RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART2-W11

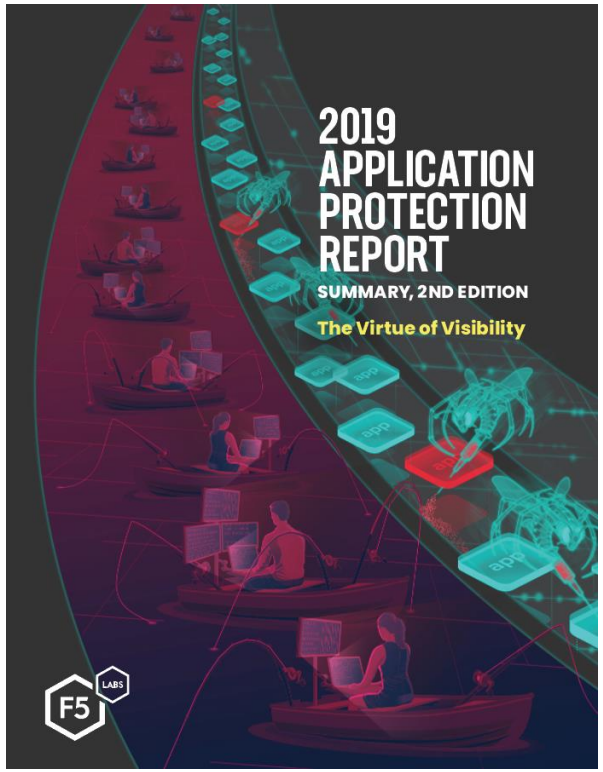
2019 Data Breaches: Stuffed Creds, Jacked Forms, and Itinerant Goalposts

Sara Boddy
Sr. Director, F5 Labs
@sarab0ddy

Sander Vinberg
Threat Research Evangelist
F5 Labs

Application Protection Research Series

Using data to unite tactics and strategy in risk-based security

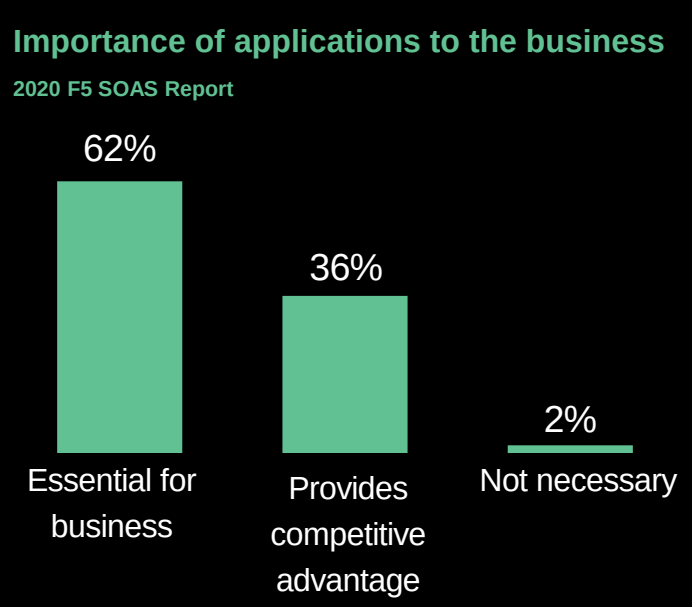


F5 LABS

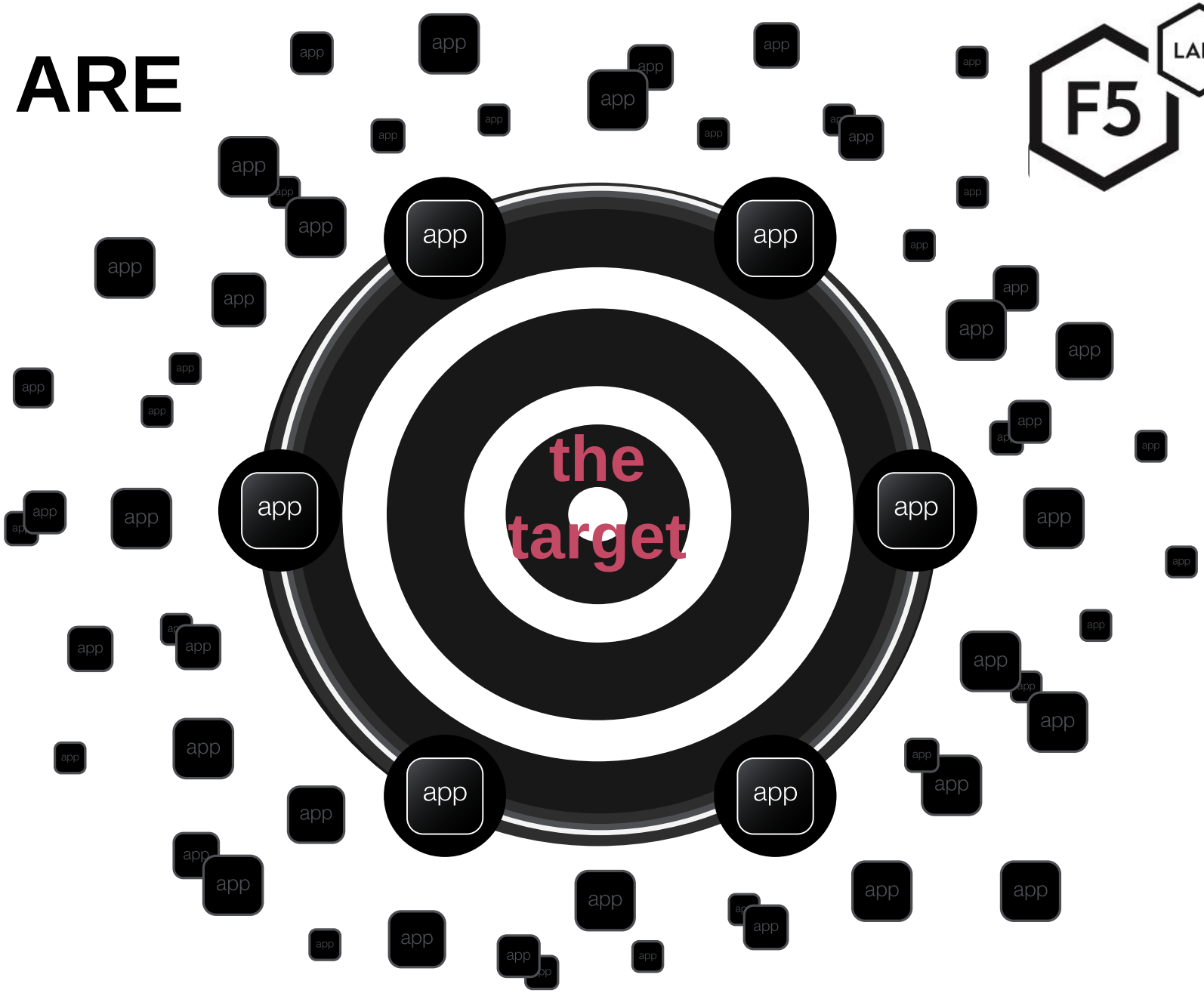
APPLICATIONS ARE

The reason people use the Internet

The business



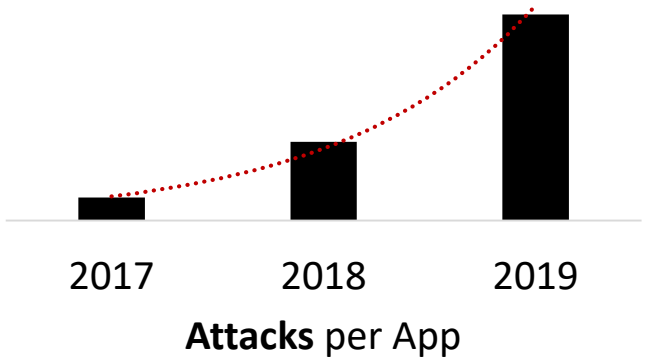
The gateway to DATA



Apps, Attacks and Breaches Rising to the Occasion

3x

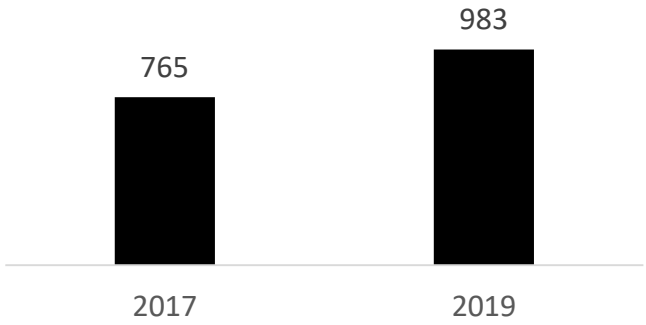
Attack growth



Attacks per App

28%

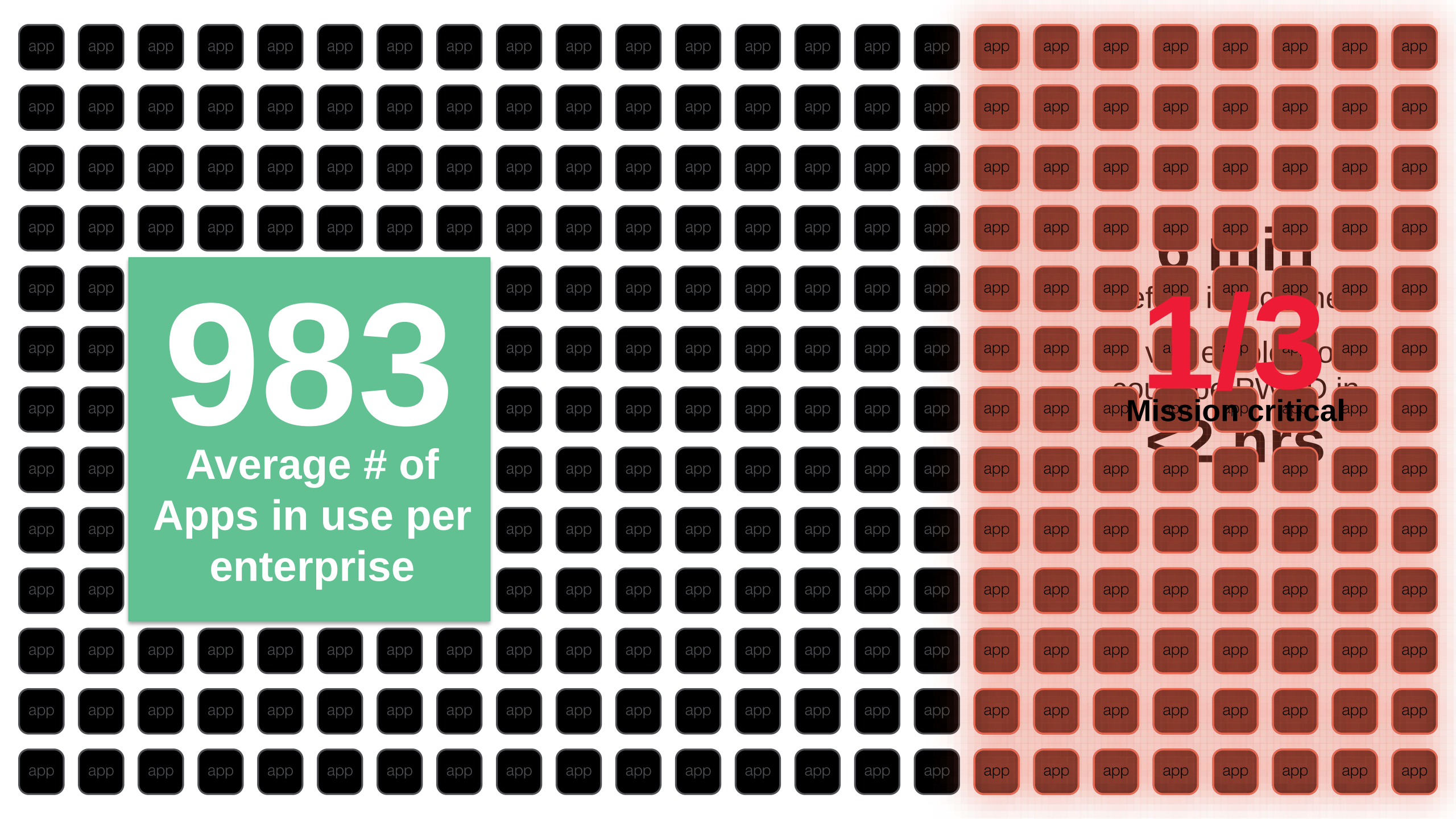
App growth



Average Apps per Enterprise

3 Billion +

credentials stollen per year


983
Average # of Apps in use per enterprise
1/3
Mission critical

Top Attack Types By Geo Target

(last 90 days as of 12/31/2019)

HTTP/HTTPS Cred Stuffing Scanning

Canada

- Port scanning (VNC, SMB, SMTP, SSH, HTTP/S, SWX, Weblogic, DNS, Hauwei)
- Cred stuffing (VNC, SSH, Telnet)
- HTTP attacks (port 443 & 8080)

US

- Port scanning (SMB, MS SQL, VNC, HTTP/S, SSH, Telnet, SMTP, DNS, WebLogic)
- Cred stuffing (VNC, SSH, Telnet, HTTP)
- HTTP attacks (Alt-HTTP port 8080)
- Malware uploads (SMB port 445)

Latin America

- Port scanning (RFB/VNC, MS SQL, SMB, Telnet, RDP, HTTP/S)
- Cred stuffing (RFB/VNC, Telnet, FTP)
- Malware uploads (SMB port 445)
- HTTP attacks (Alt-HTTP port 8080)

Middle East

- Port scanning: RFB/VNC, HTTP/S, SSH, SMTP, Telnet
- Credential stuffing: Telnet, RFB/VNC, SSH
- HTTP attacks: Alt-HTTP port 8080

Europe

- Port scanning: RFB/VNC, SMB, HTTP/S, SSH, DNS, SMTP, MS SQL, RDP, SWX, Weblogic, FTP, Radan HTTP
- Credential Stuffing: RFB/VNC, SSH, Telnet, HTTP
- Malware uploads: SMB port 445

Russia

- Port scanning: ICB/SWX port 7326, RFB/VNC, SMTP, HTTP/S, SSH, SMB, Weblogic
- Credential Stuffing: RFB/VNC, Telnet, SSH
- HTTP Attacks: Alt-HTTP port 8080

Asia

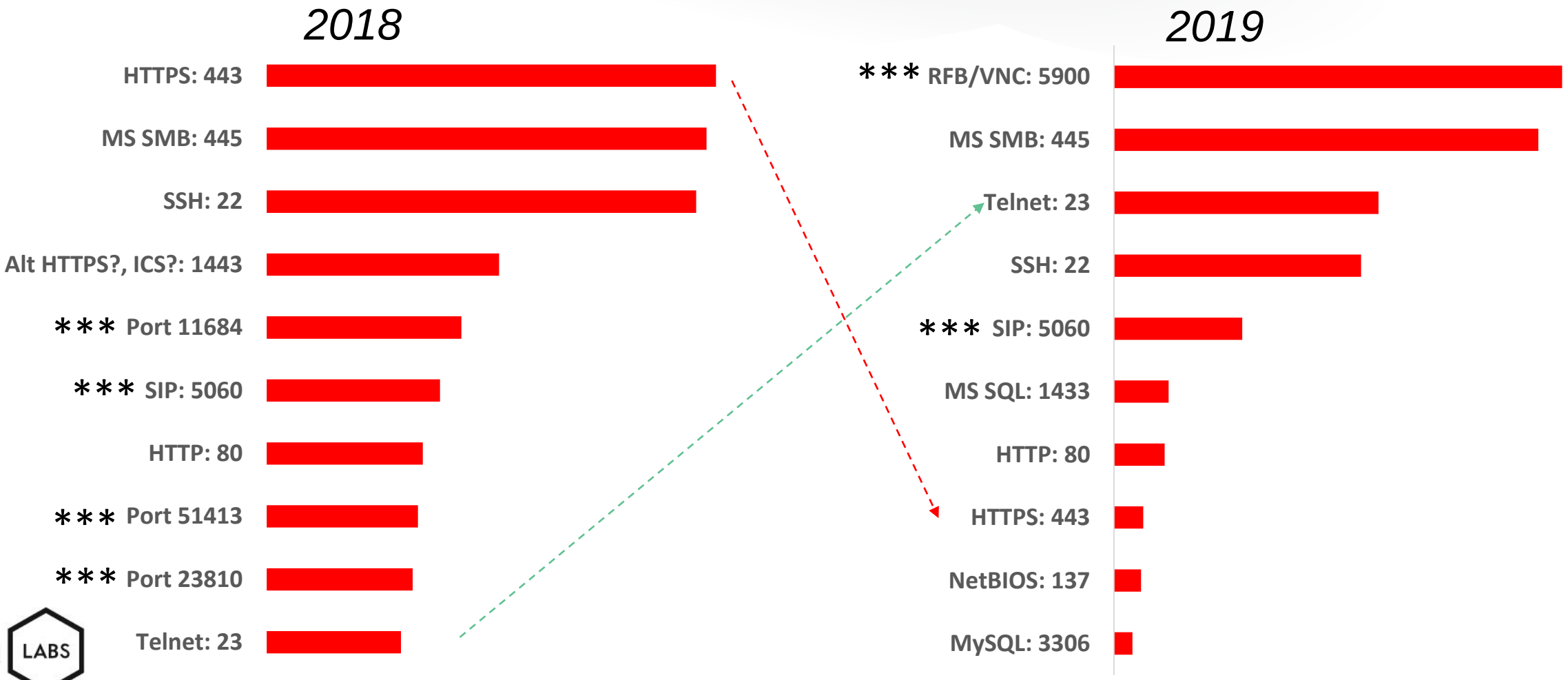
- Port scanning (SMB, MS SQL, RFB/VNC, SSH, NetBIOS, HTTP/S, Weblogic, Huewei)
- Credential Stuffing (RFB/VNC, Telnet, SSH)
- Malware uploads: SMB port 445

Australia

- Port scanning: RFB/VNC, MS SQL, SSH, Telnet, HTTP/S, SWX, Radan HTTP, Netbios,
- Credential stuffing: RFB/VNC, SSH, HTTP, FTP
- Malware uploads: SMB port 445

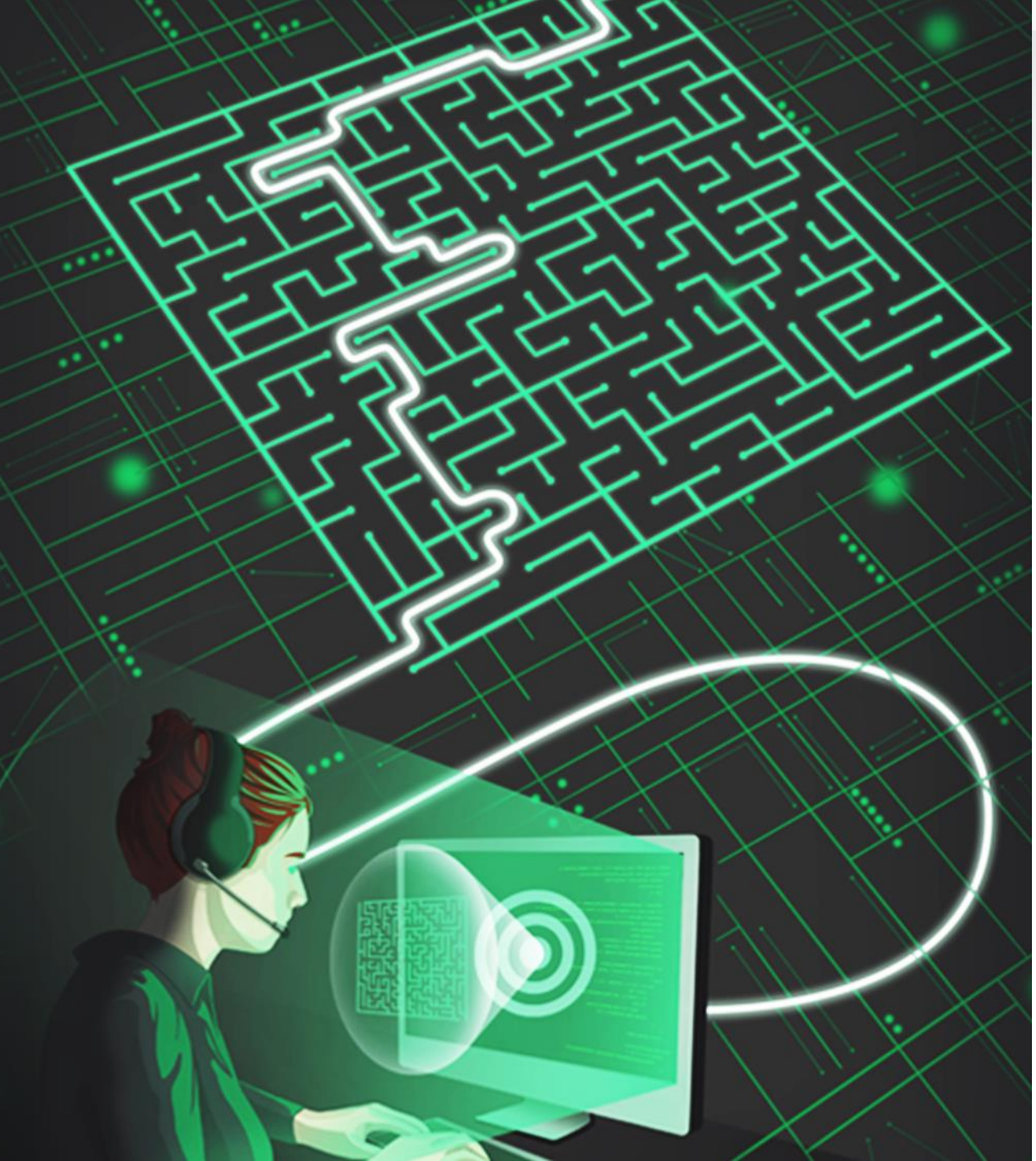
F5 LABS

Top 10 Attacked Ports Globally



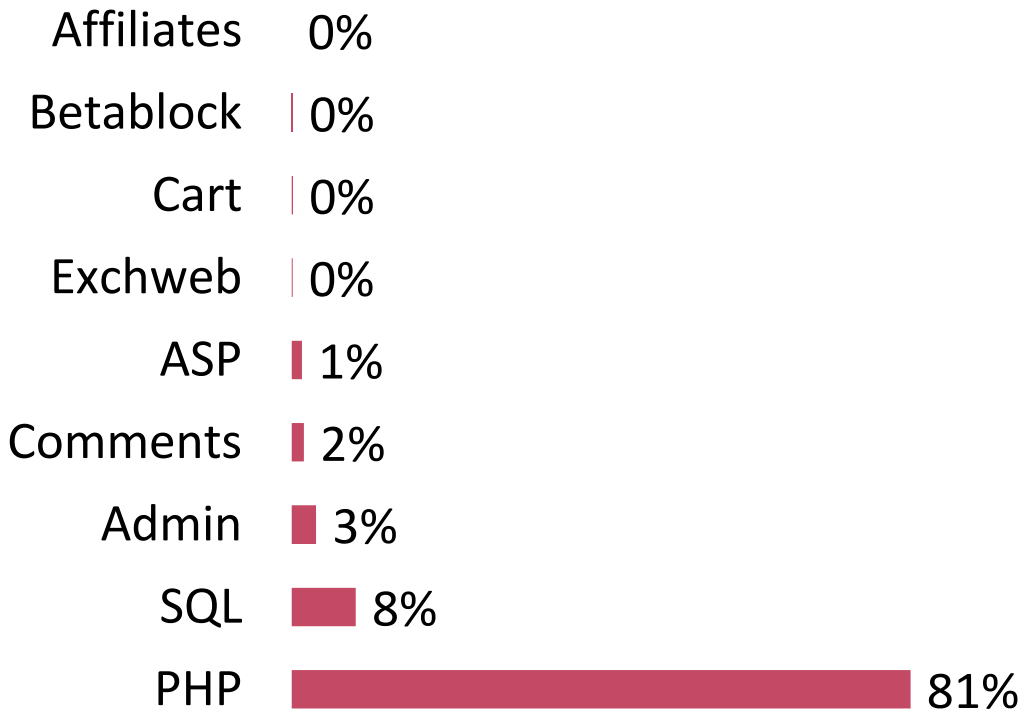
F5 LABS

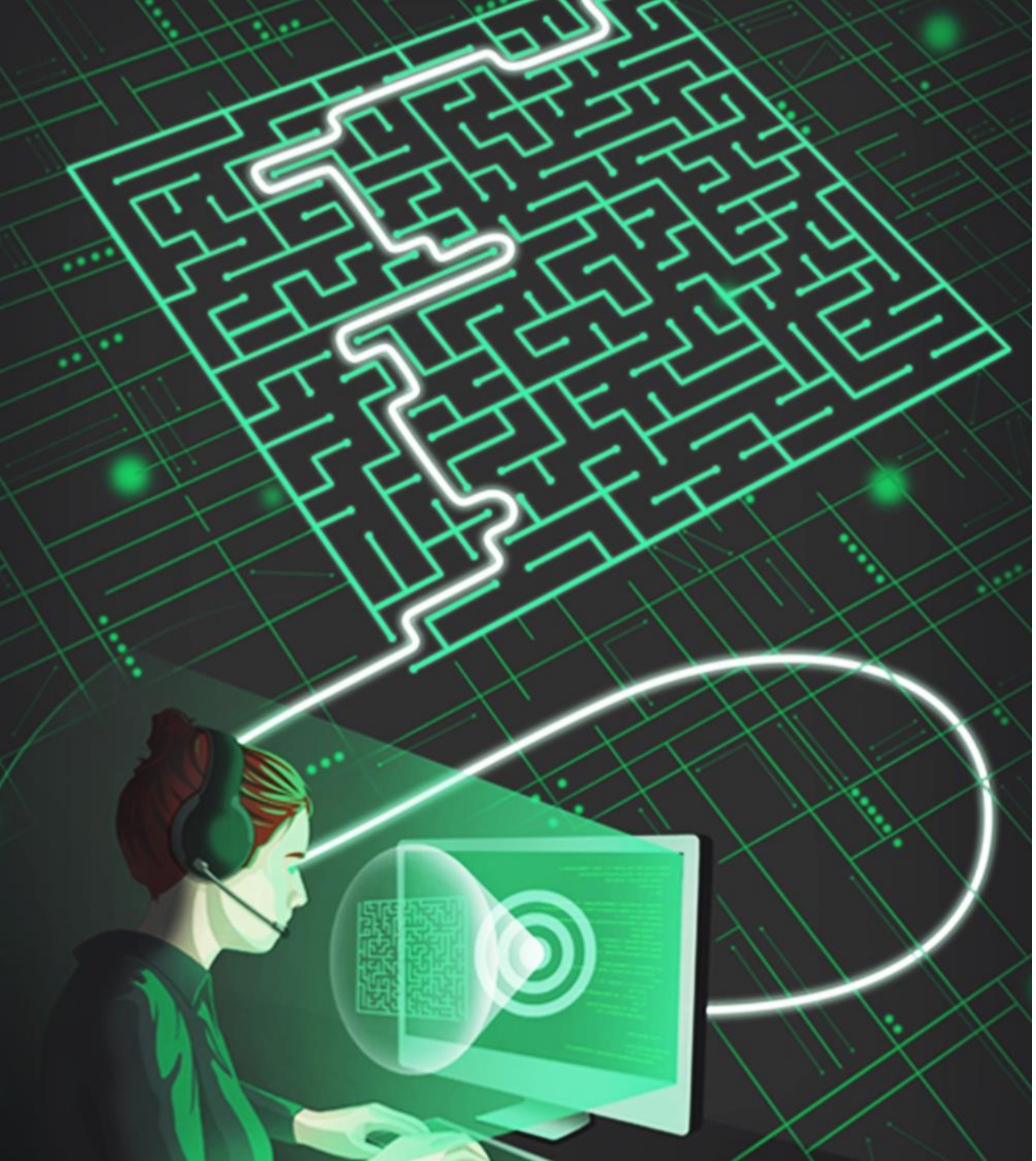
*** Attack campaign, not “normal” attack traffic.
- SIP 5060 began in 2018 and ended Q2 2019
- VNC 5900 began June 2019.



2018 HTTP Attacks

Injection → PHP



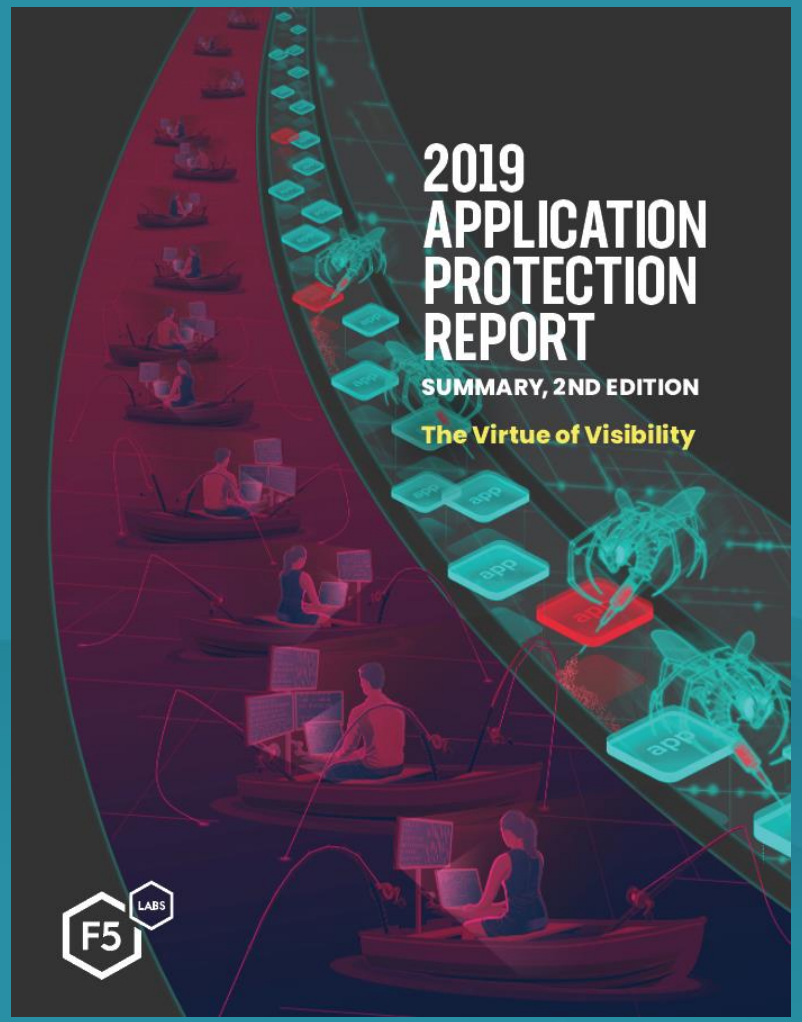


2019 HTTP Attacks

Injection → PHP

Jboss	0%
IIS Admin	0%
Comments	1%
PeopleAggregator	1%
Axis Webcam	1%
Joomla	1%
ASP	2%
SQL	3%
Admin (non PHP)	3%
PHP (no admin)	39%
PHPadmin	49%

RSAConference2020



Application Protection Research Series 2019 Conclusions

- PHP, the weak point of the Internet
- Attack methods follow business models
- Injection, rejuvenated
- Access attacks predominant
- APIs changing the landscape

Methodology & Sources

Baffin Bay Data

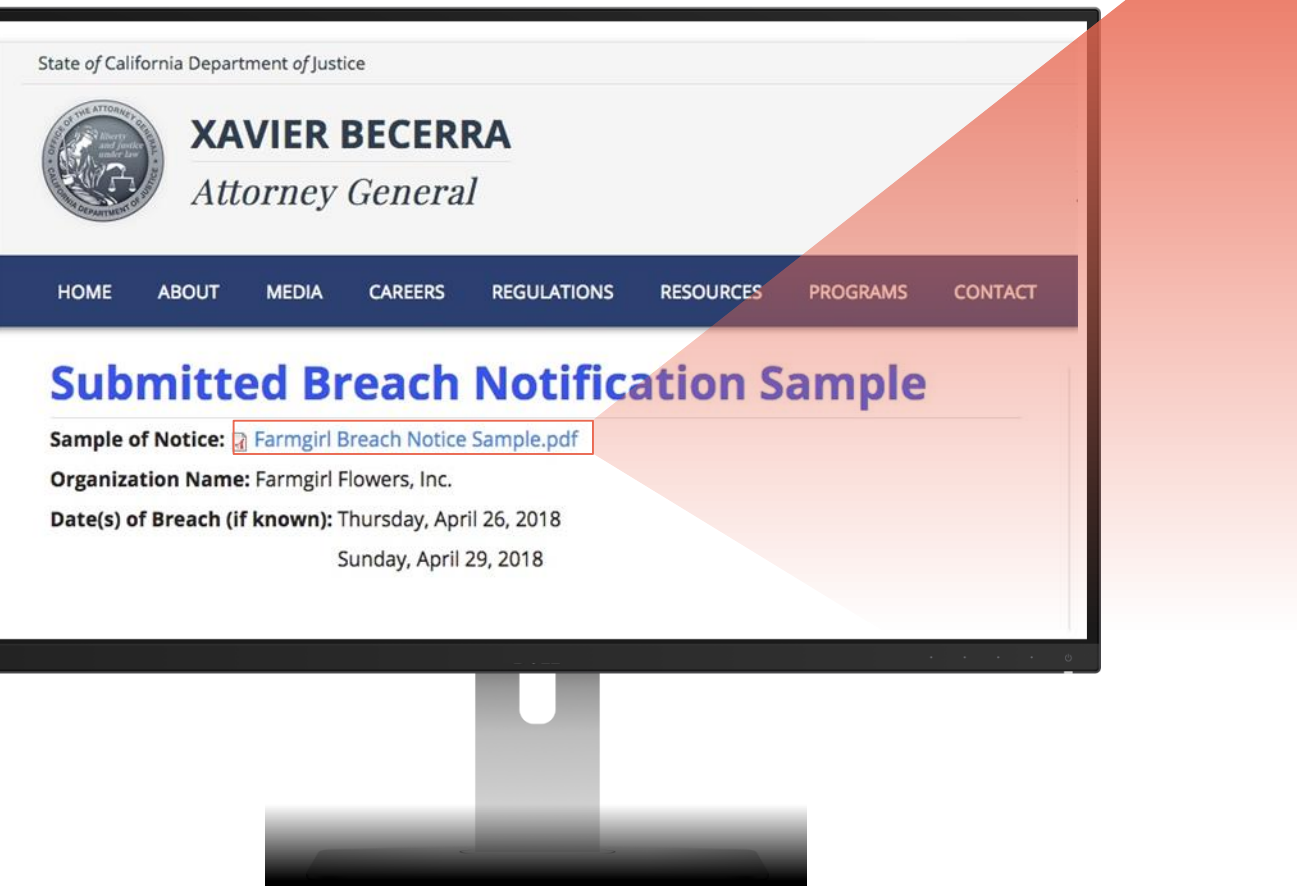
2018 Breach Data
2019 Breach Data

F5 SIRT data

Breach Analysis
State Attorney General

761
Cases 2018

87%
Had explanations



Farmgirl FLOWERS™
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00061
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 11, 2018

Re: NOTICE OF DATA BREACH

We are so sorry to inform you that we recently became aware of a data breach that may have compromised your personal information. We understand how important your privacy is, and we take the protection of your information very seriously. Our company is built on honestly, trust, and transparency, which is why I'm reaching out personally to let you know about what happened and what we're doing to address it.

What Happened?

On April 29, 2018, at approximately 4:00 p.m. (all times PST), we learned that there was unauthorized access by electronic means to our data by a person or persons whose identities remain unknown. The unauthorized access occurred sometime between 1:00 p.m., on April 26, 2018, and 3:08 p.m., on that same date. **The unauthorized access involved the insertion of rogue code into our checkout page.** The code was designed to capture the name, billing address, phone number, and email address of certain customers, and also their credit card information, and then send that data to a remote endpoint. The customer order dates for potentially compromised information are April 26, 2018, at 1:00 p.m., until April 29, 2018, at 4:10 p.m. Although we cannot be sure that any of your information was accessed or misappropriated, we are sending you this notice to make you aware of the situation and to provide you with other helpful information.

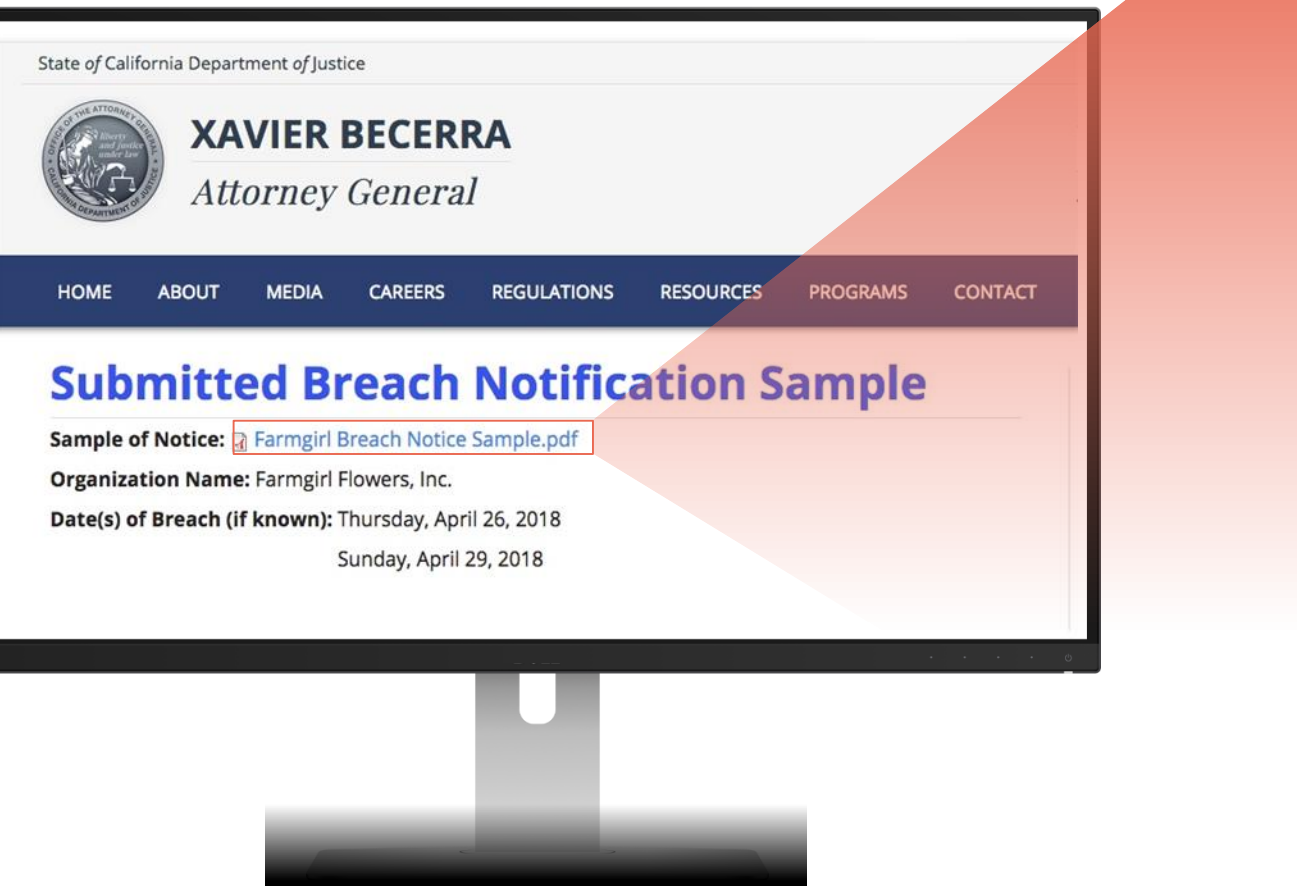
What Information Was Involved?

The information that was accessed without authorization could have included your name, billing address, for a credit card, telephone number, email address, and credit card information including card

Breach Analysis
State Attorney General

1025
Cases 2019

85%
Had explanations



Farmgirl FLOWERS™
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00061
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 11, 2018

Re: NOTICE OF DATA BREACH

We are so sorry to inform you that we recently became aware of a data breach that may have compromised your personal information. We understand how important your privacy is, and we take the protection of your information very seriously. Our company is built on honestly, trust, and transparency, which is why I'm reaching out personally to let you know about what happened and what we're doing to address it.

What Happened?

On April 29, 2018, at approximately 4:00 p.m. (all times PST), we learned that there was unauthorized access by electronic means to our data by a person or persons whose identities remain unknown. The unauthorized access occurred sometime between 1:00 p.m., on April 26, 2018, and 3:08 p.m., on that same date. **The unauthorized access involved the insertion of rogue code into our checkout page.** The code was designed to capture the name, billing address, phone number, and email address of certain customers, and also their credit card information, and then send that data to a remote endpoint. The customer order dates for potentially compromised information are April 26, 2018, at 1:00 p.m., until April 29, 2018, at 4:10 p.m. Although we cannot be sure that any of your information was accessed or misappropriated, we are sending you this notice to make you aware of the situation and to provide you with other helpful information.

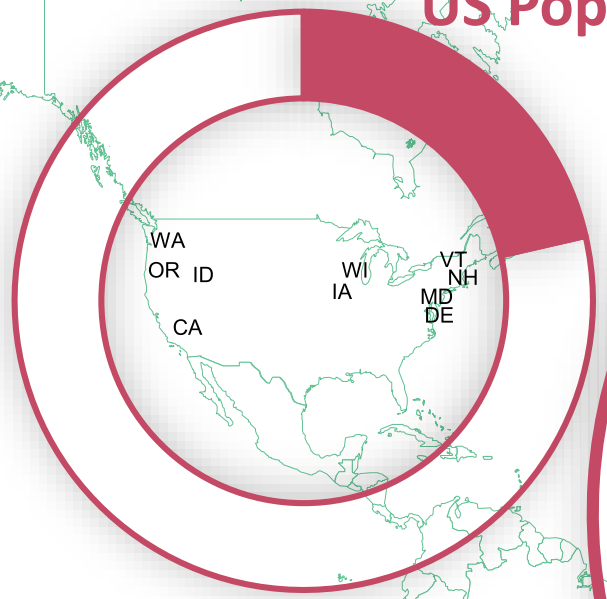
What Information Was Involved?

The information that was accessed without authorization could have included your name, billing address, for a credit card, telephone number, email address, and credit card information including card

Global Breach Notification Scope

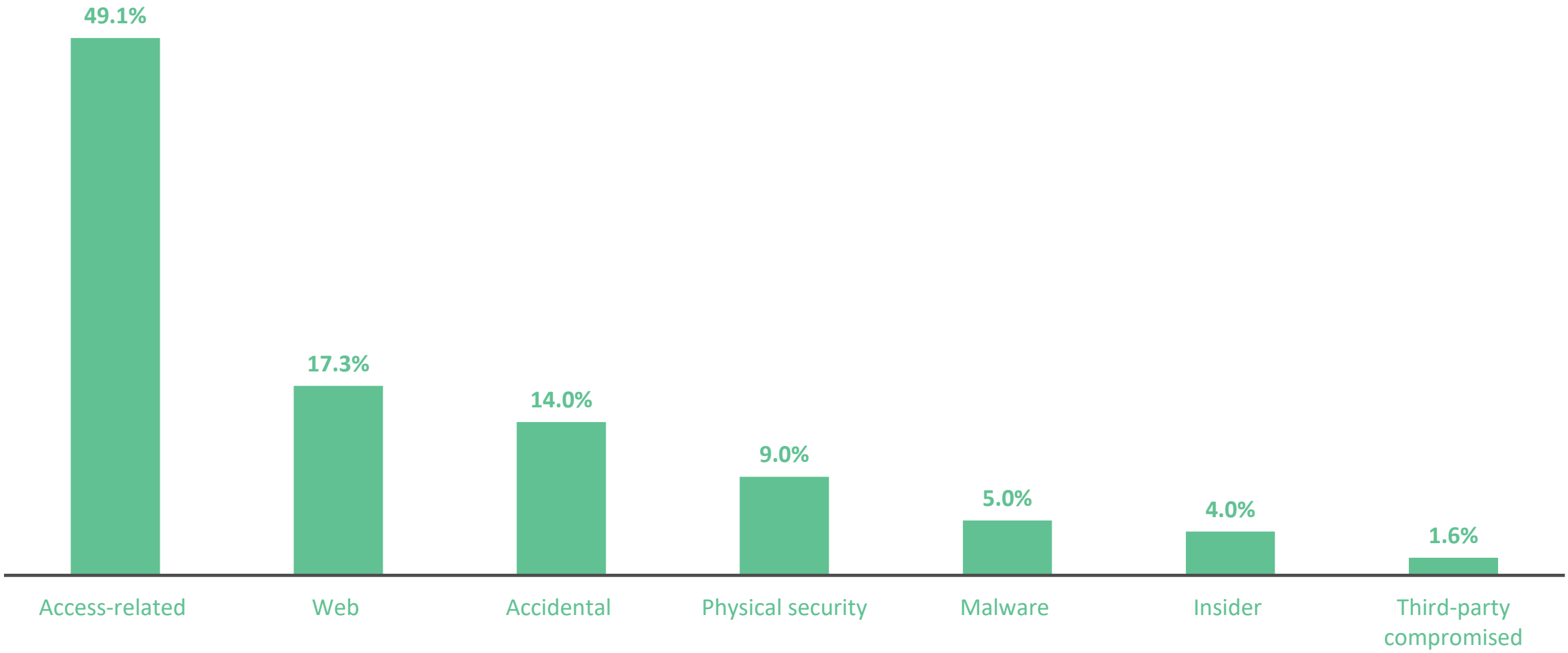
21.4%
US Population

1% **Global population**

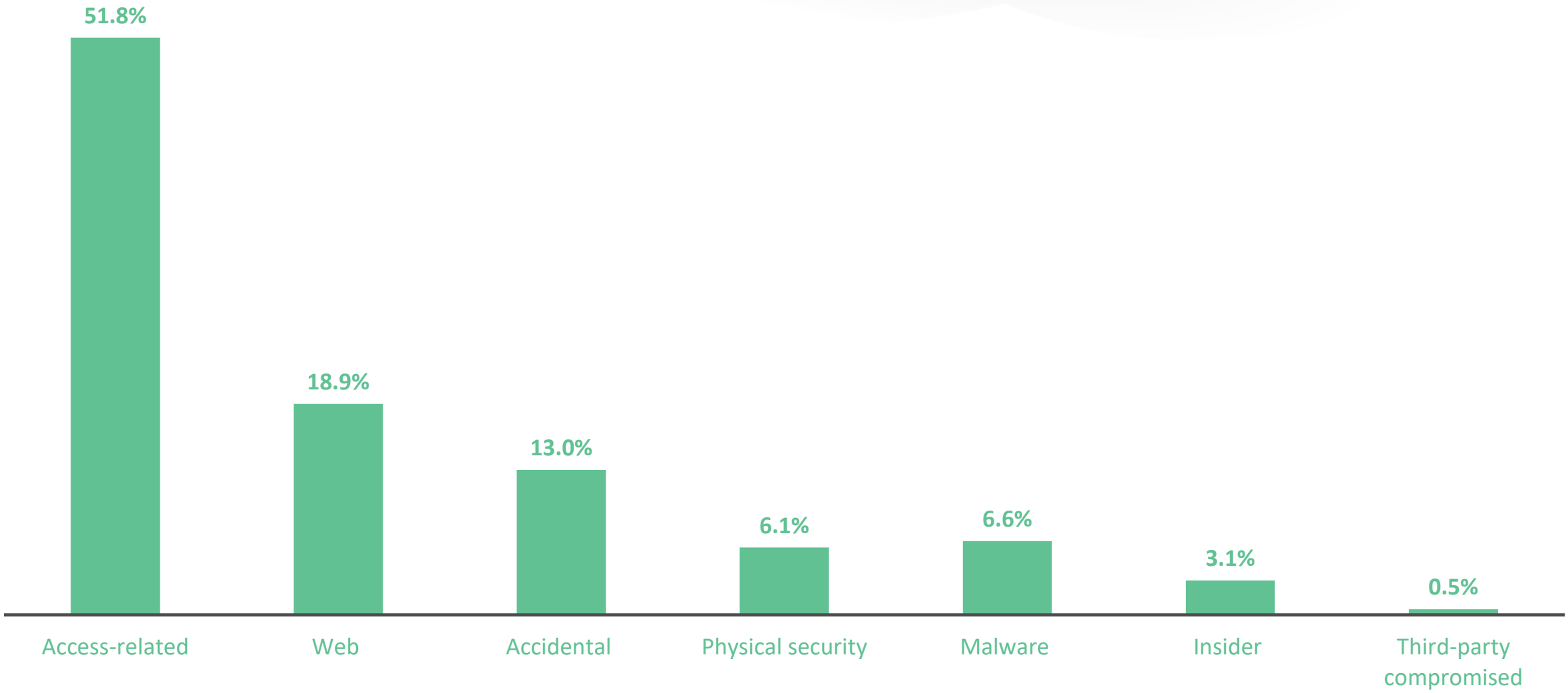


10
US States share breach records

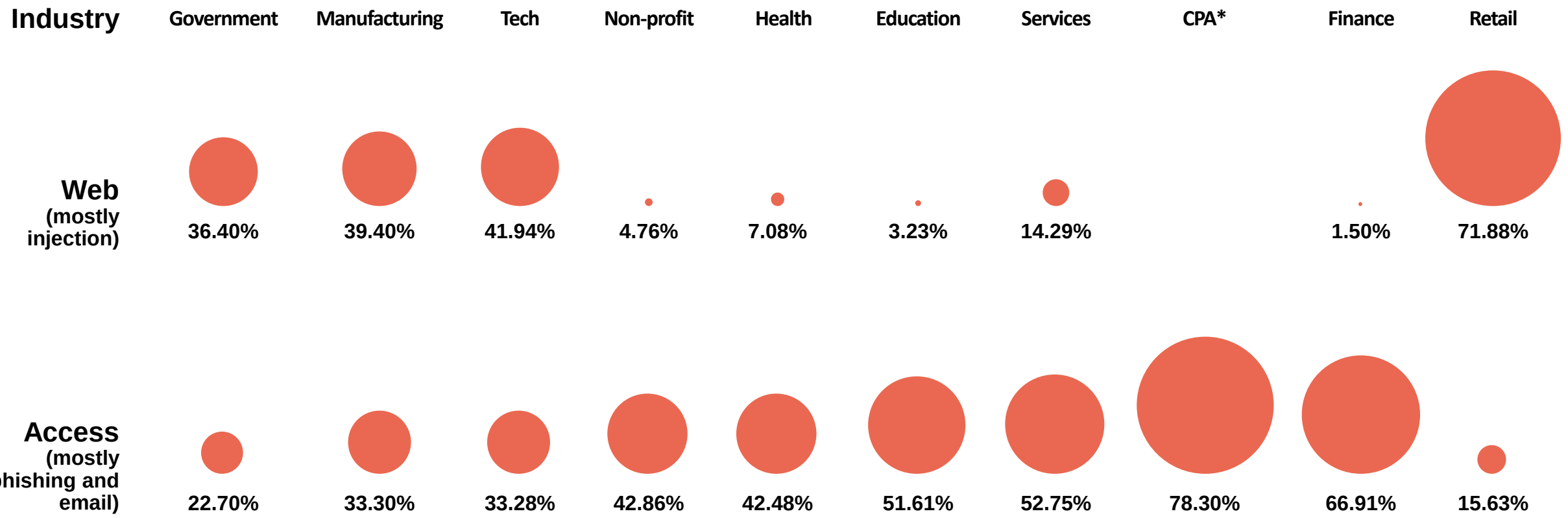
2018 US Breaches by Cause (%)



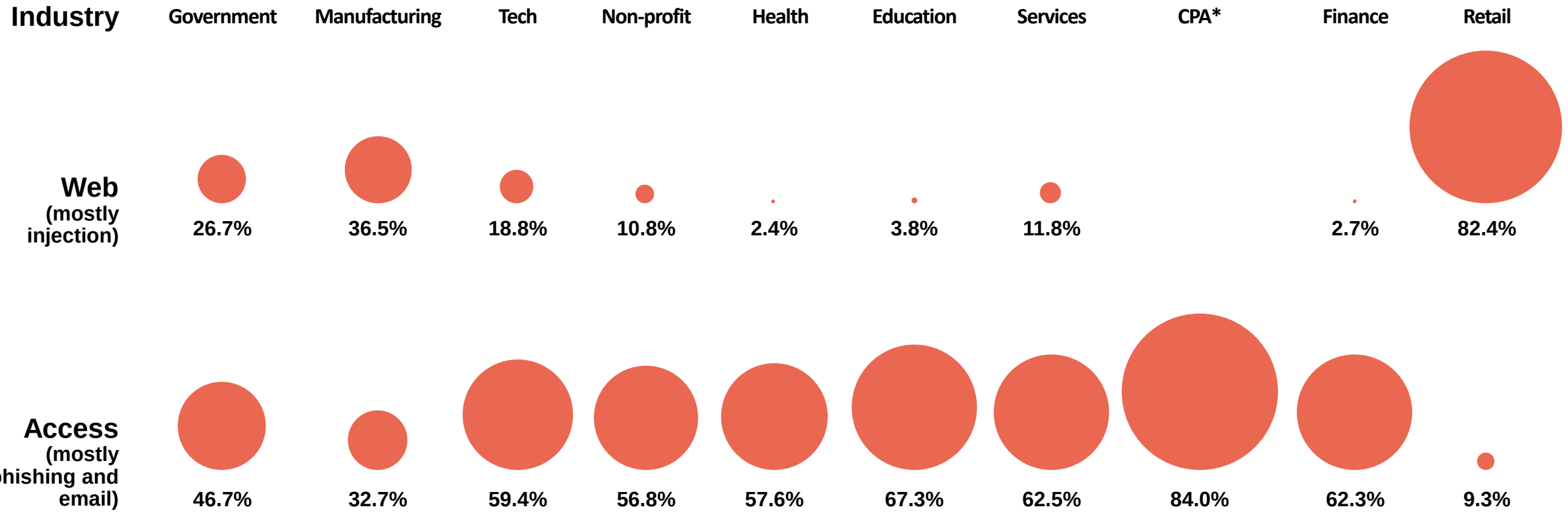
2019 US Breaches by Cause (%)



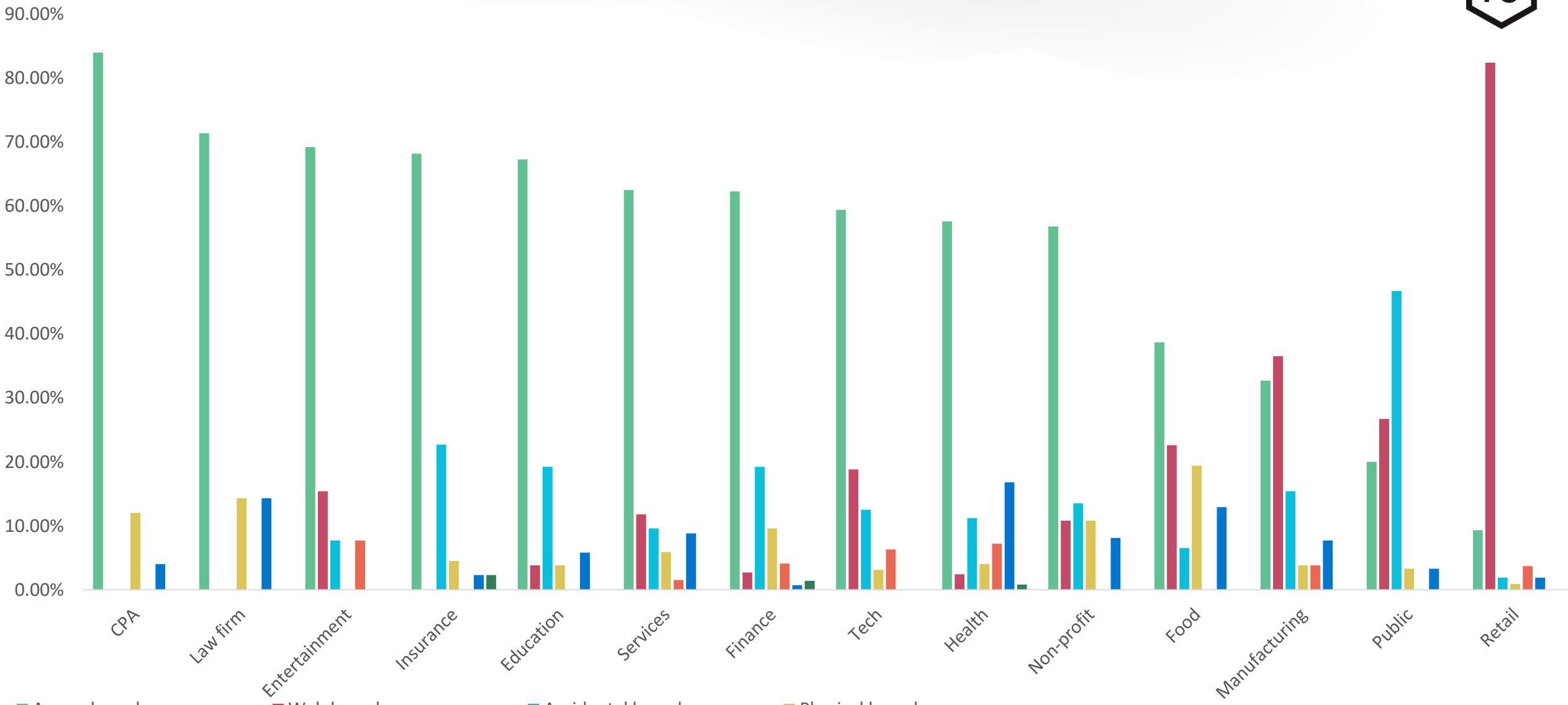
2018 Breach Root Causes

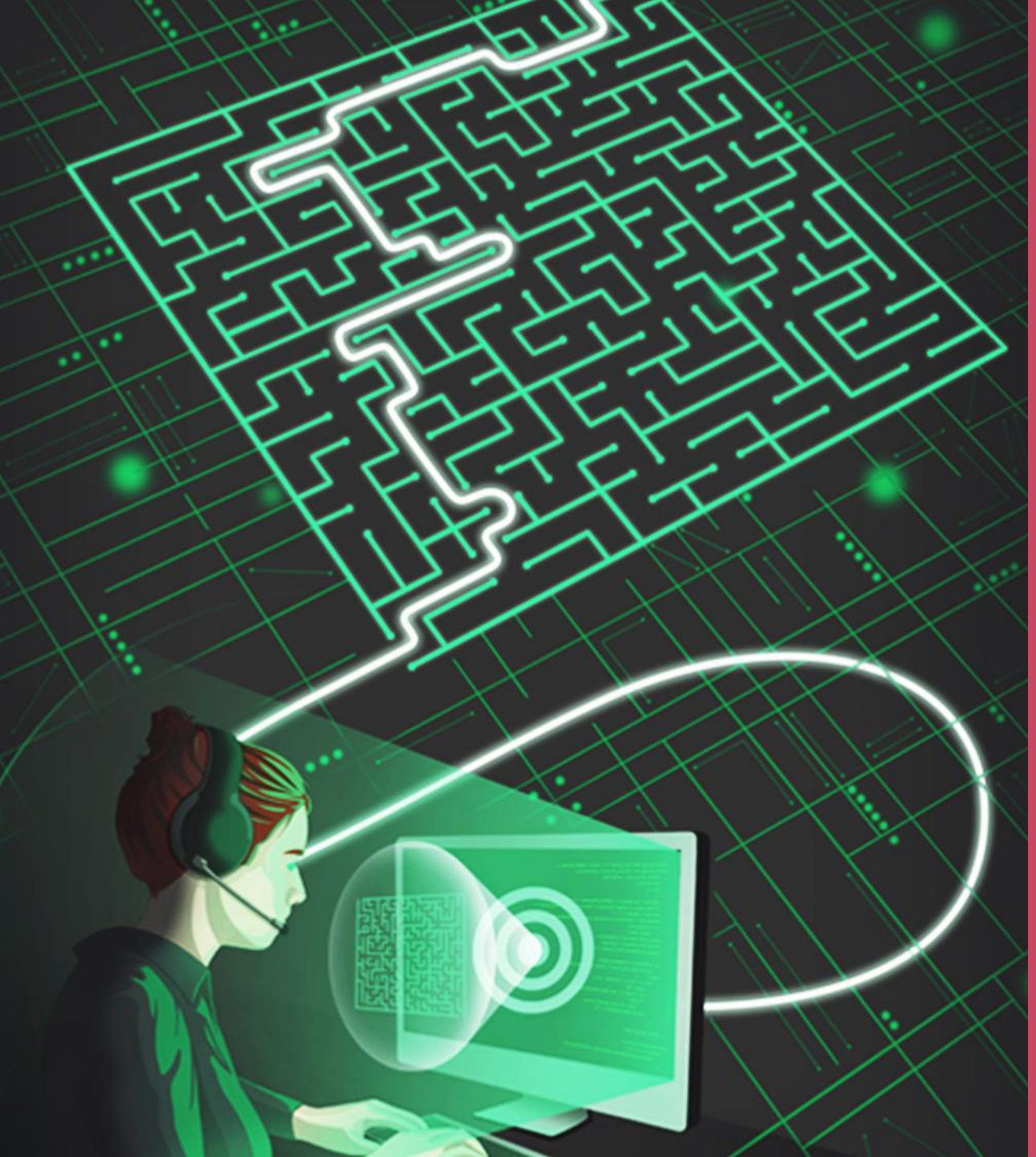


2019 Breach Root Causes



2019 Breach Methods by Sector

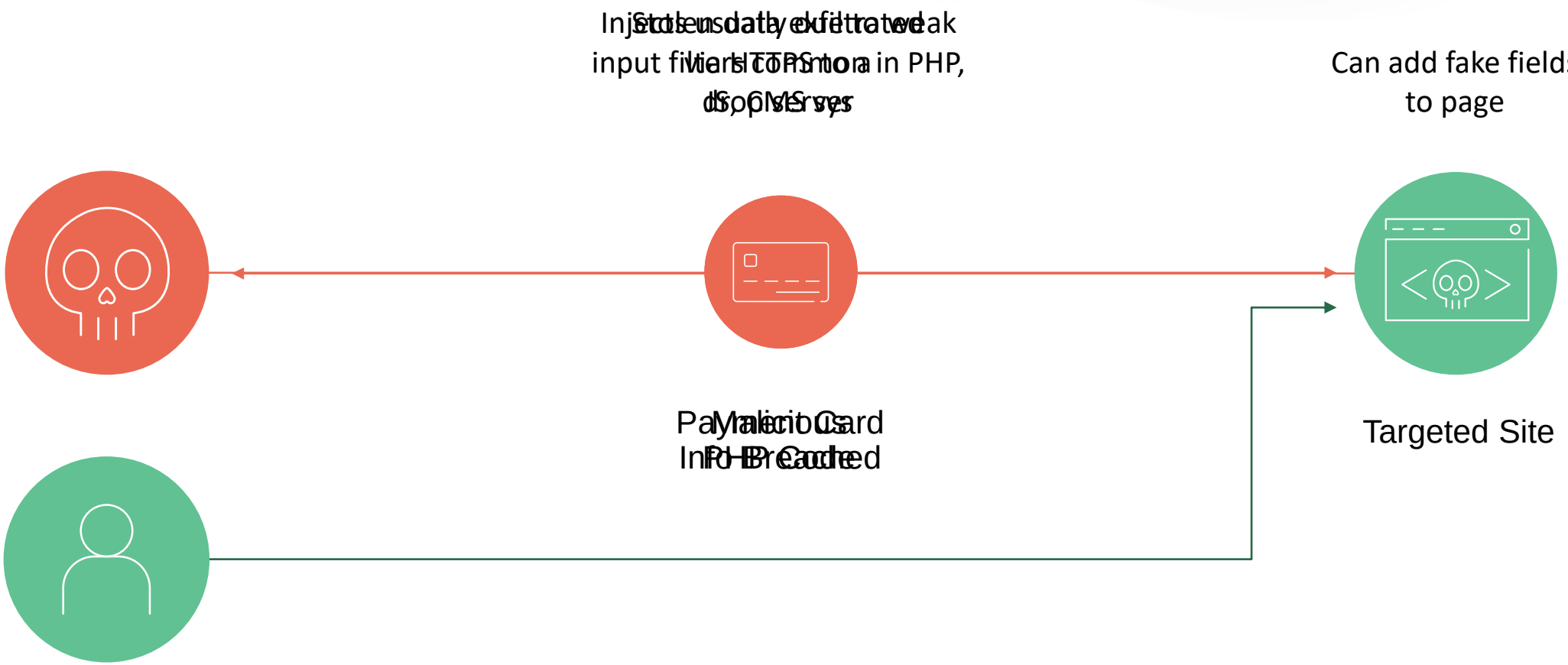




Web Attacks:

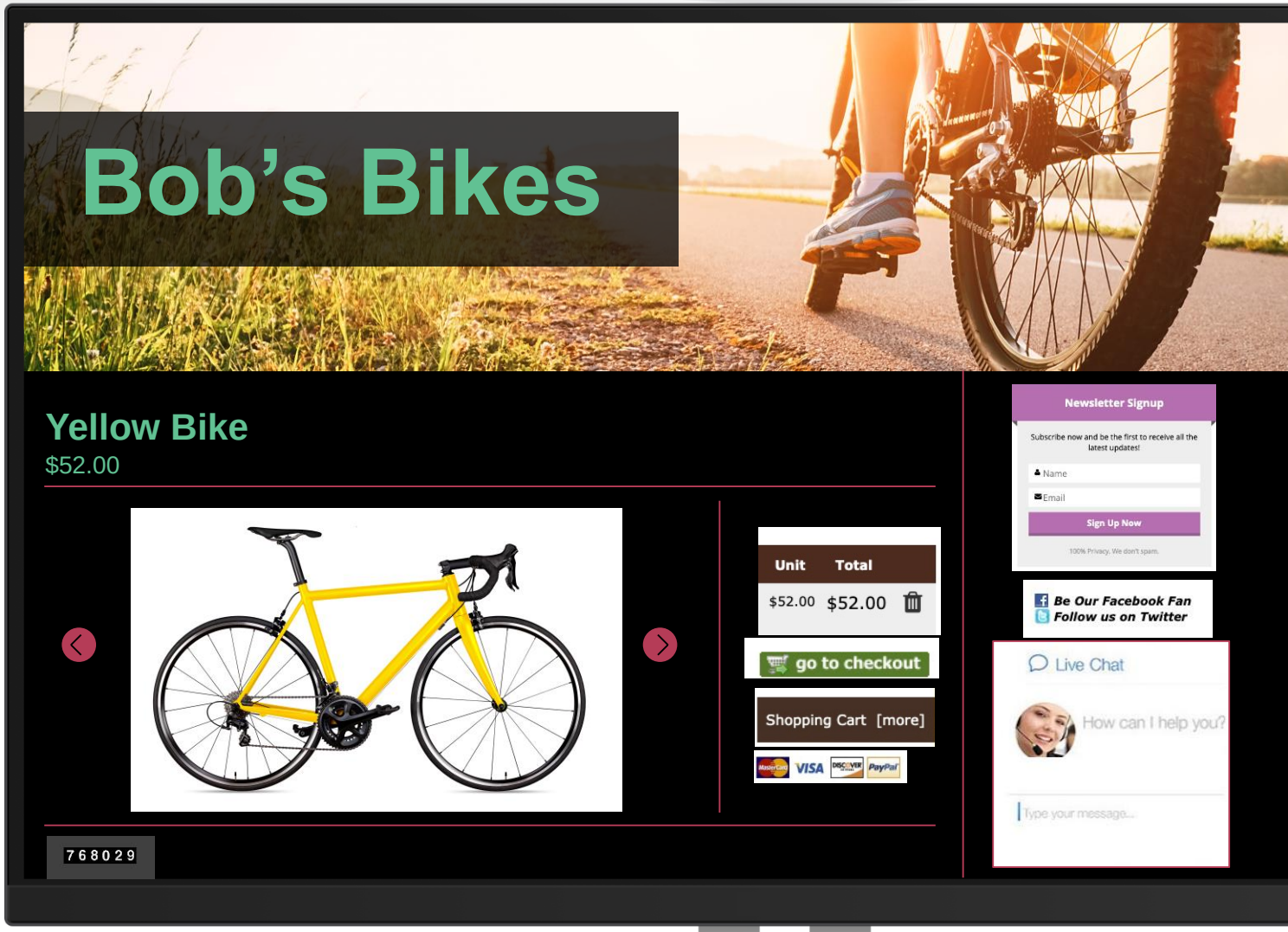
Don’t fix it if it ain’t broke

Card Stealing Web Injects



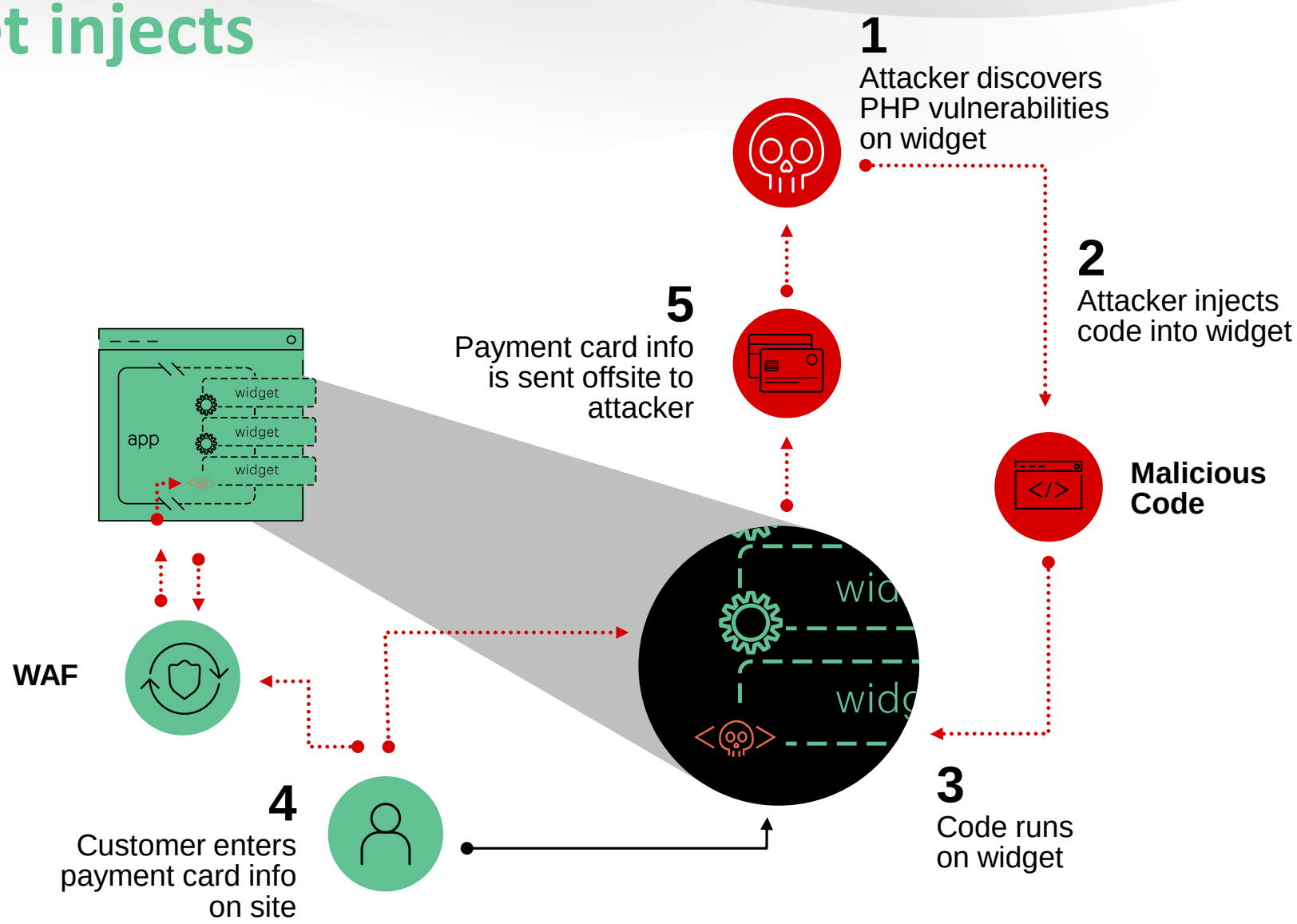
A typical shopping site

Third party widgets/content



All linked off main app site but hosted elsewhere…

Third party widget injects not seen by WAF

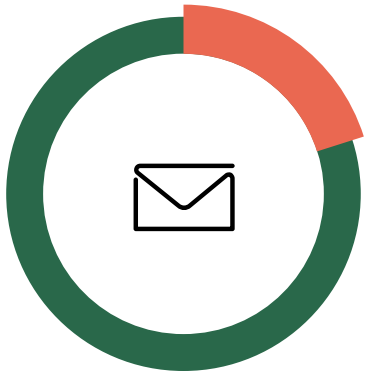


Access Attacks:

Primary cause of breach

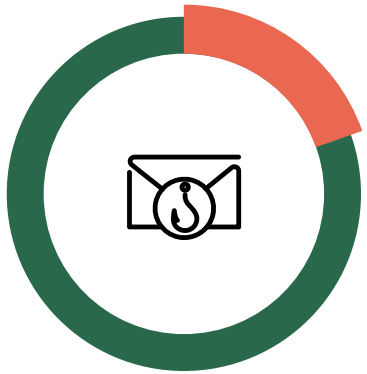
- Brute force
- Credential Stuffing
- Phishing

2018 Access Attacks Broken Down



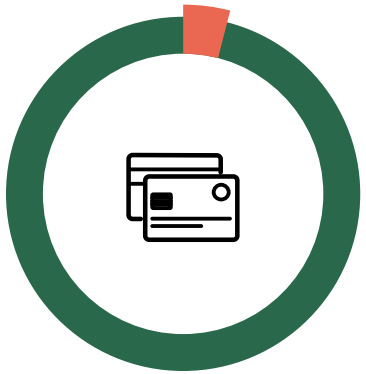
20.0%

Email cited as cause



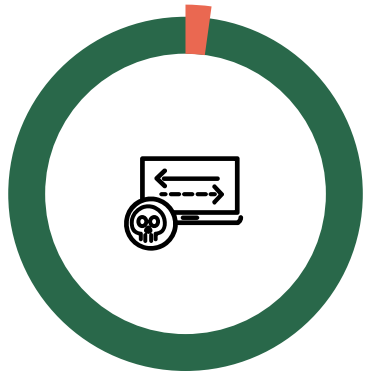
19.6%

Phishing gain access to email



4.0%

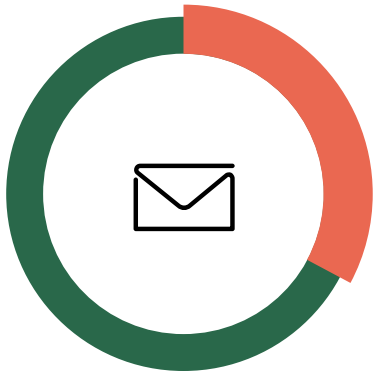
Access creds stolen



2.2%

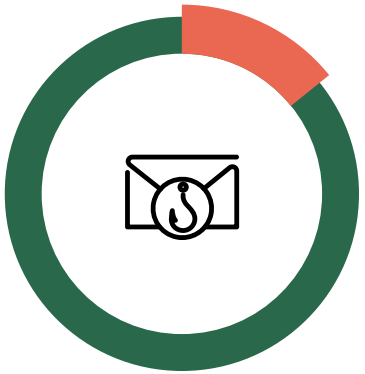
Access cred stuffing and brute

2019 Access Attacks Broken Down



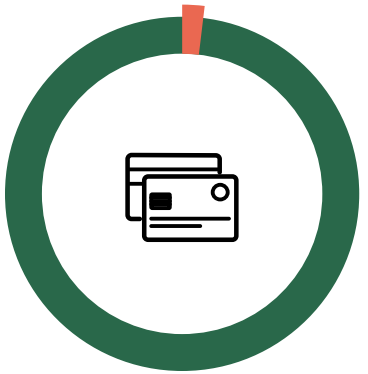
32.8%

Email cited as cause



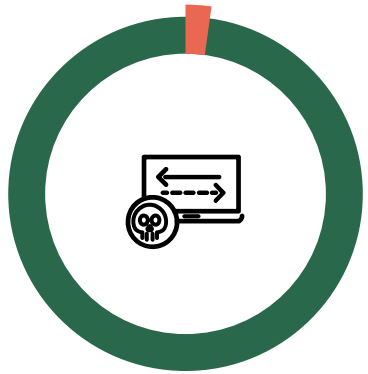
14.2%

Phishing gain access to email



1.9%

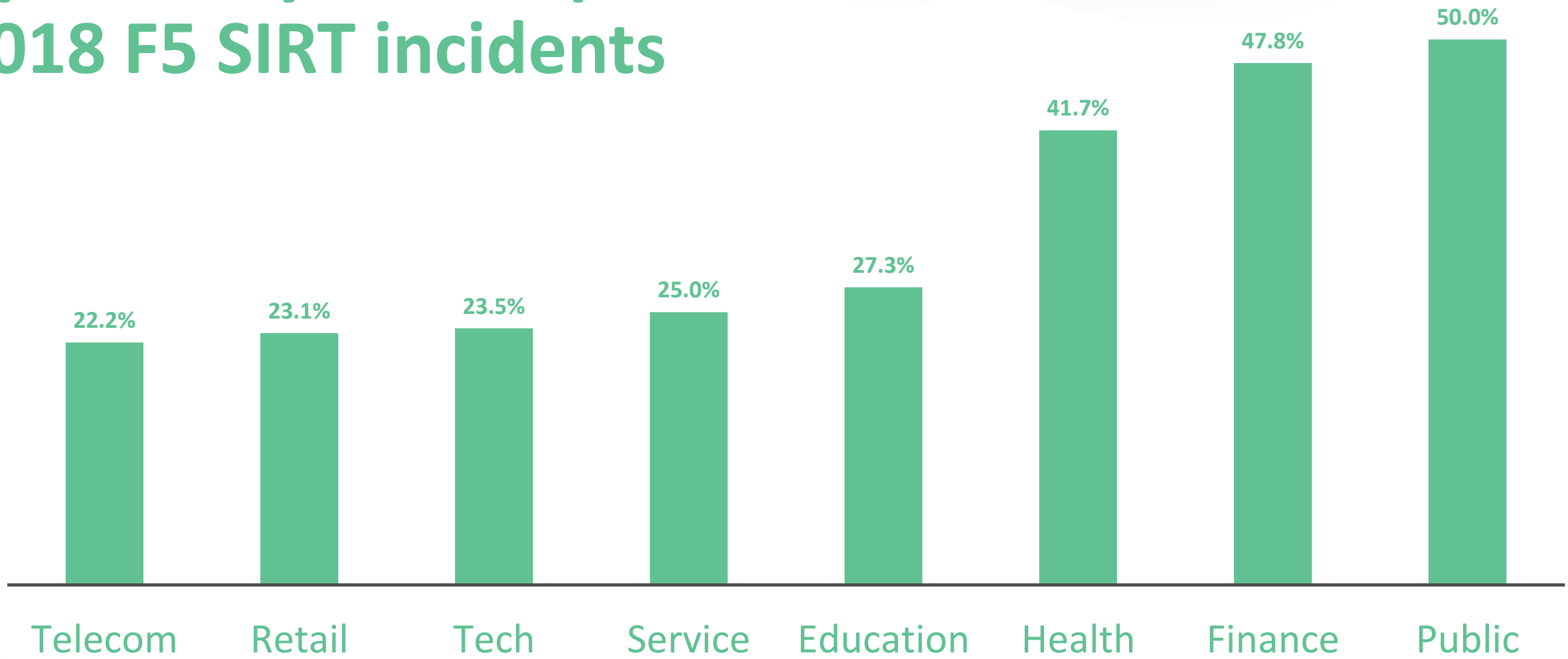
Access creds stolen



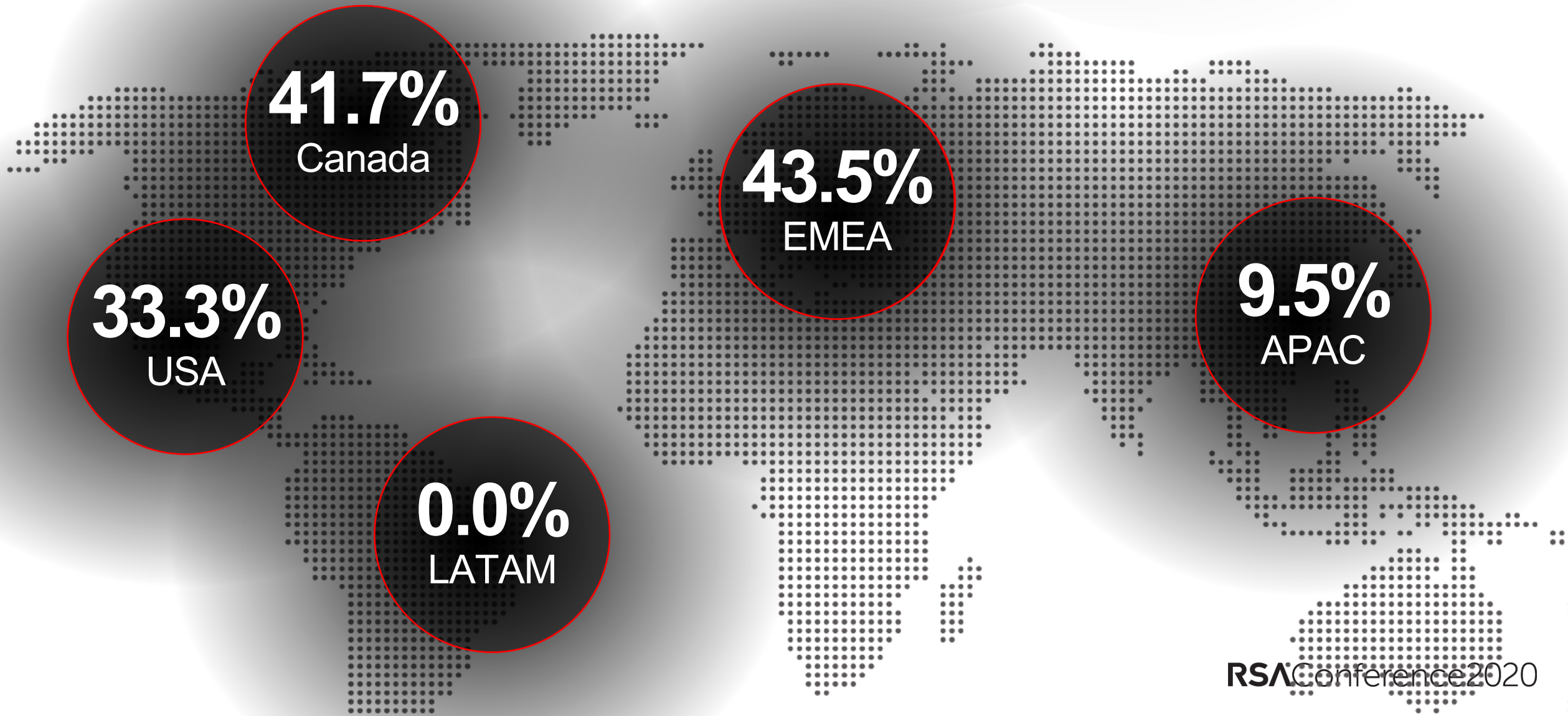
2.2%

Access cred stuffing and brute

Brute Force attacks by industry from reported 2018 F5 SIRT incidents



Brute Force incidents reported to F5 SIRT



Breach Data Conclusions

- Access attacks predominant
- Retail breaches increasingly dominated by formjacking
- Breach modes driven more by business model and application architecture than by traditional sector
- Third-party enfilade attacks make niche providers risky (more on this in 2020)

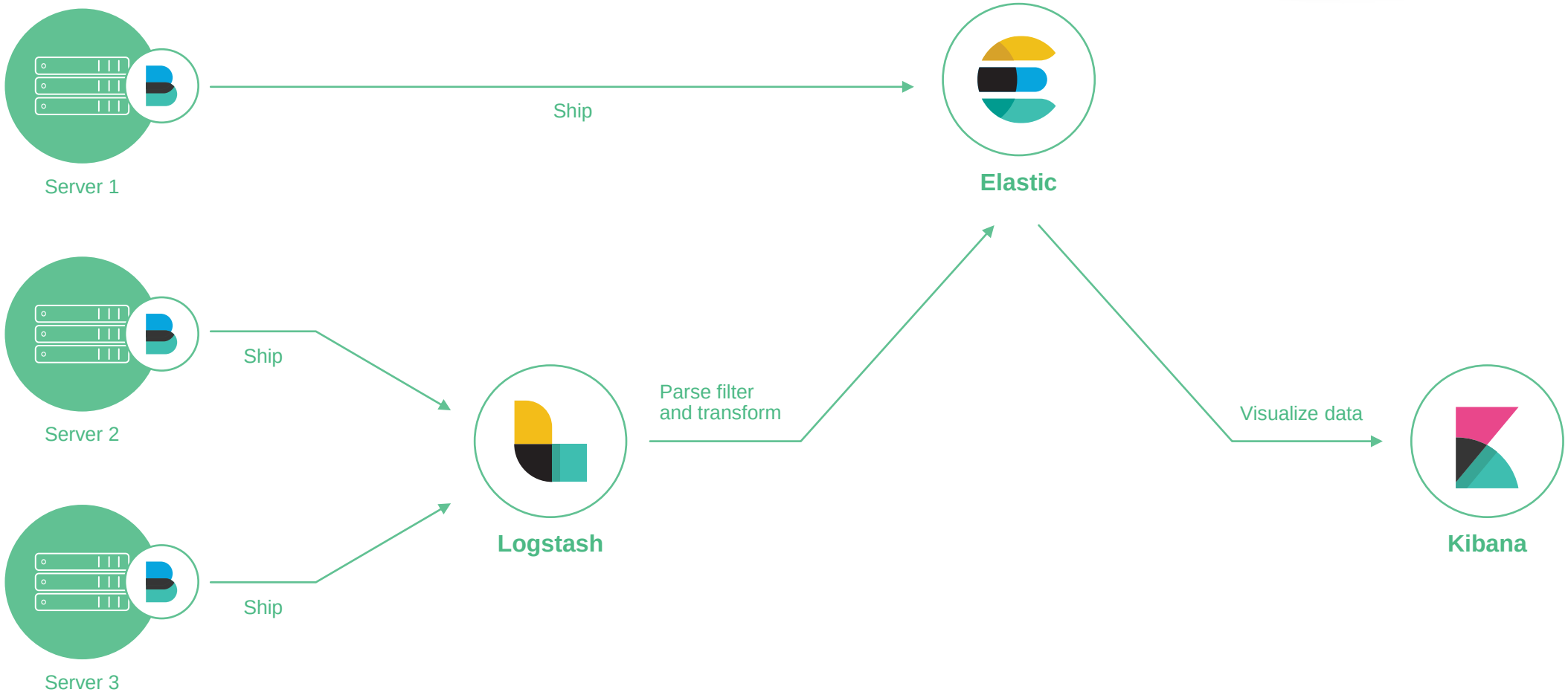
API & Cloud Attacks

API Breaches

API Incident Trends

Cloud Breaches

Apps Expose their APIs



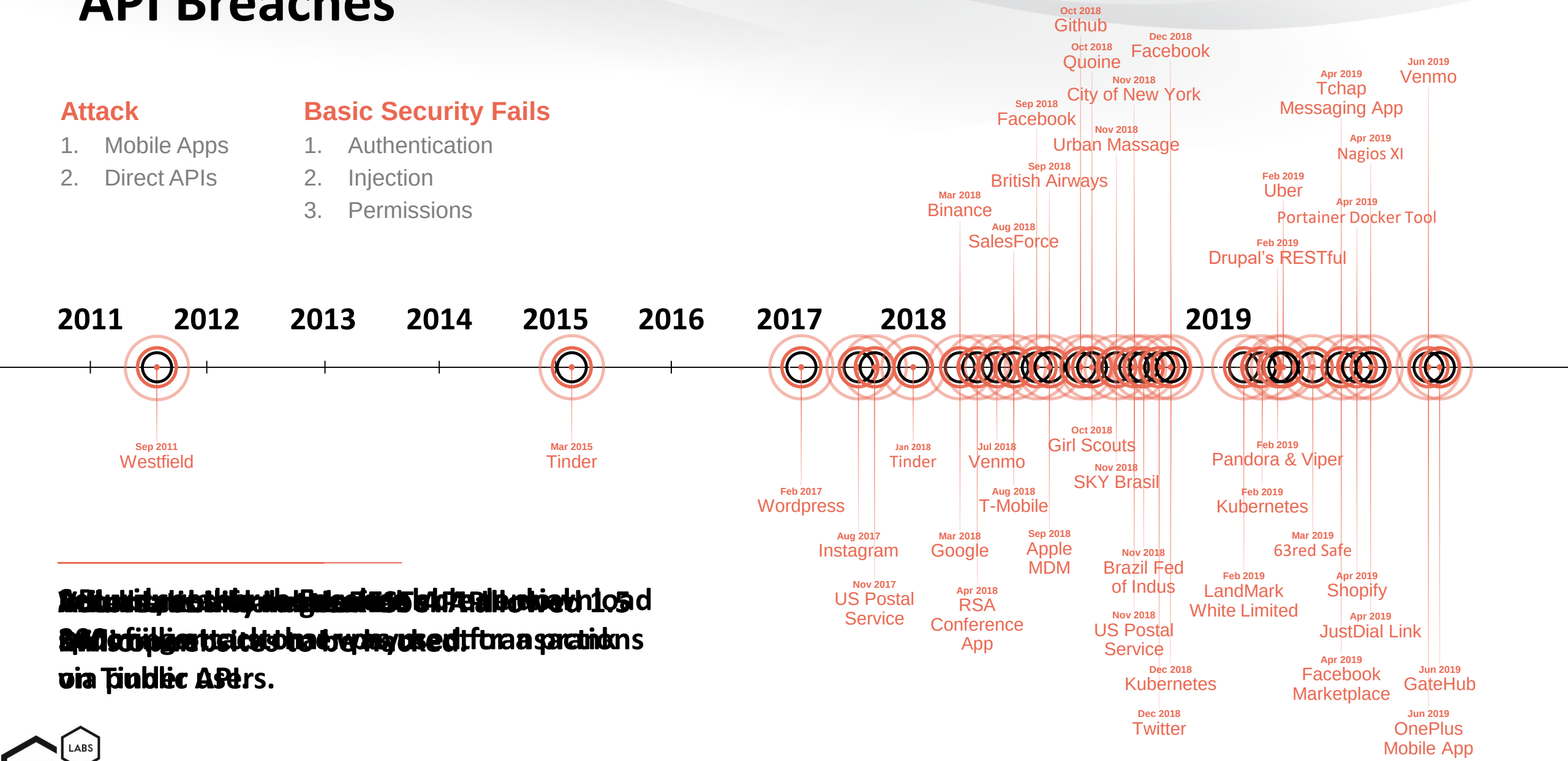
API Breaches

Attack

1. Mobile Apps
2. Direct APIs

Basic Security Fails

1. Authentication
2. Injection
3. Permissions

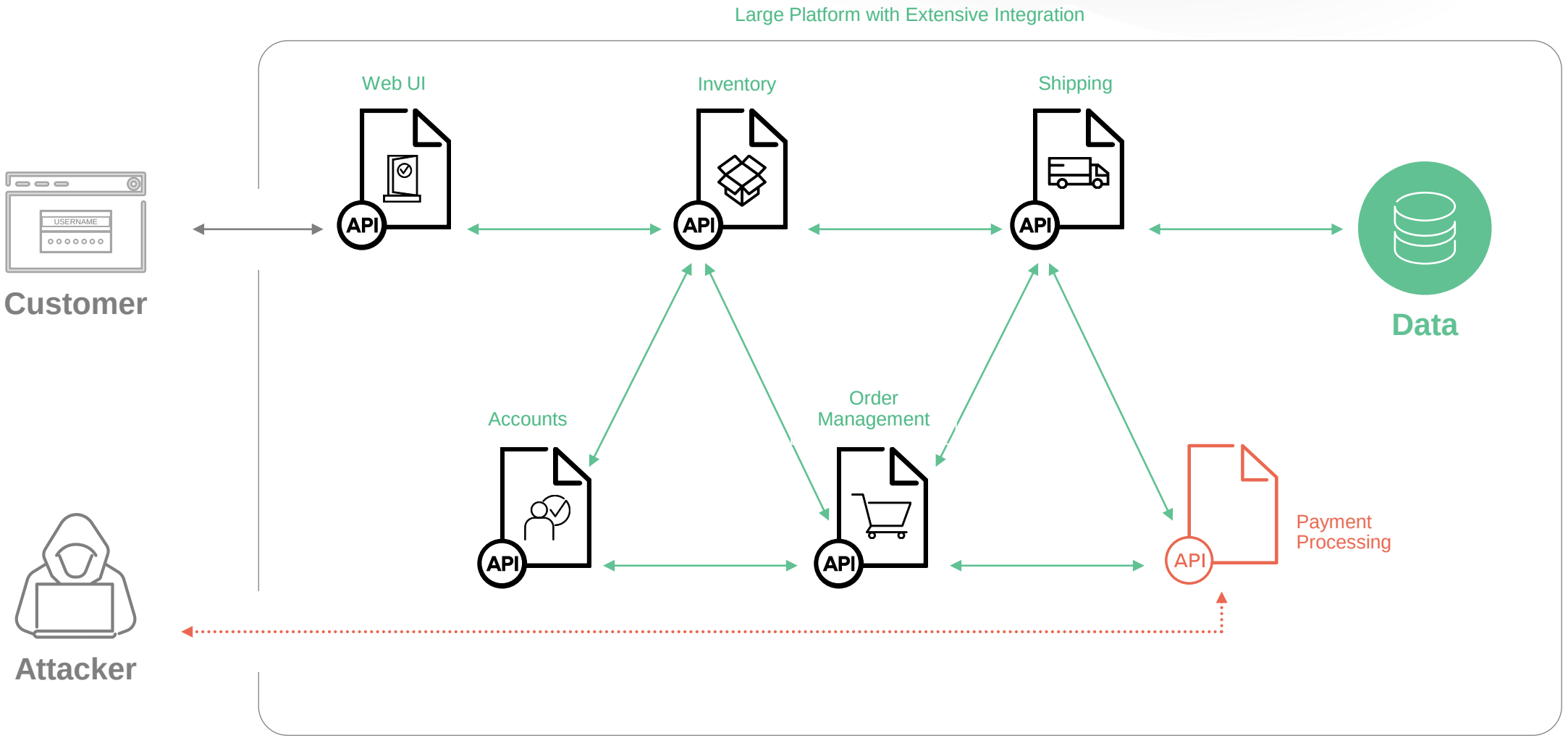


[redacted]

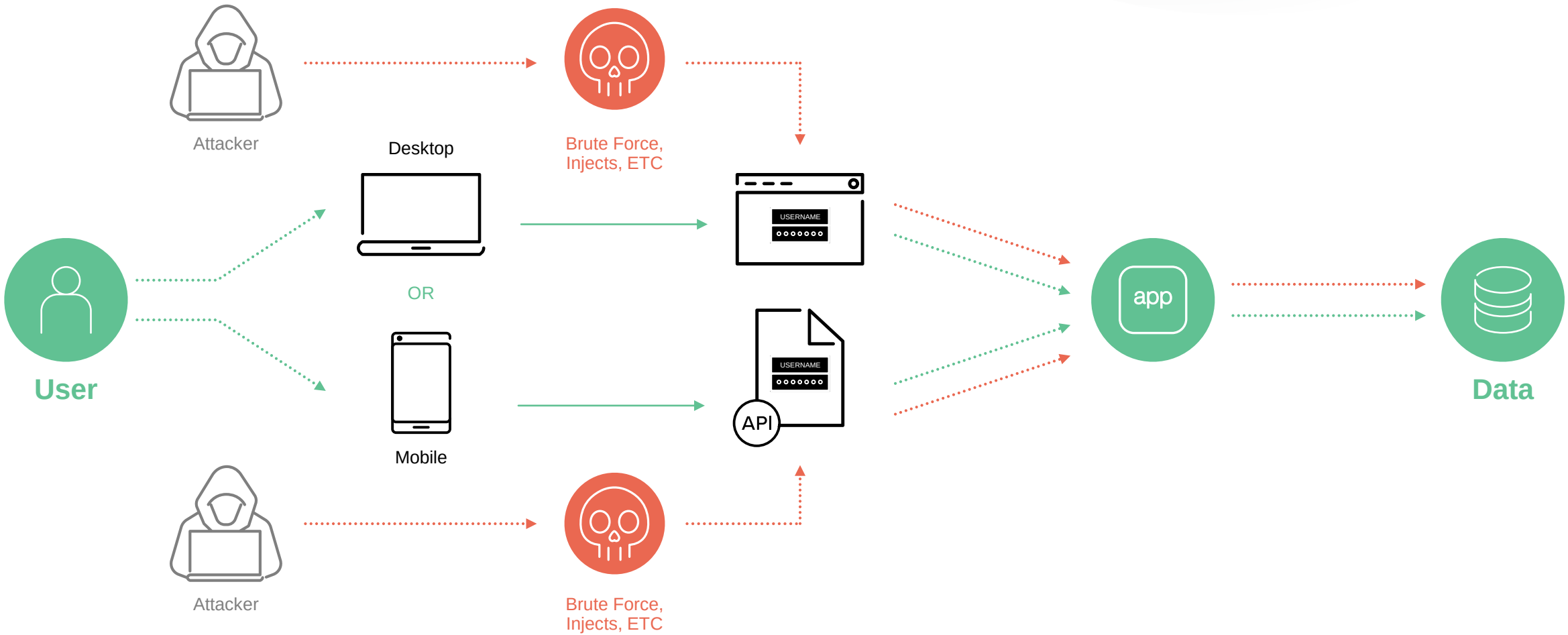
F5 LABS

RSAConference2020

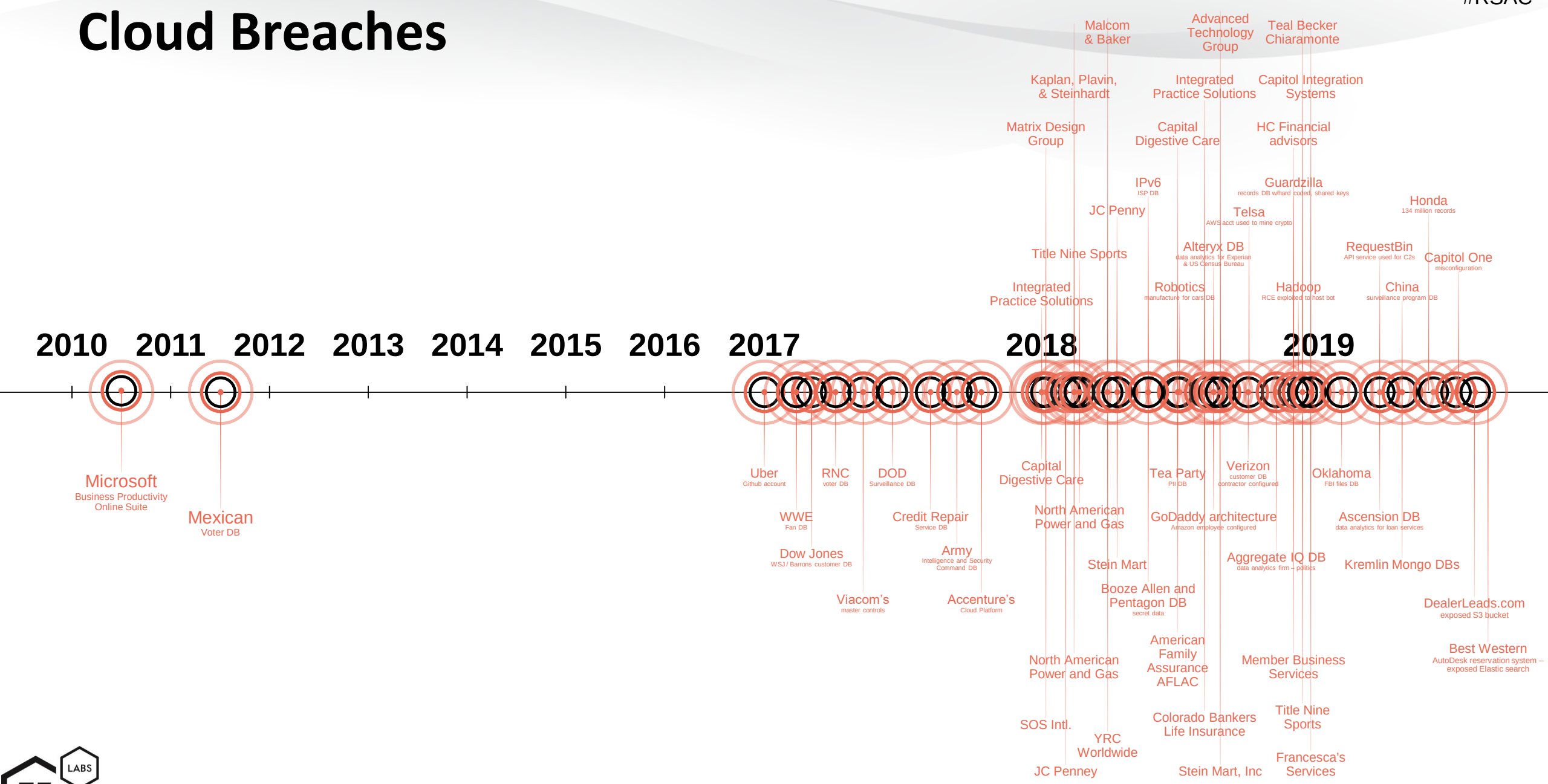
API Platform Attacks



API Mobile Attacks



Cloud Breaches



Protecting Applications

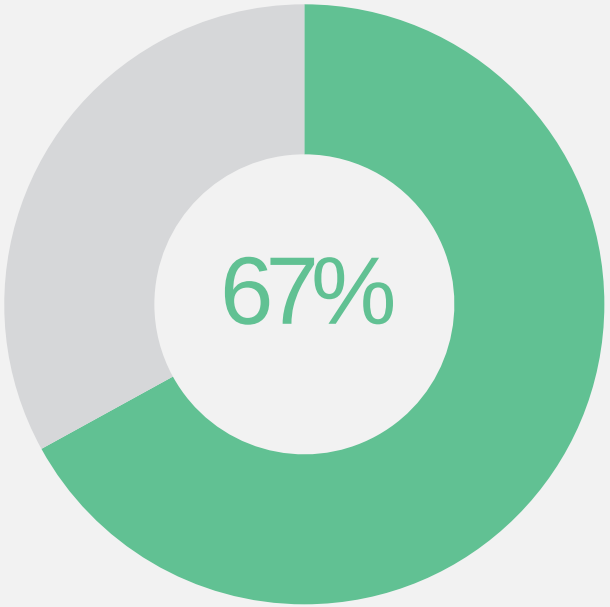
2020 SOAS Report

Recommendations

Multi-Cloud is the Norm, Security is the Challenge

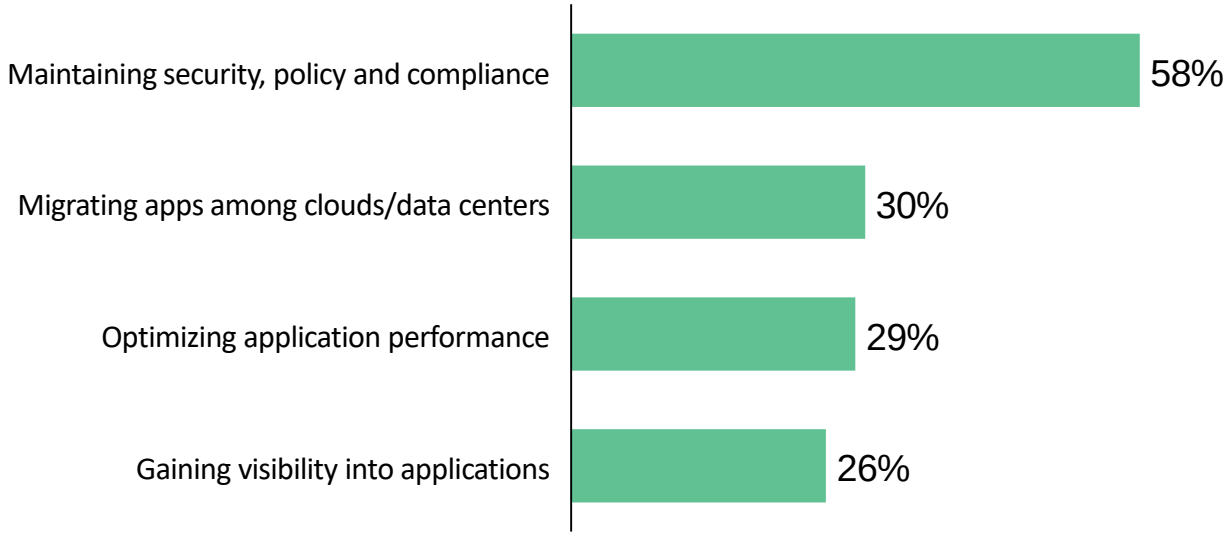
87% OF ORGANIZATIONS ARE MULTI-CLOUD, MOST STRUGGLE WITH SECURITY

Percentage reported consistency is important



Q. On a scale of 1 to 5 please rate the importance of being able to deploy and enforce the same security policies on-premises and in the cloud

Area of multi-cloud challenges

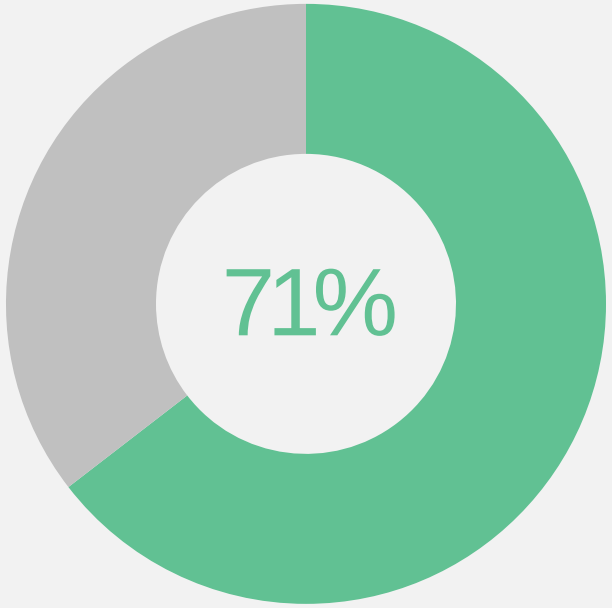


Q. As you think about managing applications in a multi-cloud environment, what part of managing the application do you find the most challenging, frustrating, or difficult? “Multi-cloud” in this case refers to multiple forms of cloud (private, public, or SaaS).

n=2583

Can Someone find anyone with Security Skills?!

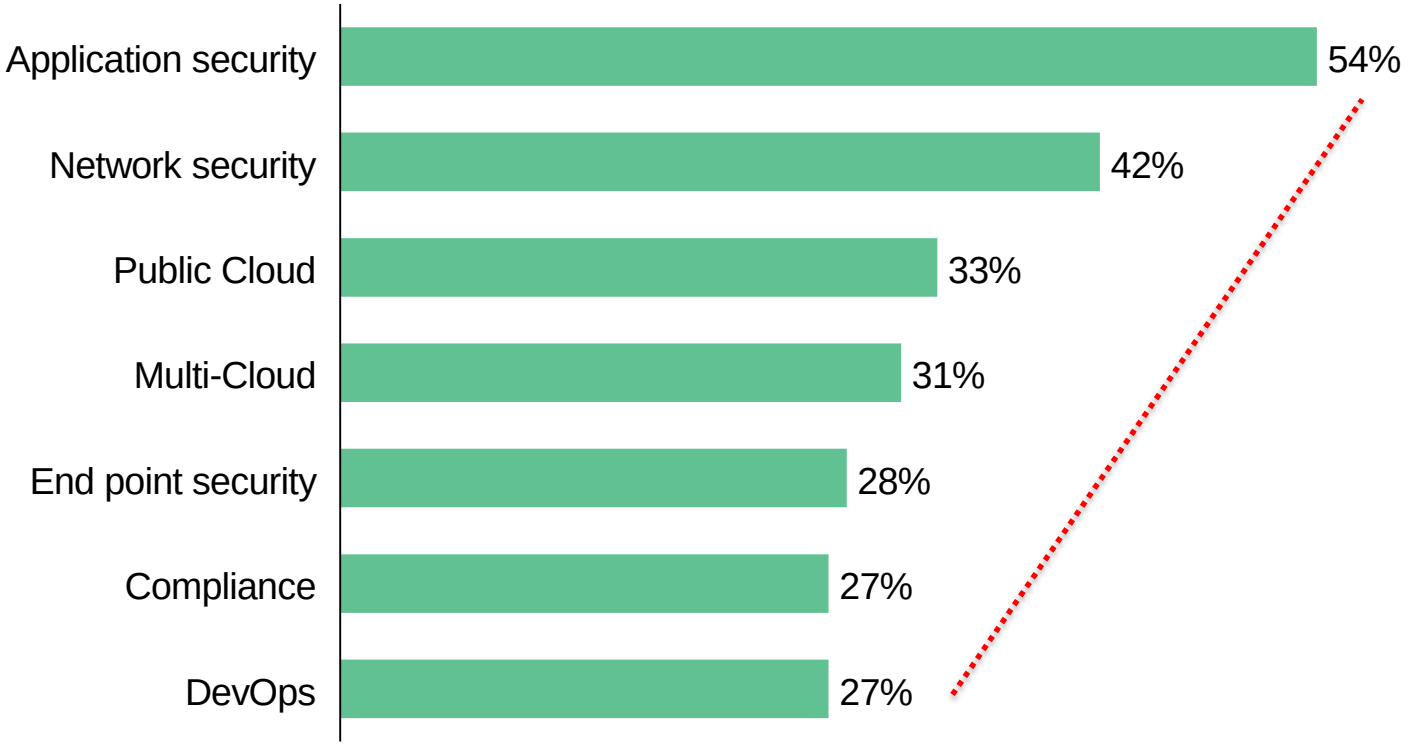
OVER HALF OF ORGANIZATIONS REPORT APPLICATION SECURITY SKILLS DEFICIT



Security skills deficit

Q. Do you have a security gap/deficit in skills in your organization?

Category of skills deficit

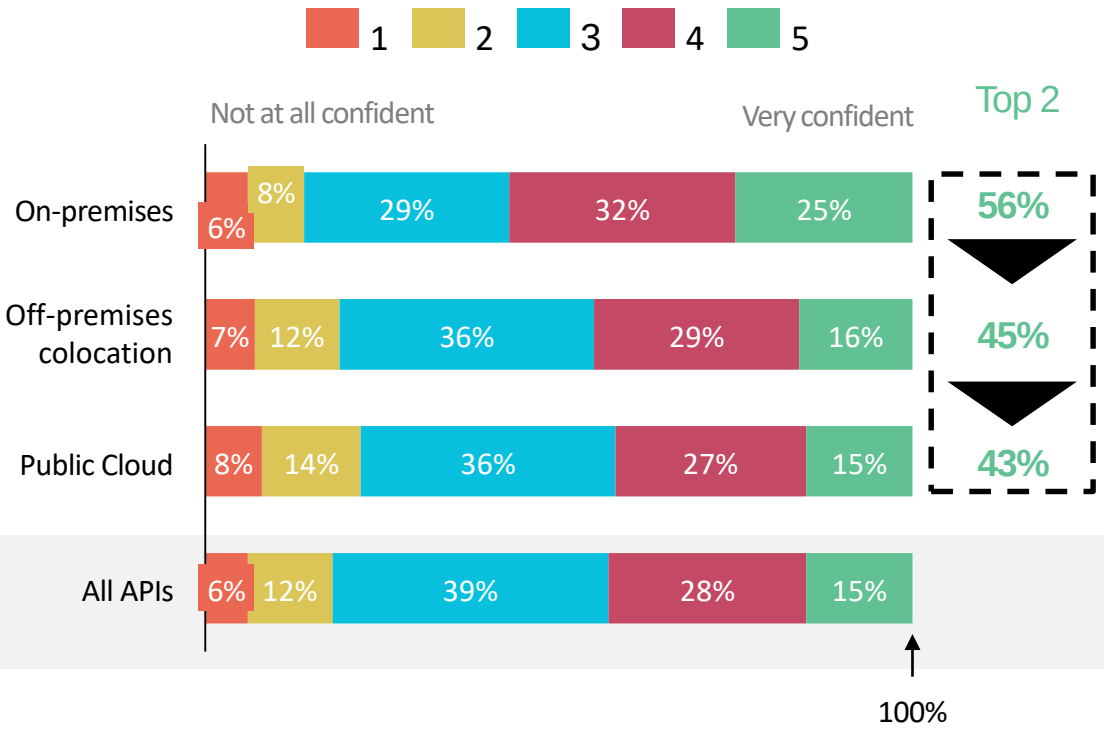


Q. Which areas do you have a security gap/deficit in skills in your organization?

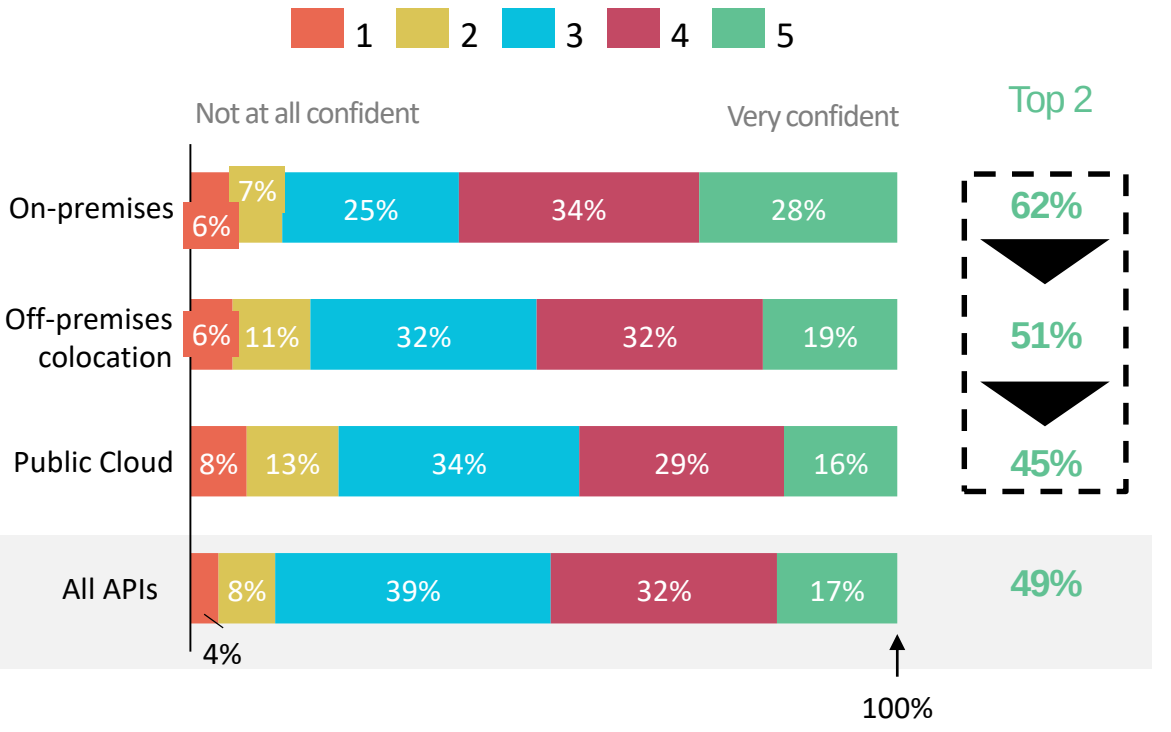
API Security Remains a Challenge

ORGANIZATIONS ARE MOST CONFIDENT IN PROTECTING APIS ON-PREMISES

Level of confidence to withstand an application-level attack against APIs



Level of confidence to withstand an application-level attack



Q. On a scale of 1-5 how confident are you in your company's ability to withstand an attack against your APIs? n=1948

Apply it: Mitigating Application Risk

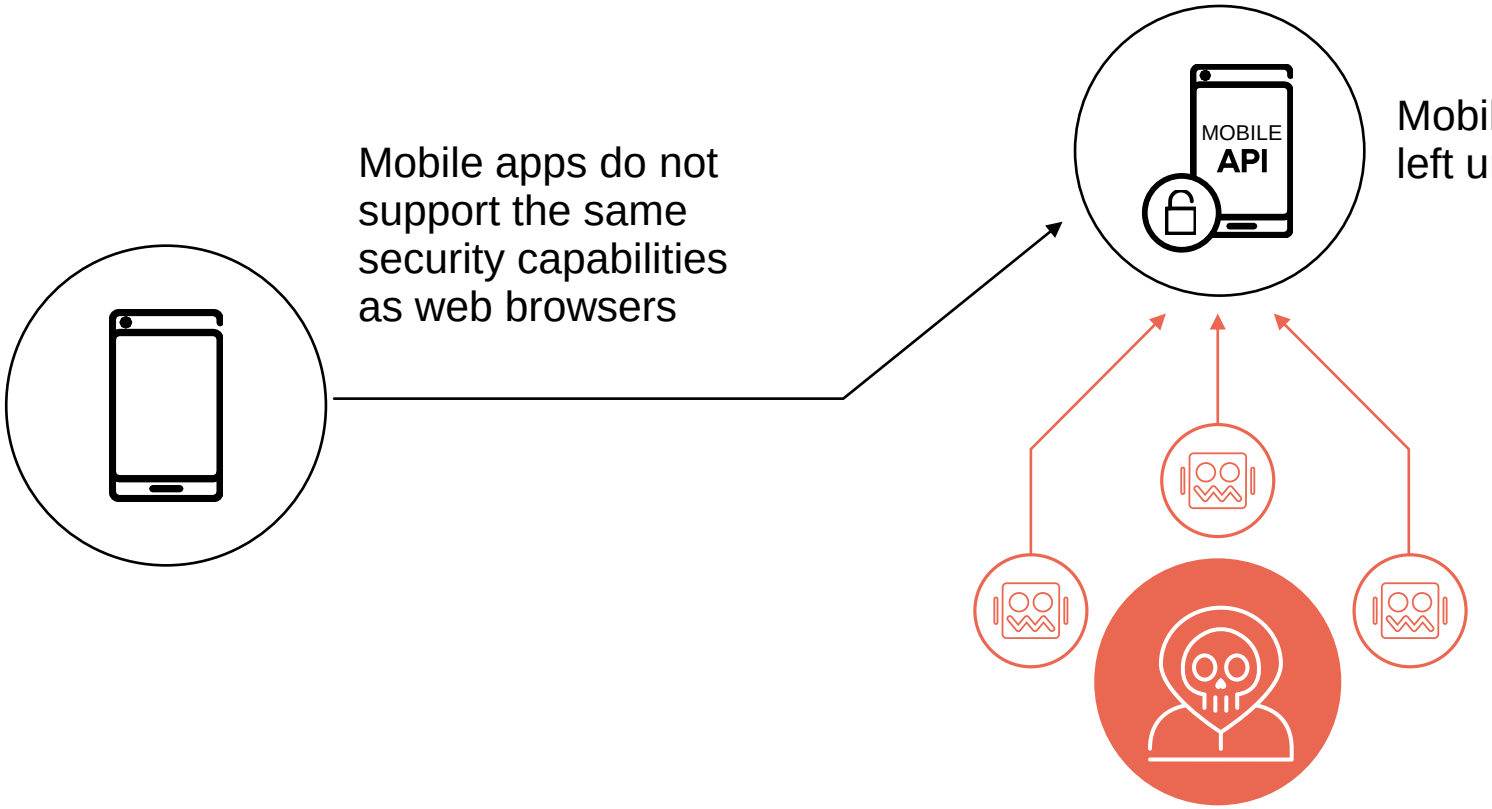
- Invest in ***program maturity***, not fancy gizmos
  - Inventory
  - Vulnerability management
  - Change control
  - Access control
  - Training
  - Monitoring and Logging
- Multifactor Authentication
- WAF/WAAP

BEGIN THIS QUARTER

BEGIN THIS WEEK

At $9.6 million per breach, breaches are cheaper to avoid.

Apply It: Protect your API / Mobile Server login



Automated attacks targeting mobile applications

- Content scraping
- Denial of serving
- API attacks

Apply It: Training Reduces Phishing Success!

33%

Phishing success **without** training.

13%

Phishing success **with** training.

F5Labs.com

Tell us what you want to read about

@F5Labs

Twitter

LinkedIn

Email Updates

RSS