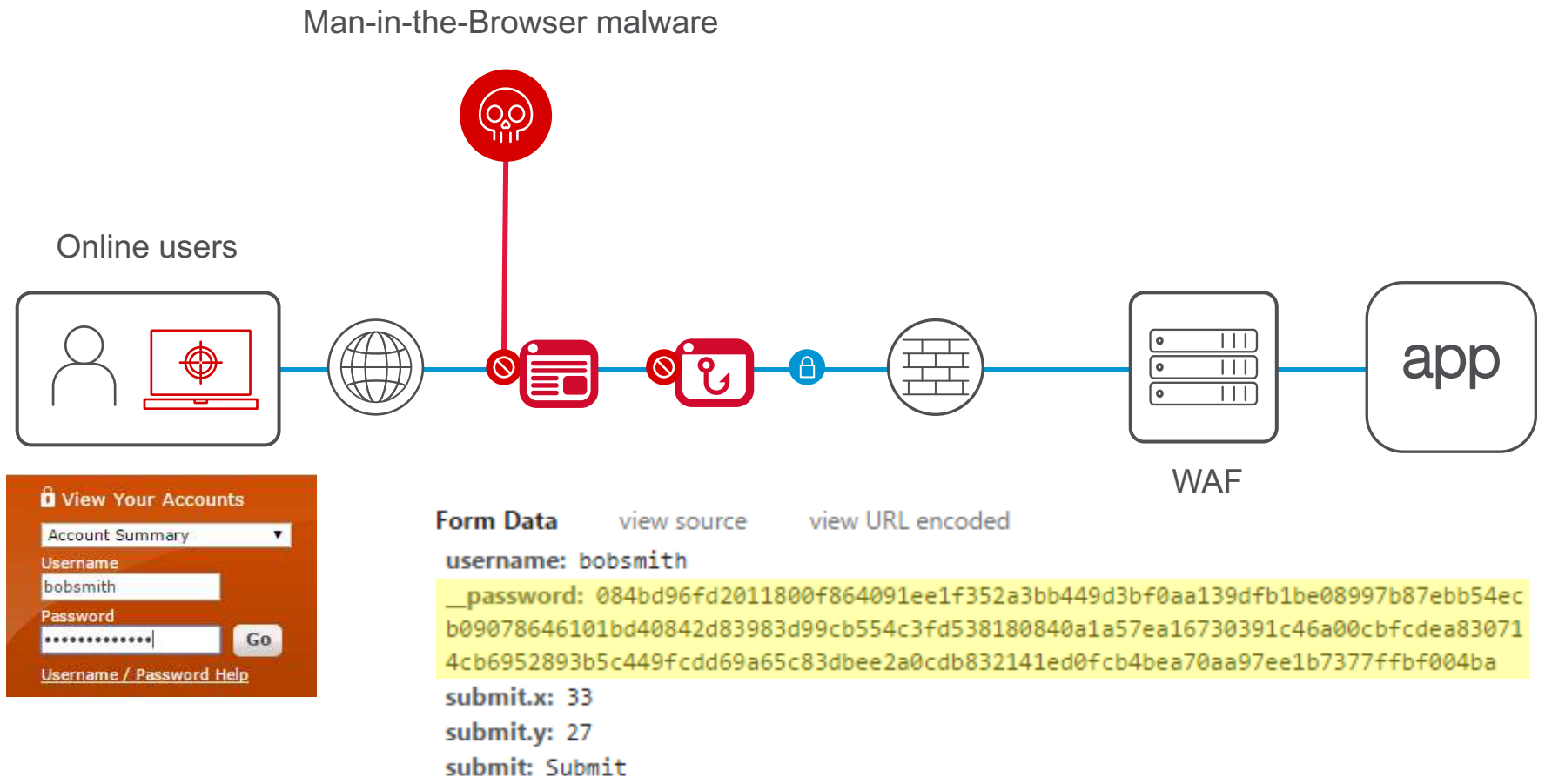
Credential Theft Using Malware (DataSafe)

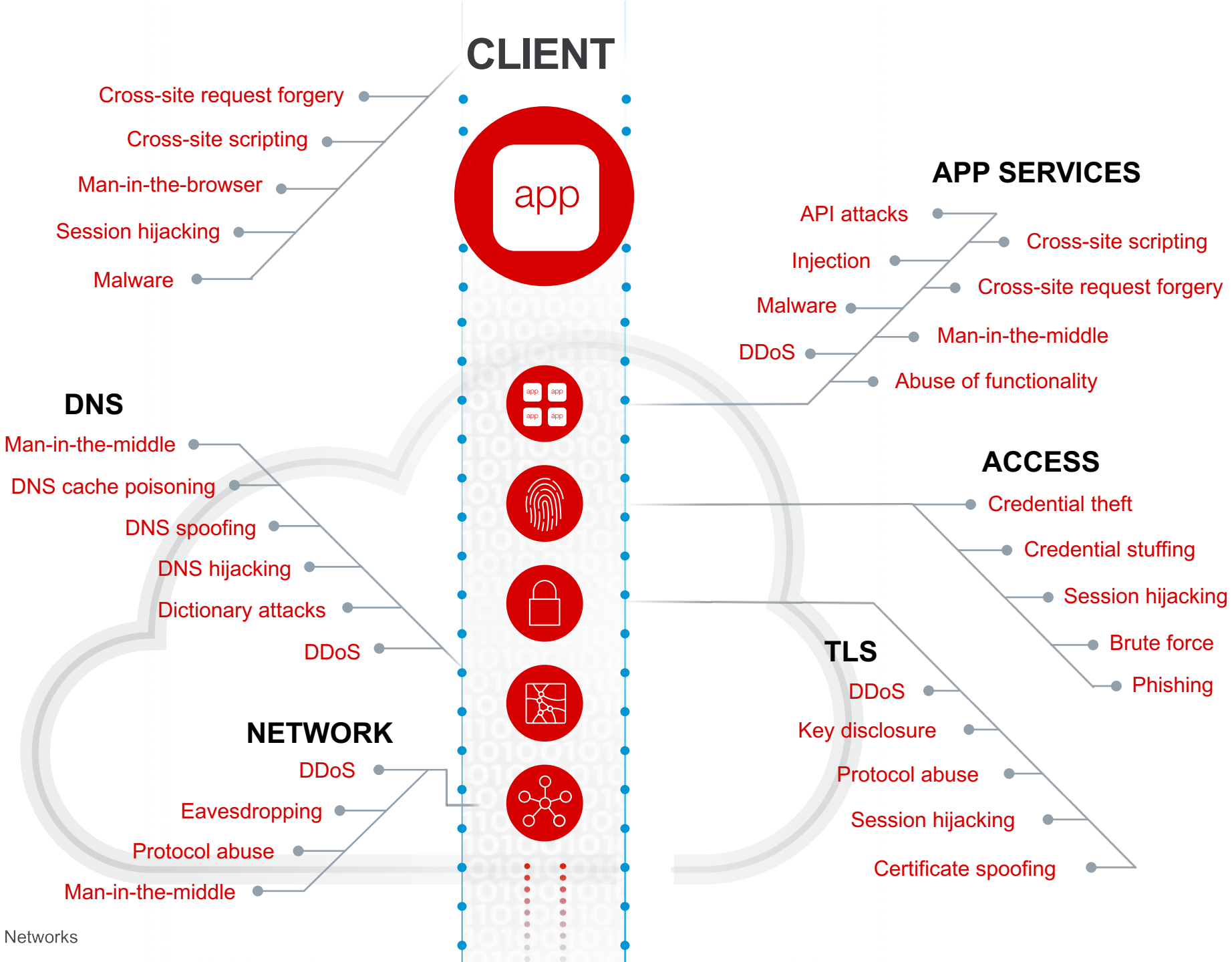
PROBLEM

Malware

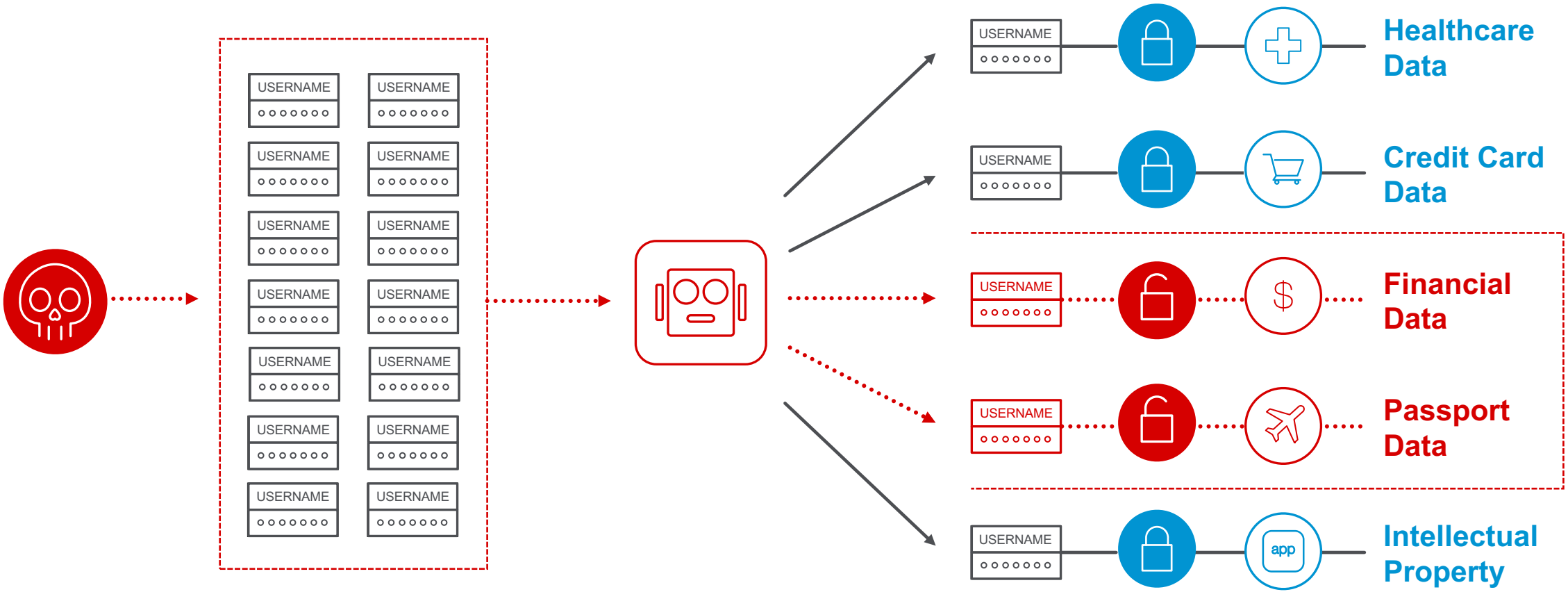
SOLUTION

App-layer encryption





How Credential Stuffing Works



Autorizace & Autentizace & Single Sign-on

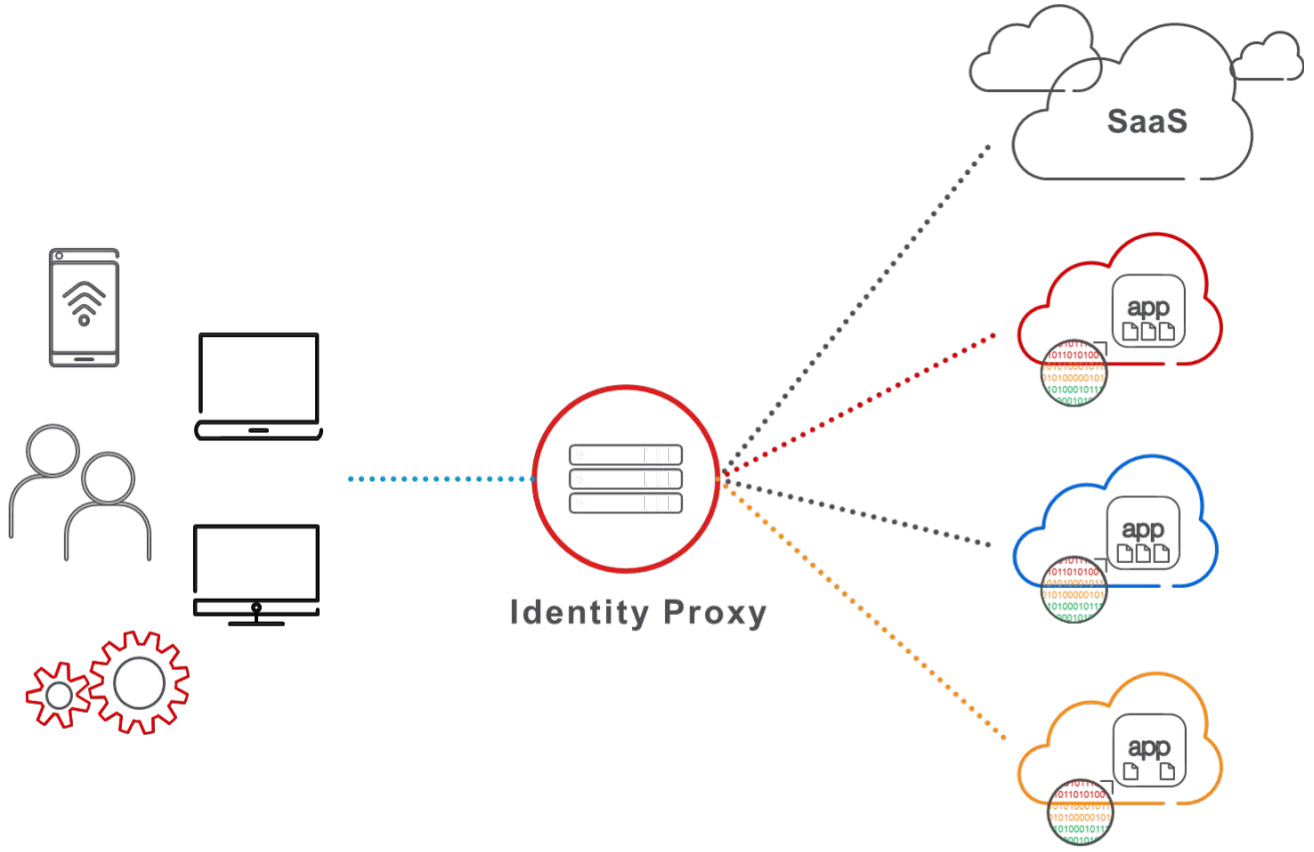
Zabezpečený, zjednodušený přístup k Vašim aplikacím nehledě na to, kde jsou provozovány

Challenges

- Complex and varied app access
- Protect assets from fraudulent access
- Password fatigue
- Concerns with user credentials in the cloud

Multi-Cloud Benefits

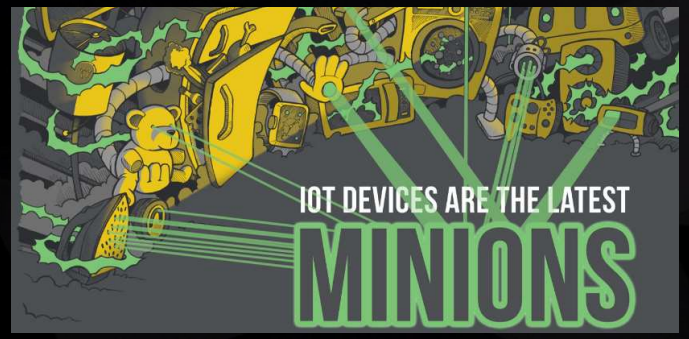
- Prevent data exfiltration from unauthorized users of cloud apps
- Simplify app access and password fatigue for end users regardless of location
- Reduce time-consuming and error-prone access policy management across clouds/SaaS



Visit Us at F5Labs.com

REPORTS

"IoT Devices are the Latest Minions in Cyber Weaponry Toolkits"



ARTICLES

"Mirai: The IoT Bot That Took Down Krebs and Launched a Tbps Attack on OVH"

BLOGS

"IoT Threats: A First Step into a Much Larger World of Mayhem"

Search by topic, type, tag, and author.

F5Labs.com

WE MAKE APPS

GO

FASTER. SMARTER. SAFER.