© Fortinet Inc. All Rights Reserved.

Vielfältige Angriffsvektoren benötigen interagierende und automatisierte Lösungen

Jens Spielberg

Agenda

- Warum Security?!
- Zahlen, Daten, Fakten
- Heutige Herausforderungen
- Interagierende und automatisierte Lösungen

FORTINET

Warum Security?!

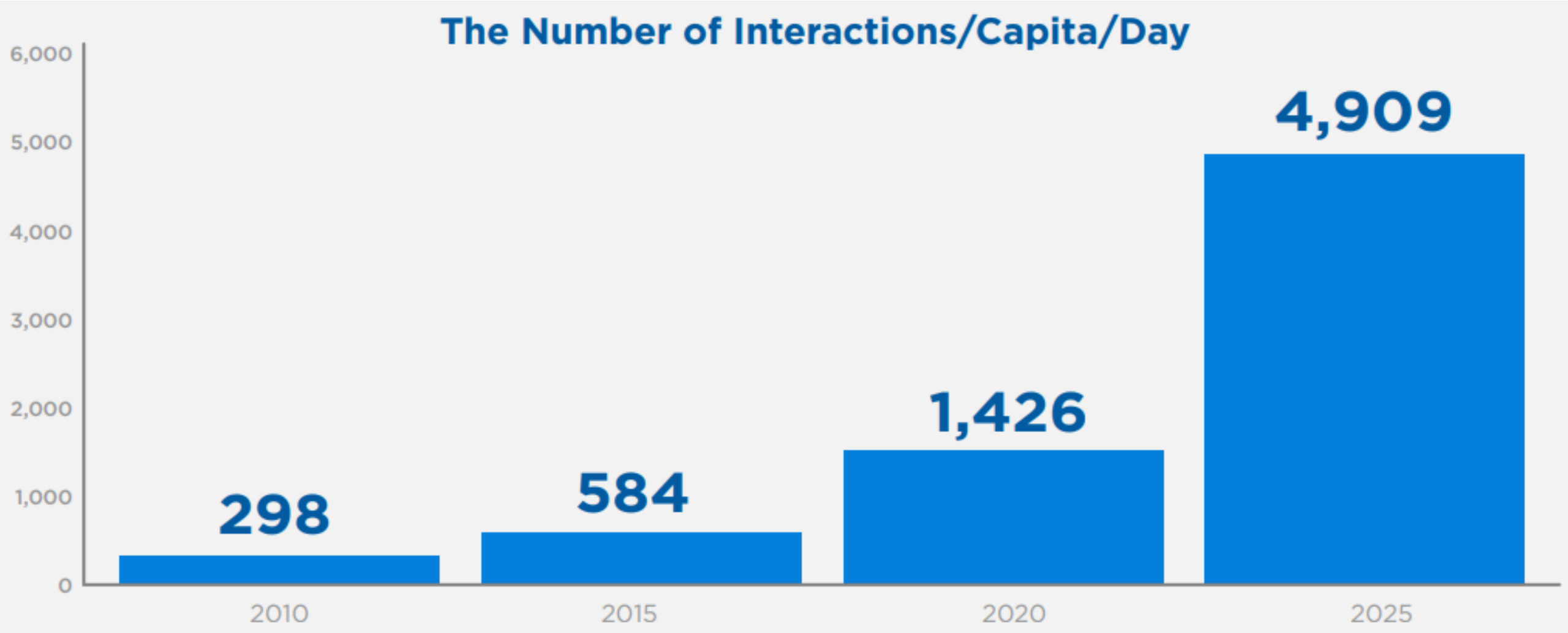
Warum Security?!

„Es gibt solche Unternehmen, die schon gehackt wurden, und solche, die es noch werden.“

https://taz.de/FBI-haelt-Cyber-Kriminalitaet-fuer-groesste-Gefahr/!5099329/

© Fortinet Inc. All Rights Reserved.

The Digitization of the world



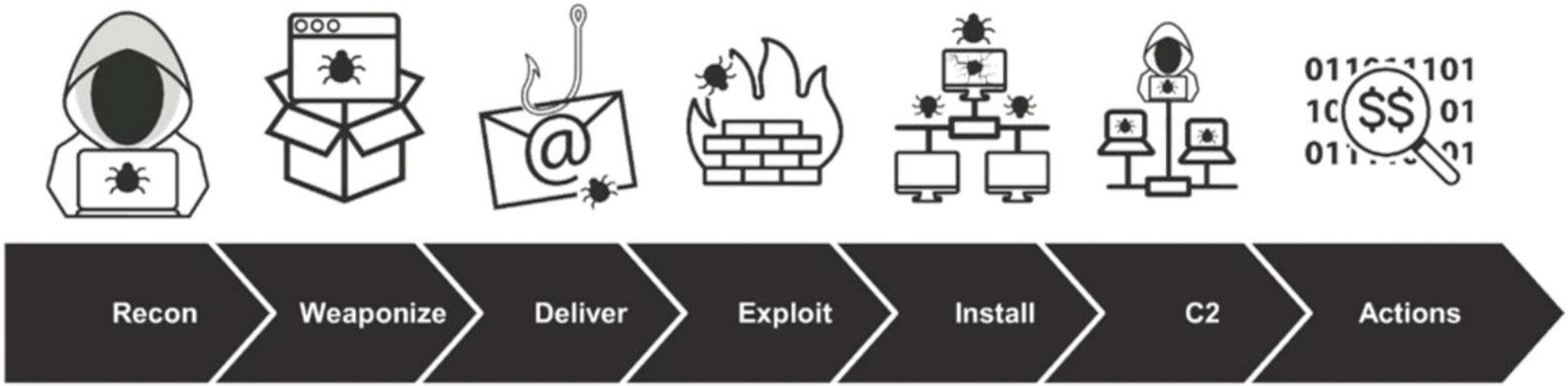
Quelle: IDC Whitepaper 2018

FORTINET

© Fortinet Inc. All Rights Reserved.

Zahlen, Daten, Fakten

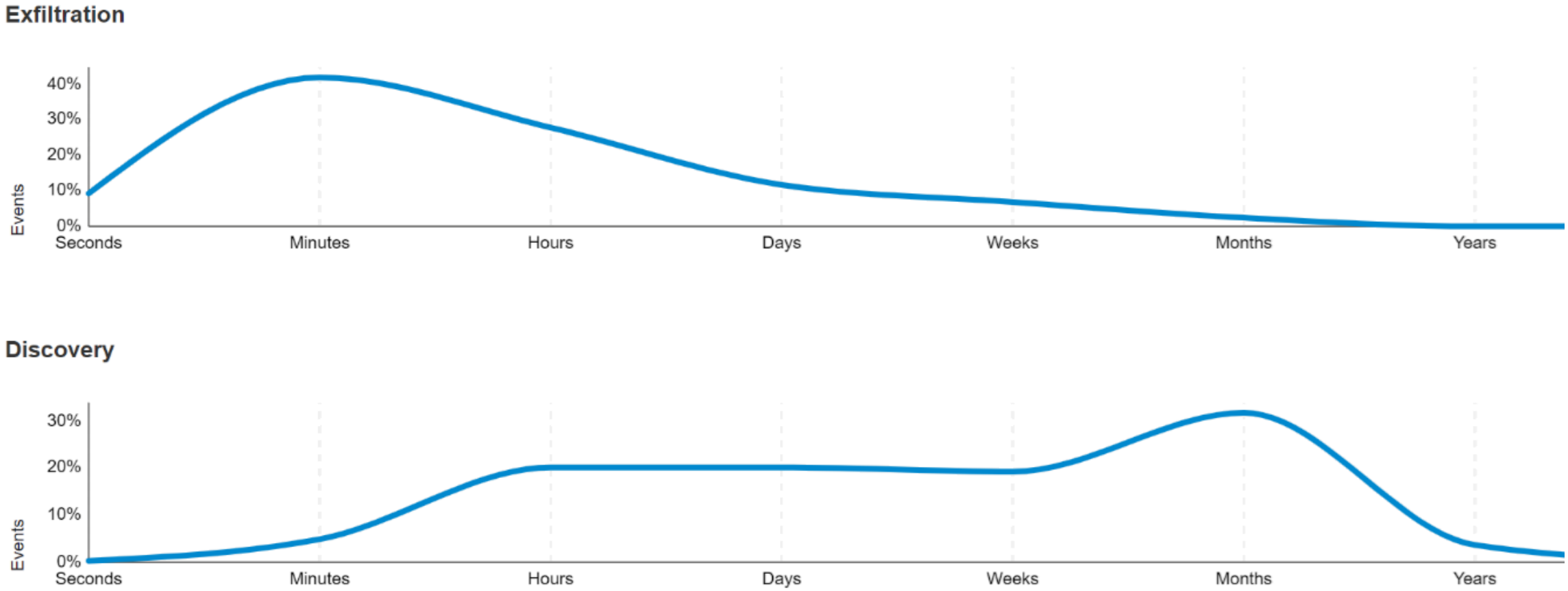
Phasen eines Angriffs



Quelle: https://www.techtag.de/it-und-hightech/it-security/cyber-kill-chain-it-infrastruktur/

© Fortinet Inc. All Rights Reserved.

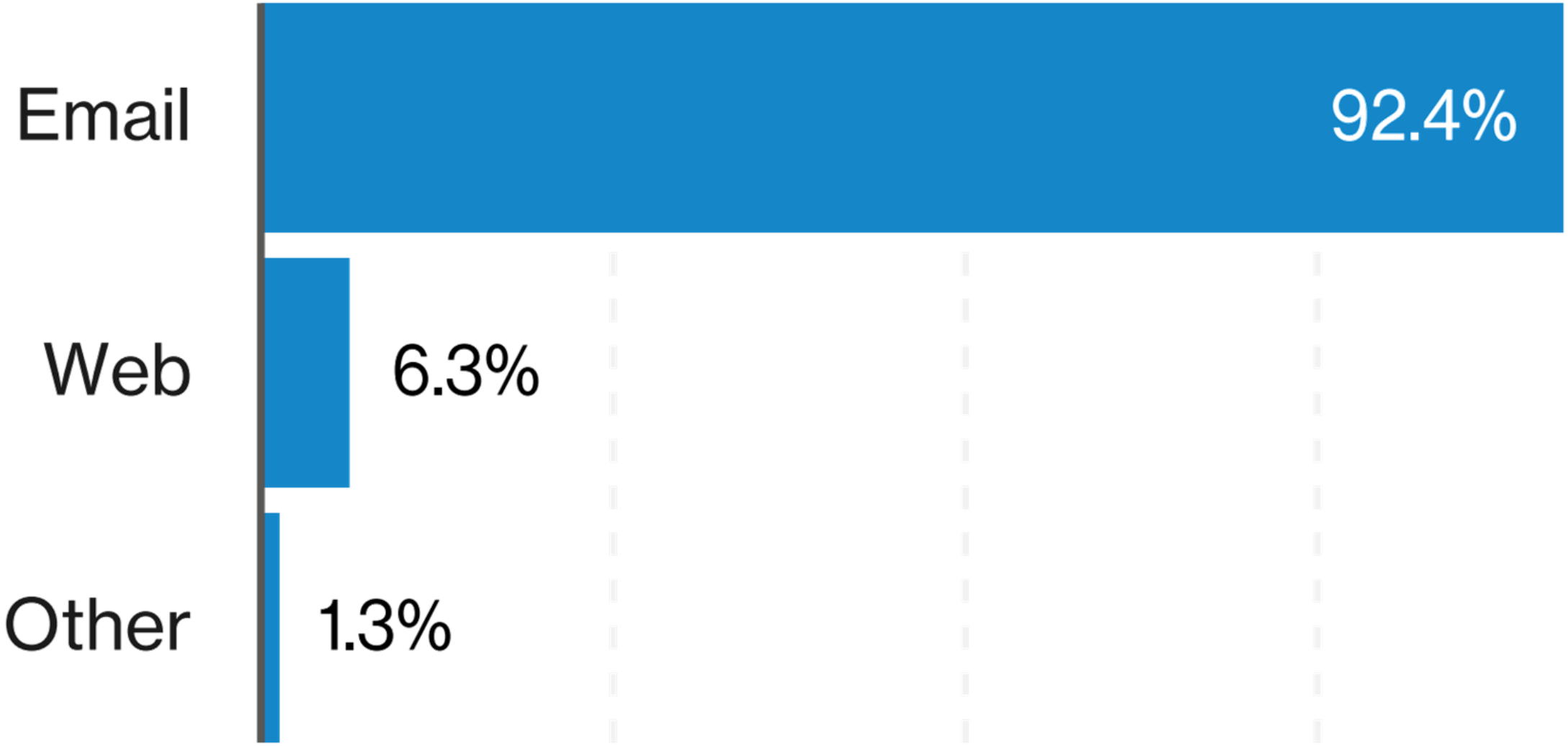
Wann werden Angriffe entdeckt?



Quelle: Verizon Data Breach Investigation Report 2018

© Fortinet Inc. All Rights Reserved.

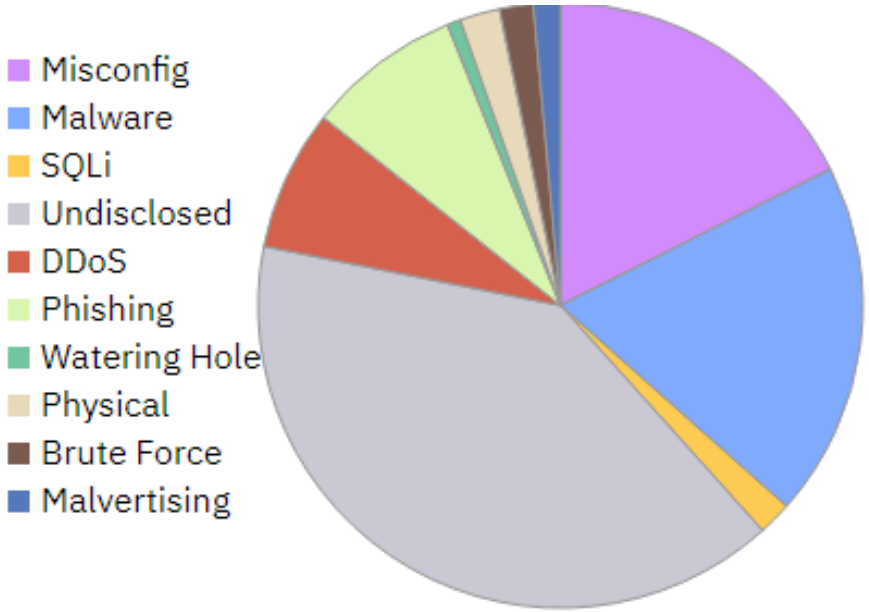
Infektionswege

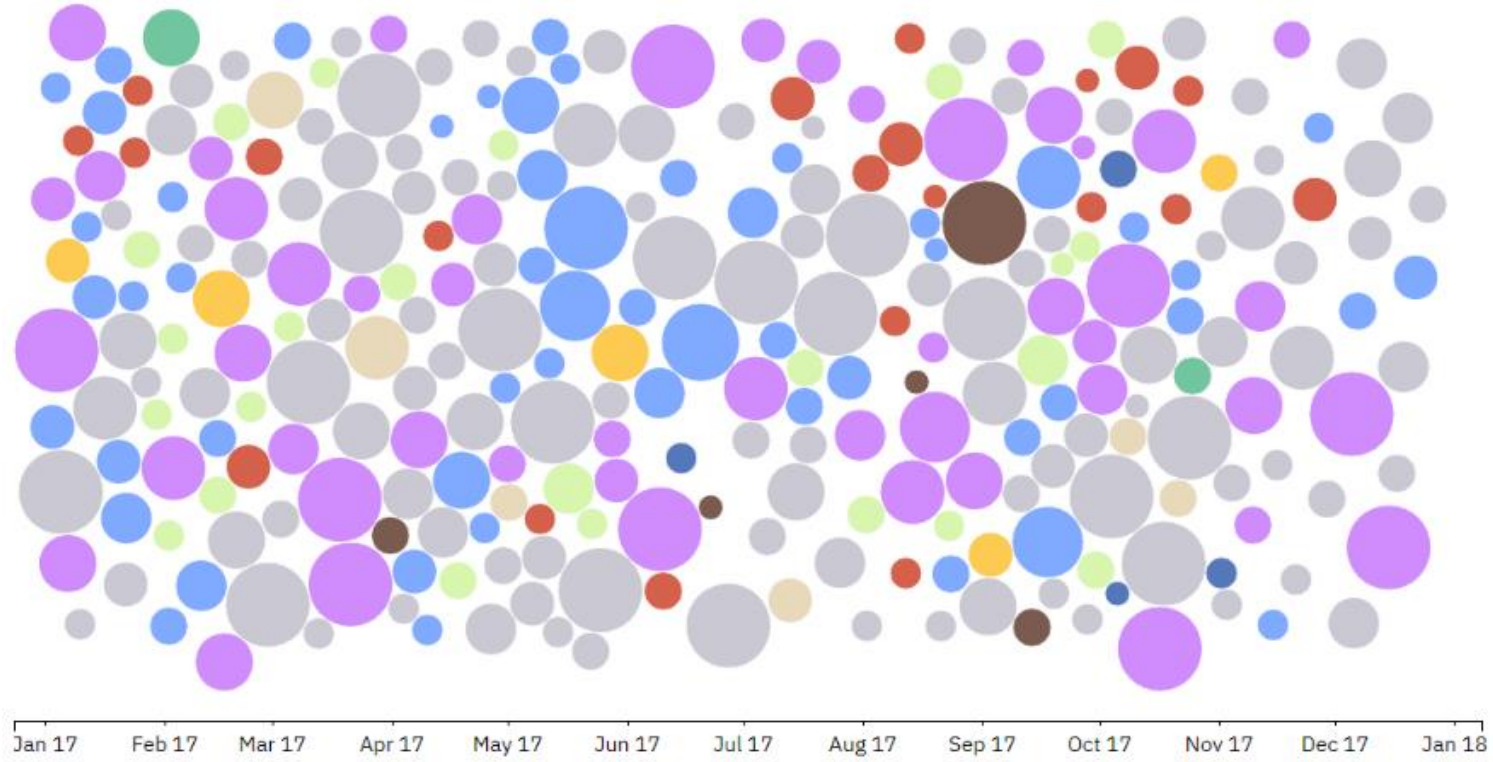


Quelle: Verizon Data Breach Investigation Report 2018

© Fortinet Inc. All Rights Reserved.

Infektionsarten



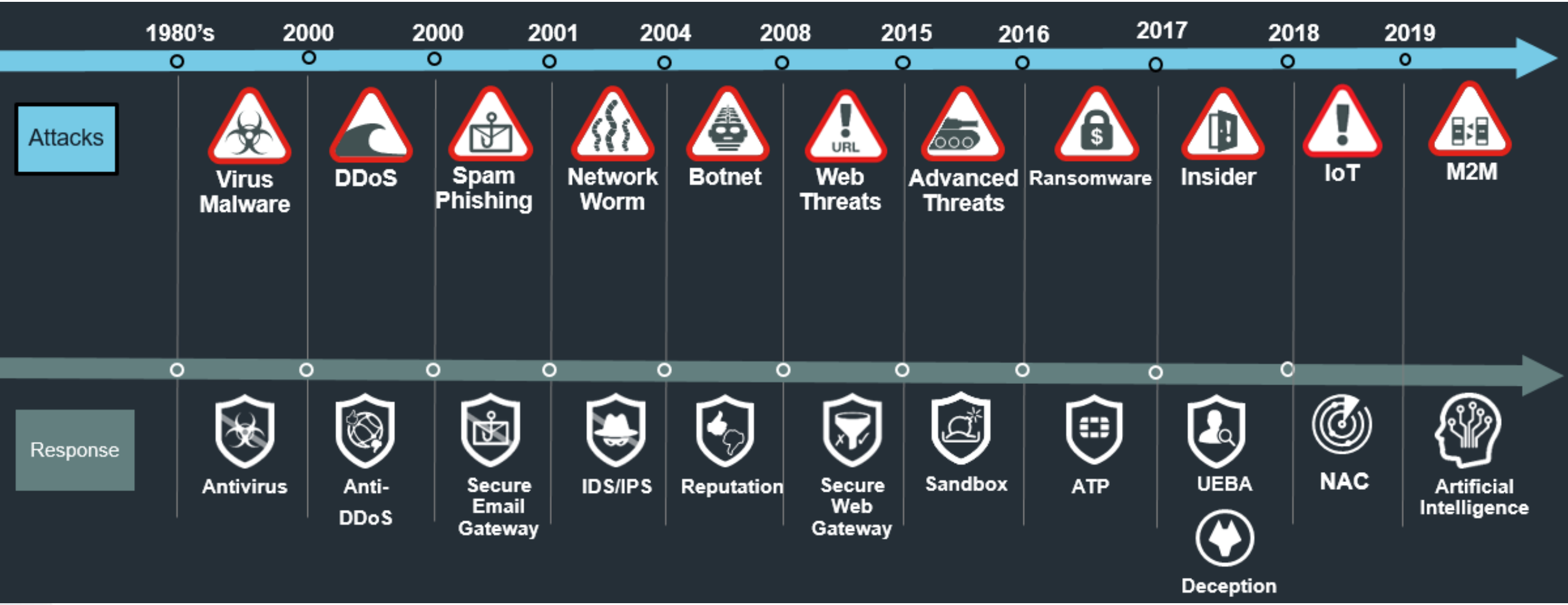


Quelle: https://www.ibm.com/security/resources/xforce/xfisi/

© Fortinet Inc. All Rights Reserved.

Heutige Herausforderungen

Entwicklung der Bedrohungslage



© Fortinet Inc. All Rights Reserved.

Facebook is looking down the barrel of a $2.2 billion fine for storing millions of passwords insecurely

British Airways faces $230 million fine. It would be a record under Europe's tough data privacy law

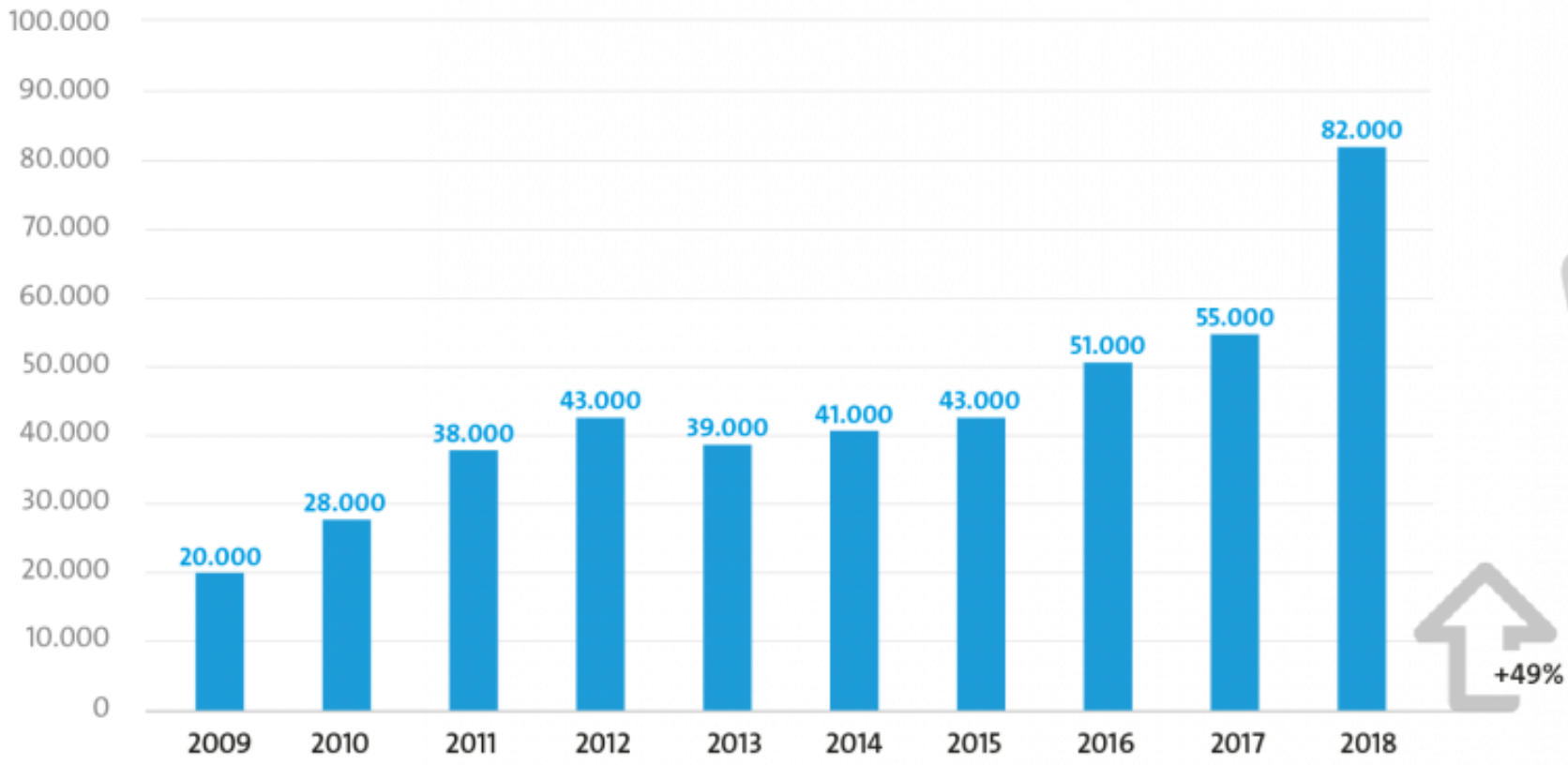
UK proposes another huge data fine. This time, Marriott is the target

© Fortinet Inc. All Rights Reserved.

FACHKRÄFTEMANGEL

82.000 offene Stellen für IT-Experten

Anzahl zu besetzender IT-Stellen in der Gesamtwirtschaft



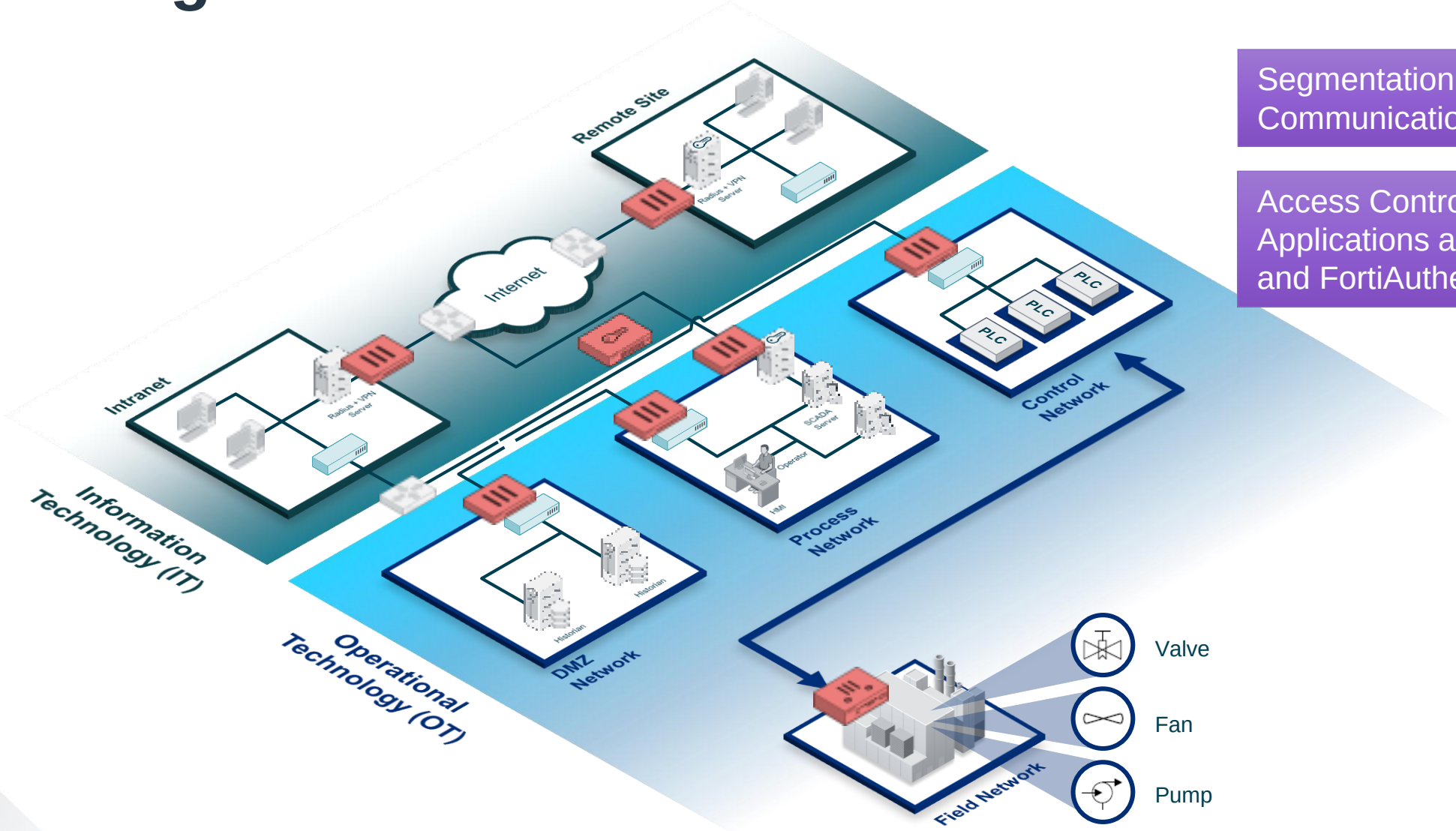
Basis: Unternehmen (Gesamtwirtschaft) ab 3 Mitarbeitern in Deutschland | Datenerhebung: jeweils im September
Quelle: Bitkom Research

bitkom

© Fortinet Inc. All Rights Reserved.

Interagierende und automatisierte Lösungen

Integriert und automatisiert



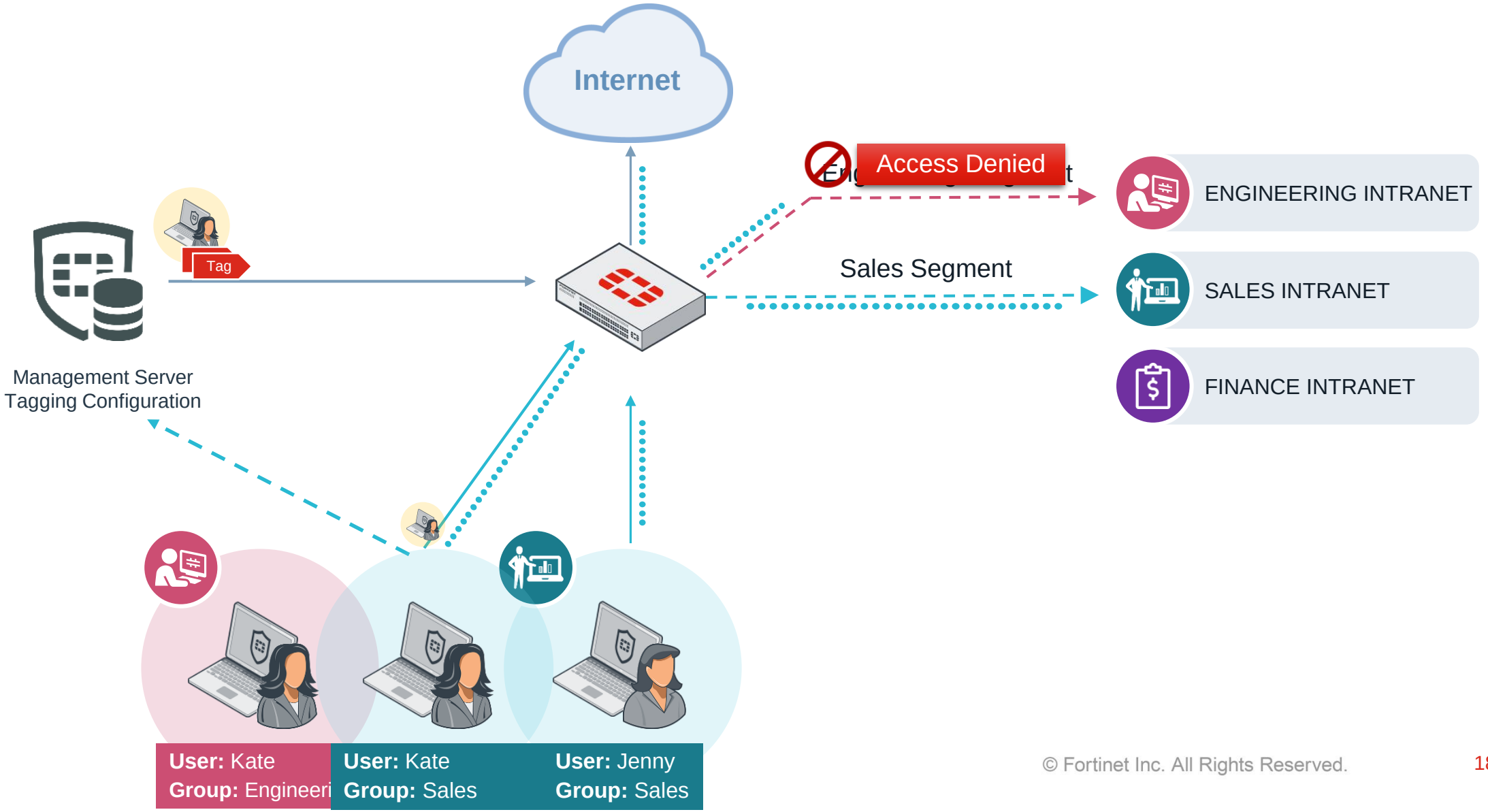
Segmentation / Encrypted Communication / Antivirus (FortiGate)

Access Control – Users, Devices, Applications and Protocols (FortiGate and FortiAuthenticator)

© Fortinet Inc. All Rights Reserved.

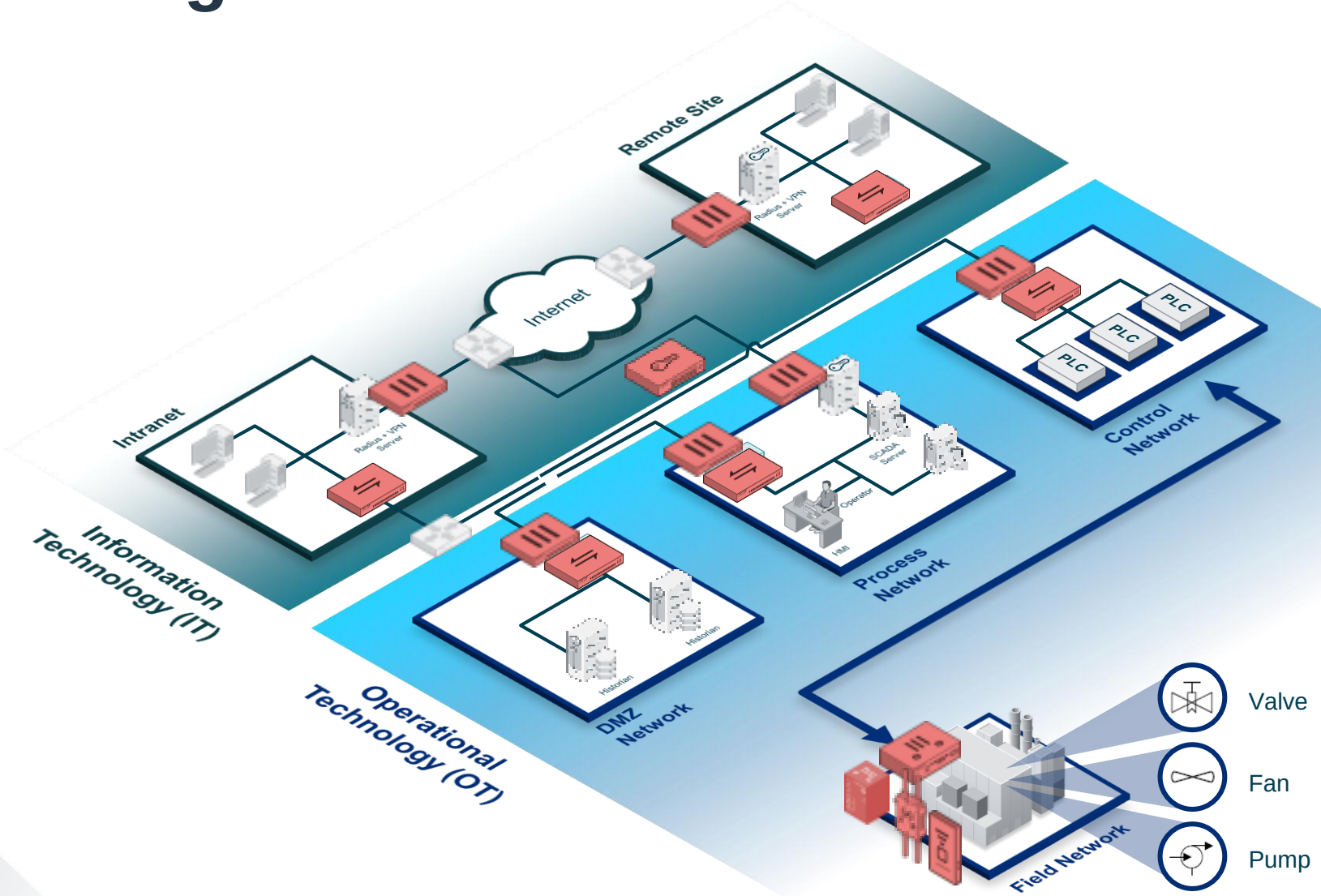
IDENTY & ACCESS (INTENT BASED SEGMENTATION)

Use Case: Access Based on AD Groups



© Fortinet Inc. All Rights Reserved.

Integriert und automatisiert



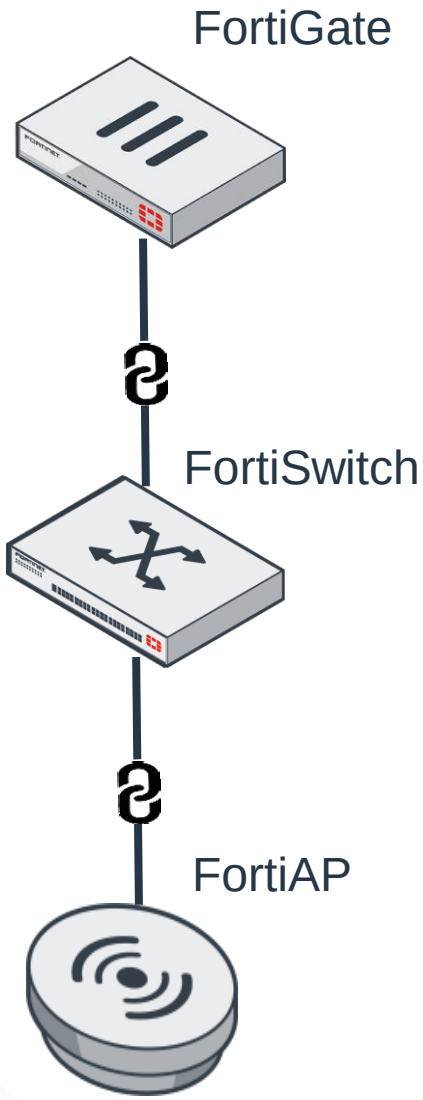
Segmentation / Encrypted Communication / Antivirus (FortiGate)

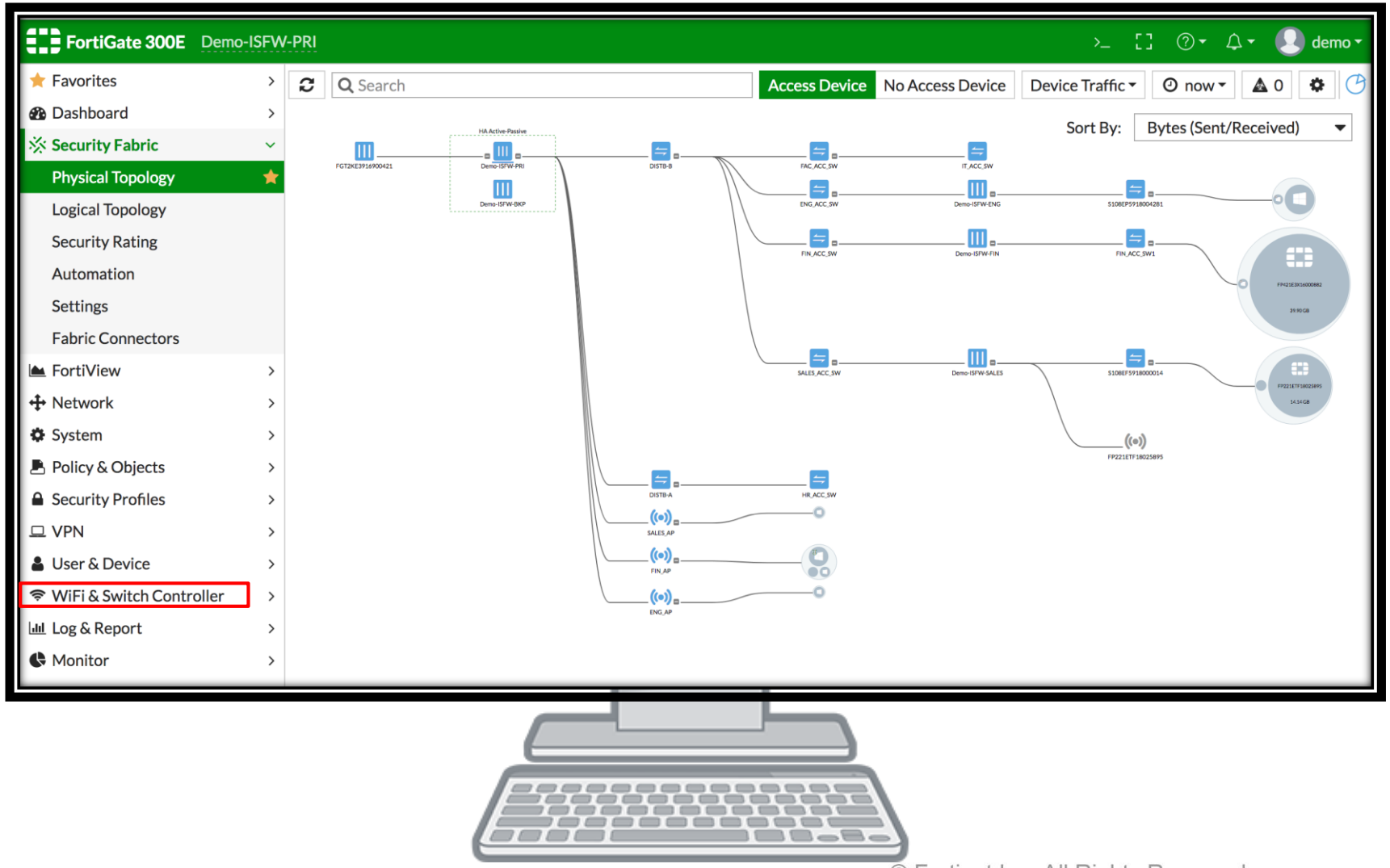
Access Control – Users, Devices, Applications and Protocols (FortiGate and FortiAuthenticator)

Secure Access (FortiSwitch/FortiAP/FortiExtender)

© Fortinet Inc. All Rights Reserved.

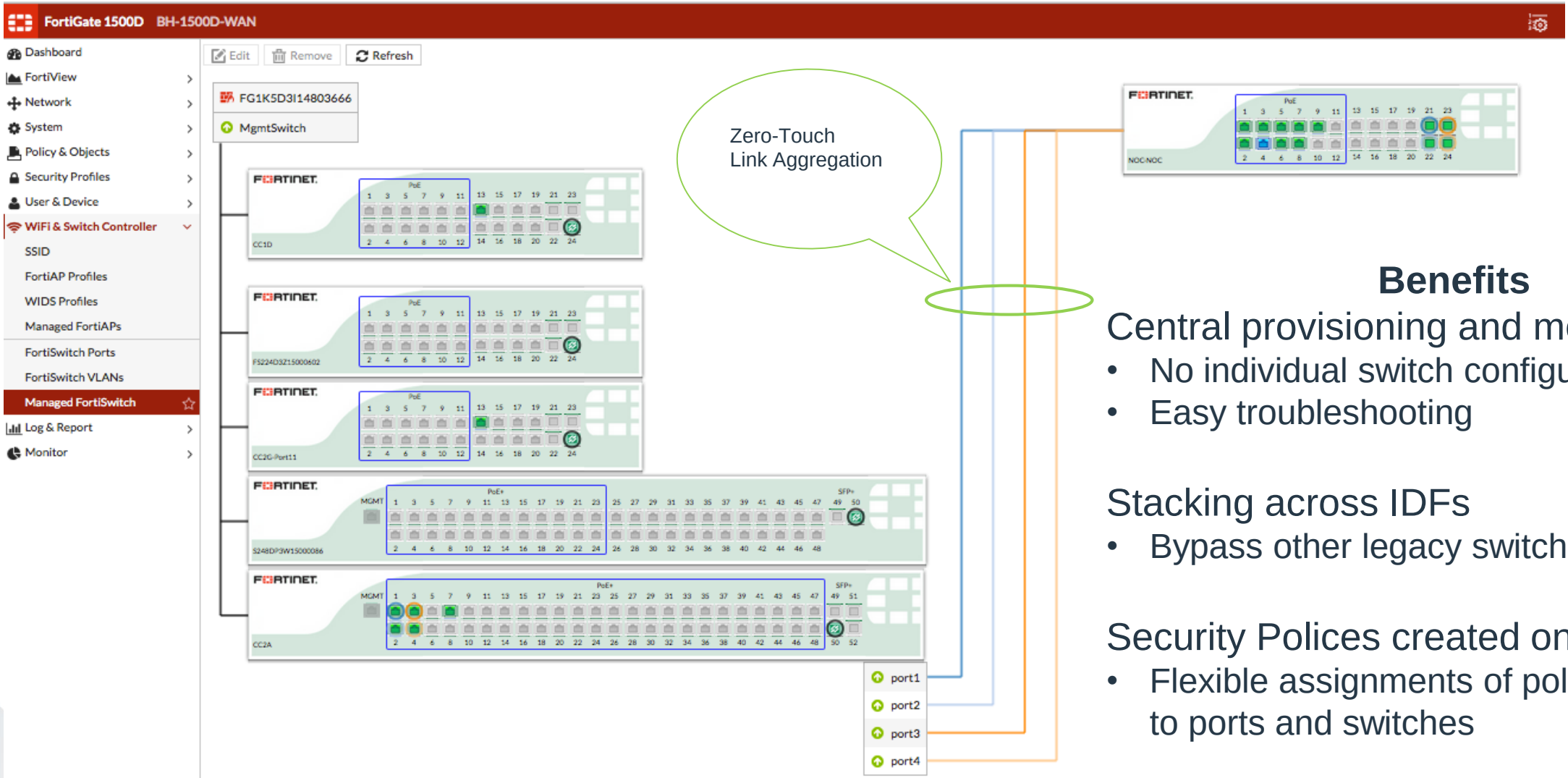
Network Deployment and Management with FortiLink





© Fortinet Inc. All Rights Reserved.

Managed Switch View



Benefits

Central provisioning and monitoring

- No individual switch configuration
- Easy troubleshooting

Stacking across IDFs

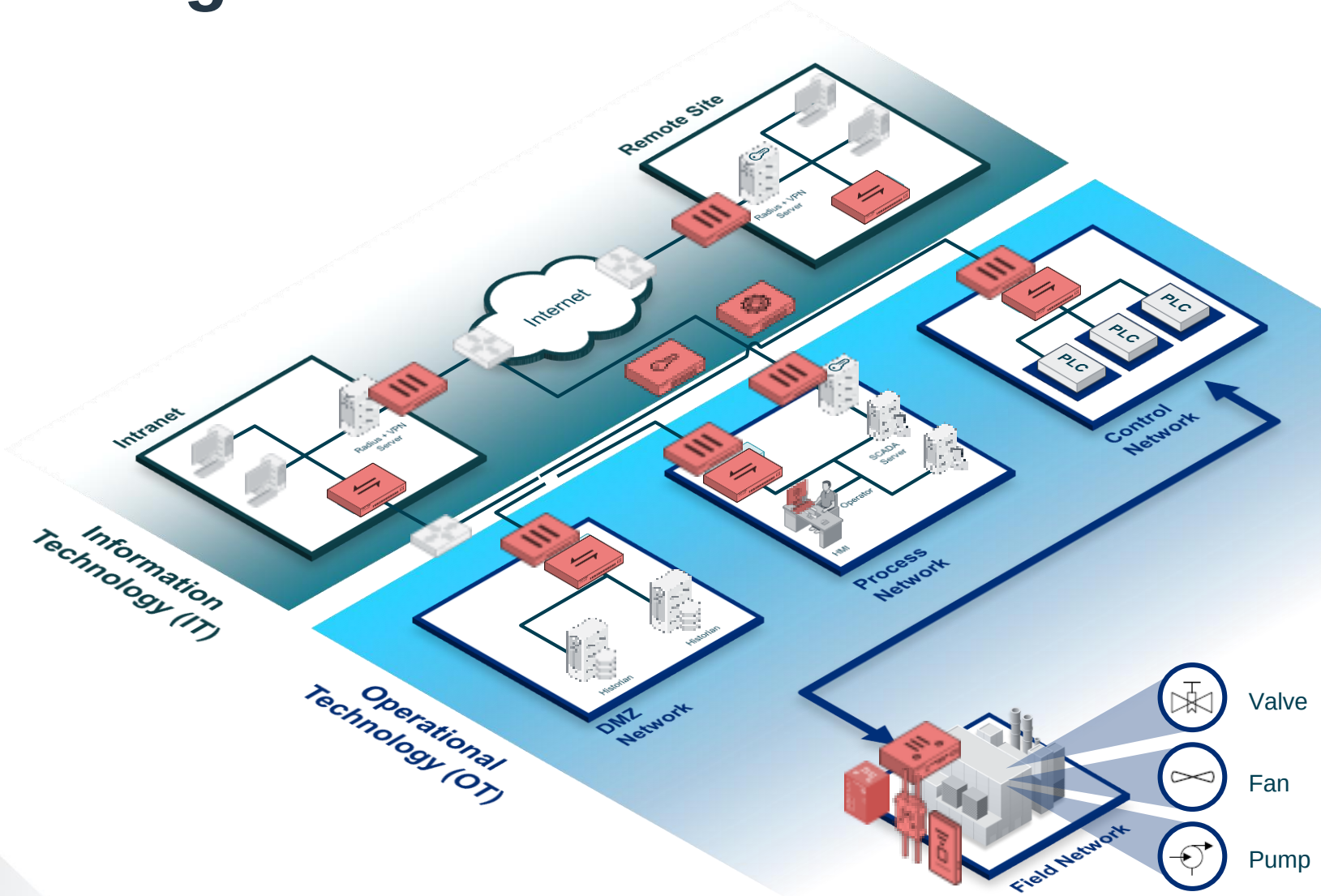
- Bypass other legacy switches on site

Security Polices created on global basis

- Flexible assignments of policy and VLANs to ports and switches

© Fortinet Inc. All Rights Reserved.

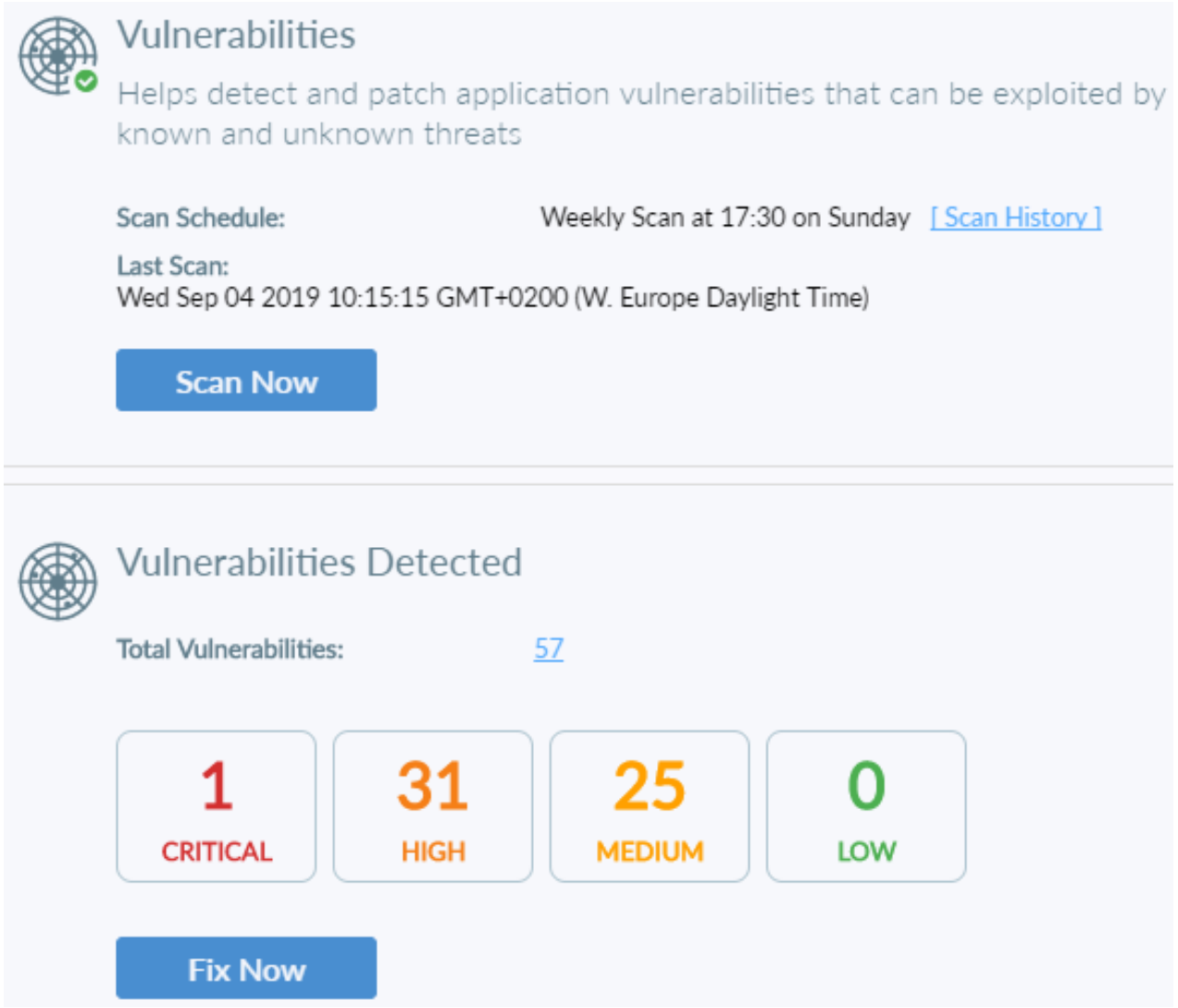
Integriert und automatisiert

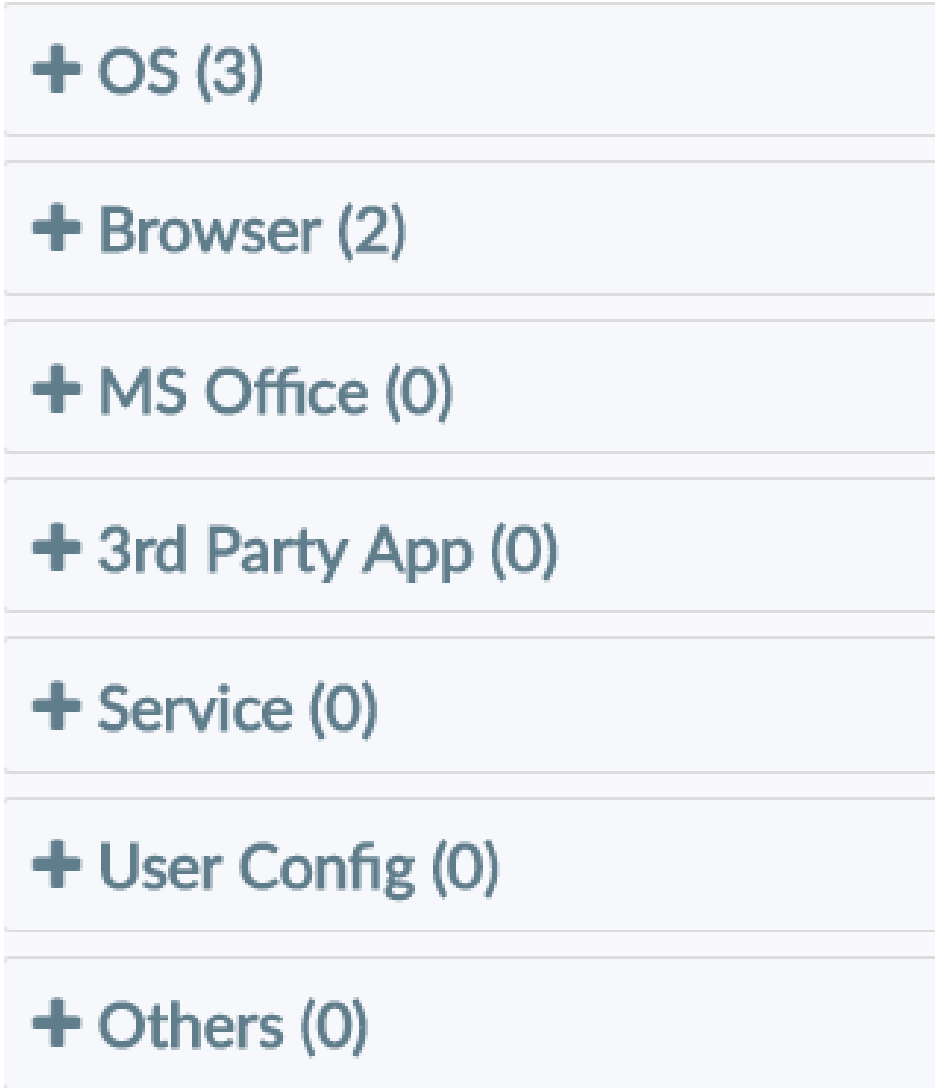


- Segmentation / Encrypted Communication / Antivirus (FortiGate)
- Access Control – Users, Devices, Applications and Protocols (FortiGate and FortiAuthenticator)
- Secure Access (FortiSwitch/FortiAP/FortiExtender)
- Vulnerability and Patch Management (FortiWeb, FortiClient and FortiGate)

© Fortinet Inc. All Rights Reserved.

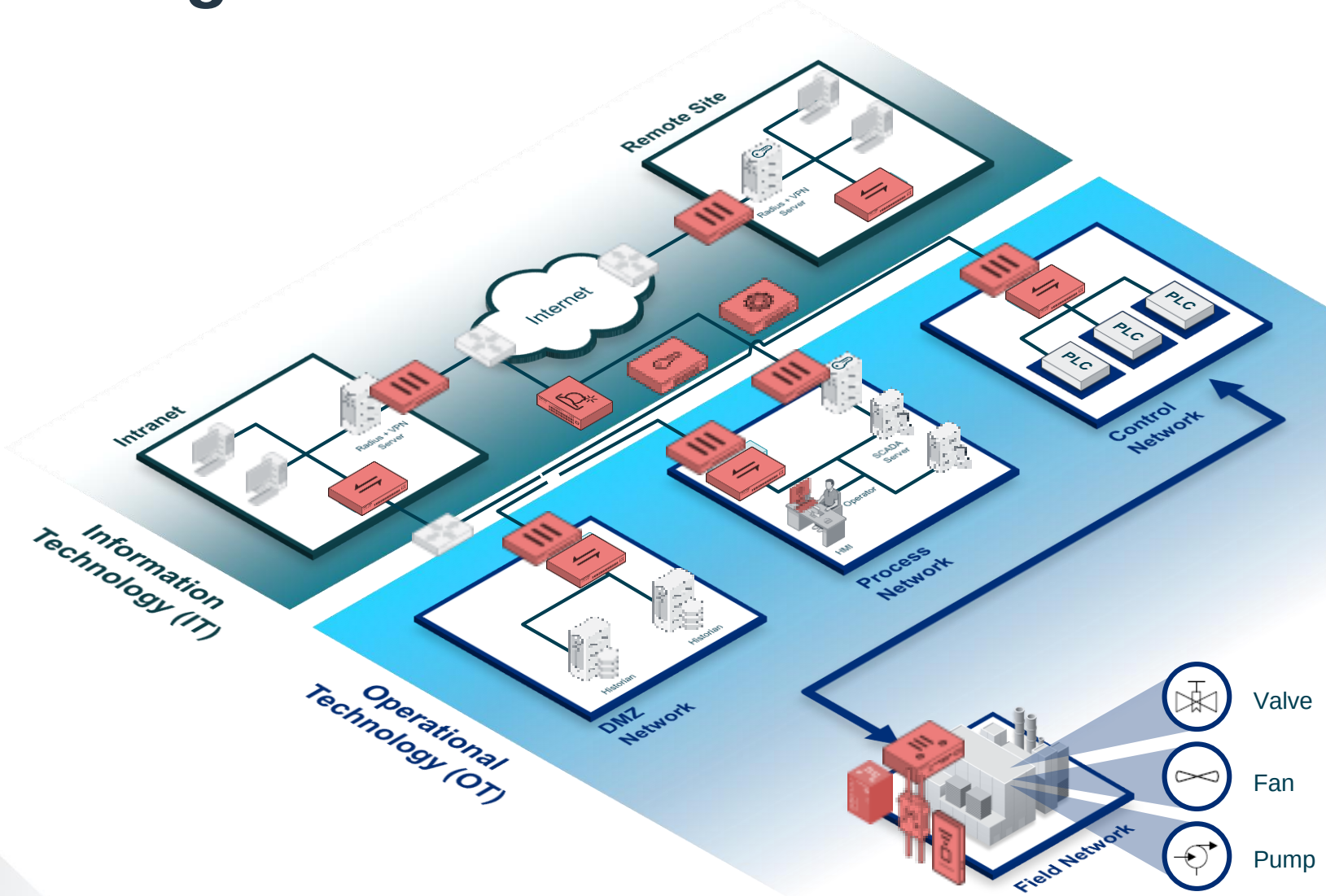
Schwachstellen





© Fortinet Inc. All Rights Reserved.

Integriert und automatisiert



Segmentation / Encrypted Communication / Antivirus (FortiGate)

Access Control – Users, Devices, Applications and Protocols (FortiGate and FortiAuthenticator)

Secure Access (FortiSwitch/FortiAP/FortiExtender)

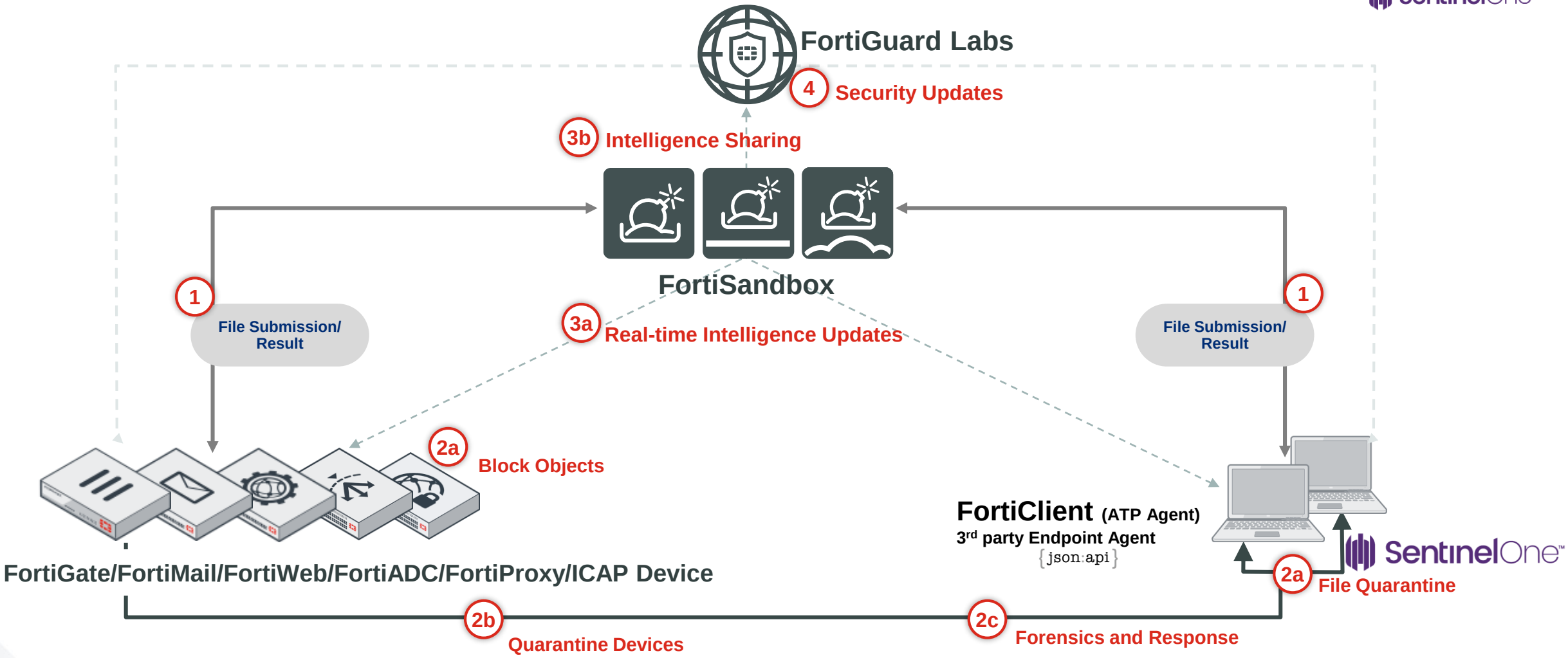
Vulnerability and Patch Management (FortiWeb, FortiClient and FortiGate)

FortiGate, FortiMail, FortiWeb & FortiClient send unknown samples to FortiSandbox for analysis

© Fortinet Inc. All Rights Reserved.

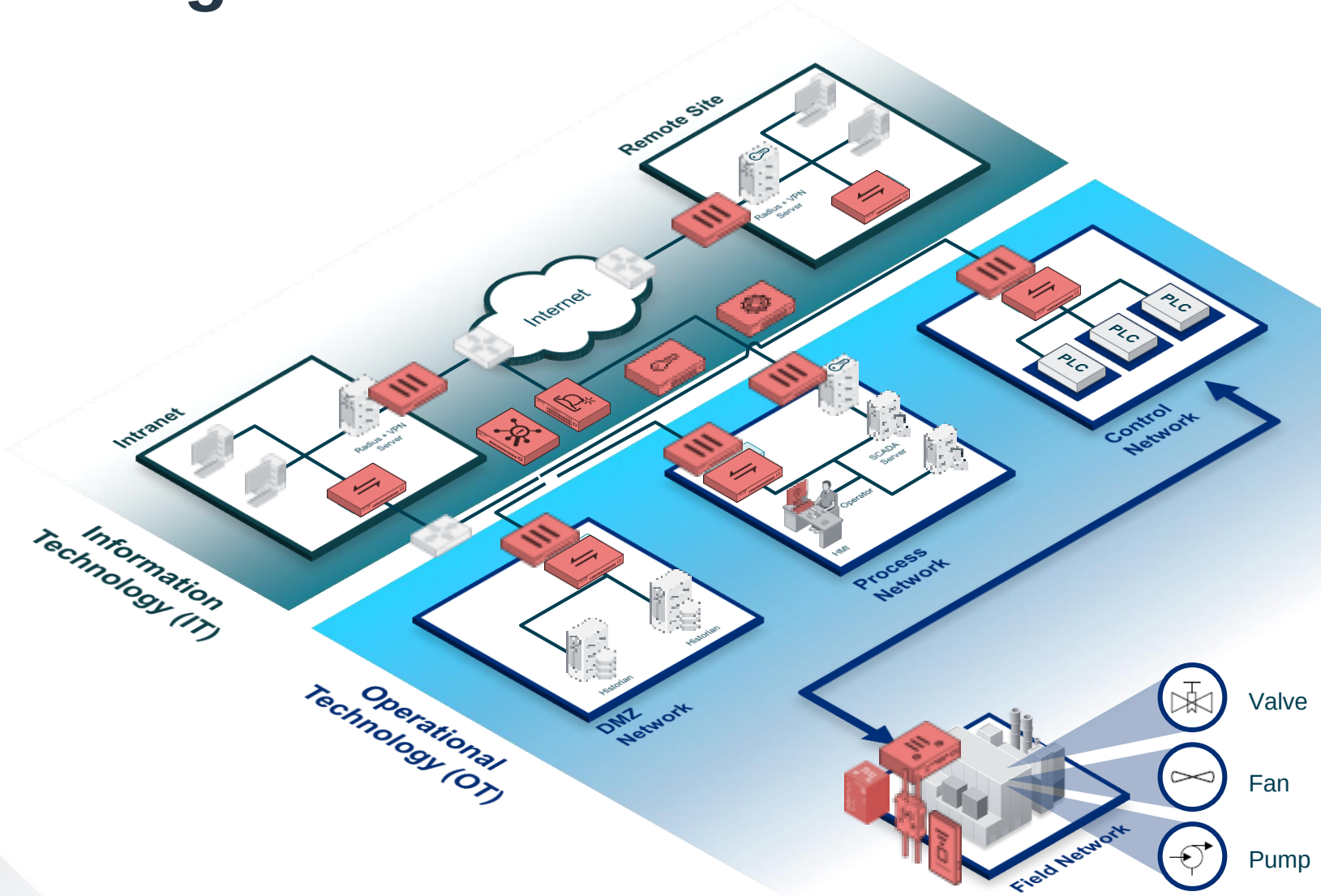
Kommunikation der Security-Produkte

Automated Intelligence Sharing and Response



© Fortinet Inc. All Rights Reserved.

Integriert und automatisiert



Segmentation / Encrypted Communication / Antivirus (FortiGate)

Access Control – Users, Devices, Applications and Protocols (FortiGate and FortiAuthenticator)

Secure Access (FortiSwitch/FortiAP/FortiExtender)

Vulnerability and Patch Management (FortiWeb, FortiClient and FortiGate)

FortiGate, FortiMail, FortiWeb & FortiClient send unknown samples to FortiSandbox for analysis

FortiSIEM collects logs and performs correlation and security auditing

© Fortinet Inc. All Rights Reserved.

Key takeaways

- User Awareness erhöhen
- Verschiedene Technologien nutzen
- Einen integrierten Ansatz fahren
  - Automatismen etablieren
  - Einheitliches Management einführen
- Prävention - Detektion - Reaktion

Jens Spielberg - Systems Engineer
Email: jspielberg@fortinet.com
Tel.: +49 176 314 88 076