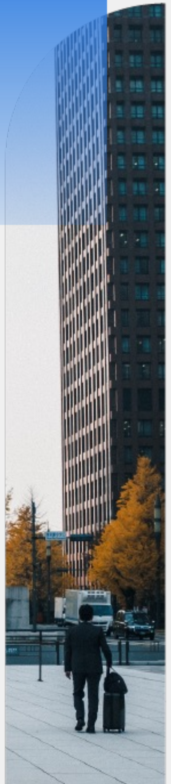
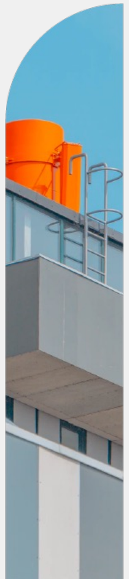
FORTINET

Fortinet Security Fabric – Det nordiske trusselslandskab & NIS2

Christian Rutrecht, System Engineering Director & Security Specialist





NIS2-direktiv overblik

EU regulatory direktiv

NIS2-direktivet er en revidering af det nuværende NIS-direktiv

Direktivet er vedtaget i Europa-Parlamentet 10. november 2022 og afventer nu endelig vedtagelse i Rådet. NIS2-direktivet skal være implementeret i dansk lovgivning senest 21 måneder efter direktivet træder i kraft; forventet efterår 2024.

Formålet

Formålet med NIS2-direktivet er at yderligere styrke og ensarte cybersikkerheden og modstandsdygtigheden overfor cybertrusler på tværs af EU for virksomheder inden for en lang række sektorer og for offentlige institutioner, som anses for at være kritiske for økonomien og samfundet.

Hvad med den nationale sikkerhed og prioritering?

Hvorfor nu?

IT/OT convergence, More threats impacting OT & ICS, Incidents unreported, Ransomware, Geopolitics & warware, Long life span 30/40/50 years implementations, EU leading the market.

Ramsomware & RaaS is crowing exponentially.

Geo-political uncertainty

Hvad mangler vi for at komme i gang?

Den nationale fortolkning er essentiel!

Vi skal I gang NU, der er fare for at vi kan få et nyt GDPR scenarie hvor virksomheder og organisationer for sent kommer i gang med at følge de nye retningslinjer

Hvem er omfattet

- Essensielle enheder
- Energi (elektricitet, fjernvarme, olie, gas og brint)
- Transport (luft, jernbane, vand og vej)
- Bankvirksomhed (kreditinstitutter)
- Finansielle markedsinfrastrukturer (markedspladser)
- Sundhedssektoren (sundhedstjenesteydere og producenter af lægemidler
- Vigtige enheder
- Post- og kurertjenester
- Affaldshåndtering
- Fremstilling, produktion og distribution af kemikalier

Sanktioner

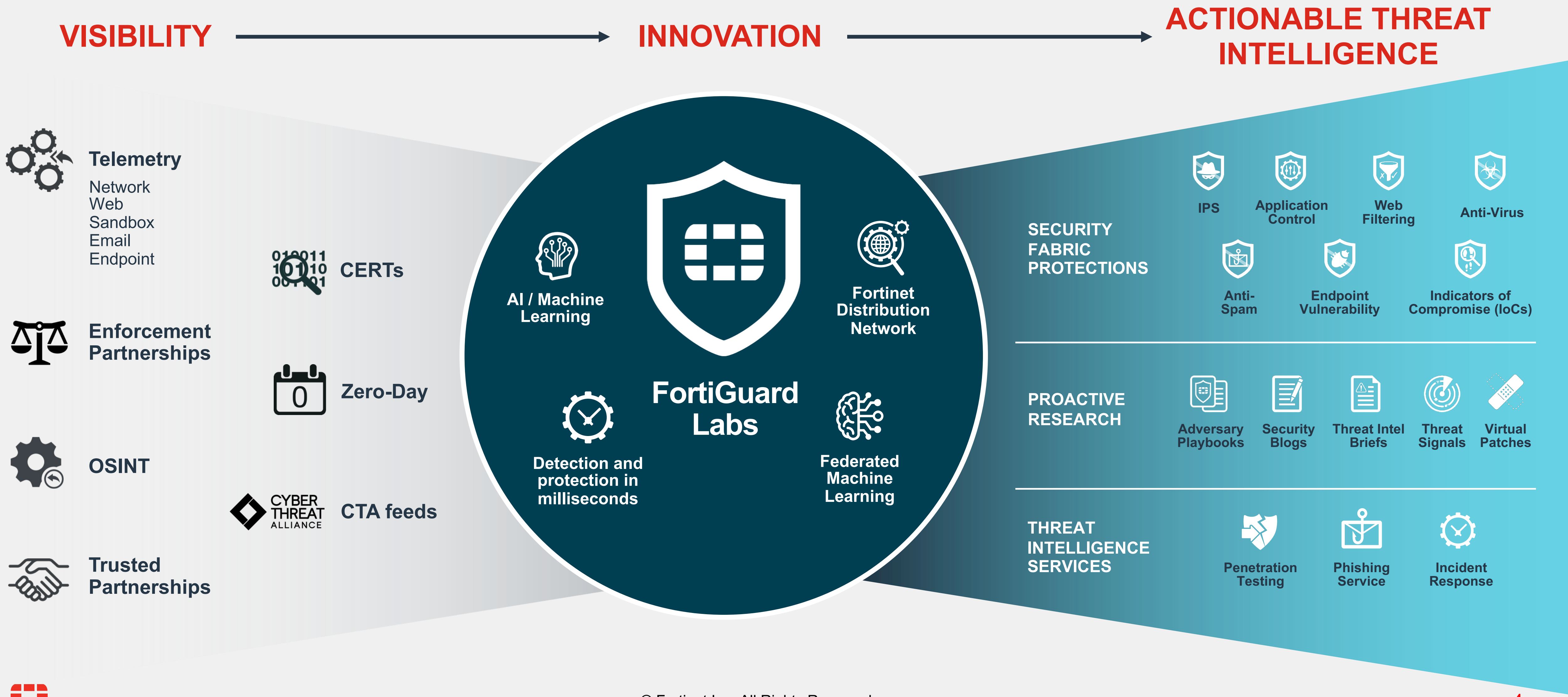
Enheden kan pålægges bøder på op til det højeste af 10 mio. EUR eller 2 % af virksomhedens samlede globale årsomsætning.

Ledelse ansvar og den nationale myndigheds beføjelse til at hjemsende og/eller stille ledelsen til ansvar for manglede kontrol både før og efter en hændelse

Krav til sikkerhedskontroller og policies

- Politikker for risikoanalyse og informationssikkerhed
- Håndtering af hændelser
- Driftskontinuitet og krisestyring (back-up mv.)
- Forsyningskædesikkerhed, herunder leverandørstyring/ sikkerhed
- Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer
- Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici
- Retningslinjer for basal "computer hygiejne" og træning i cybersikkerhed
- Politikker for brug af kryptografi og kryptering
- Medarbejdersikkerhed, adgangskontrol og asset management
- Sikring af interne kommunikationssystemer.

FortiGuard Labs



VISIBILITY → INNOVATION → ACTIONABLE THREAT INTELLIGENCE

Telemetry
Network
Web
Sandbox
Email
Endpoint

CERTs

Enforcement Partnerships

Zero-Day

OSINT

CYBER THREAT ALLIANCE CTA feeds

Trusted Partnerships

AI / Machine Learning

Fortinet Distribution Network

FortiGuard Labs

Detection and protection in milliseconds

Federated Machine Learning

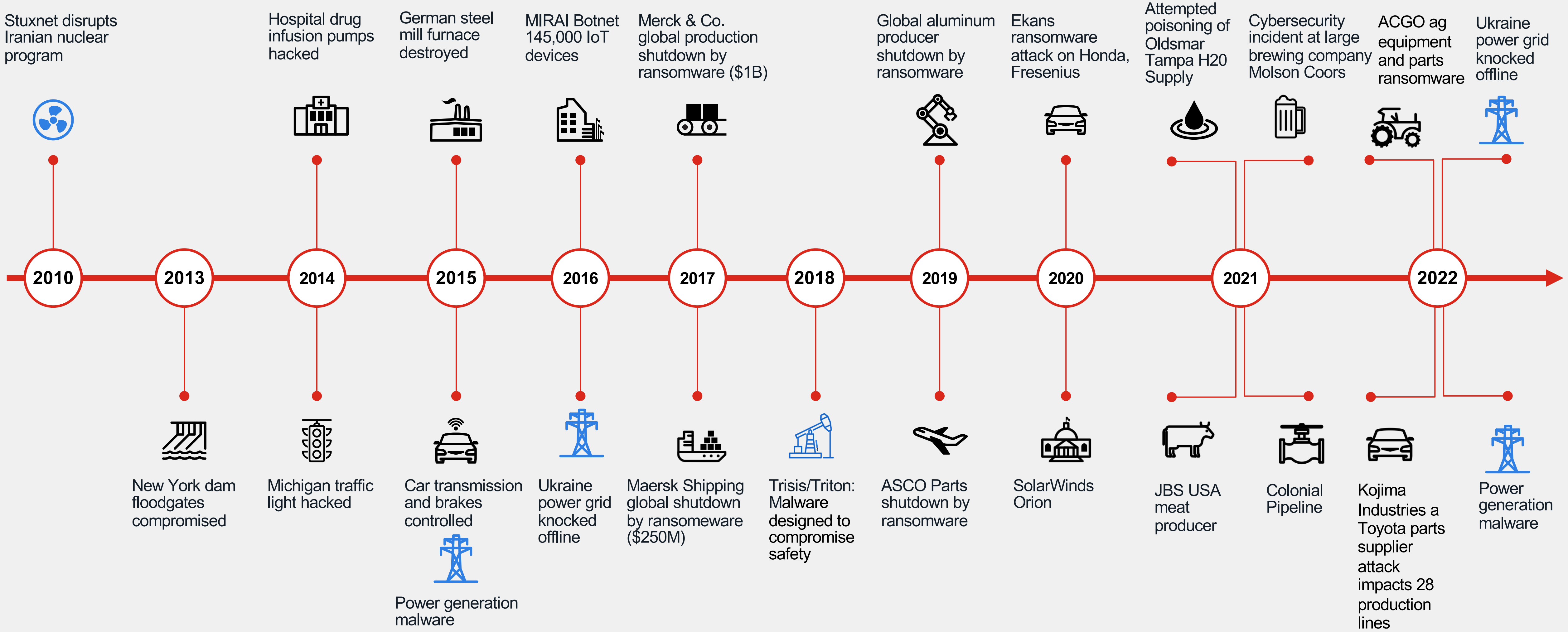
SECURITY FABRIC PROTECTIONS
IPS
Application Control
Web Filtering
Anti-Virus
Anti-Spam
Endpoint Vulnerability
Indicators of Compromise (IoCs)

PROACTIVE RESEARCH
Adversary Playbooks
Security Blogs
Threat Intel Briefs
Threat Signals
Virtual Patches

THREAT INTELLIGENCE SERVICES
Penetration Testing
Phishing Service
Incident Response

OT Infrastructure Attacks

Attacks are increasing in frequency and impact



2010

Stuxnet disrupts Iranian nuclear program

2013

New York dam floodgates compromised

2014

Hospital drug infusion pumps hacked

Michigan traffic light hacked

2015

German steel mill furnace destroyed

Car transmission and brakes controlled

Power generation malware

2016

MIRAI Botnet 145,000 IoT devices

Ukraine power grid knocked offline

2017

Merck & Co. global production shutdown by ransomware ($1B)

Maersk Shipping global shutdown by ransomeware ($250M)

2018

Trisis/Triton: Malware designed to compromise safety

2019

Global aluminum producer shutdown by ransomware

ASCO Parts shutdown by ransomware

2020

Ekans ransomware attack on Honda, Fresenius

SolarWinds Orion

2021

Attempted poisoning of Oldsmar Tampa H20 Supply

Cybersecurity incident at large brewing company Molson Coors

JBS USA meat producer

Colonial Pipeline

2022

ACGO ag equipment and parts ransomware

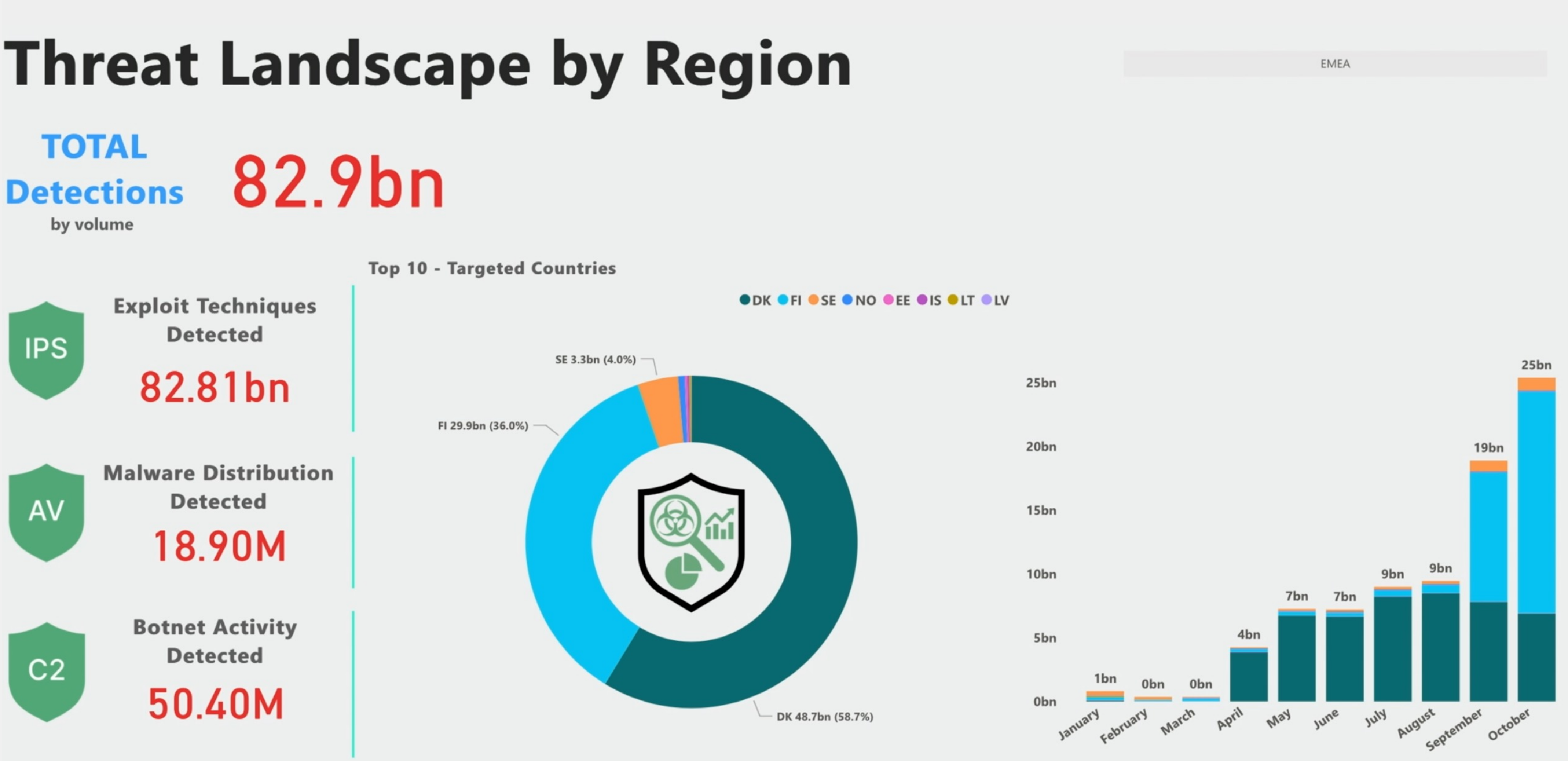
Ukraine power grid knocked offline

Kojima Industries a Toyota parts supplier attack impacts 28 production lines

Power generation malware

OT targeted attacks

2022 Nordic Threat Landscape



Threat Landscape by Region

EMEA

TOTAL Detections by volume **82.9bn**

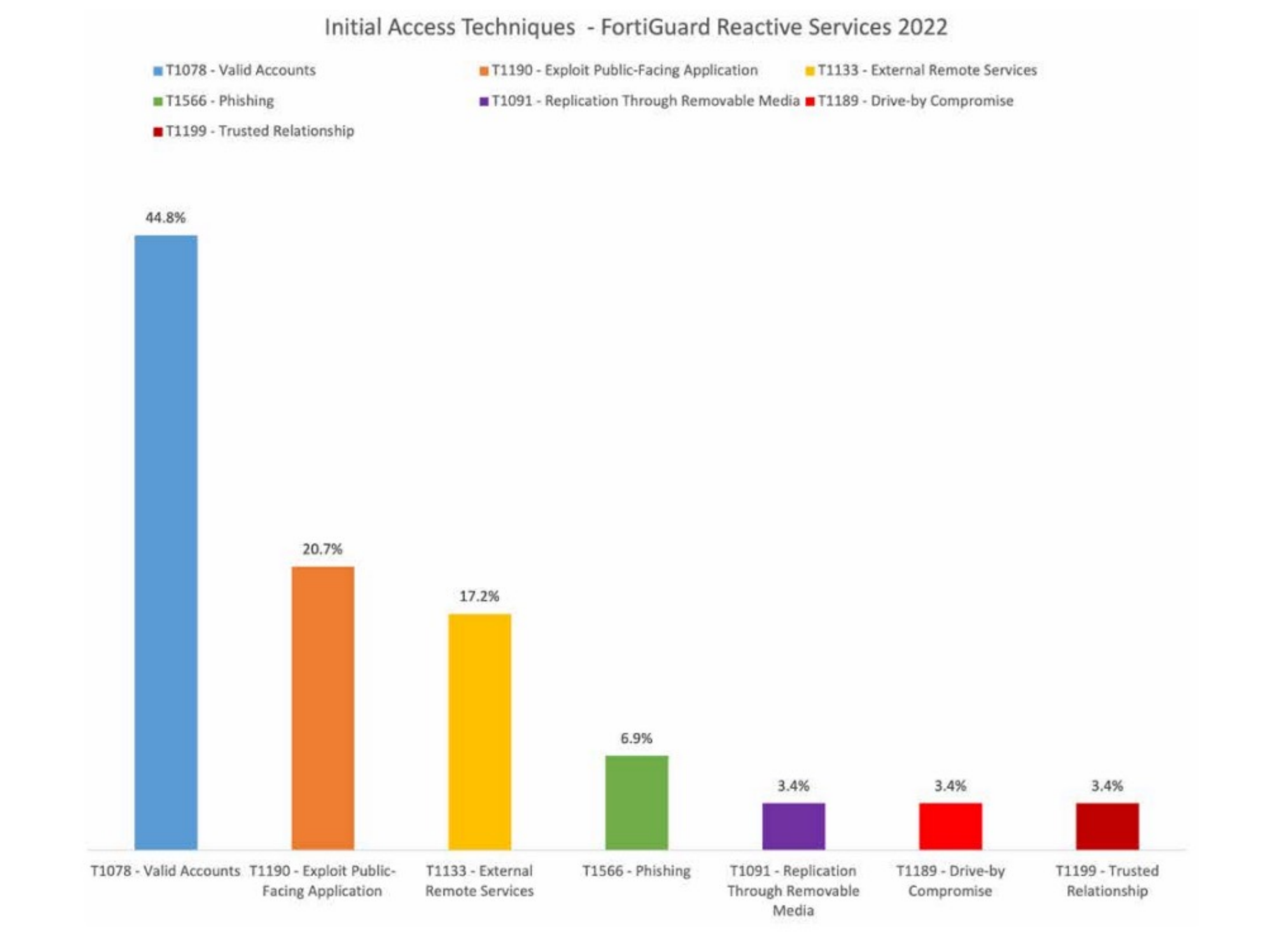
IPS — Exploit Techniques Detected: **82.81bn**

AV — Malware Distribution Detected: **18.90M**

C2 — Botnet Activity Detected: **50.40M**

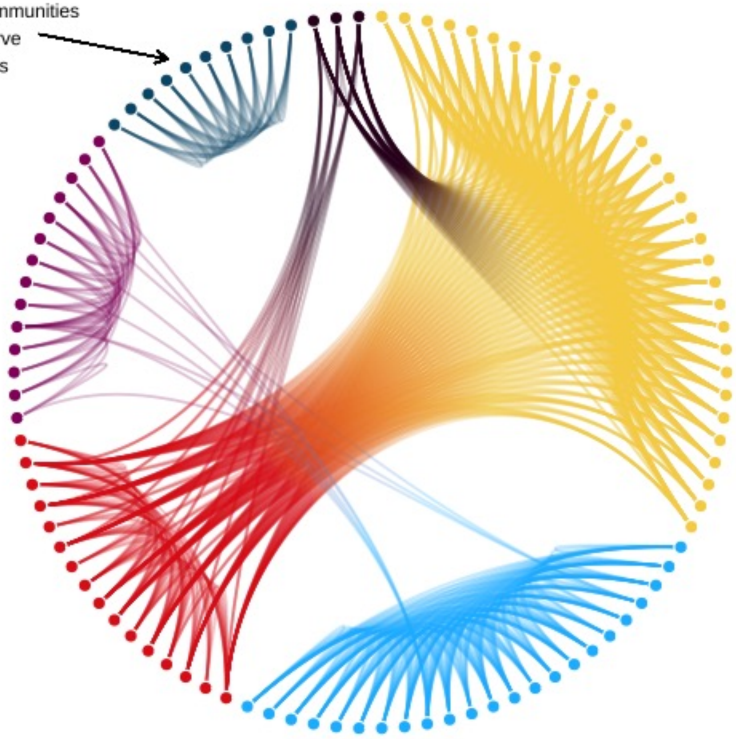
Top 10 - Targeted Countries

2022 H2 – Facts from the field – Initial Access



https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-2h-2022

2022 H2 – Facts from the field – Code reuse



Code is shared among most communities of Emotet variants, yet we observe at least one community that does not share code with others.

Figure 16 - Code reuse within and across communities of Emotet variants

https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-2h-2022

2022 H2 – Facts from the field – Contributing fails

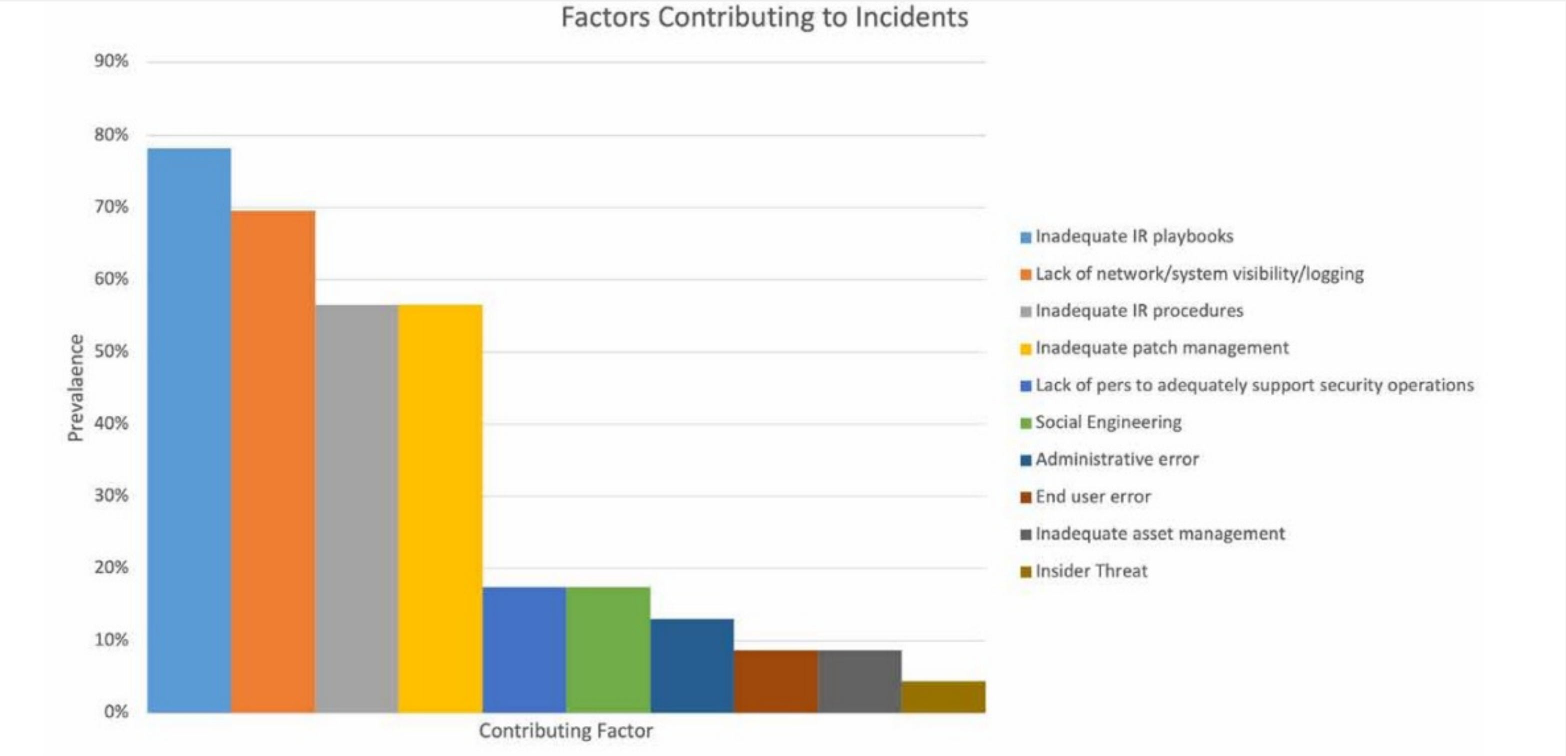
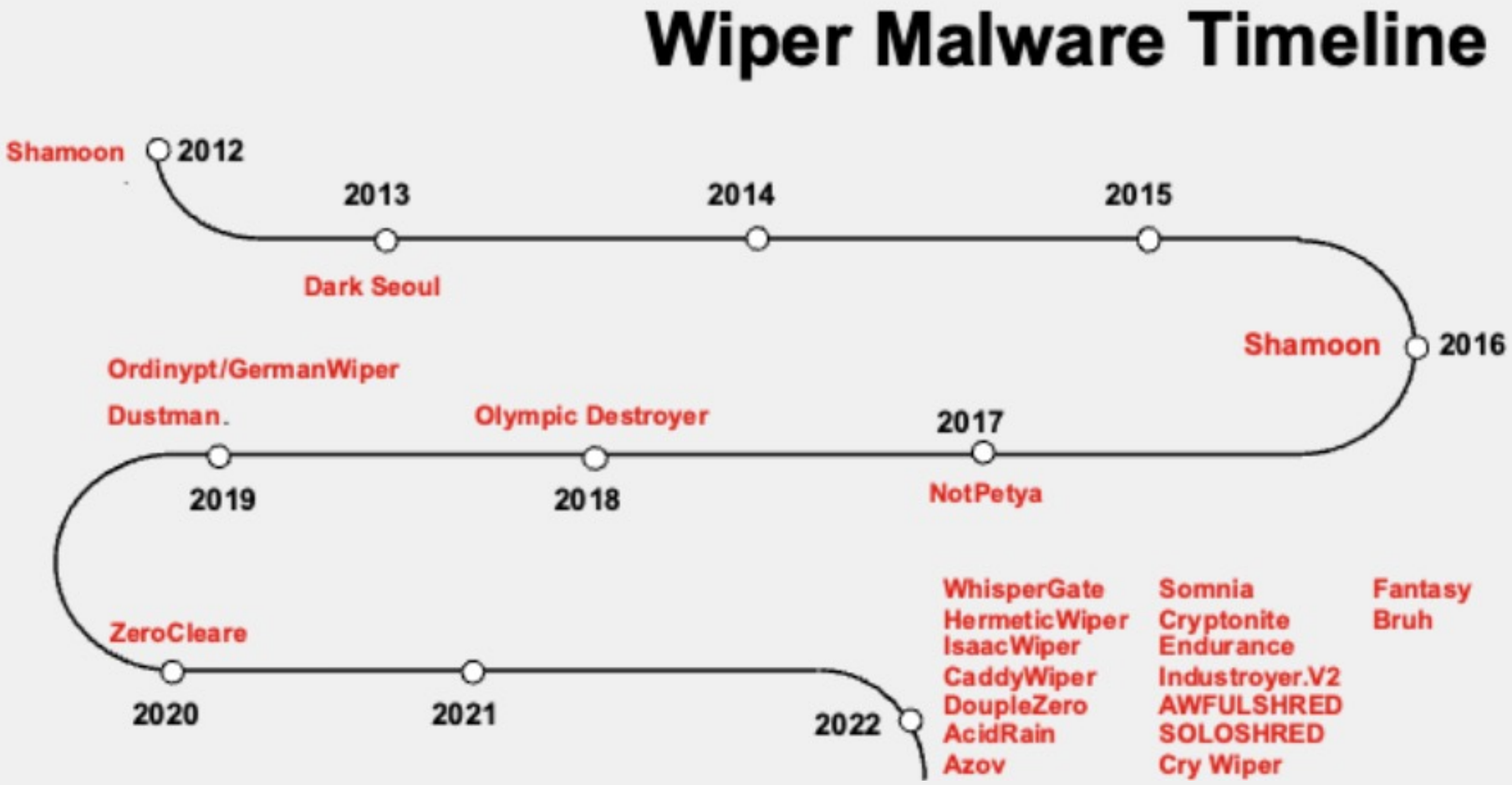


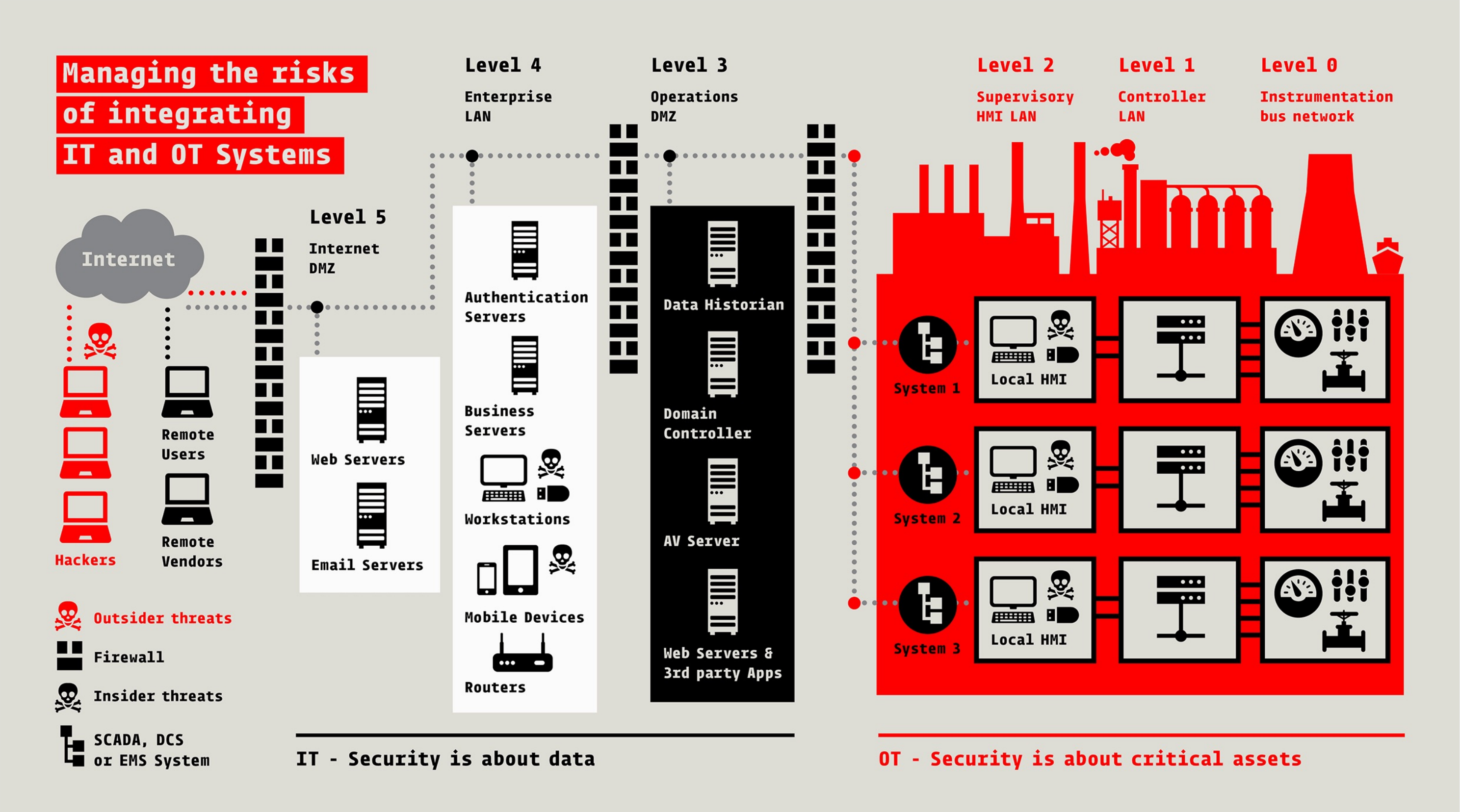
Figure 32 - Factors contributing to intrusions for incidents investigated by the FortiGuard IR team in 2022

https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-2h-2022

2022 – Wiper Malware



IT vs OT Threats – why the convertion & risk?



Managing the risks of integrating IT and OT Systems

Level 5
Internet DMZ

Level 4
Enterprise LAN

Level 3
Operations DMZ

Level 2
Supervisory HMI LAN

Level 1
Controller LAN

Level 0
Instrumentation bus network

Internet

Hackers

Remote Users

Remote Vendors

Web Servers

Email Servers

Authentication Servers

Business Servers

Workstations

Mobile Devices

Routers

Data Historian

Domain Controller

AV Server

Web Servers & 3rd party Apps

System 1

System 2

System 3

Local HMI

Local HMI

Local HMI

Outsider threats

Firewall

Insider threats

SCADA, DCS or EMS System

IT - Security is about data

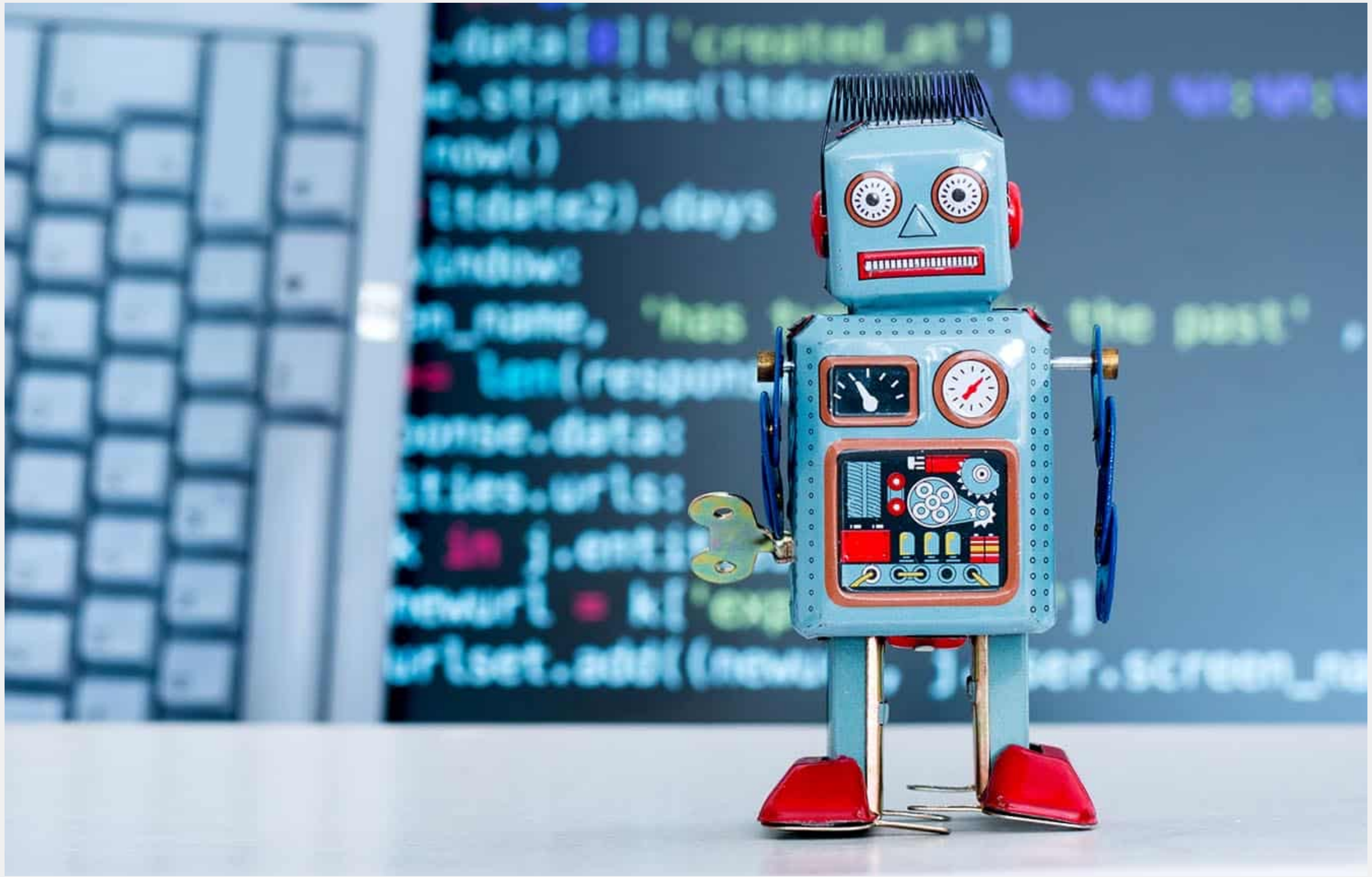
OT - Security is about critical assets

- Most attacks hitting operational operations are IT threats Colonial Pipeline

- Converged Networking & data usage complicates air gapped strategies

- What has historically been the biggest threat to OT environments? People, squirrels and birds – This has changed and is the new reality.

Weaponization of AI



The way of the lazy threat actor:

Good at

- Code to Code conversion
- Campaign Creation – Phishing attacks
- New tools (Polymorphic malware)
- Intelligence Gathering

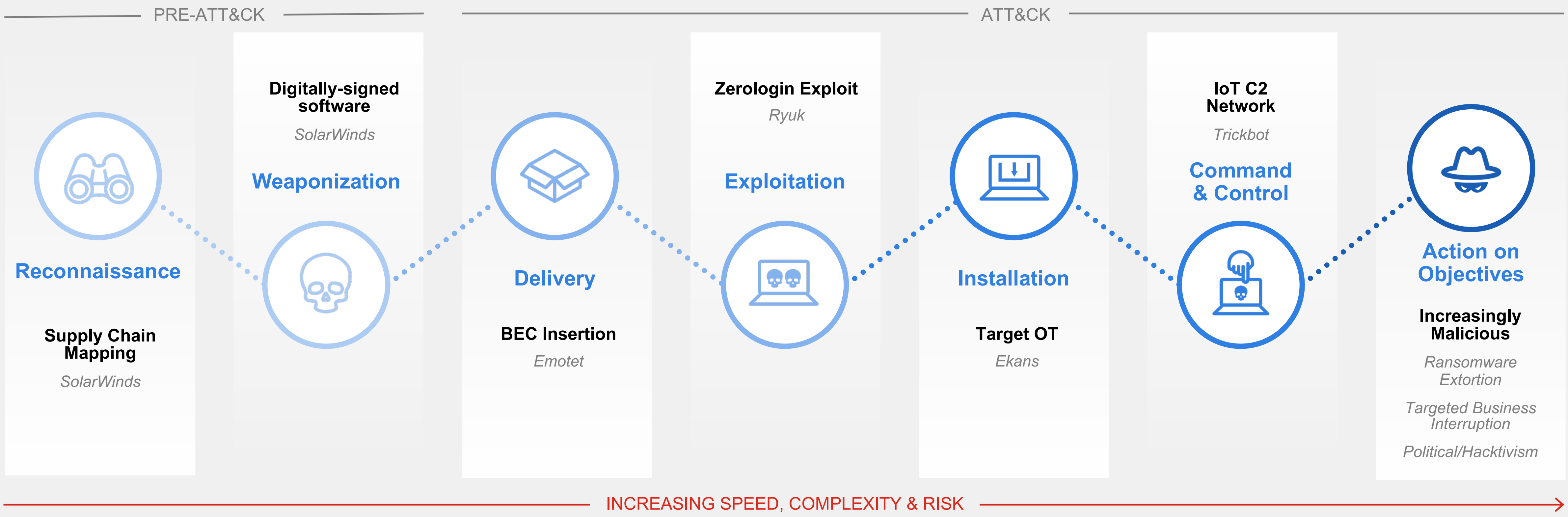
Bad at (For now)

- Dynamic code analysis
- Abstract Threat Hunting
- Resetting AI model flow

Remember AI neural network platforms (For now) are simulating being Human, it is not human or can think with the same abstractation level

Speed: The key to breaking the kill chain

To break the attack sequence and protect the organization, we need to detect and rapidly adjust the security posture to effectively protect against newly discovered attack's tactics across ever expanding attack surface.



PRE-ATT&CK

ATT&CK

Reconnaissance

Supply Chain Mapping

SolarWinds

Digitally-signed software

SolarWinds

Weaponization

Delivery

BEC Insertion

Emotet

Zerologin Exploit

Ryuk

Exploitation

Installation

Target OT

Ekans

IoT C2 Network

Trickbot

Command & Control

Action on Objectives

Increasingly Malicious

Ransomware Extortion

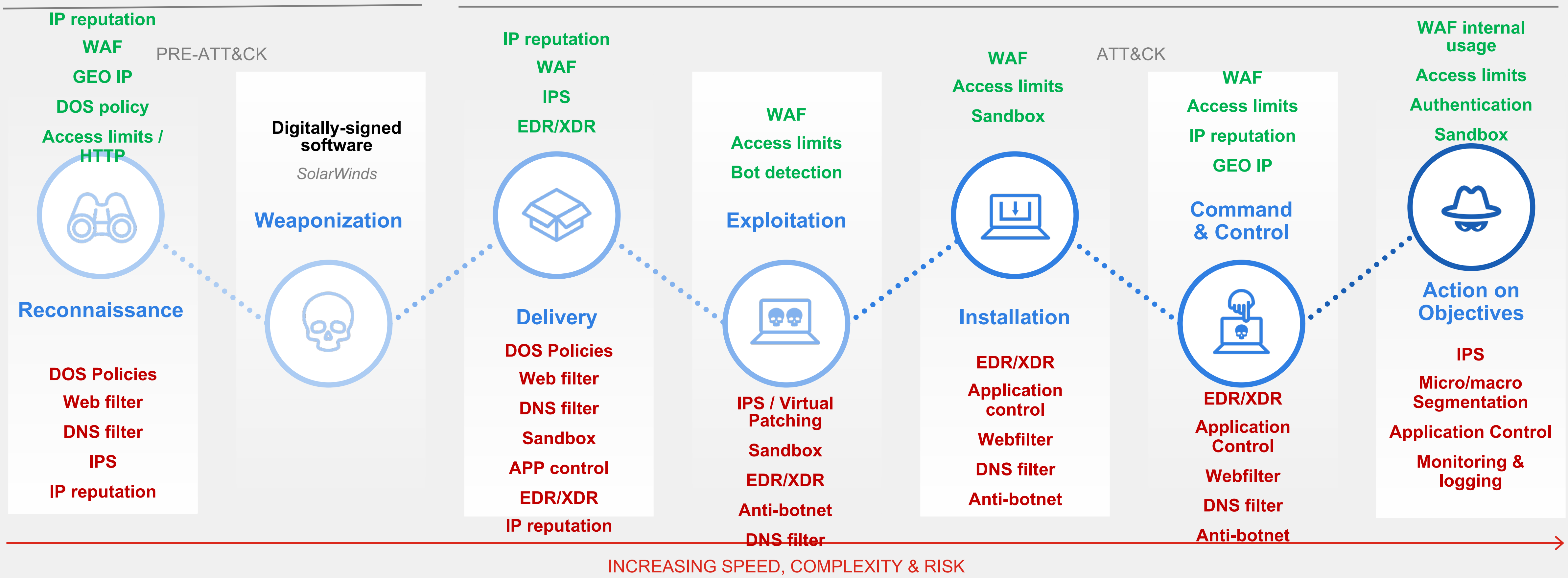
Targeted Business Interruption

Political/Hacktivism

INCREASING SPEED, COMPLEXITY & RISK

Speed: The key to breaking the kill chain

To break the attack sequence and protect the organization, we need to detect and rapidly adjust the security posture to effectively protect against newly discovered attack's tactics across ever expanding attack surface.



PRE-ATT&CK

ATT&CK

Reconnaissance

IP reputation
WAF
GEO IP
DOS policy
Access limits / HTTP

DOS Policies
Web filter
DNS filter
IPS
IP reputation

Weaponization

Digitally-signed software
SolarWinds

Delivery

IP reputation
WAF
IPS
EDR/XDR

DOS Policies
Web filter
DNS filter
Sandbox
APP control
EDR/XDR
IP reputation

Exploitation

WAF
Access limits
Bot detection

IPS / Virtual Patching
Sandbox
EDR/XDR
Anti-botnet
DNS filter

Installation

WAF
Access limits
Sandbox

EDR/XDR
Application control
Webfilter
DNS filter
Anti-botnet

Command & Control

WAF
Access limits
IP reputation
GEO IP

EDR/XDR
Application Control
Webfilter
DNS filter
Anti-botnet

Action on Objectives

WAF internal usage
Access limits
Authentication
Sandbox

IPS
Micro/macro Segmentation
Application Control
Monitoring & logging

INCREASING SPEED, COMPLEXITY & RISK

Fortinet Security Fabric

Broad

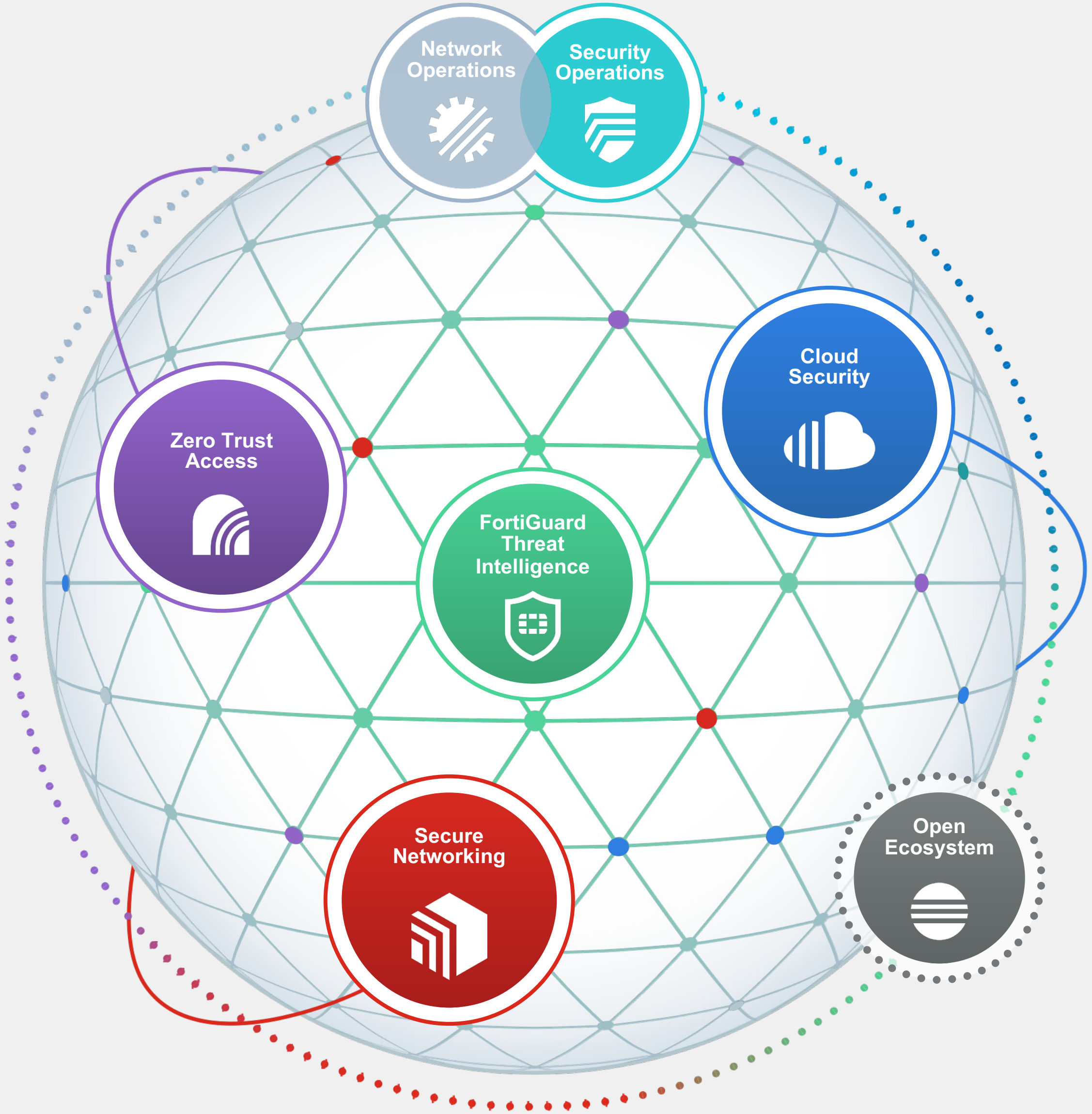
Visibility and protection of the entire digital attack surface to better manage risk

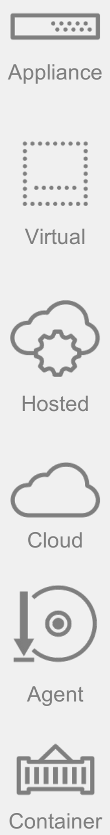
Integrated

Solution that reduces management complexity and shares threat intelligence

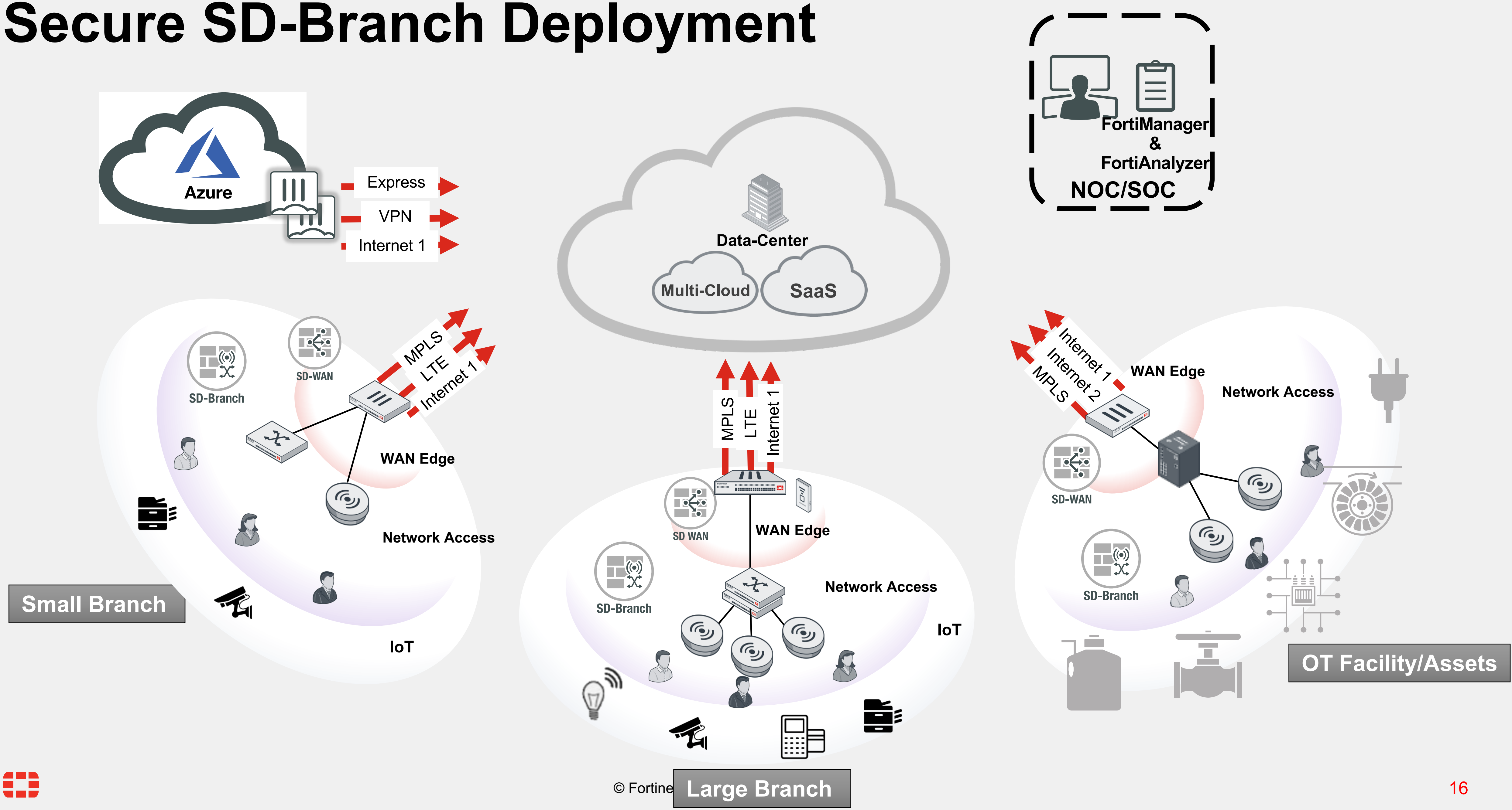
Automated

Self-healing networks with AI-driven security for fast and efficient operations

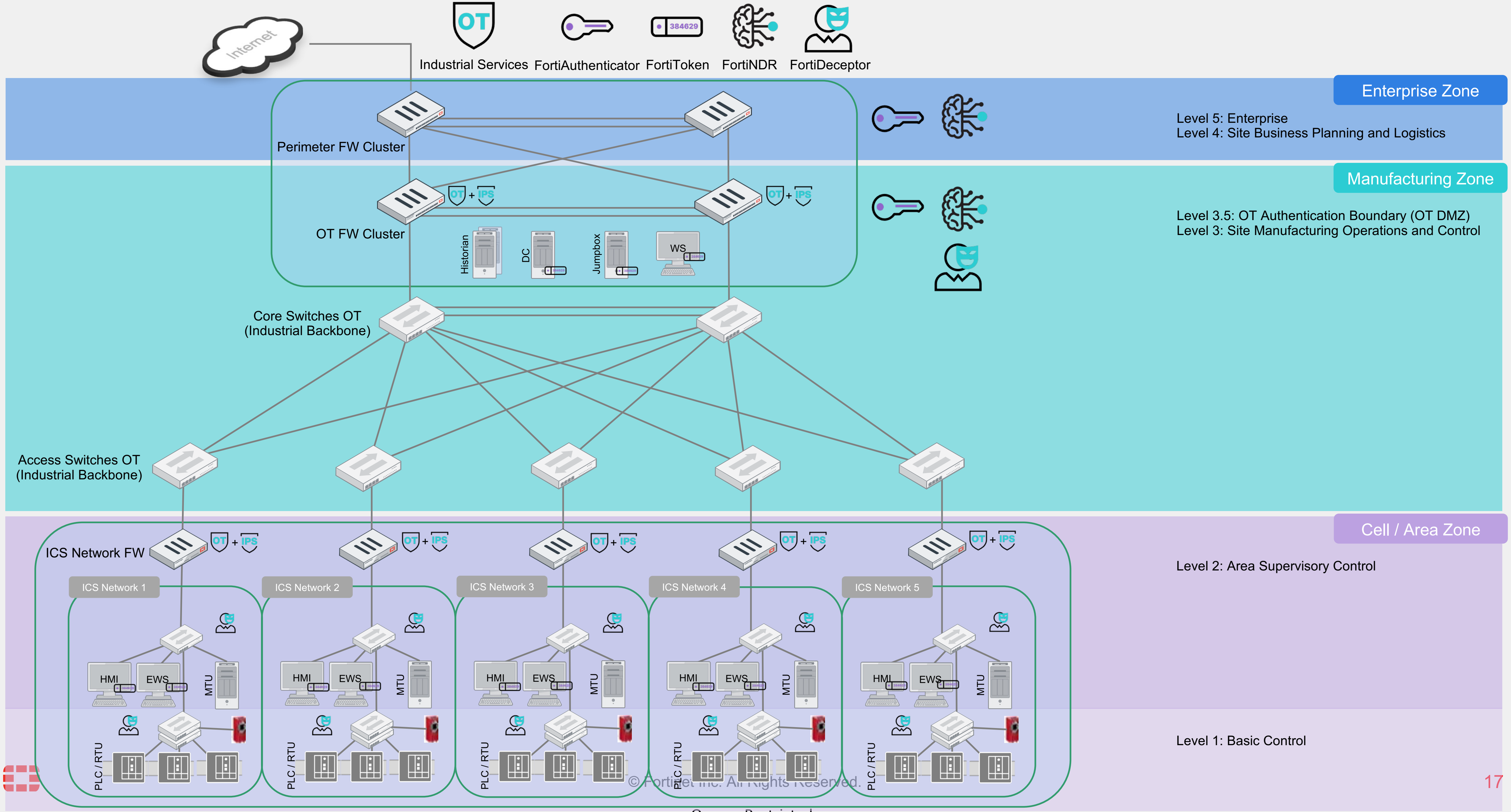




Secure SD-Branch Deployment



IEC 62443 and Micro-Segmentation - availability



Enterprise Zone

Level 5: Enterprise
Level 4: Site Business Planning and Logistics

Manufacturing Zone

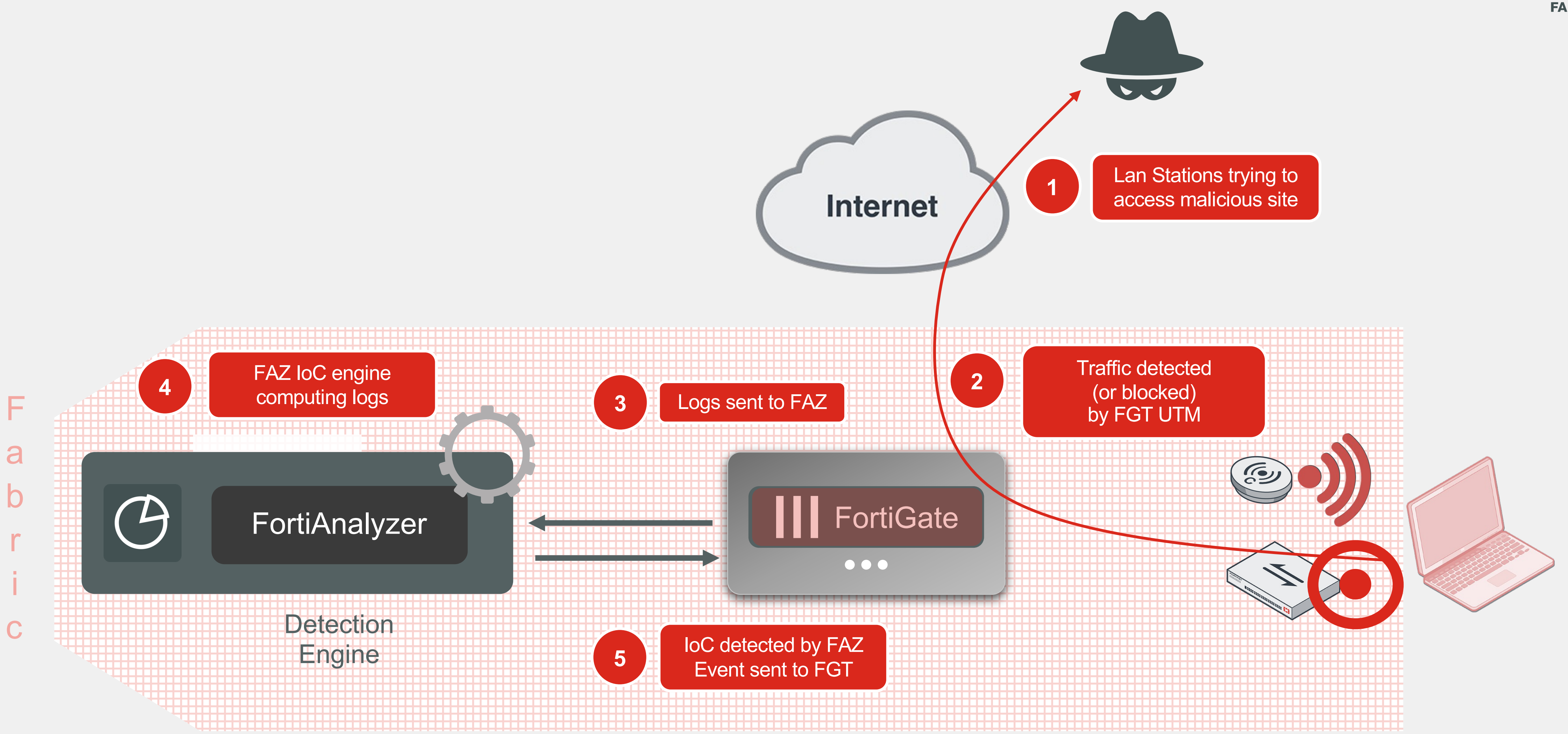
Level 3.5: OT Authentication Boundary (OT DMZ)
Level 3: Site Manufacturing Operations and Control

Cell / Area Zone

Level 2: Area Supervisory Control

Level 1: Basic Control

Fabric Use Case – Security Access



1 Lan Stations trying to access malicious site

2 Traffic detected (or blocked) by FGT UTM

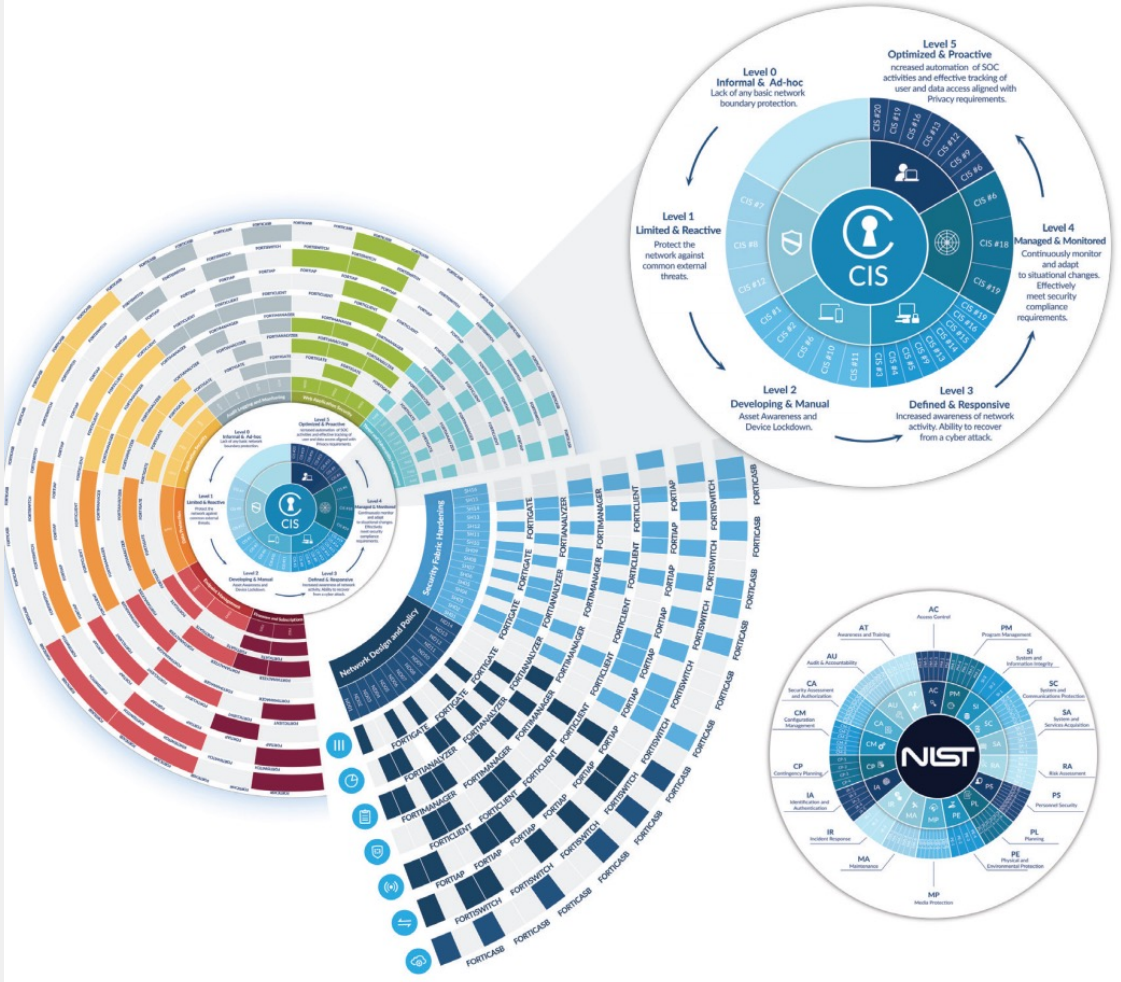
3 Logs sent to FAZ

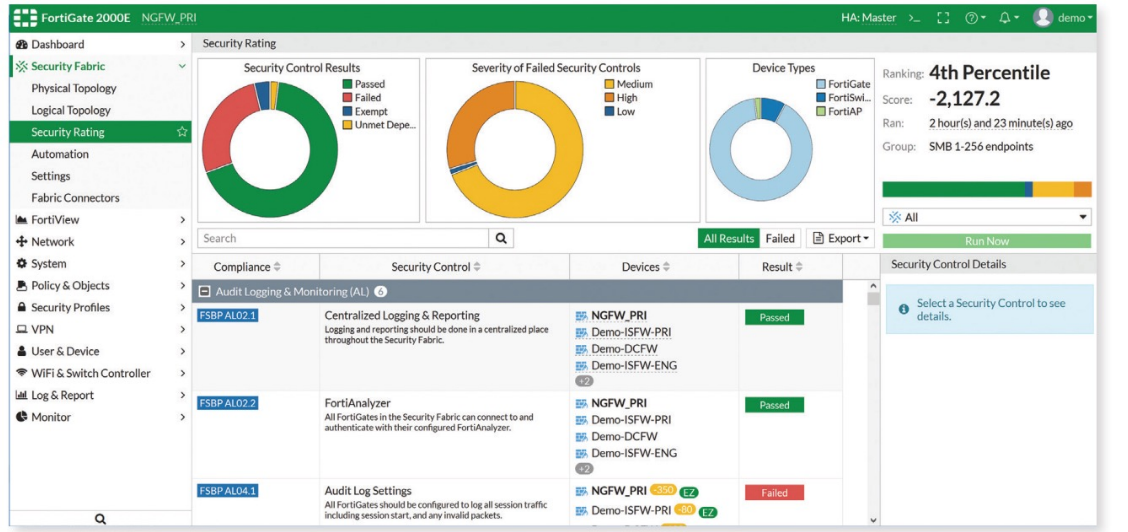
4 FAZ IoC engine computing logs

5 IoC detected by FAZ Event sent to FGT

Continious Monitoring & Mitigating Misconfiguration

Security Rating Services help CISO monitor NIST & CIS controls, (NIS2)


Level 0
Informal & Ad-hoc
Lack of any basic network boundary protection.
Level 1
Limited & Reactive
Protect the network against common external threats.
Level 2
Developing & Manual
Asset Awareness and Device Lockdown.
Level 3
Defined & Responsive
Increased awareness of network activity. Ability to recover from a cyber attack.
Level 4
Managed & Monitored
Continuously monitor and adapt to situational changes. Effectively meet security compliance requirements.
Level 5
Optimized & Proactive
ncreased automation of SOC activities and effective tracking of user and data access aligned with Privacy requirements.
CIS
CIS #20
CIS #19
CIS #16
CIS #13
CIS #12
CIS #9
CIS #6
CIS #18
CIS #15
CIS #14
CIS #5
CIS #4
CIS #3
CIS #11
CIS #10
CIS #2
CIS #1
CIS #8
CIS #7
Network Design and Policy
Security Fabric Hardening
FORTIGATE
FORTIANALYZER
FORTIMANAGER
FORTICLIENT
FORTIAP
FORTISWITCH
FORTICASB
NIST
AC
Access Control
AT
Awareness and Training
AU
Audit & Accountability
CA
Security Assessment and Authorization
CM
Configuration Management
CP
Contingency Planning
IA
Identification and Authentication
IR
Incident Response
MA
Maintenance
MP
Media Protection
PE
Physical and Environmental Protection
PL
Planning
PS
Personnel Security
RA
Risk Assessment
SA
System and Services Acquisition
SC
System and Communications Protection
SI
System and Information Integrity
PM
Program Management

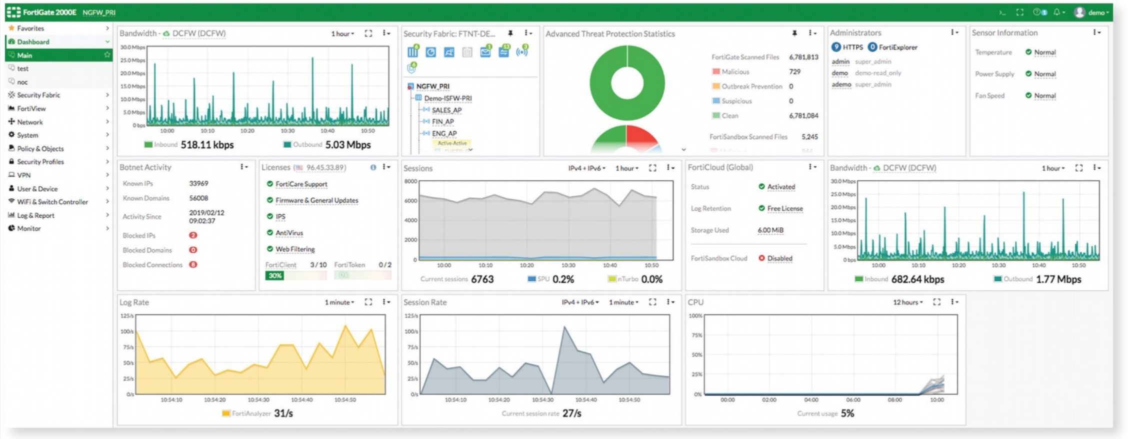


Security Rating

Ranking: 4th Percentile
Score: -2,127.2
Ran: 2 hour(s) and 23 minute(s) ago
Group: SMB 1-256 endpoints

Select a Security Control to see details.

Compliance	Security Control	Devices	Result
Audit Logging & Monitoring (AL) 6			
FSBP AL02.1	Centralized Logging & Reporting Logging and reporting should be done in a centralized place throughout the Security Fabric.	NGFW_PRI Demo-ISFW-PRI Demo-DCFW Demo-ISFW-ENG +2	Passed
FSBP AL02.2	FortiAnalyzer All FortiGates in the Security Fabric can connect to and authenticate with their configured FortiAnalyzer.	NGFW_PRI Demo-ISFW-PRI Demo-DCFW Demo-ISFW-ENG +2	Passed
FSBP AL04.1	Audit Log Settings All FortiGates should be configured to log all session traffic including session start, and any invalid packets.	NGFW_PRI -350 EZ Demo-ISFW-PRI -80 EZ	Failed



Open Ecosystem

500+ Best-in-class integrated solutions for comprehensive protection

Fabric Connectors	Fortinet-developed deep integration automating security operations and policies	aws, aruba (a Hewlett Packard Enterprise company), cisco, Google Cloud, IBM Cloud, Microsoft Azure, ORACLE, servicenow, Symantec.
Fabric APIs	Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions	ARISTA, ASAVIE, DELL, DRAGOS, EQUINIX, intel, SIEMENS Ingenuity for life, splunk>, TIGERA, tufin
Fabric DevOps	Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration	aws, Google Cloud, HashiCorp, Microsoft Azure, openstack., ORACLE, RED HAT ANSIBLE Automation, refactr, vmware
Extended Ecosystem	Integrations with threat sharing initiatives and other vendor technologies	CYBER THREAT ALLIANCE, MITRE, STIX, INTERPOL, OT CSA Firewalls, Switching, Wireless, Endpoint Security

Figures as of March 31, 2021
Note: Logos are a representative subset of the Security Fabric Ecosystem

Fortinet Security Fabric

Broad

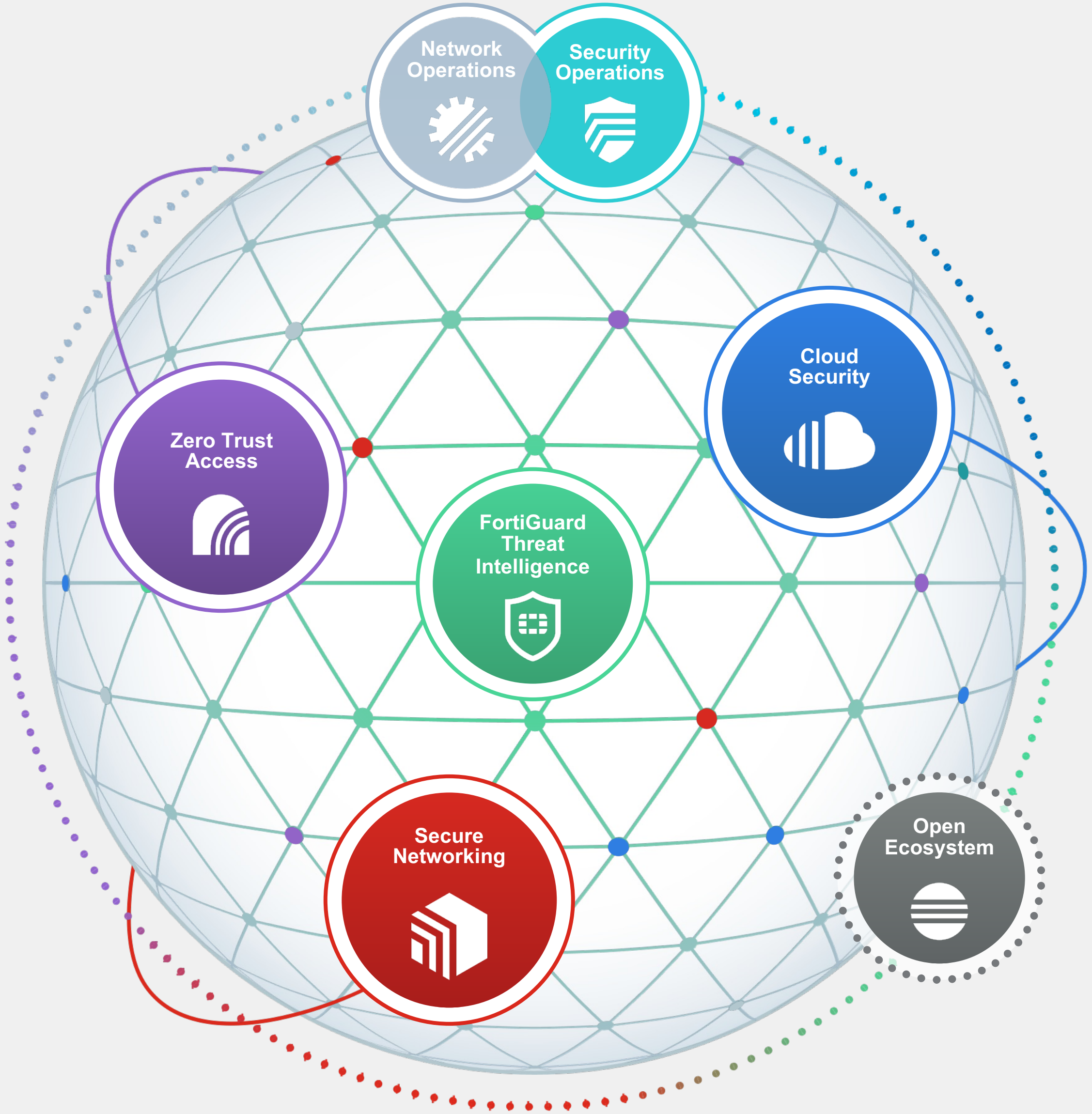
Visibility and protection of the entire digital attack surface to better manage risk

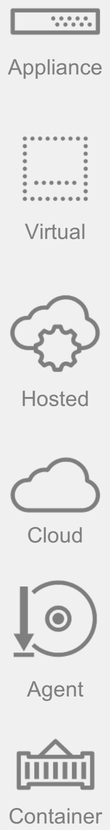
Integrated

Solution that reduces management complexity and shares threat intelligence

Automated

Self-healing networks with AI-driven security for fast and efficient operations





FORTINET®