Absicherung Ihrer OT Umgebung unter Einhaltung der Compliance Anforderungen

Benefits of OT Modernization

Data-driven business decisions

Increased Efficiency

Optimizing the critical resources of people and processes to do more with less

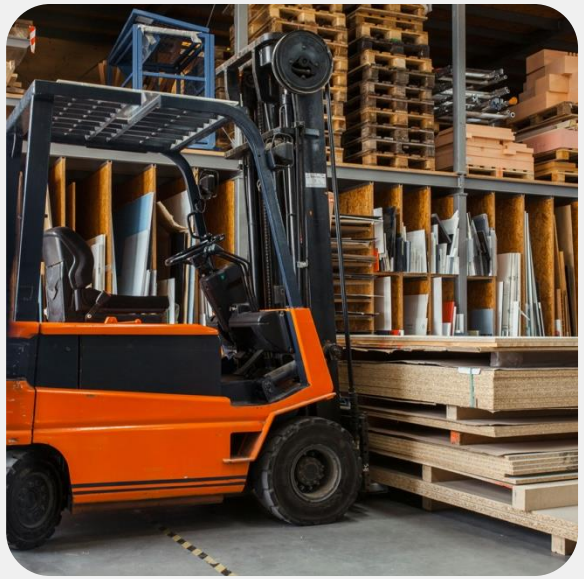
Lower Operational Costs

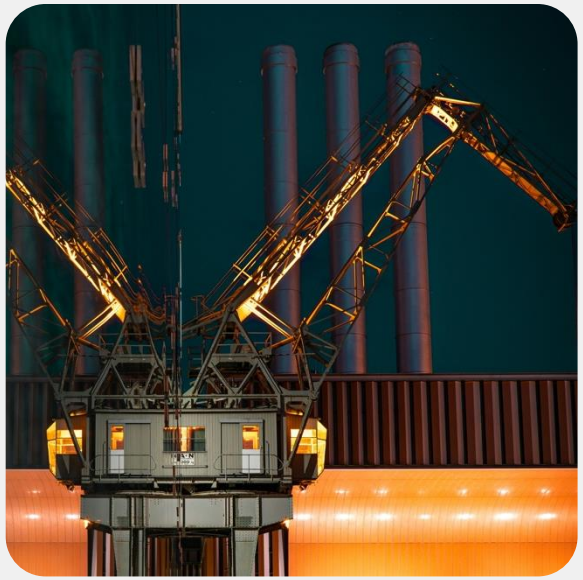
Competitive advantage of nimbleness, profitability and scalability

Real-time Decision Insight

Instantaneous ability to alter operations, leverage data and enable AI

Securing Operational Technology Challenges






Most industrial control systems lack security by design and are sensitive to change

The attack surface for cyber-physical assets is expanding, dependence on air-gap protection is diminishing

Digital transformation (Industry 4.0) initiatives driving IT-OT network convergence

Increasing adoption of new technologies, such as 5G, IIoT, and Cloud

Remote access requirements for third-parties and employees causing additional risks

Asset owners' reliance on OEMs and SIs exposes critical systems to additional risks

Manufacturing Industry Threat Landscape

Global Threats Detected
35.35bn

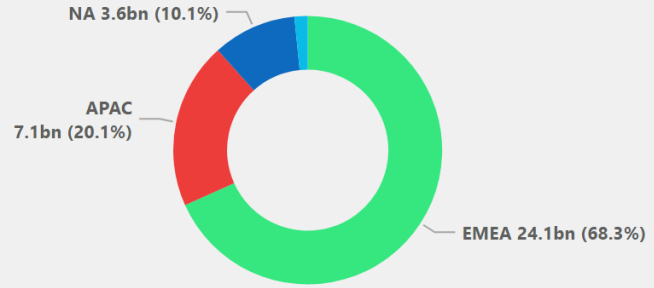
Exploit Techniques Detected (IPS)
29.26bn

Malware Distribution Detected (AV)
94.59M

Botnet Activity Detected (C2)
116.15M

Malicious Activity Distribution by Region

EMEA APAC NA LATAM



Cyber Kill Chain Model

Reconnaissance
- Crime as a Service DarkWeb

Weaponization

Delivery
- Drive by Download: 11.87M
- Mal Office Docs: 38.13M

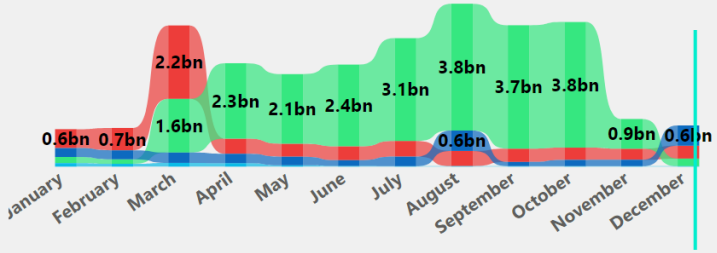
Exploitation
- DoublePulsar: 2.34bn
- IoT RCE: 332.70M

Installation
- Trojans: 52.00M
- CryptoMiner: 188.04K

Command & Control
- Andromeda: 36.11M
- XorDDOS: 120.26M

Action on Objectives
- Denial of Service Detected: 956.04M
- Ransomware Detected: 50.86K

Behavioral Trend Analysis by Region



- Active Scans Detected: 4.23bn

Energy & Utilities Threat Landscape

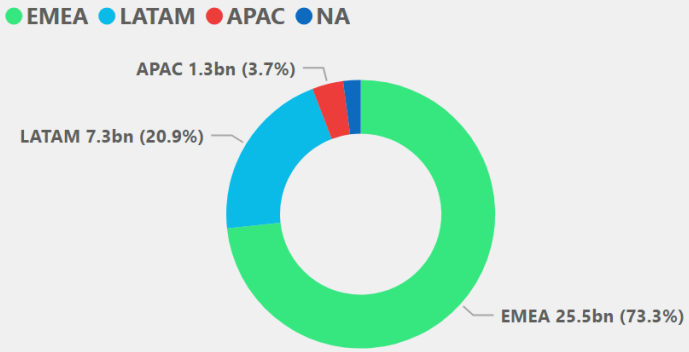
Global Threats Detected
34.84bn

Exploit Techniques Detected (IPS)
19.40bn

Malware Distribution Detected (AV)
25.57M

Botnet Activity Detected (C2)
240.24M

Malicious Activity Distribution by Region



Cyber Kill Chain Model

Reconnaissance

Weaponization
- Crime as a Service DarkWeb

Delivery
- Drive by Download: 8.27M
- Mal Office Docs: 5.12M

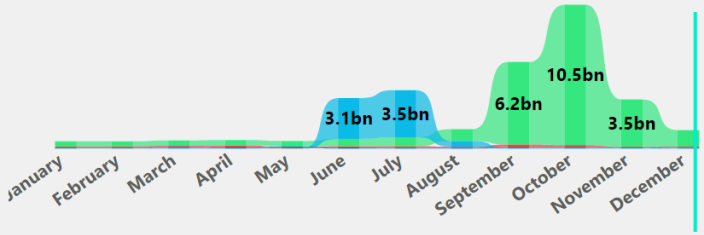
Exploitation
- DoublePulsar: 167.63M
- IoT RCE: 174.36M

Installation
- Trojans: 20.47M
- CryptoMiner: 9,968

Command & Control
- Andromeda: 9.56M
- IoT- MIRAI: 1.32M

Action on Objectives
- Denial of Service Detected: 1.70bn
- Ransomware Detected: 288.41K

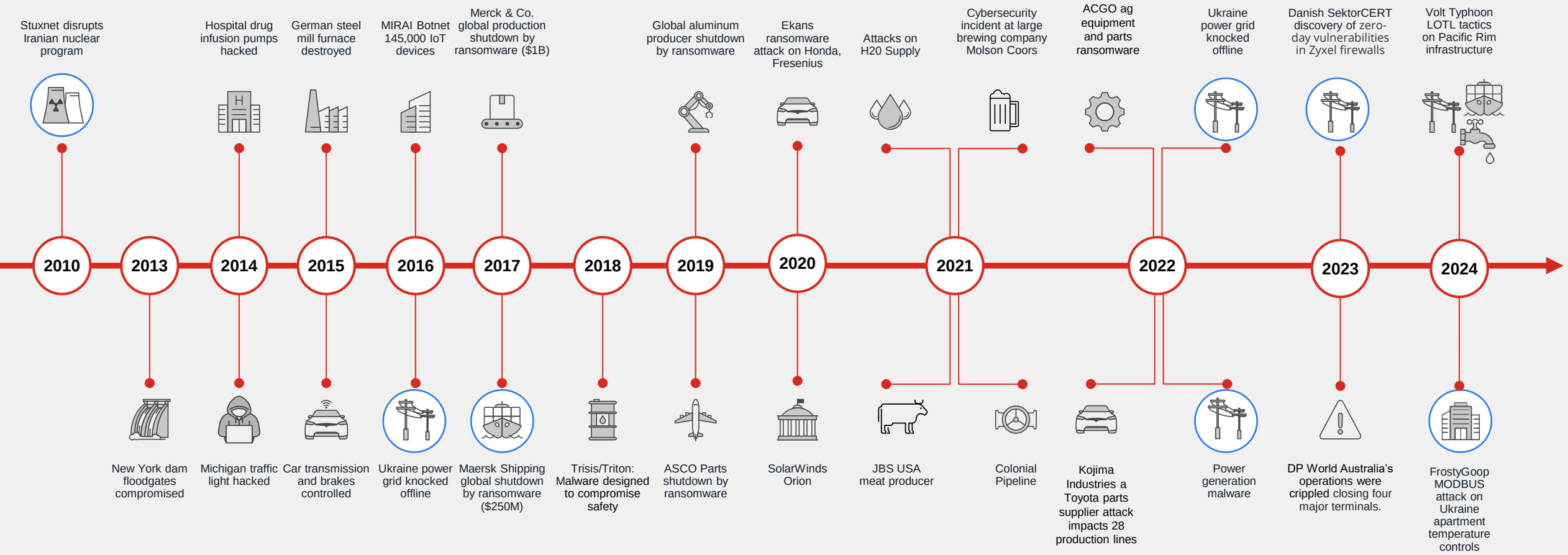
Behavioral Trend Analysis by Region



- Active Scans Detected: 13.25bn

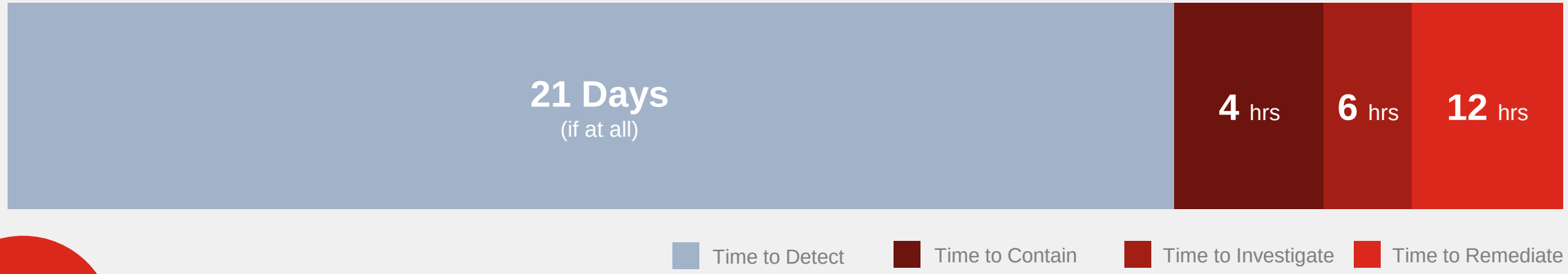
OT Infrastructure Attacks Are Getting Worse

Attacks are increasing in frequency and impact



When Attackers Get in, They Stay Longer and Cost You More

Average time from detection to remediation



52%

of organizations report SecOps is harder than two years ago, citing threats, attack surface, volume/complexity[1]

SEC Rule

4 Days

to disclose material of a cybersecurity incident

$9.4M

Avg breach cost

Source: Enterprise Strategy Group, 1. ESG Research, SOC Modernization Survey, January 2025.

NIS2-EU Rechtsakte

NEU: Umsetzungsempfehlungen seitens der EU

EU’s Cybersecurity Strategy: Scope der Workshops

EU’s Cybersecurity Strategy

Resilience Critical Entity Directive (RCE)
- **Scope: Critical Entities (KRITIS)**
- Resilienz, physische Security
- Critical Entity **Risk Assessment**

Cyber Security Act (CSA)
- **Scope:** Prozessrahmen zur Erstellung von EU Cybersecurity **Certification Schemes**
- Basis: EU-Common Criteria
- 2 Schemata: 5G, Cloud Services

§14

§24

NIS* 2 Directive
- **Scope: erweiterte KRITIS**
- **Risikomanagement** & Meldung
- techn. & org. Maßnahmen
- Stand der Technik
- Mehr Kooperation in der EU

?

?

Cyber Resilience Act (CRA)
- **Scope: Produkte mit digit. Elementen**
- **Risiko**: normal / kritisch / hoch kritisch
- Konformitätsbewertung & CE
- Prozesse Umgang Schwachstellen: Meldung & Patches mind. 5 Jahre

?

Digital Operational Resilience Act (DORA)
- **Scope: Finanzunternehmen**

Umsetzung der EU-Direktiven in nationales Gesetz, sowie Vorgaben für EU-Acts

RKE-Gesetz
- als nationale Umsetzung der EU-Richtlinie (RKE-RL)
- sieht Verpflichtungen und Strafbestimmungen vor
- Fokus auf Risikobewertung und BCM sowie organisatorische Maßnahmen

Netz- und Informationssystemsicherheitsgesetz 2024 (NISG2024)

- Änderungs- bzw. Artikelgesetz zu folgenden Gesetzten:

Telekommunikationsgesetz 2021

Gesundheitstelematikgesetz 2012


WKO
WIRTSCHAFTSKAMMER ÖSTERREICH
Die Finanzdienstleister

Sie wollen mehr Informationen?
Dann schauen Sie auch in unsere
Wissensdatenbank!
www.wko.at/wissensdatenbank oder
www.wko.at/wdb

Fachverband Finanzdienstleister
Bundessparte Information und Consulting
Wirtschaftskammer Österreich
Wiedner Hauptstraße 63 | 1045 Wien
T 05 90 900-4818
E finanzdienstleister@wko.at

Datum
13.3.2023

Digital Operational Resilience Act (DORA)

*** Network and Information Security /// Act = unmittelbar rechtskräftig /// Directive = Umsetzung in jeweiliges nationales Gesetz notwendig**

From NIS1 to NIS2: Changes in Terminology and Scoping

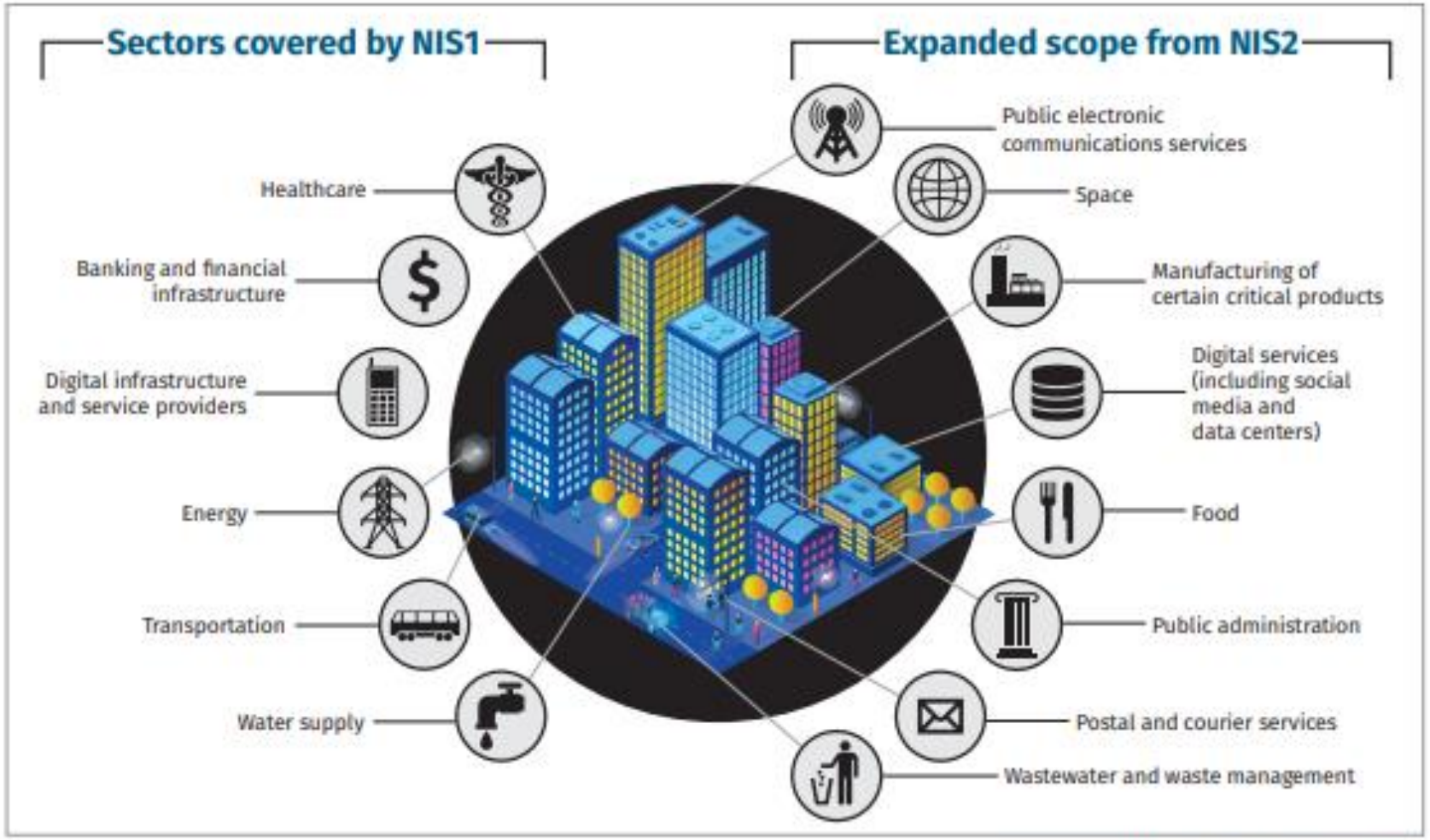


Figure 4. NIS2 In-Scope Sectors

Source: SANS NIS Implementation Guide
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-sans-enabling-nis-compliance-with-fortinet-ot.pdf

NIS 2.0 - 5 Pillars

Figure 12. Capabilities Within the NIS-D

- **Asset Management**
- **Access Control**
- **Network Segmentation**
- **Logging & Monitoring**
- **Risk Management**

Source: SANS NIS Implementation Guide
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-sans-enabling-nis-compliance-with-fortinet-ot.pdf

Pflichten für Betreiber (abgeleitet aus NIS2-EU §21)

Organisatorische Maßnahmen

- Sicherheitsvorgaben
- Incident Management
- Business Continuity
- Sicherheit in der Lieferkette
- Sicherheit im Life-Cycle
- Bewertung der Wirksamkeit
- Schulungen
- Sicherheit des Personals

Technische Maßnahmen

- Kryptografie
- Zugriffskontrolle
- Asset Management
- Multi-Faktor-Authentifizierung & kontinuierliche Authentifizierung
- Gesicherte Kommunikation
- Gesicherte Notfalls-kommunikationssysteme

Wie erreiche ich Compliance?

Anwendung von Normen und Richtlinien, Stand der Technik

(Inter-) Nationale Normen & Guidelines

Internationale Standards

Nationale Standards, Richtlinien

BDWE + OE + VSE Empfehlung für z.B. EVUs

Anforderungen an Einzelkomponenten, als Teil von Systemen und Anwendungen, inkl. Prozesse

- Scope Erweiterung: neu sind Lieferanten und Hersteller
- aktualisierte Normenanforderungen: Basis ist nun ISO/IEC 27002:2022, neu IEC 62443, BSI TR-03183, NIST SP 800-190
- Dokumentationsanforderungen: über den gesamten Lebenszyklus von Design, Betrieb und Wartung (u.a. System-/ Netz-architektur, Sicherheitspatches, SBOM, Log/Audit Meldungen, automatisiertes Auslesen von Geräte Parameter)
- Funktionstests: müssen nach einem Update automatisiert durchgeführt werden (Funktion ist vorzuhalten), bei kritischen Systemen ggf. durch ein zusätzliches, kundenspezifisches Testsystem
- Patch-Management: verpflichtend zu implementieren und während Betriebsphase durch ein Wartungsvertrag sicherzustellen
- Verschlüsselung: bei offensichtlichem Schutzbedarf per Default (z.B. Authentisierungsinformationen), nur anerkannte Verfahren aber Abweichungen mittels AG Freigabe möglich, Post-Quantum-Kryptographie beachten
- Neue, wesentliche Anforderungen:
  - Systeme zur Erkennung von Anomalien und Angriffen inkl. Dokumentation: Host & Netzwerk Monitoring, SIEM, Anomalieerkennung auf Basis von Baselining, Angriffserkennung auf Basis von IoCs, IPS nur nach Risikoanalyse (alles muss in die Zonenstruktur des AG)
  - Industrial IoT: Anbindung an OT über gesicherte Proxies, Krypto-Protokolle, Härtung der IoT-Komponenten, Update/Patch Management
  - Sicherheits- und Abnahmetests: erfolgen durch Auftragnehmer, Prüfkonfiguration muss von Auftraggeber kommen (abgestufte FAT/SAT)
  - Containervirtualisierung: getrennte Workspaces, Segmentierung / Separierung, Verwaltung, sichere Quellen inkl. Signaturen
  - granulare Zugriffskontrolle: Basissystem mit Admin & Bediener, Fernzugang mittels 2FA (AG kann fest vorgeben), 802.11X oder MAC
  - Cloud-Dienste: volle Kontrolle durch Betreiber, einschlägige Zertifikate und ggf. ergänzende Vereinbarungen

Recommended Best Practices for Technical Measures

Segmentation

Visibility & Compensating Controls

SOC & IR

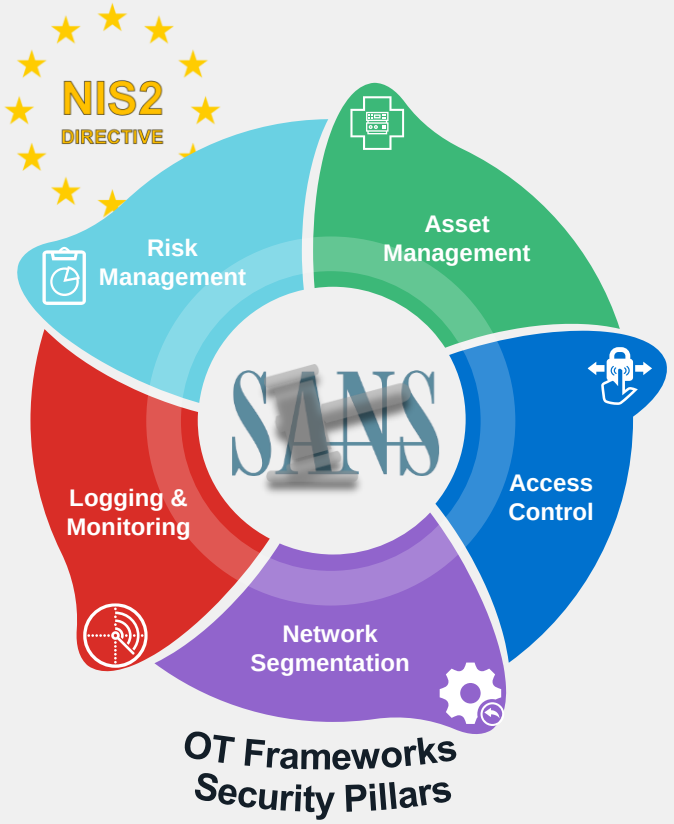
Platform Approach

OT threat intelligence

Safeguarding OT

A Technology Mapping for Compliance

Promoting an Integrated Security Platform for Automation, Orchestration, and **Compliance**



ISA | ISO | IEC

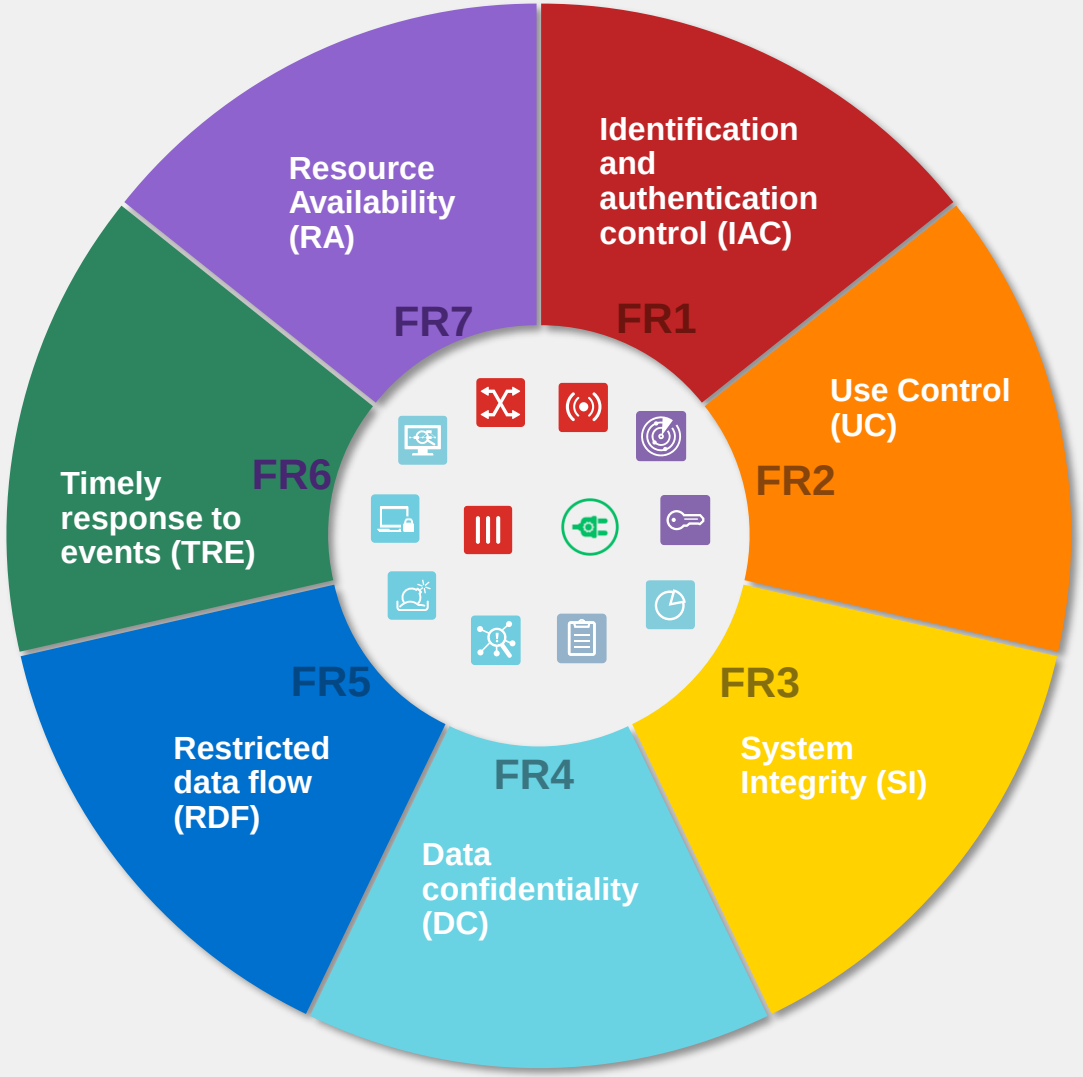
NERC North American Electric Reliability Corporation | NIST National Institute of Standards and Technology U.S. Department of Commerce | Center for Internet Security

Asset Management	SIEM	NAC	NGFW	API	
Access Control to Networks & Assets	NGFW	NAC	FAC	Client	Tokens
Segmentation, Protection & Response	NGFW	Switch	WIFI	XDR	Tokens
Events, Alerts and Incident Detection	SOAR	SIEM	Analyzer	SandBox	Deception
Risk Management	Manager	SIEM	Analyzer		

- Single Pane Management
- Threat Intelligence
- Interoperability

Fortinet Security Fabric and Compliance IEC 62443 Framework

Organizations can use IEC 62443 to strengthen their protection of ICS by using it as a framework to assess and mitigate ICS security vulnerabilities



1 FortiGate, FortiWiFi/FortiAP, FortiNAC FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSIEM

2 FortiGate, FortiWiFi/FortiAP, FortiNAC, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM

3 FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandobox, FortiSIEM, FortiTester, FortiResponder

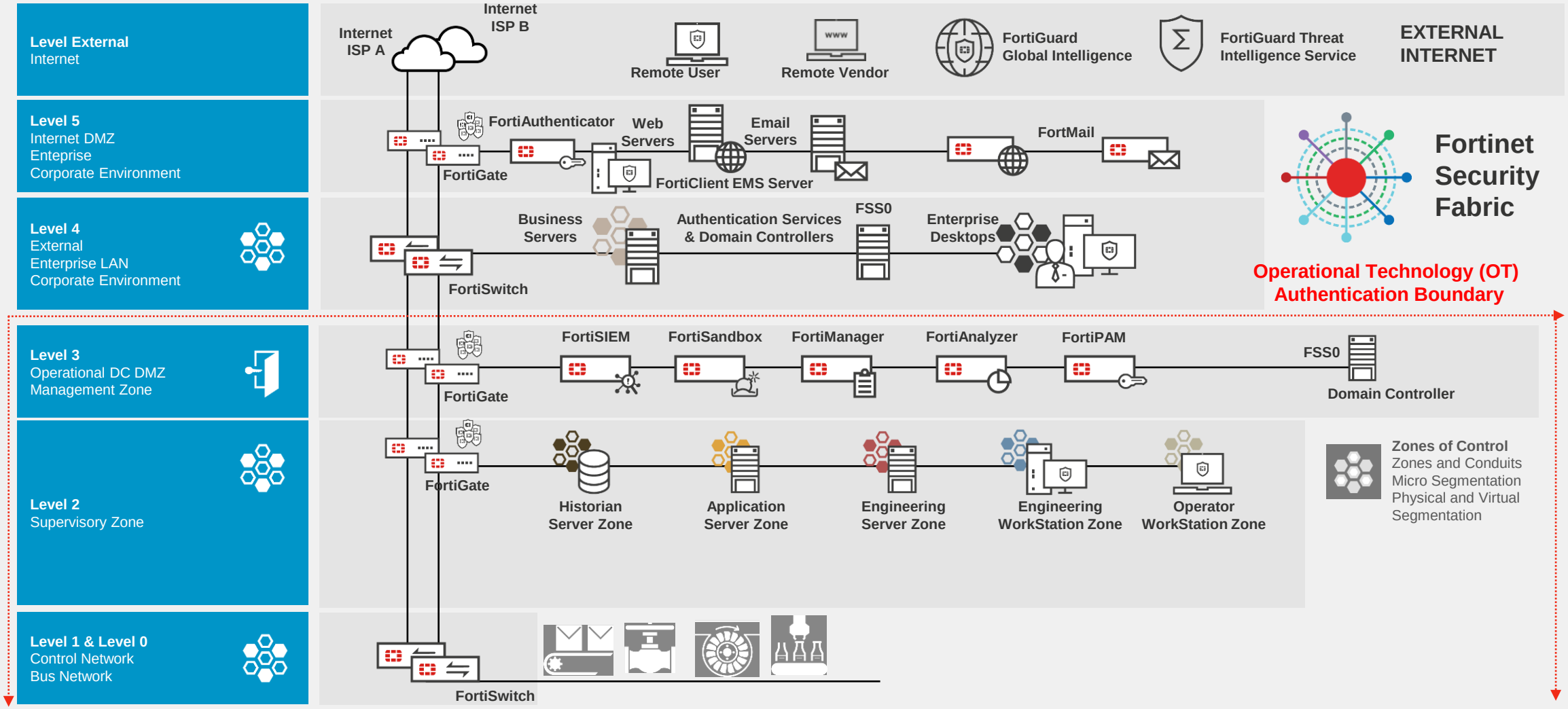
4 FortiGate, FortiSwitch, FortiAP, FortiEDR

5 FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer

6 FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiSIEM, FortiManager

7 FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions

IEC 62443 Compliant Solution Architecture



NIS2 Pflichten: Umsetzung durch FTNT & Partner

	Organisatorische Maßnahmen		Technische Maßnahmen
	FTNT Partner*	FortiGuard Services	Technical Products **
• **Sicherheitsvorgaben:** Risikoanalyse	x		
• **Incident management**	x	x	x
• **Aufrechterhaltung des Betriebs**	x		
• **Sicherheit in der Lieferkette**	x		
• **Maßnahmen im Lebenszyklus**	x		
• **Bewertung der Wirksamkeit**	x	x	x
• **Cyberhygiene und Schulungen**	x		
• **Kryptografie**			x
• **Personal**	x		
• **Zugriffskontrolle**	x		x
• **Asset Management**	x		o
• **Multi-Faktor-/Kontinuierliche Authentifizierung**			x
• **Gesicherte Kommunikation**			x
• **Gesicherte Notfallkommunikationssysteme**			x

* PS – Professional Service der Fortinet

** incl. FortiCare Services with Deployment & Operational Assistance (Advanced Services)

FTNT Portfolio: The Broadest Platform in Cybersecurity

Secure Networking

FortiGate
NGFW with ASIC acceleration and industry leading Convergence

FortiSwitch
Protected Ethernet connectivity via Secure Networking convergence with FortiGate

FortiAP
Protected Wi-Fi connectivity via Secure Networking convergence with FortiGate

FortiManager
Centralized management of your Fortinet security infrastructure

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiGate Cloud
SaaS platform offering zero-touch deployment, network management and security analytics

FortiEdge Cloud
Cloud management for standalone LAN, WLAN and 5G gateway equipment

FortiAIOps
AI based insights for rapid analysis and remediation of network issues

FortiFone
Robust IP phones and softclient to stay connected from anywhere

FortiVoice
Unified communications with secure voice, chat, conferencing, and fax

FortiCamera
Physical security with intelligent motion detection in any light condition

FortiRecorder
Secure NVR with smart AI analysis and centralized visibility

FortiConverter
Secure and automated firewall migration from a broad spectrum of vendors

FGaaS
Hardware as a service for FortiGate

Unified SASE

SASE

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiClient EPP Agent
Endpoint Protection Agent with AV, URL and Sand-box

FortiClient ZTA Agent
Remote access, application access, and risk reduction

FortiSASE
Cloud-delivered Security Services Edge

FortiProxy
Enforce internet compliance and granular application control

FortiMonitor
SaaS based DEM platform, performance monitoring

FortiCASB
Prevent misconfigurations of SaaS apps and meet compliance

CLOUD

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate CNF
Hosted cloud-native firewall for simplified cloud network security

FortiWeb
Prevent web application attacks against critical web assets

FortiADC
Application-aware intelligence for distribution of application traffic

FortiGSLB
Ensure business continuity during unexpected network downtime

FortiDDoS
Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiFlex
Flexible daily usage-based consumption licensing for a broad catalog of solution

FortiPoints
Simplified, flexible licensing for annual contracts, renewals, upgrades, and co-terms

Security Operations

FortiAnalyzer
Security Fabric log management, monitoring and response

FortiMail
AI-powered, protection against email-borne threats

FortiSIEM
Enterprise-wide monitoring, threat detection, and response

FortiSandbox
AI-powered real-time protection against unknown and 0-day threats

FortiEDR/XDR
Automated endpoint protection and correlated incident response

FortiToken
Cloud/HW/Mobile MFA provide passwordless adaptive authentication

FortiSOAR
Automated security operations, investigation, and response

FortiAuthenticator
Centralized identity and access management solution

FortiNDR
AI-driven analysis to detect and respond to threats

FortiGuard MDR Service
Managed threat detection, investigation, and response

SOCaaS
Continuous security monitoring, incident triage, and escalation

FortiRecon
Proactive digital risk protection service and external/internal threat monitoring

IR Services
Rapid detection, containment, and recovery of cyberattacks

FortiPAM
Privileged identity and access management, and session monitoring

FortiDeceptor
Active deception platform for early in-network attack detection and response

FortiTester
Network performance testing and breach attack simulation (BAS)

FortiTrust Identity
Identity and Access Management as a Service (IDaaS)

FortiDevSec
Orchestrated and automated continuous application security testing

FortiGuest
Access management solution for temporary access to guests and visitors

FortiDAST
Automated black-box dynamic application security testing

FortiCNAPP
Secure code to cloud with a single, data-driven platform

FortiScanner Cloud
Cyber Asset Attack Surface Management Service

FortiNextDLP
Endpoint DLP and Insider Risk management

FortiAI
Integrated GenAI Assist for SOC and NOC

OT Security Platform

OT Security Service
FortiGuard subscription for FortiGate NGFW enables protection against OT-specific threats

Ruggedized Products
Rugged NGFW, switch, AP, and 5G extenders provide secure connectivity in harsh outdoor environments

FortiSRA
Agentless secure remote access offers robust remote access control, management, session logging, monitoring, and recording

SecOps for OT
Advanced cybersecurity controls bring OT networks into the SOC and incident response plans

Open Ecosystem

FNDN
Advanced tools for Fortinet community to develop custom solutions

Fabric Connectors
Fortinet-developed integrations for automation and security

Fabric API
Partner-developed integrations for end-to-end visibility and protection

DevOps Tools
Community-driven scripts automate network/security tasks

Extended Ecosystem
Integrates with third-party systems and orgs for sharing threat-intel

Resources

Product Matrix
Specifications for top selling models

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
Fortinet is committed to training over 1 million people by 2025

Free Assessment
Perform an assessment in your network to validate your existing controls

FortiOS
The Heart of the Fortinet Security Fabric

FortiCare
Support and mitigation services

AI-Powered FortiGuard Security

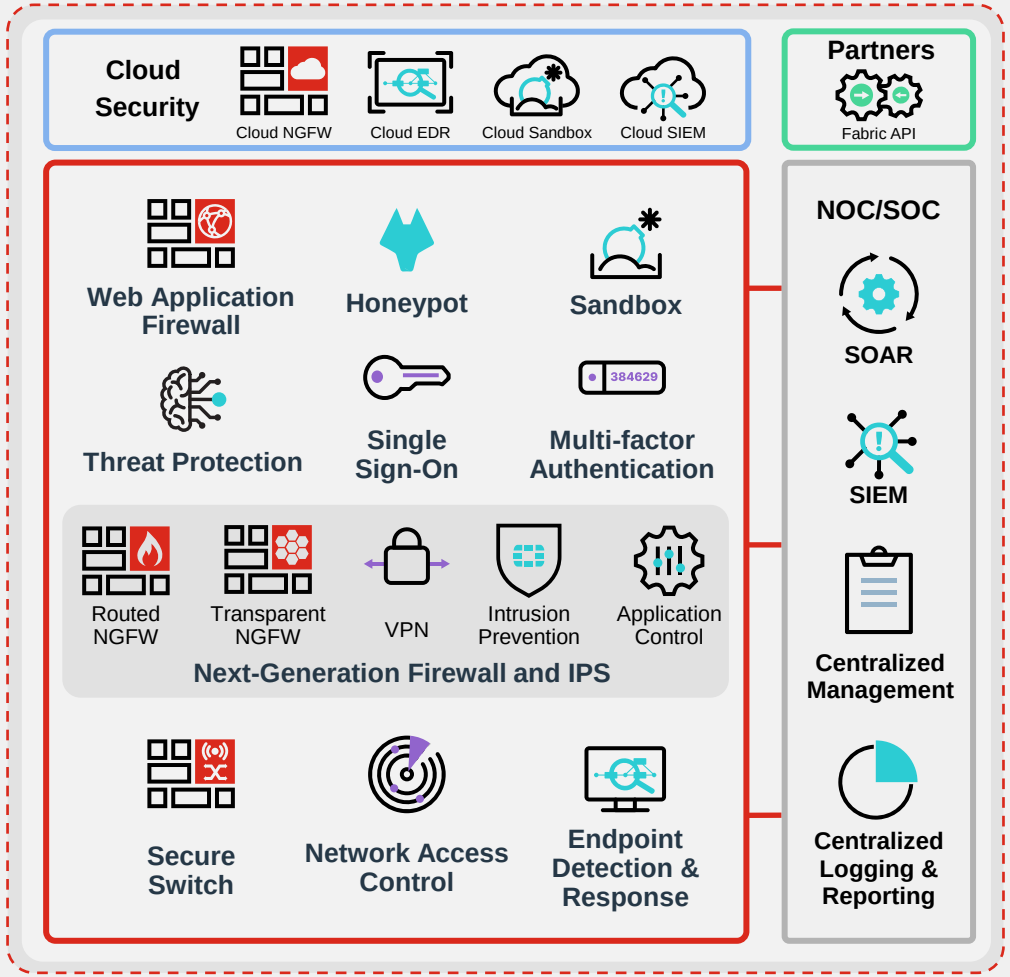
- Web Filtering
- IPS
- AV
- Sandbox
- IL MPS
- Application Control
- Attack Surface
- DLP
- OT Security Services
- IoC
- IL CASB

Fortinet Securing the IT & OT

- Network Segmentation
- Network Microsegmentation
- Network Access Control
- Web Services Security
- Secure Remote Access
- Threat Protection
- Application Control
- Endpoint Security
- Honeypot
- Sandbox
- NOC/SOC

	Levels		
Cloud & External Zones		External Networks	Internet, Cloud, VPN
Major Enforcement Boundary		5.5	Information Technology (IT) Boundary
Business & Enterprise Zones	5	Enterprise Network	Corporate Systems & Networks
	4	Business Planning & Logistics	Site Systems & Networks
Major Enforcement Boundary		3.5	Operational Technology (OT) Boundary
Operations & Control Zones	3	Operations & Control	Simulation, Engineering, Test
Minor Enforcement Boundary		2.5	Industrial Control System (ICS) Boundary
Process Control Zones	2	Area Supervisory Control	HMIs, Historians
	1	Basic Control	PLCs, RTUs, IEDs
	0	Process	Actuators, Sensors
Major Enforcement Boundary		Air-gap / Safety Related Control Systems Boundary	
Safety Zone	S	Safety	Safety Instrumented System

Fortinet Security Fabric



Boundary: Demilitarized Zone (DMZ), Security Conduit
Zones: Security Zones
IPS: Intrusion Prevention System
SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response

Anforderungen an Risikomanagement, Melde-, Registrierungs-, Nachweis und Unterrichtungspflichten

NIS2UmsuCG: neu §30 (Scope: besonders wichtige Einrichtungen & wichtige Einrichtungen)

§ 30 BSIG: Risikomanagementmaßnahmen (an den Scope)

(2) **Maßnahmen** nach Absatz 1 **sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen**. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management & Wiederherstellung nach einem Notfall, & Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit,
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Anforderungen an Risikomanagement, Melde-, Registrierungs-, Nachweis und Unterrichtungspflichten

NIS2UmsuCG: neu §30 (Scope: besonders wichtige & wichtige Einrichtungen)

§ 30 BSIG: Risikomanagementmaßnahmen (des Scopes)

(6) Besonders wichtige Einrichtungen und wichtige Einrichtung dürfen durch Rechtsverordnung nach § 56 Absatz 3 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen.

Certifications by Fortinet, via trust.fortinet.com

ISO/IEC 15408

ISO/IEC 27001

Use Case Ia: NIS2-EU Durchführungsrechtsakt

Fokus des Use Cases „Network Segmentation (Chapter 6.8)“

6.8.1. The relevant entities shall segment systems into networks or zones in accordance with the results of the risk assessment referred to in Chapter 2.1. They shall segment their systems and networks from third parties' systems and networks.

6.8.2. For that purpose, the relevant entities shall:

(a) consider the functional, logical and physical relationship, including location, between trustworthy systems and services;

(b) grant access to a network or zone based on an assessment of its security requirements;

(c) keep systems that are critical to the relevant entities operation or to safety in secured zones;

(d) deploy a demilitarized zone within their communication networks to ensure secure communication originating from or destined to their networks;

(e) restrict access and communications between and within zones to those necessary for the operation of the relevant entities or for safety;

(f) separate the dedicated network for administration of network and information systems from the relevant entities operational network;

(g) segregate network administration channels from other network traffic;

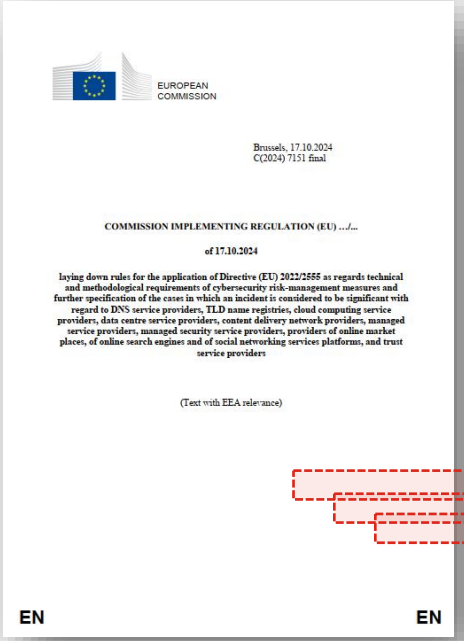
(h) separate the production systems for the relevant entities' services from systems used in development & testing, including backups.

6.8.3. …

Quelle: Brussels, 17.10.2024 C(2024) 7151 final, ANNEX to the Commission Implementing Regulation

Use Case Ia: NIS2-EU Durchführungsrechtsakt

Schritte: Umsetzung „Network Segmentation (Chapter 6.8)“



EUROPEAN COMMISSION

Brussels, 17.10.2024
C(2024) 7151 final

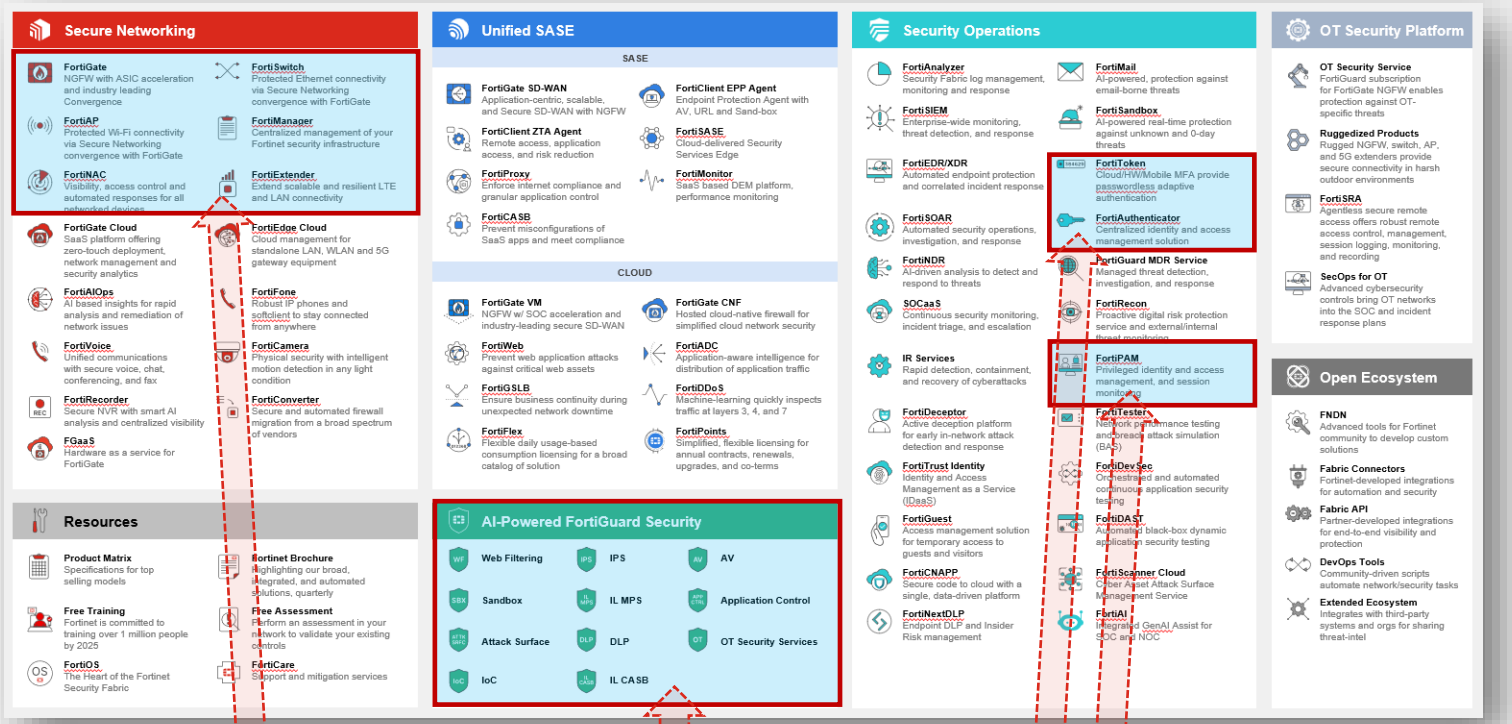
COMMISSION IMPLEMENTING REGULATION (EU) .../...

of 17.10.2024

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

EN EN



segmentation & separation

restrict communications

(privileged) access management

Use Case Ic: Whitepaper BDWE + OE + VSE

Schritte: IT/OT Sicherheitsanforderungen für Prozesssteuerungen in der Energieversorgung

oesterreichs energie.

VSE AES

bdew
Energie. Wasser. Leben.

BDEW Bundesverband
der Energie- und
Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin

Österreichs E-Wirtschaft
Brahmsplatz 3
1040 Wien
Österreich

Verband Schweizerischer
Elektrizitätsunternehmen
Hintere Bahnhofstrasse 10
5000 Aarau
Schweiz

Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

Vollständig überarbeitete Version 3.0 09/2024:

Aarau/Berlin/Wien, 30. September 2024

www.oesterreichsenergie.at www.strom.ch www.bdew.de

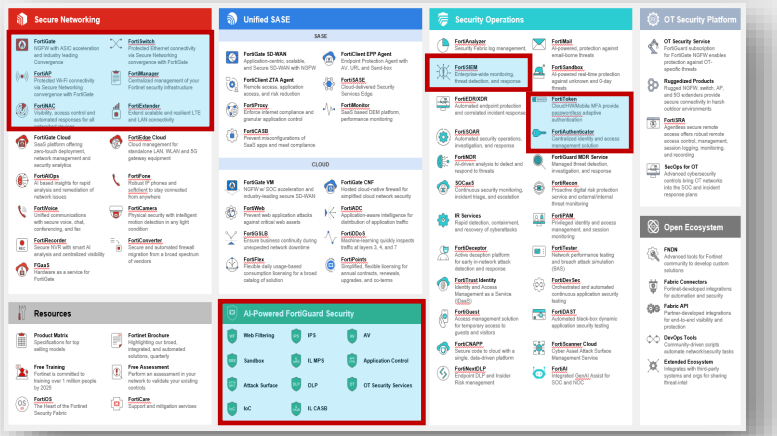
segmentation & separation

restrict communications

(privileged) access management

Ausgewählte Sicherheitsanforderungen:

- Definition einer Zonenstruktur durch AG mittels Segmentierung durch Firewalls
- Anbindung von IoT mittels Proxies
- Host & Netzwerk Monitoring mit freigegebenen Tools (Kompatibilitätsmatrix z.B. Siemens)
- Einsatz eines SIEM (Nutzung von Indicators of Compromise - IoC)
- granulare Zugriffskontrolle (2FA, IEEE 802.X oder MAC)



Use Case IIa: NIS2-EU Durchführungsrechtsakt

Produktauswahl bzgl. Umsetzung „Monitoring & Logging“ (Chapter 3)

3.1. Incident handling policy

3.2. Monitoring and logging

3.2.1. The relevant entities shall lay down procedures and use tools to monitor and log activities on their network and information systems to detect events that could be considered as incidents and respond accordingly to mitigate the impact.

3.2.2. To the extent feasible, monitoring shall be automated and carried out either continuously or in periodic intervals, subject to business capabilities. The relevant entities shall implement their monitoring activities in a way which minimizes false positives and false negatives.

3.2.3. Based on the procedures referred to in point 3.2.1., the relevant entities shall maintain, document, and review logs. The relevant entities shall establish a list of assets to be subject to logging based on the results of the risk assessment carried out pursuant to point 2.1. Where appropriate, logs shall include: …

3.2.4. The logs shall be regularly reviewed for any unusual or unwanted trends. Where appropriate, the relevant entities shall lay down appropriate values for alarm thresholds. If the laid down values for alarm threshold are exceeded, an alarm shall be triggered, where appropriate, automatically. The relevant entities shall ensure that, in case of an alarm, a qualified and appropriate response is initiated in a timely manner.

3.2.5. The relevant entities shall maintain and back up logs for a predefined period and shall protect them from unauthorized access or changes.

3.2.6. To the extent feasible, the relevant entities shall ensure that all systems have synchronized time sources to be able to correlate logs between systems for event assessment. The relevant entities shall establish and keep a list of all assets that are being logged and ensure that monitoring and logging systems are redundant. The availability of the monitoring and logging systems shall be monitored independent of the systems they are monitoring.

3.2.7. The procedures as well as the list of assets that are being logged shall be reviewed and, where appropriate, updated at regular intervals and after significant incidents.

3.3. Event reporting

3.4. Event assessment and classification

3.5. Incident response

3.6. Post-incident reviews

Quelle: Brussels, 17.10.2024 C(2024) 7151 final, ANNEX to the Commission Implementing Regulation

Use Case IIa: NIS2-EU Durchführungsrechtsakt

Produktauswahl bzgl. Umsetzung „Incident Response“ (Chapter 3)

3.1. Incident handling policy

3.2. Monitoring and logging

3.3. Event reporting

3.4. Event assessment and classification

3.5. Incident response

3.5.1. The relevant entities shall respond to incidents in accordance with documented procedures and in a timely manner.

3.5.2. The incident response procedures shall include the following stages:

(a) incident containment, to prevent the consequences of the incident from spreading;

(b) eradication, to prevent the incident from continuing or reappearing,

(c) recovery from the incident, where necessary.

3.5.3. The relevant entities shall establish communication plans and procedures:

(a) with the CSIRTs or, where applicable, the competent authorities, related to incident notification;

(b) for communication among staff members of the relevant entity, and … with relevant stakeholders external to the relevant entity.

3.5.4. The relevant entities shall log incident response activities in accordance with the procedures referred to in point 3.2.1., and record evidence.

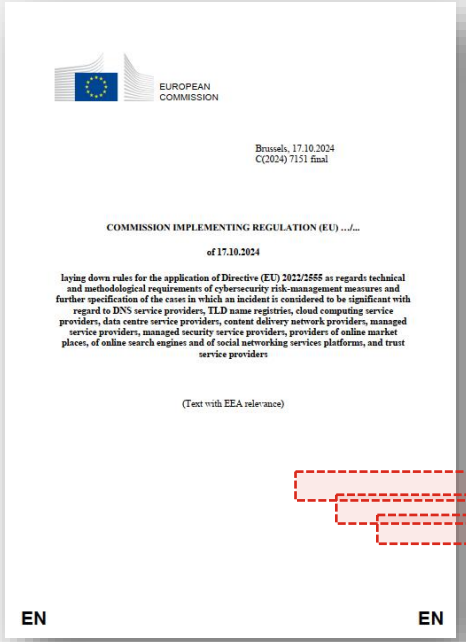
3.5.5. The relevant entities shall test at planned intervals their incident response procedures.

3.6. Post-incident reviews

Quelle: Brussels, 17.10.2024 C(2024) 7151 final, ANNEX to the Commission Implementing Regulation

Use Case II: NIS2-EU Durchführungsrechtsakt

Produktauswahl bzgl. Umsetzung „Incident handling (Chapter 3)“



EUROPEAN COMMISSION

Brussels, 17.10.2024
C(2024) 7151 final

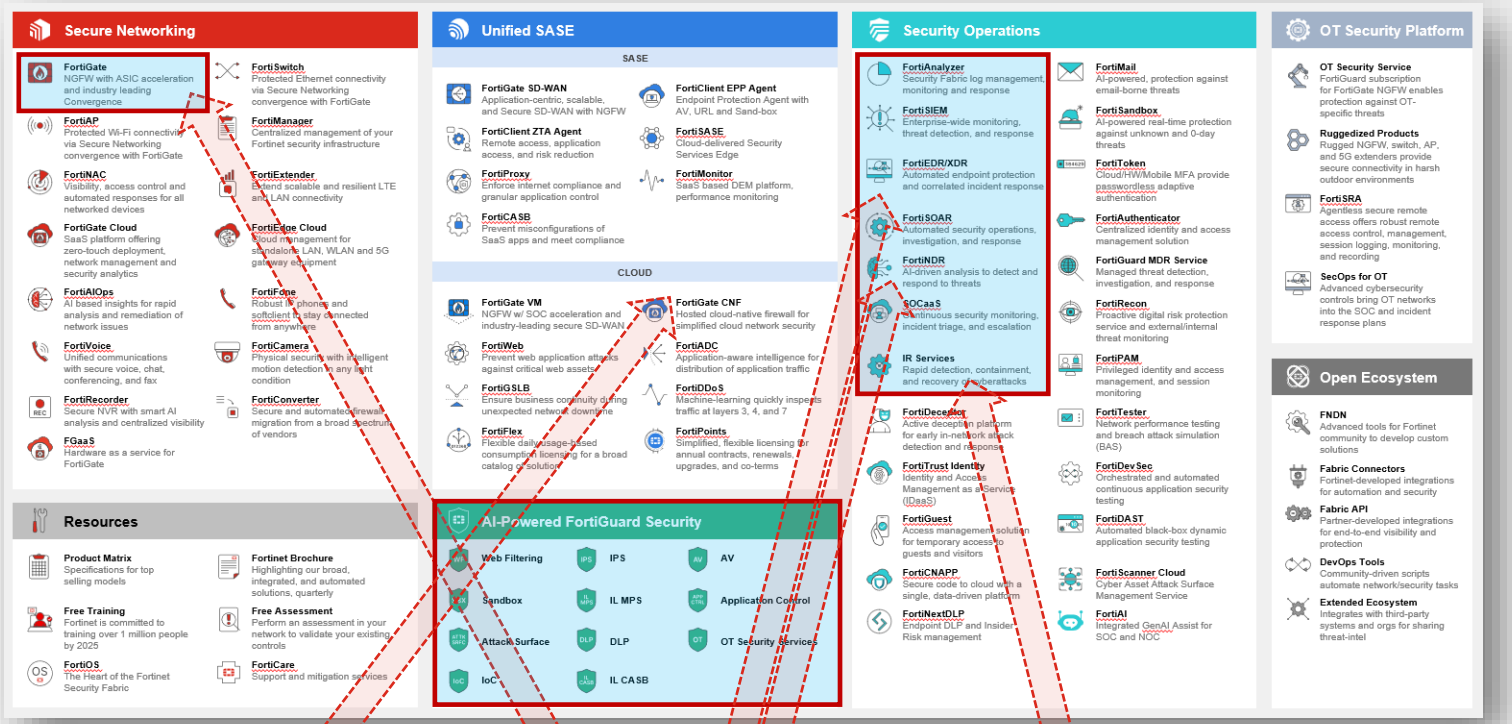
COMMISSION IMPLEMENTING REGULATION (EU) …/…

of 17.10.2024

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

EN EN



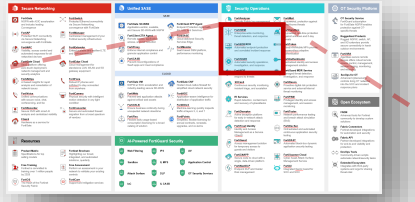
automated alarm management

automated, continuously monitoring (MSSP)

incident response components & services*

Solution: FortiSOAR

A leader in the KuppingerCole
2023 SOAR Leadership Compass



incident response components & services*

Connect anything – automate everything

500+ integrations, 800+ playbooks for SOC/NOC/OT

Security incident management

Automated features from investigation through response

Threat Intelligence management

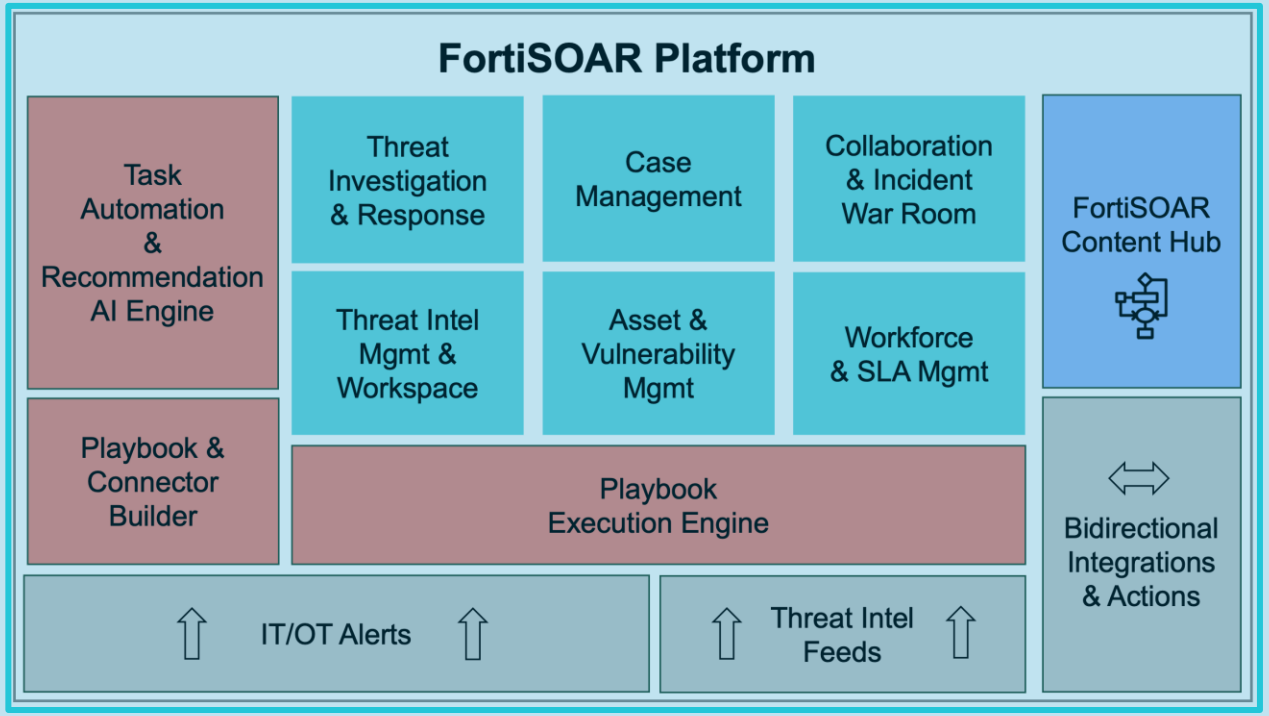
Powered by FortiGuard Labs and any source

Automated & intelligent analyst support

AI Assistant and Recommendation Engine drive results

No/low-code playbook creation

Patented development modes for any user & workflow



Centralize, automate, and optimize SOC, NOC, enterprise/MSSP operations

AI-based SOAR features

Generative AI assistant for investigation, response, playbook building, and more

Incident Management

Threat Intelligence Management

Playbook Creation

Vulnerability Management

Asset Visibility & Risk Management

View and track IT/OT asset inventory and complete asset security status
Enrich and prioritize threat investigation activities

- Asset criticality and risk-based alert & vulnerability views
- Flexible view alignments including OT Purdue model
- Asset mgmt system 2-way integrations

Dashboard displays include:

- Asset criticality, alert & vulnerability status
- Alerts by asset, by zone, by asset class
- MITRE IT/OT ATT&CK views

Compliance Automation

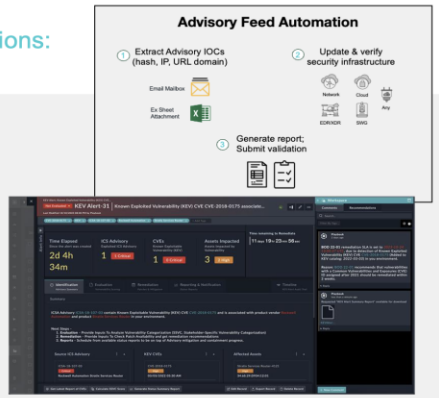
Automate processing of advisory feeds
Complete Solution Packs for specific regulations:
NIST, GDPR, CISA BOD 22-01, …

Advisory Feed Automation

- Process communication & extract IOCs (email, spreadsheet, other)
- Execute proper updates across infrastructure
- Generate compliance report

Regulatory Compliance

- Solution Packs for importing required intel feeds, specific action playbooks, tracking dashboards, reports and more



FortiSOAR for OT

Monitor OT assets and risk levels
Respond immediately to OT alerts
Protect OT assets from outside attack

- Integrated OT security & ecosystem products
- OT threat intel feeds and management
- Unified IT/OT workflows with MITRE ATT&CK ICS mapping
- Complete asset & risk views w/Purdue Model
- OT-specific remediation playbooks

NOZOMI NETWORKS, CLAROTY, everbridge, SCADAfence, ARMIS, DRAGOS, Microsoft Sentinel

Integrations across multi-vendor IT/OT security products and OT specialty solutions

How to Break the Attack Sequence

	Pre-Attack		Attack				
	Recon	Weapon	Delivery	Exploit	Installation	C&C	Action
Products and Solutions	FortiRecon FortiDeceptor	FortiRecon FortiDeceptor	FortiGate (HW/VM/CN/SASE) FortiProxy FortiClient FortiEDR FortiADC FortiWeb FortiNDR AV+ANN FortiMail FortiCASB FortiCWP FortiSandbox	FortiGate (HW/VM/CN/SASE) FortiProxy FortiClient FortiEDR Defuse compromised endpoint FortiADC FortiWeb Web application FortiDeceptor Threat detection, analysis, and response FortiSIEM UEBA	FortiGate (HW/VM/CN/SASE) FortiClient FortiEDR Defuse exploit FortiDeceptor Defuse Lateral Movement FortiCWP FortiSIEM UEBA	FortiGate (HW/VM/CN/SASE) FortiClient FortiEDR Defuse compromised endpoint FortiNDR FortiSIEM UEBA	FortiAnalyzer Event handlers & reports FortiSIEM Rules Engine & Threat Hunting FortiSOAR Playbooks IOC Threat hunting Outbreak Detection ZTNA Auto tagging FortiClient Endpoint search FortiEDR|XDR FortiDeceptor Threat intelligence, & attack isolation
FGD AI-Powered Security		Credential Stuffing Prevention Service	Anti-malware, AV pre-Filter, SBX, Endpoint Vulnerability Protection, App Control, IL CASB, Credentials AV, IL SBX, IL CASB	IPS, Application, FW, IOT, OT IPS, IoT, OT	URL, AV URL, AV	Botnet, C2, DNS BOT, C2, DNS	
SOC Augmentation by FortiGuard	Know Your Risks & vulnerabilities **Security Assessments**		Train your SOC **IRR, Playbooks, Training**	Managed Detection & Response **MDR**	Augment your SOC **SOC as a Service**	Respond Faster and More Effectively **Incident Response**	

Convergence of Networking & Security Delivers Total Protection

Evolving Enterprise

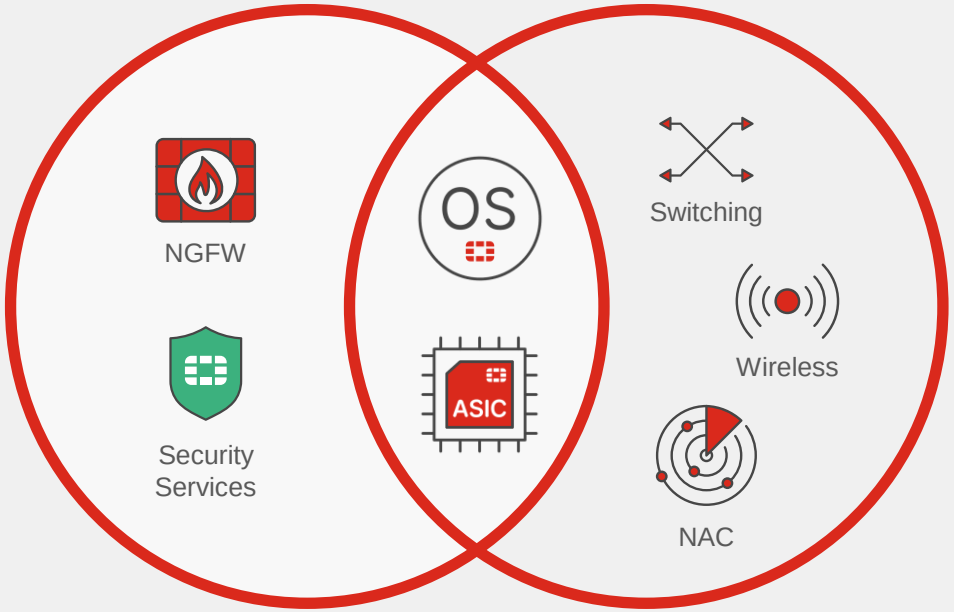
Complexity
Managing multiple vendors & configurations with complicated integrations.

Inconsistent Security
With separate tools, monitoring, logging, and threat detection are disjointed.

High TCO
Multiple vendors with separate licenses, hardware, and support costs.

Lack of User Experience
Network performance is degraded as security features are added.

Convergence



High ROI & Low TCO

PLATFORM

Consolidate
Single OS eliminate silo products and complexity

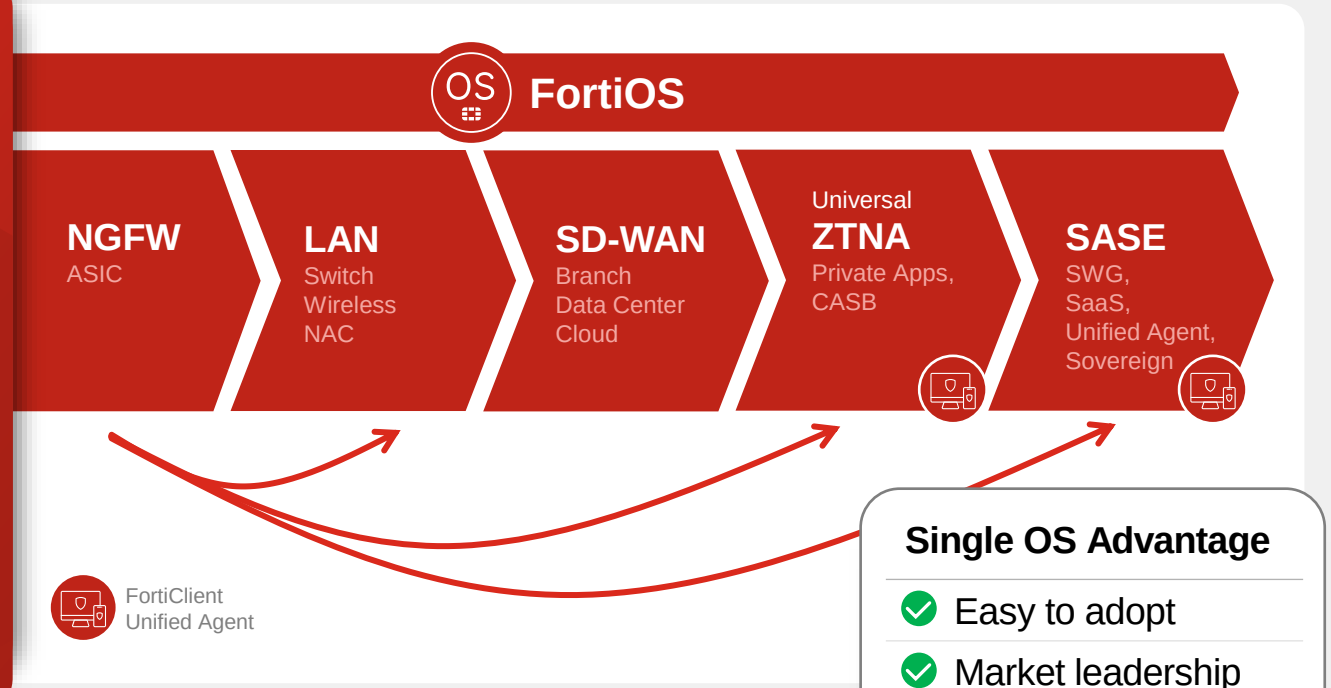
Integrated
AI-powered Consistent security across all edges

Automation
Faster time to prevention and efficient operations

The Fortinet Journey: A Seamless Security Evolution

With FortiGate NGFW, customers gain industry-leading protection and can seamlessly activate SD-WAN for optimized performance and extend to SASE for secure remote access.

Your Journey to Secure Networking Begins Here



Single OS Advantage

- Easy to adopt
- Market leadership
- Proven

ROI
300%

Reduction in MTTR
95%

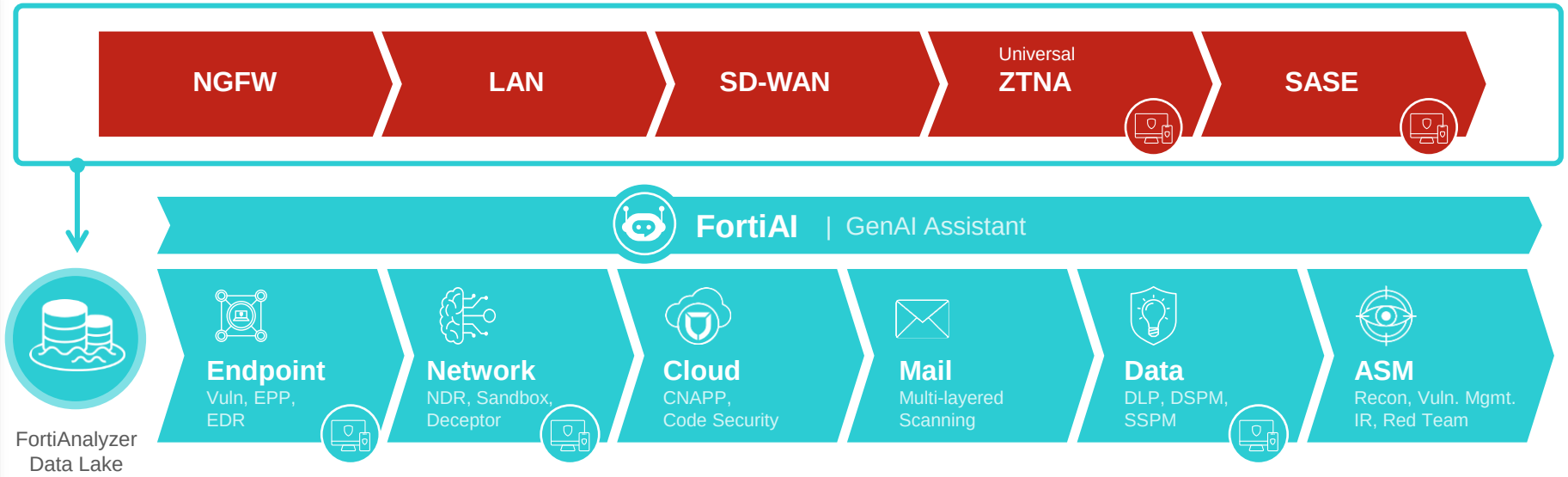
Reduction in threats
99.9%

Increase IT productivity
50%

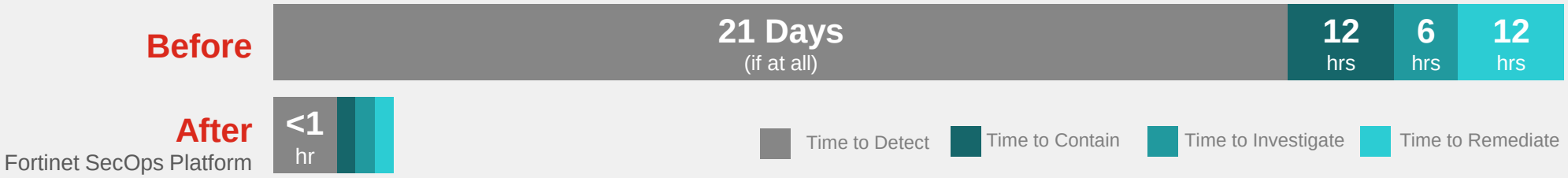
Transforming SOC Capabilities for AI-Driven Cyber Defense

Centralizing security and networking data to enhance visibility, orchestration, and automation

Transform Insights into Outcomes with the Fortinet Security Fabric



Speed the time to fully investigate and remediate incidents from 18.5 hours to an average of 10 minutes.



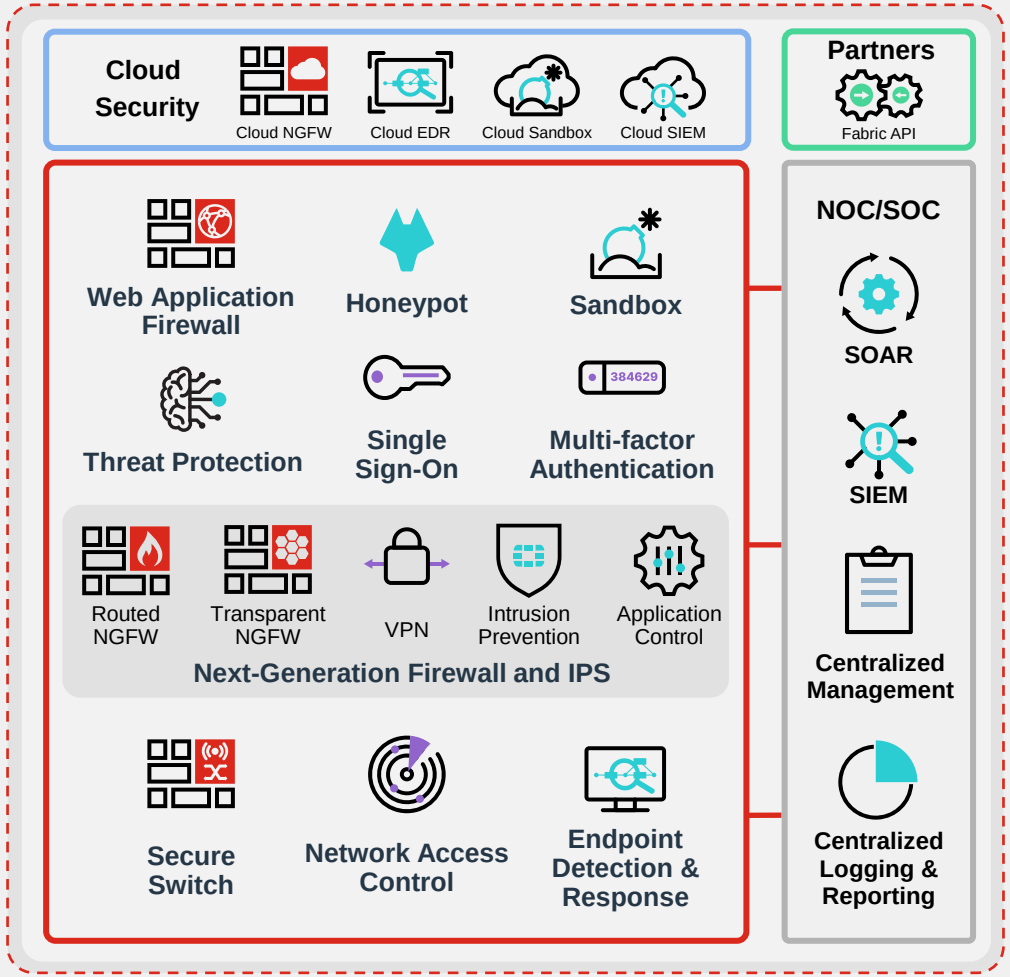
Source: Enterprise Strategy Group, ESG Research, SOC Modernization Survey, January 2025.

Fortinet Securing the IT & OT

- Network Segmentation
- Network Microsegmentation
- Network Access Control
- Web Services Security
- Secure Remote Access
- Threat Protection
- Application Control
- Endpoint Security
- Honeypot
- Sandbox
- NOC/SOC

	Levels		
Cloud & External Zones		External Networks	Internet, Cloud, VPN
Major Enforcement Boundary		5.5 Information Technology (IT) Boundary	
Business & Enterprise Zones	5	Enterprise Network	Corporate Systems & Networks
	4	Business Planning & Logistics	Site Systems & Networks
Major Enforcement Boundary		3.5 Operational Technology (OT) Boundary	
Operations & Control Zones	3	Operations & Control	Simulation, Engineering, Test
Minor Enforcement Boundary		2.5 Industrial Control System (ICS) Boundary	
Process Control Zones	2	Area Supervisory Control	HMIs, Historians
	1	Basic Control	PLCs, RTUs, IEDs
	0	Process	Actuators, Sensors
Major Enforcement Boundary		Air-gap / Safety Related Control Systems Boundary	
Safety Zone	S	Safety	Safety Instrumented System

Fortinet Security Fabric



Boundary: Demilitarized Zone (DMZ), Security Conduit
Zones: Security Zones
IPS: Intrusion Prevention System
SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response

FORTINET