The General Data Protection Regulation… Reconciling Regulations with Technology

Leonidas Tougiannidis, Country Manager, Greece & Cyprus

PARTNERSYNC

IT Trends increase the ATTACK SURFACE & LIABILITIES

- Digital Transformation entails sharing data
- IoT brings Trillion new Devices Online
- Cloud breaks the Borders
- Mobility Disperses Users and Data
- SD-WAN stretchers enterprise networks
- Regulations (ie GDPR)

“WE DON’T KNOW WHAT WE DON’T KNOW.”

DONALD RUMSFELD
FORMER US SECRETARY OF DEFENSE

FORTINET

Chronology

c1995

Data Protection Directive 95/46/EC

- EU directive, individual national laws

2016

General Data Protection Regulation (EU) 2016/679)

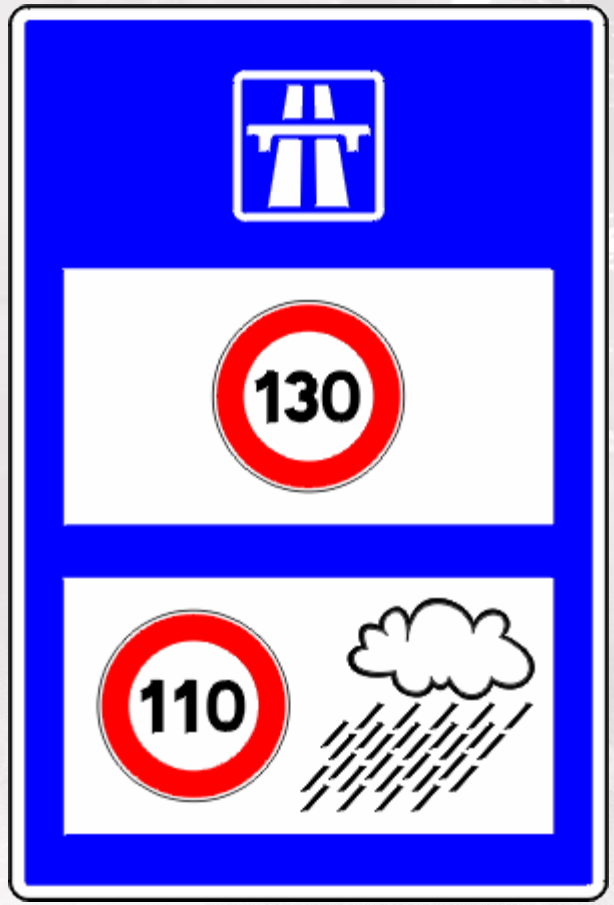
- Adopted 27 April 2016
- 28 countries, 1 law
- 200 pages, 99 Articles, 173 recitals..

2018

Effective 25 May 2018

- What a weekend that's going to be…

Understanding the Basis of GDPR - Compare



Understanding the Basis of GDPR - Contrast

WHY GDPR IS NEEDED AND OTHER HORROR STORIES

FORTINET

Reason #1

Changing Business Models

Google

Google allegedly involved in exposing user data to Cambridge Analytica

YouTube should be fined billions for illegally collecting children's data, privacy groups claim

- In a complaint filed to the Federal Trade Commission (FTC) on Monday, a coalition of more than 20 advocacy, consumer and privacy groups claim that Google's video platform is violating U.S. child protection laws by collecting personal data on users aged less than 13 years old.
- The claim comes hot on the heels of the data scandal that has hit Facebook in recent weeks, as the tech behemoth looks to tackle allegations it improperly shared information with London-based elections consultancy firm Cambridge Analytica.
- Google said that while it had not received the complaint, "protecting kids and families has always been a top priority."

facebook

Up to 87 million Facebook users had their data exposed to Cambridge Analytica

Reason #2

Connected Society

Reason #3

Disregard for Data Protection

Reason #4

Lack of Effective Deterrent

5M CHILDREN'S RECORDS COMPROMISED
FINE = $650,000

SONY

UP TO 100M USERS PRIVATE DATA LOST
(PLAYSTATION NETWORK BREACH)
FINE = £250,000 ($300,000)

Carphone Warehouse

UP TO 3M USERS PRIVATE DATA LOST
FINE = £400,000 ($480,000)

LET'S PLAY "WHAT IF"...

FORTINET

What Can Happen…

Tesco Bank (UK) Data Breach

EARLY NOVEMBER 2016

£25M STOLEN FROM 9,000 ACCOUNTS

4 POSSIBLE EXPLANATIONS

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

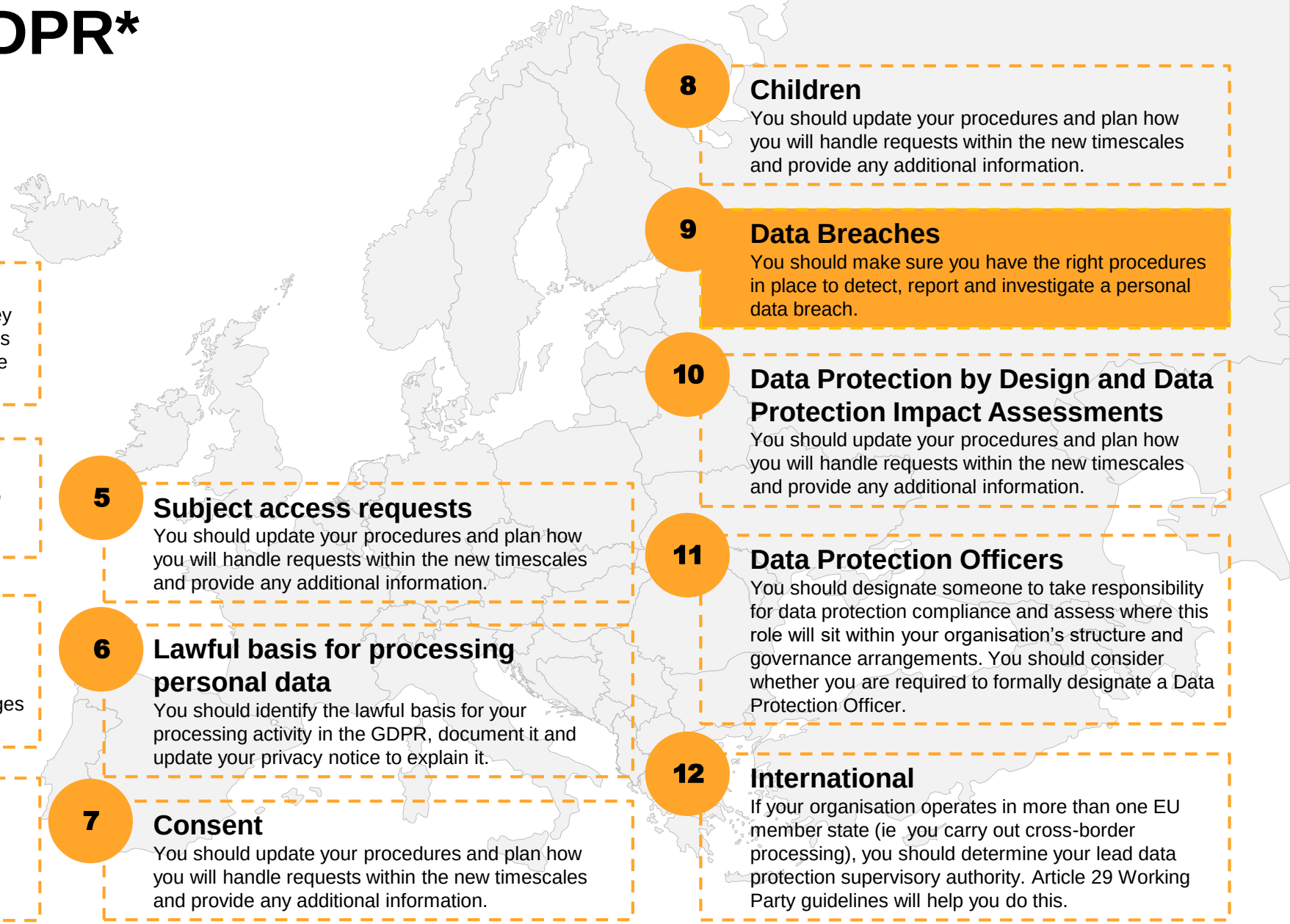
What We Could Expect in the Future…

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

WHAT DO I NEED TO KNOW

FORTINET

Preparing for GDPR*



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

Key Aspects of GDPR

1. 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 personal data breach, 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,"

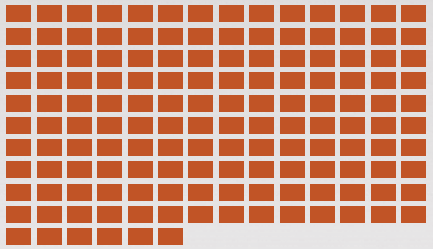
Looking to the Future - What GDPR Requires

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

Average time between intrusion and detection =



146 DAYS*

The Hacker's Advantage:

Window of Opportunity

The Fortinet Objective:

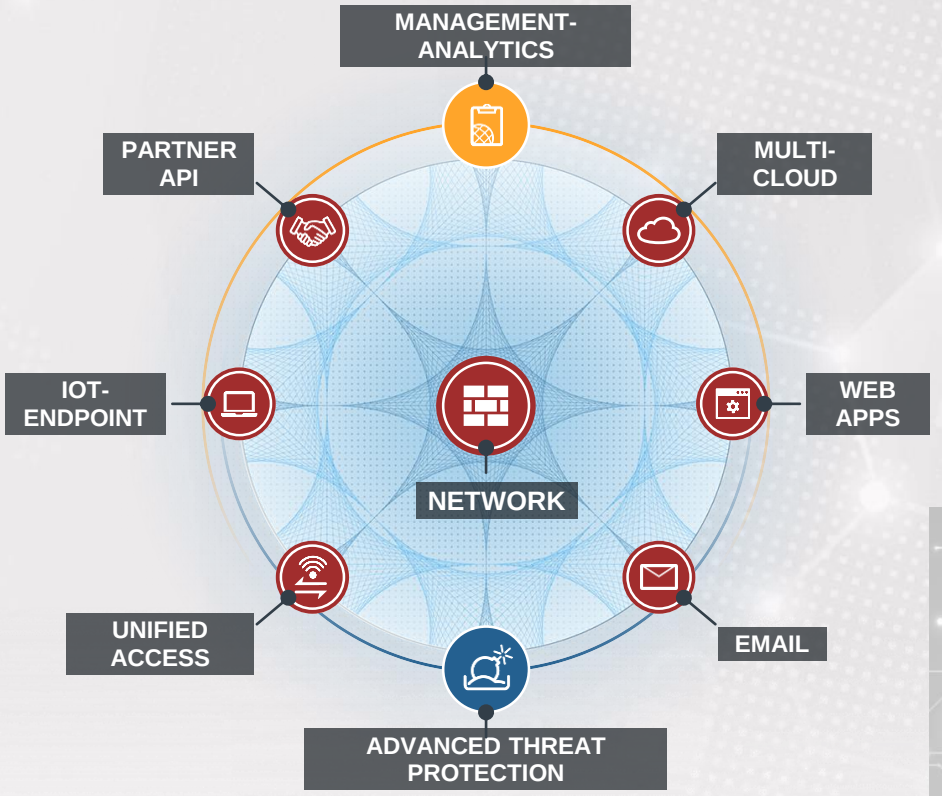
Close the Window of Opportunity

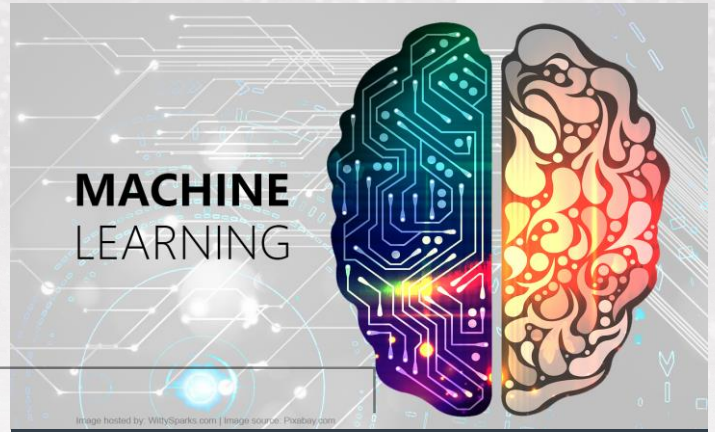
- **KNOW SOONER**
- **REACT FASTER**

FORTINET AND GDPR. WHERE, WHAT, WHY AND HOW.

FORTINET

The Fortinet Security Fabric





A Security Architecture that is:

BROAD

Provides Visibility and Protection Across the Entire Digital Attack Surface

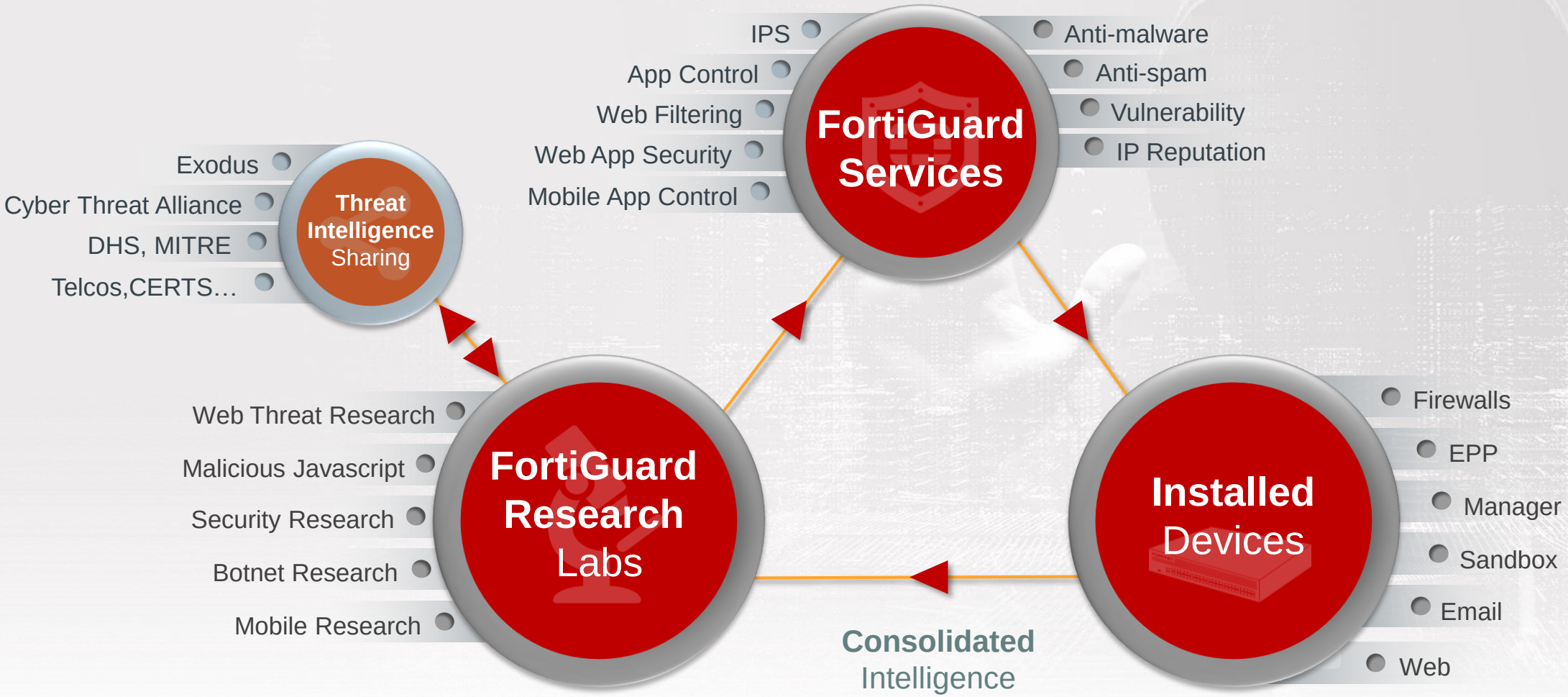
INTEGRATED

Multiple Technologies Working Together for the Detection of Advanced Threats

AUTOMATED

Embedded Intelligence for Automatic Response & Continuous Trust Assessment

FortiGuard - An Integrated Threat Intelligence Ecosystem



Global Network Security Leader in Market Recognition

Gartner

LEADER

MAGIC QUADRANT

ENTERPRISE NETWORK

FIREWALLS UTM SMB

IDC ANALYZE THE FUTURE

#1

MARKETSHARE

OVER 700.000 APPLIANCES DEPLOYED

ALMOST DOUBLE THE NEXT COMPETITOR

350.000

CUSTOMERS WOLDWIDE

NSS LABS

MOST

RECOMMENTED PASSES

BEST

THROUGHPUT/TCO

HIGHEST

BLOCK RATE

99.47%

Gartner peerinsights

nielsen

Tech Data

ICSA labs CERTIFIED FIREWALL - CORPORATE

Gartner peerinsights customers' choice 2018 ™

The Road to GDPR Compliance

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

www.fortinet.com/GDPR