FORTINET

Fortinet Security Fabric, Bezpečnosť nielen osobných údajov

ITAPA

14.11.2017

Zsolt Géczi, Fortinet, regional account manager, Slovakia

Fortinet: Global Network Security Leader

Highlights: 2000 - present

FOUNDED IN
2000
BY KEN XIE

HEADQUARTERED IN
SUNNYVALE CALIFORNIA

100+
OFFICES
ACROSS THE GLOBE

4,700+
EMPLOYEES WORLDWIDE

IN EXCESS OF
$1bn
REVENUE

$1.46bn
IN CASH

30%
GROWTH
YEAR ON YEAR

3.3m
SHIPPED SECURITY DEVICES

320K
CUSTOMERS

395
PATENTS ISSUED

316 IN PROCESS

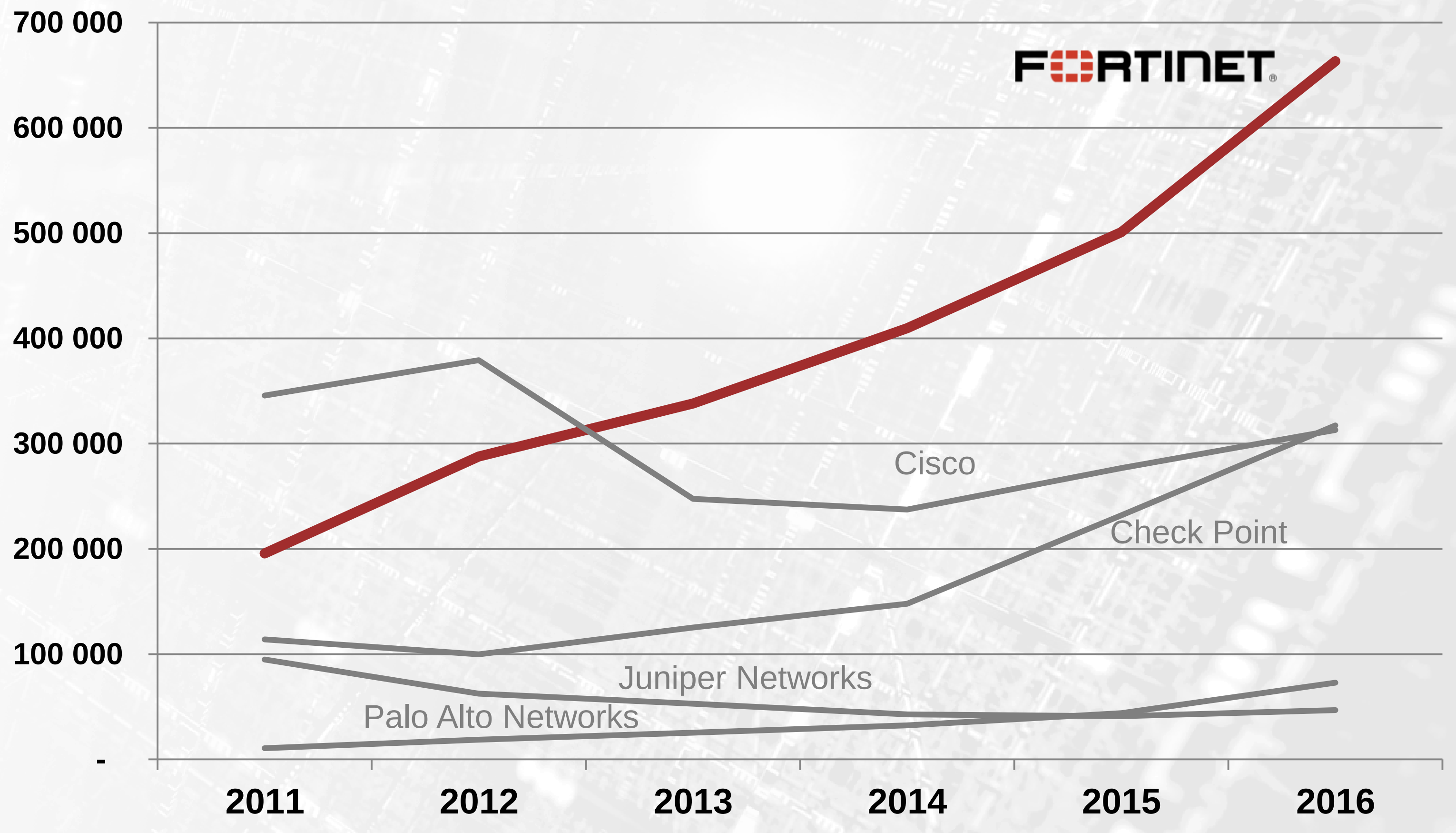
PATENTED

Fortinet: Gaining Share in a Growing Market

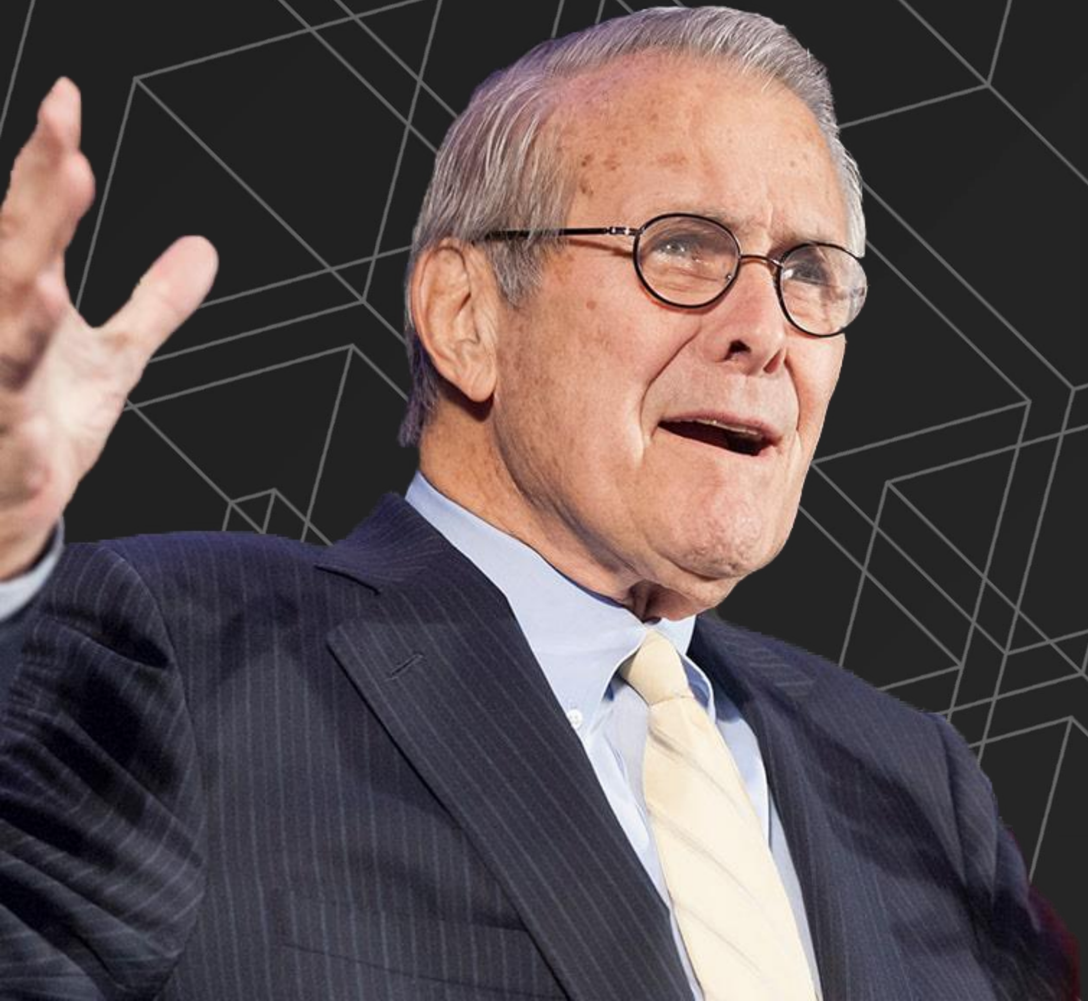
Fortinet vs the Competition

Solving a broad range of challenges…

- Fortinet is the largest network security appliance vendor in the world
- Fortinet has developed a visionary suite of security solutions



Source: IDC Worldwide Security Applicances Tracker, March 2016 (based on annual unit shipments)



“WE DON’T KNOW WHAT WE DON’T KNOW.”

Donald Rumsfeld

Former US Secretary of Defense

PREPARING FOR GDPR*

12 Steps To Take Now

1

Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2

Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3

Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5

Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6

Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7

Consent

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

8

Children

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

9

Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10

Data Protection by Design and Data Protection Impact Assessments

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

11

Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12

International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

*ico.org.uk

PREPARING FOR GDPR*

12 Steps To Take Now

1

Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2

Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3

Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5

Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6

Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7

Consent

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

8

Children

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

9

Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10

Data Protection by Design and Data Protection Impact Assessments

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

11

Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12

International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

*ico.org.uk

What Are We Talking About

Data Protection *vs.* Cyber Security

Data Protection…

…is the process of protecting data and involves the relationship between the collection and dissemination of data…It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes.

Cyber Security…

…is the body of technologies, processes and practices designed to **protect** networks, computers, programs and **data from attack, damage or unauthorized access.**

Two Key Aspects of GDPR

1. Consequences for GDPR violations

- Empowers supervisory authorities to assess fines that are "effective, proportionate and dissuasive."
- Two tiers of maximum fines depending upon severity of violation
  - »**2% or €10M, whichever is higher**
  - »**4% or €20M, whichever is higher**
- Allows data subjects to seek monetary damages in court from controllers who violate their rights and from processors as well.

Two Key Aspects of GDPR

2. Data Breach notifications

- A personal data breach" is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
- Data controllers must notify the supervisory authority "competent under Article 55"
- Notice must be provided "without undue delay and, where feasible, **not later than 72 hours** after having become aware of it."

- Notification to the authority must consist of at least:
  - » Describe the nature of the personal data breach, including the number and categories of data subjects and personal data records affected;
  - » Provide the data protection officer's contact information;
  - » Describe the likely consequences of the personal data breach
  - » Describe how the controller proposes to address the breach, including any mitigation efforts
  - » If data processor experiences a [illegible] it must notify the controller
- Notice **is not** required if "the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons,"

LET'S PLAY
"WHAT IF"…

Tesco Bank (UK) Data Breach

The Numbers

EARLY
NOVEMBER
2016

£25M
STOLEN FROM
9,000
ACCOUNTS

4
POSSIBLE
EXPLANATIONS

- INSIDER THREAT
- MOBILE APP
- INSUFFICIENT INTERNAL PROCESSES
- REACHED THROUGH 3RD PARTIES

What We Could Expect in the Future…

TESCO COULD FACE FINES OF UP TO "£1.9B" IF GDPR HAD BEEN IN EFFECT AT THE TIME*

*computing.co.uk Nov 2016

Looking to the Future - What GDPR Requires

🔒 DATA BREACH DETECTED!

⚠ DATA BREACH REPORTED!

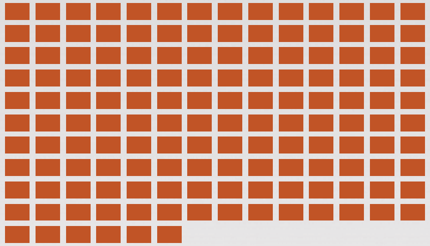
JANUARY 2019

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
			1	2	3	4
5	6	7	8	9	10	11
12	13 🔒	14	15	16 ⚠	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

What Your Network Requires

INITIAL INTRUSION!

Average time between intrusion and detection =



146 DAYS*

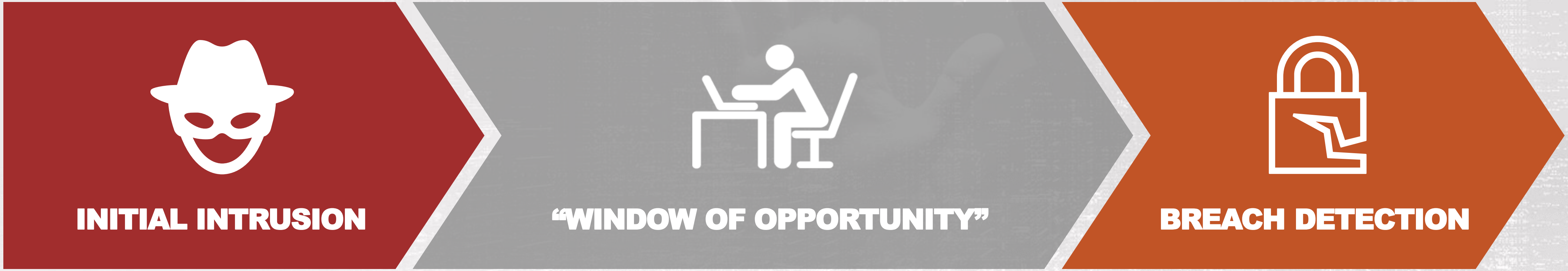
AUGUST 2018

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

* M-Trends 2016

The Hacker's Advantage:

Window of Opportunity



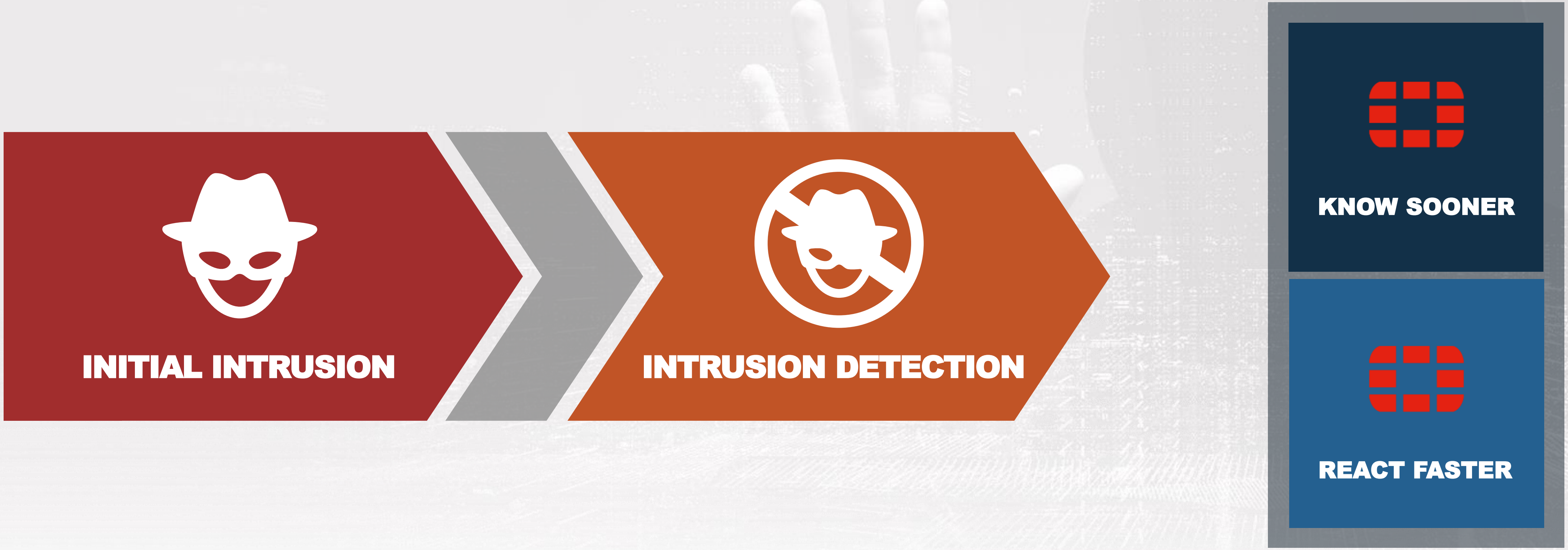
INITIAL INTRUSION

"WINDOW OF OPPORTUNITY"

BREACH DETECTION

The Fortinet Objective:

Close the Window of Opportunity



INITIAL INTRUSION

INTRUSION DETECTION

KNOW SOONER

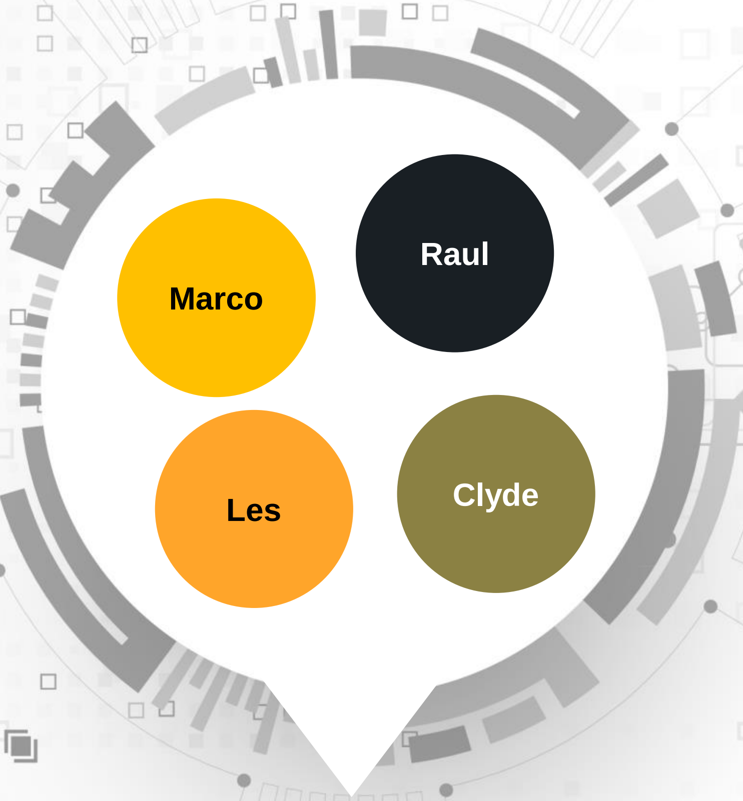
REACT FASTER

THE ROAD TO GDPR COMPLIANCE

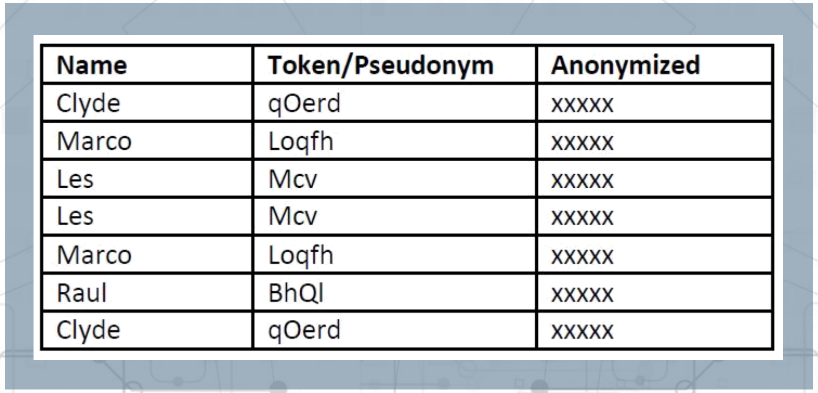
KONTINUÁLNE POSÚDENIE RIZÍK

PSEUDONYMIZÁCIA A SEGMENTÁCIA

Pseudonymizácia vs. Anonymizácia



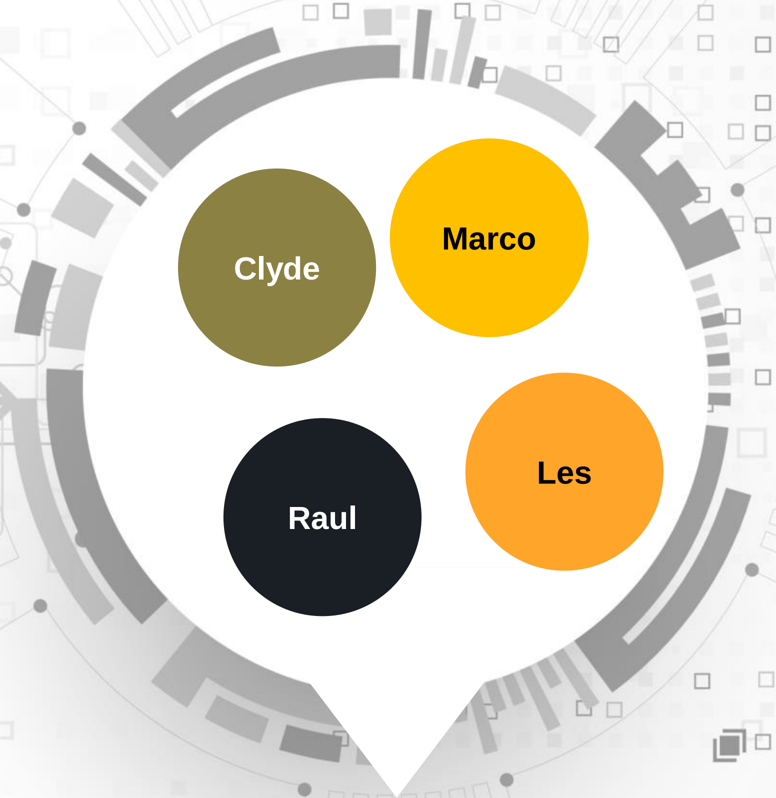
Pseudonymized Data Record



Name	Token/Pseudonym	Anonymized
Clyde	qOerd	xxxxx
Marco	Loqfh	xxxxx
Les	Mcv	xxxxx
Les	Mcv	xxxxx
Marco	Loqfh	xxxxx
Raul	BhQI	xxxxx
Clyde	qOerd	xxxxx

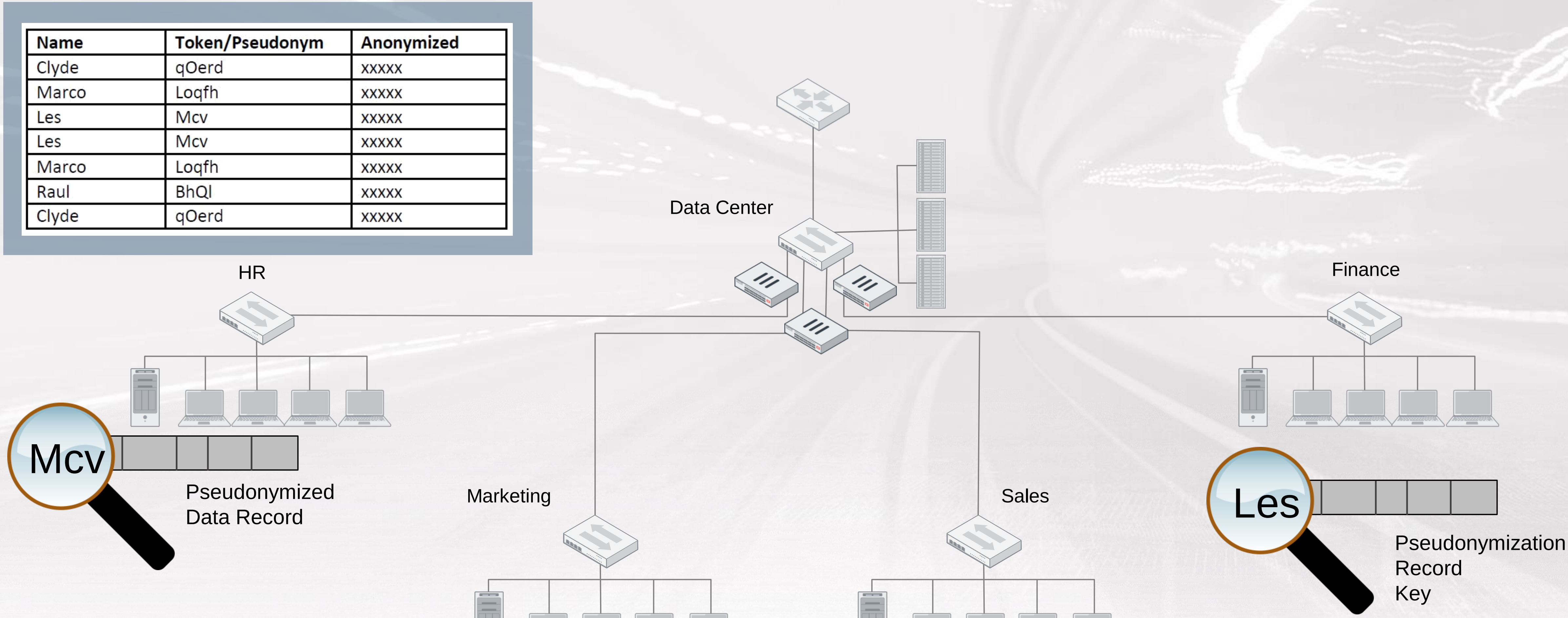
“Pseudonymizácia je metóda nahrádzania identifikovateľných údajov s reverzibilnou, konzistentnou hodnotou.

Anonymizácia je zničenie identifikovateľných údajov.”



Anonymized Data Record

Segmentácia pre zvýšenú ochranu údajov



Name	Token/Pseudonym	Anonymized
Clyde	qOerd	xxxxx
Marco	Loqfh	xxxxx
Les	Mcv	xxxxx
Les	Mcv	xxxxx
Marco	Loqfh	xxxxx
Raul	BhQl	xxxxx
Clyde	qOerd	xxxxx

Pseudonymized Data Record

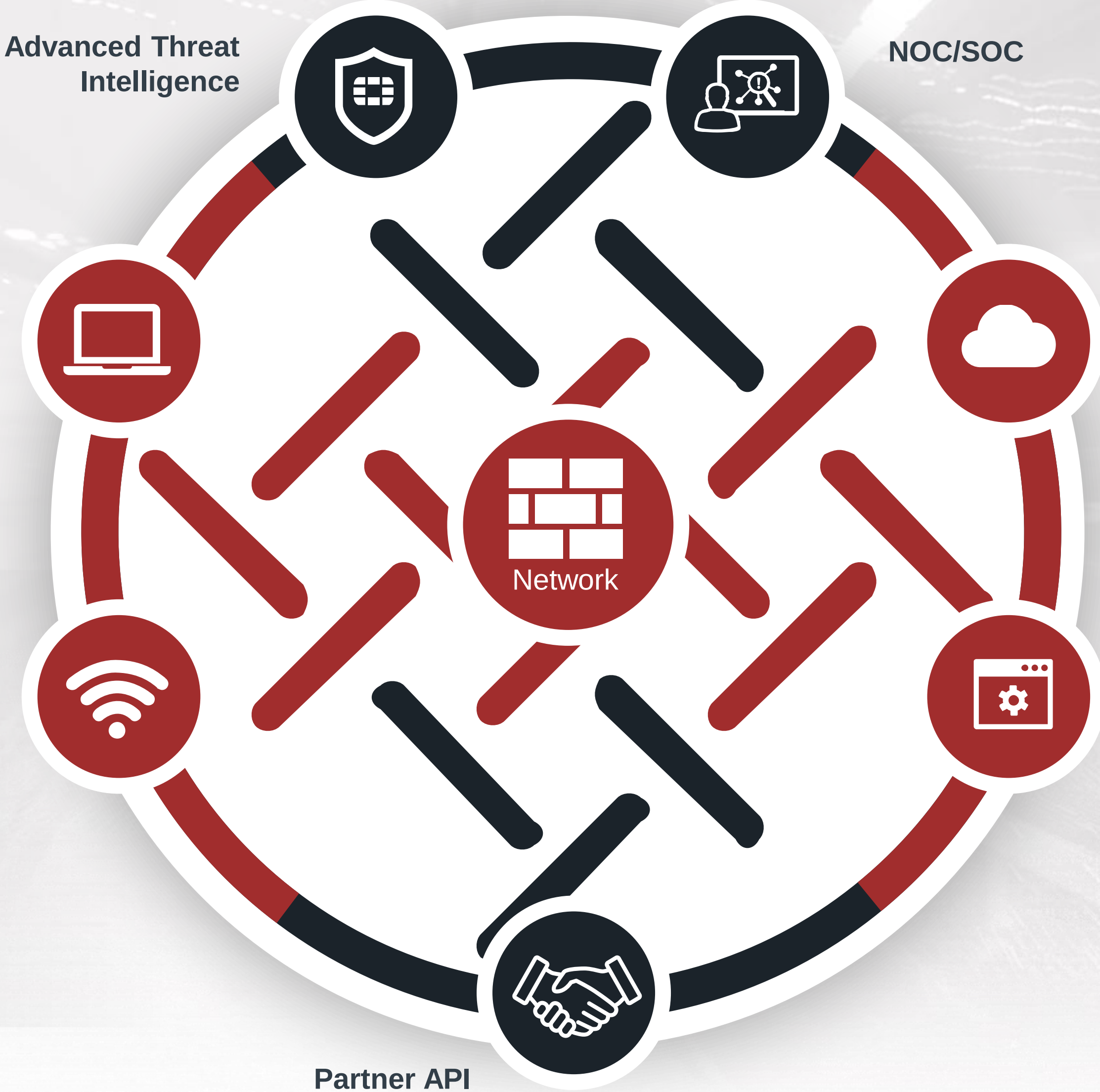
Pseudonymization Record Key

The First Step…

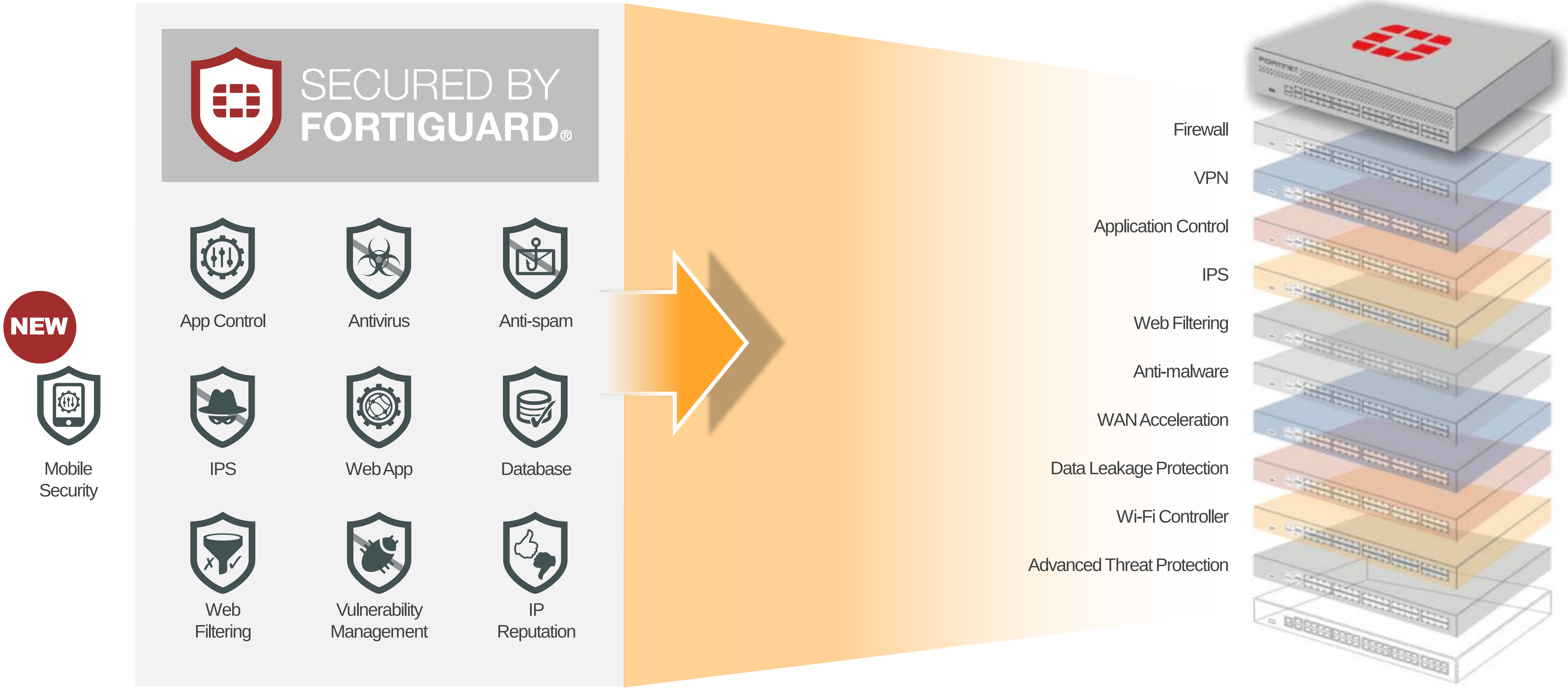
…towards GDPR Compliance

FORTINET SECURITY FABRIC

- **BROAD**
- **POWERFUL**
- **AUTOMATED**



Security Services and Technologies



SECURED BY FORTIGUARD®

NEW

Mobile Security

App Control

Antivirus

Anti-spam

IPS

Web App

Database

Web Filtering

Vulnerability Management

IP Reputation

Firewall

VPN

Application Control

IPS

Web Filtering

Anti-malware

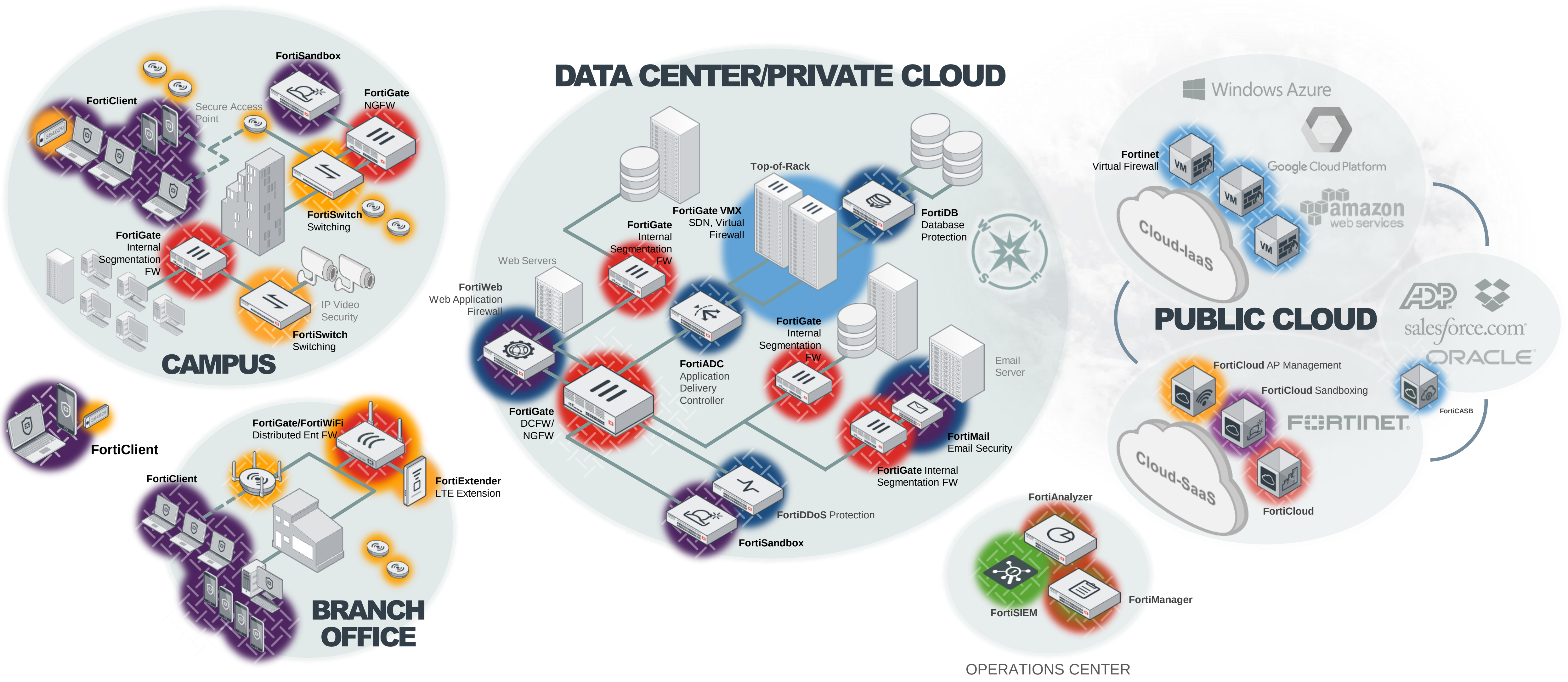
WAN Acceleration

Data Leakage Protection

Wi-Fi Controller

Advanced Threat Protection

The Fortinet Security Fabric Realized



Comprehensive Security Solutions

ENTERPRISE FIREWALL

FortiGate
- Next-Generation FW
- Data Center FW
- Internal Segmentation FW
- Secure SD-WAN
FortiManager
FortiAnalyzer
FortiGuard Services

CLOUD SECURITY

FortiGate VM (Virtual FW)
FortiGate VMX (SDN Virtual FW)
FortiGate VM for Public Cloud
- AWS
- Microsoft Azure
- Googe Cloud
- OpenStack-based
FortiHypervisor
FortiCASB
FortiGuard Services

ADVANCED THREAT PROTECTION

FortiSandbox
FortiMail
FortiWeb
FortiClient
FortiCloud Sandboxing
FortiGuard Services

APPLICATION SECURITY

FortiWeb
FortiADC
FortiDDoS
FortiWAN
FortiCache
FortiGuard Services

SECURE ACCESS

FortiAP
FortiGate AP Management
FortiCloud AP Management
FortiWLC/WLM AP Management
FortiSwitch
FortiAuthenticator
FortiToken
FortiExtender
FortiGuard Services

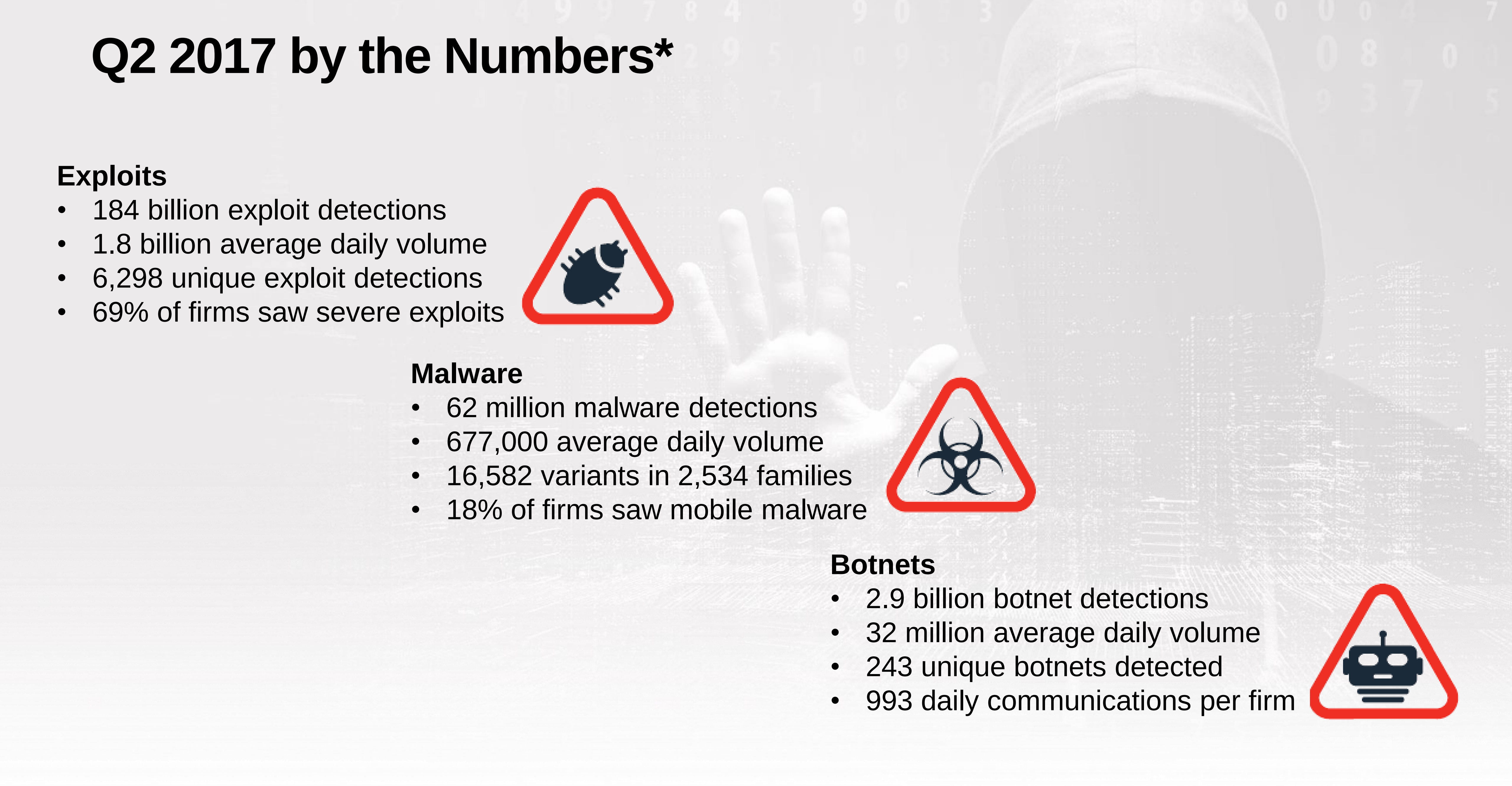
SECURITY OPERATIONS

FortiSIEM
FortiManager
FortiAnalyzer
FortiGuard Services
- Indicators of Compromise

FortiGuard

Since 2000, FortiGuard Labs has provided in-house, industry-leading security intelligence and research, powering the Fortinet Security Fabric and delivering a suite of advanced security services

Q2 2017 by the Numbers*



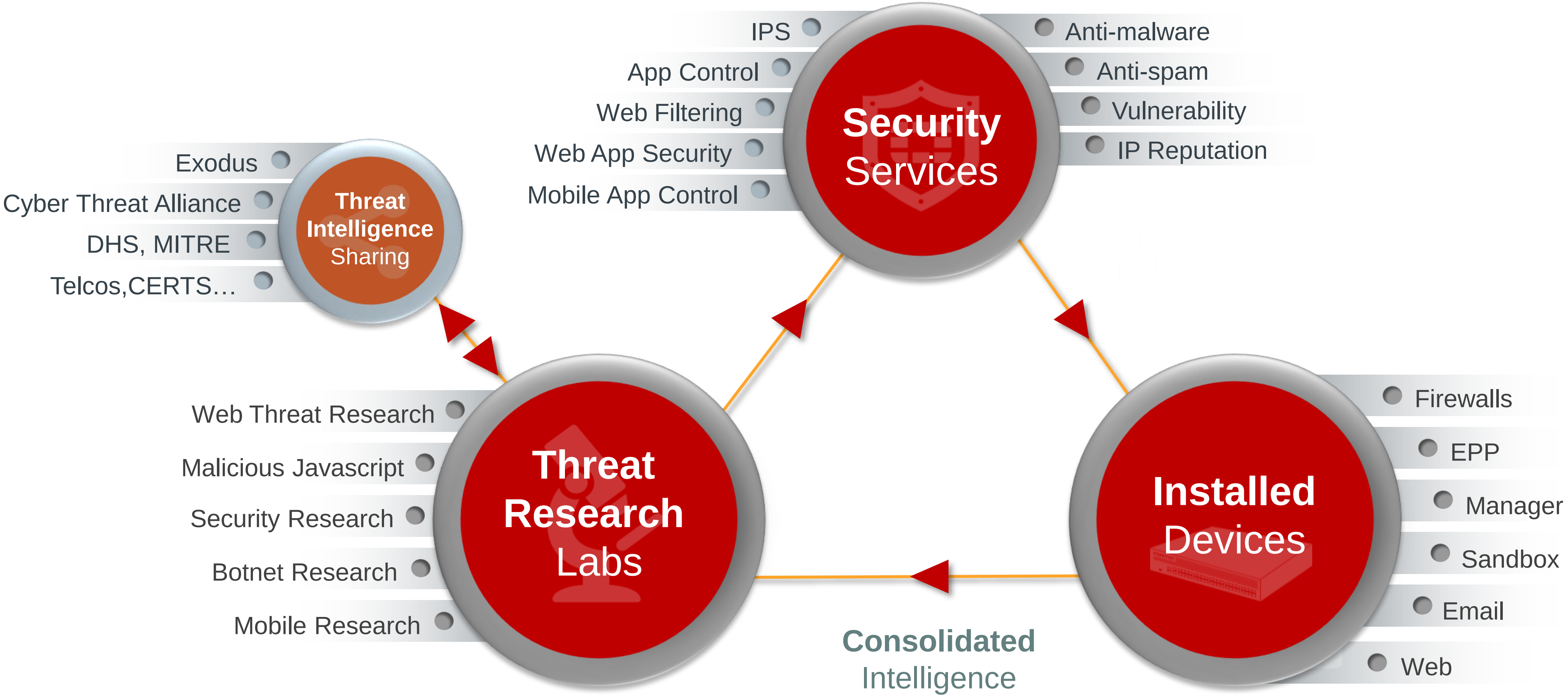
Exploits
- 184 billion exploit detections
- 1.8 billion average daily volume
- 6,298 unique exploit detections
- 69% of firms saw severe exploits

Malware
- 62 million malware detections
- 677,000 average daily volume
- 16,582 variants in 2,534 families
- 18% of firms saw mobile malware

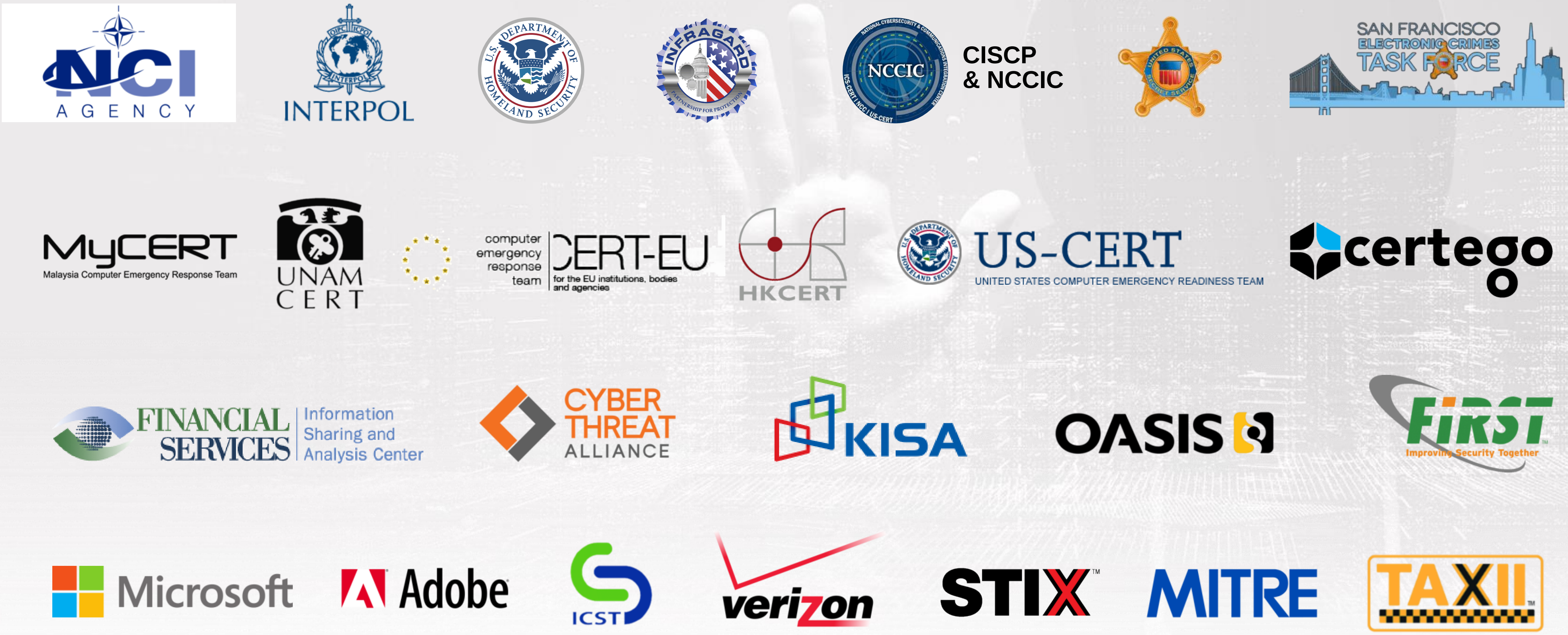
Botnets
- 2.9 billion botnet detections
- 32 million average daily volume
- 243 unique botnets detected
- 993 daily communications per firm

*FortiGuard Q2 2017 Threat Landscape Report

An Integrated Threat Intelligence Ecosystem



FortiGuard Threat Intelligence Projects


NCI AGENCY
INTERPOL
U.S. DEPARTMENT OF HOMELAND SECURITY
INFRAGARD PARTNERSHIP FOR PROTECTION
NCCIC
CISCP & NCCIC
UNITED STATES SECRET SERVICE
SAN FRANCISCO ELECTRONIC CRIMES TASK FORCE
MyCERT Malaysia Computer Emergency Response Team
UNAM CERT
computer emergency response team CERT-EU for the EU institutions, bodies and agencies
HKCERT
US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM
certego
FINANCIAL SERVICES Information Sharing and Analysis Center
CYBER THREAT ALLIANCE
KISA
OASIS
FIRST Improving Security Together
Microsoft
Adobe
ICST
verizon
STIX
MITRE
TAXII

The Road to GDPR Compliance

So Much More Than Just Technology

Complex

Potentially long, complicated and expensive

Impact

Potential impact across the whole of the organization

Product/Service
Process
People

Threat

Think ahead of the Threat – Close the “Window of Opportunity”

“Harden” the Network

Ďakujeme za pozornosť!

FORTINET®