infinigate
spark your growth

Herzlich Willkommen

Cybersecurity, die verkauft:

Neue Potenziale mit SecOps

Aufgaben

- Unterstützung & Entwicklung von Partnern
- Enablement Fortinet
- Sales Schulungen/Webinare
- Schnittstelle zum Hersteller

Julia Seifert

Business Development Manager Fortinet

T.: +49 (0) 40 – 23 73 01- 244

Mail: julia.seifert@infinigate.de

Agenda

- **Wer wir sind** – Vorstellung Infinigate
- **Was ist SecOps?** – Einleitung & Grundverständnis
- **Wo liegen die Probleme?** – Angriffe, Angriffsflächen, Anforderungen an Teams
- **Wie setzt man es um?** – SecOps in der Praxis
- **Welche Lösungen für den Einstieg?** – FortiAnalyzer & FortiDeceptor
- **Womit schließen wir ab?** – Fazit & Outro

infinigate
spark your growth

Über Infinigate

Ihr Cybersecurity Trusted Advisor

Infinigate ist die führende Technologieplattform und Ihr Berater in den Bereichen Cybersicherheit, Cloud und Netzwerkinfrastruktur.

- Australia
- Austria
- Bahrain
- Belgium
- Bulgaria
- Croatia
- Denmark
- Egypt
- Finland
- France
- Germany
- Ireland
- Jordan
- KSA
- Kuwait
- Morocco
- Netherlands
- New Zealand
- Norway
- Oman
- Pakistan
- Poland
- Qatar
- Romania
- Slovenia
- Spain
- Sweden
- Switzerland
- South Africa
- UAE
- United Kingdom

1.700+
Hersteller-akkreditierungen

25+
Jahre Erfahrung

2:1
Sales to Technical

1.500+
Mitarbeiter

25%
CAGR für 15+ Jahre

€2,8bn
FY25 Revenue

Leistungsübersicht – Wir an Ihrer Seite…

Sales	Services	Marketing	Logistics
• Partner Enablement • Fortinet Sales Academy • Fokussierte Businessplanung • Produktvorstellungen vor Ort / Webinar • Lösungsvertrieb • Trainings vor Ort / Webinar • Pre-Sales Unterstützung • Projektbegleitung • Partneraufbau anhand des Partnerprogrammes • Call-Out Unterstützung	• Pre-Sales & Support • Technical Support • Extended Support • 24X7 • Advanced Replacement Service • Web Based Education • Solution Workshops • Solution & Product Training • Solution Engineering • Pre-Staging & Testing • Advanced Support • Fortinet Tech Academy	• Finanzielle Unterstützung durch Market Development Funds (MDF) • Erarbeitung von zielgerich-teten Strategien • Unterstützung bei Events, Workshops, End-User-Webinaren, Call-Outs und Markenauftritt • Individuelles Erstellen von Broschüren/ Flyern • Event out of the Box • Telemarketing	• Dedizierte Abteilung für die Auftragsabwicklung und dedizierter Ansprechpartner pro Auftrag • Reklamationsmanagement • International shipments • One day delivery • Unterstützung bei der Umsetzung von Auslandslieferungen • Eigener Dienstleister für die Verzollung im Ausland bei Bedarf • Versand mit UPS Express Saver und Palletten Versand über DHL Express • Zentrallager für unsere gängigen Produkte

Ihr Fortinet Team bei Infinigate

Ihr Team für die Angebotserstellung

infinigate
spark your growth

Fortinet SecOps

Sind SecOps das SOC und Technologien...

Oder sind es ...
Attacken, Taktiken & Techniken von Bedrohungsakteuren?

Oder sind es gar politische Gruppen?

tagesschau

tagesschau24 live

Startseite ▸ Inland ▸ Regional ▸ Berlin ▸ Cyberangriff: Hacker erbeuten Daten von Berliner Justizsenatorin

rbb

00:33 Min

Berlin

Hacker erbeuten persönliche Daten von Justizsenatorin

Stand: 19.08.2025 14:01 Uhr

Hacker haben offenbar bei einem gezielten Angriff Daten der Berliner Justizsenatorin Felor Badenberg abgegriffen. Laut einem Bericht des Spiegel haben Sicherheitskreise eine Gruppe aus Iran im Verdacht.

© dpa/Sebastian Gollnow

Exklusiv / Nach Cyberangriff auf Berliner Justizsenatorin SPD fordert besseren Schutz – Sicherheitsexperte warnt vor Iran

Nach der Cyberattacke auf Berlins Justizsenatorin Felor Badenberg (CDU) fordert die SPD mehr Schutz. Ein Sicherheitsexperte sieht indes mehrere Gründe, warum es Badenberg getroffen haben könnte.

Von Stefanie Witte

Stand: heute, 05:00 Uhr

Versuch einer Definition

SecOps steht für **Security Operations** bzw. Sicherheits-IT-Betrieb.

Der Begriff bezeichnet allgemein Teams, Prozesse und Tools, die dafür sorgen, dass IT-Sicherheit im Unternehmen nicht nur eingerichtet, sondern auch aktiv überwacht, betrieben und verbessert wird.

Die wichtigsten Punkte:

- Automatisierung
- Zentralisierung
- Effizienz

QUICK QUIZ

infinigate

Wie lange dauert es durchschnittlich bis zur Erkennung von Vorfällen?

a) 7 Stunden

b) 5 Tage

c) 21 Tage

Wie lange bleiben Vorfälle durchschnittlich unentdeckt?

52 %

der Unternehmen geben an, dass SecOps komplexer ist als vor zwei Jahren.

SEC Rule:
Nach Kenntniserlangung

24 h

für die frühe Erstmeldung

Kosten eines Datenlecks in Deutschland bei etwa:

3,87 Mio. €

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

Aktuelle Herausforderungen

1. Evolution von Angriffen / zunehmende Bedrohungen

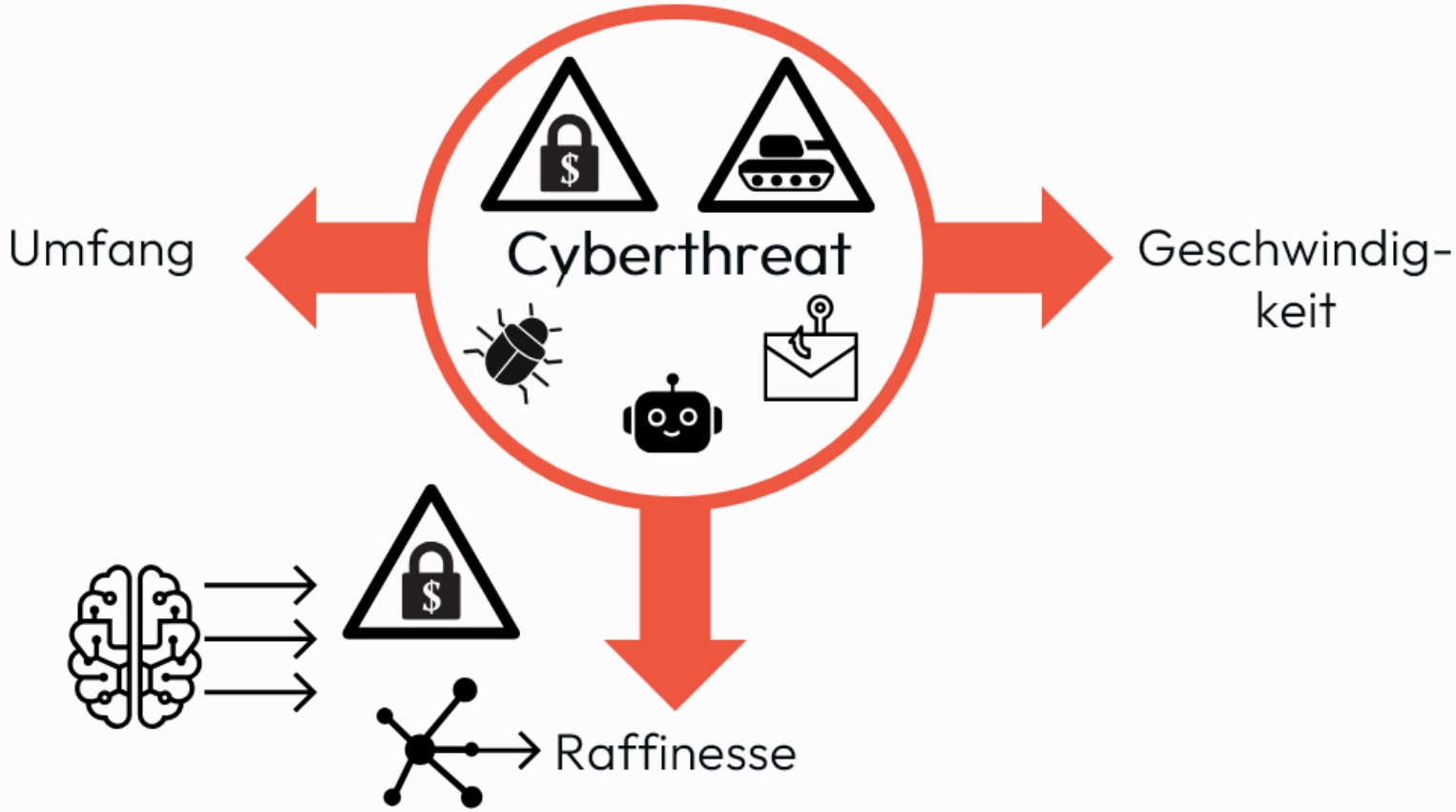
2. Ausweitung der Angriffsfläche / immer mehr Einfallstore

3. Erhöhung des Aufkommens und der Komplexität

1. Evolution von Angriffen

Beschleunigung im digitalen Geschäft

Wissenslücke im Bereich Cybersicherheit



Geschwindigkeit

Früher dauerte es Tage oder Wochen, bis Angreifer Daten verschlüsselten. Heute passiert das innerhalb von Stunden.

Komplexität

„Malware-as-a-Service, KI und automatisiertes Fuzzing machen Angriffe heute schneller, ausgefeilter und schwerer abzuwehren.“

Umfang

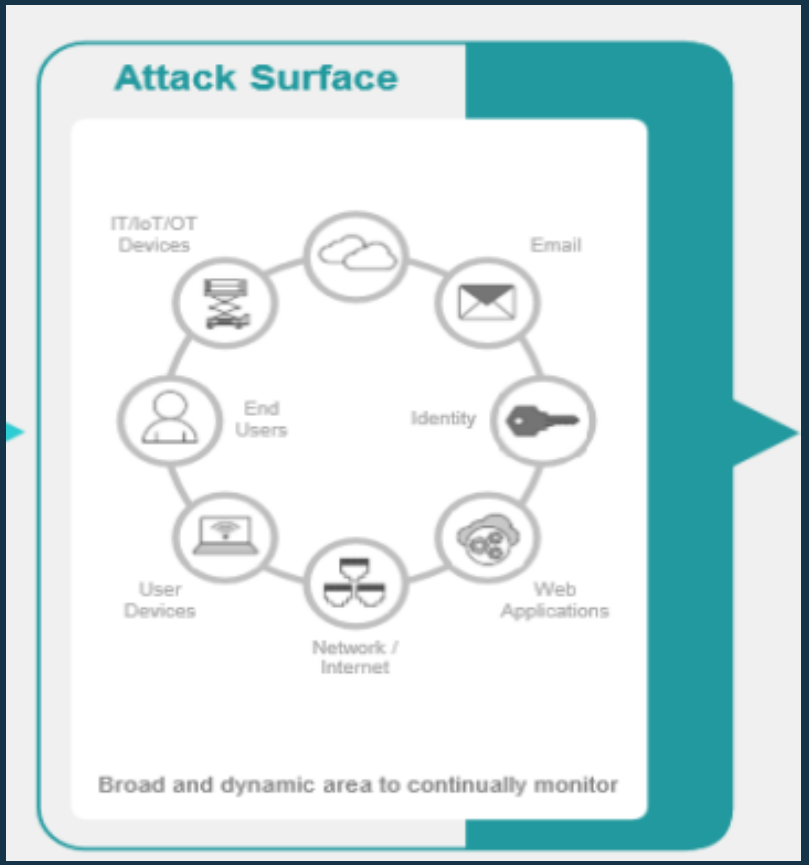
Selbstlernende Botnetze verbreiten erfolgreiche Angriffsmethoden wie ein Lauffeuer – in Sekunden tausendfach.

2. Ausweitung der Angriffsfläche

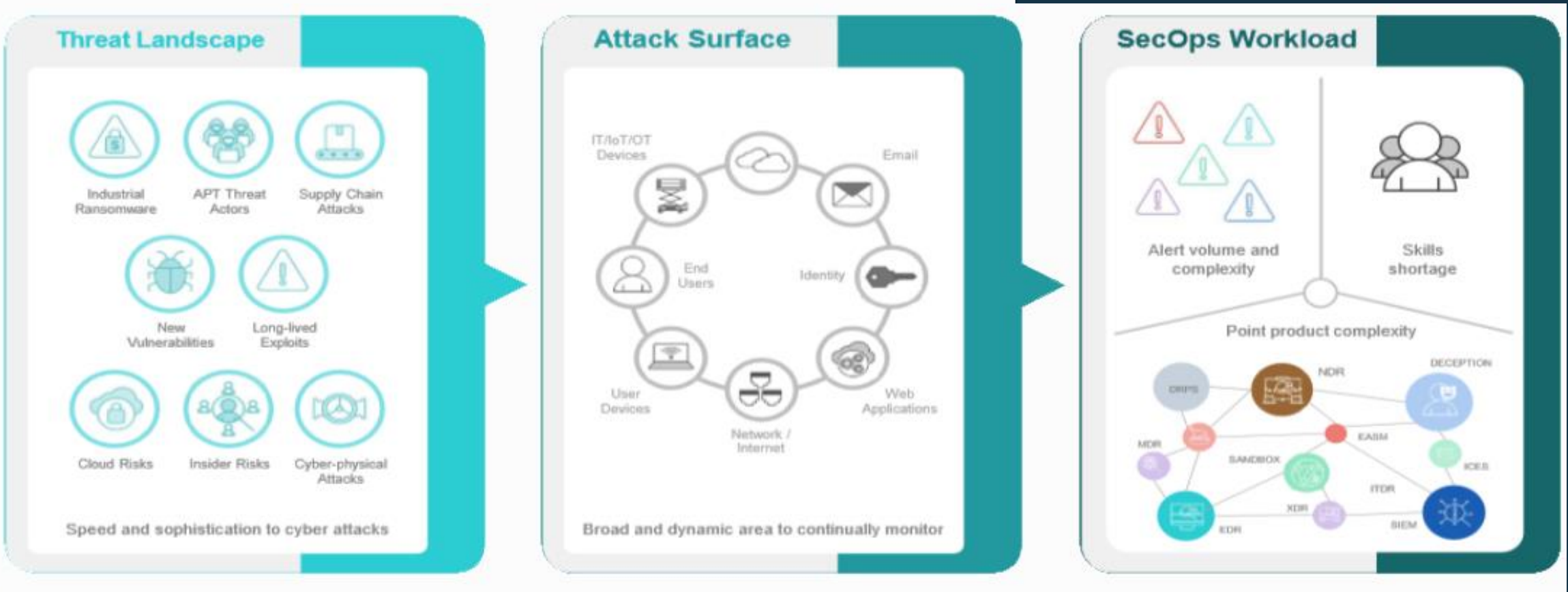
Immer mehr Einfallstore durch z.B.:

- Arbeiten von überall, von überall soll auf das Unternehmensnetzwerk zugegriffen werden
- BYOD, immer mehr „Smarte“ Geräte vom Auto bis zur Kaffeemaschine, die sich ins Netzwerk einloggen

Das sind alles potentielle Einfallstore!



3. Erhöhung des Aufkommens und Komplexität



QUICK QUIZ

infinigate

Wie viele Alerts laufen aktuell in einem SOC im Durchschnitt an einem Tag auf?

a) Ca. 650 und bis zu 800 bei großen SOCs

b) Ca. 4.500 und bis zu 11.000 bei großen SOCs

c) Ca. 1.000 und bis zu 3.000 bei großen SOCs

Wie viele Alerts laufen aktuell in einem SOC im Durchschnitt an einem Tag auf?

a) Ca. 650 und bis zu 800 bei großen SOCs

b) **Ca. 4.500 und bis zu 11.000 bei großen SOCs**

c) Ca. 1.000 und bis zu 3.000 bei großen SOCs

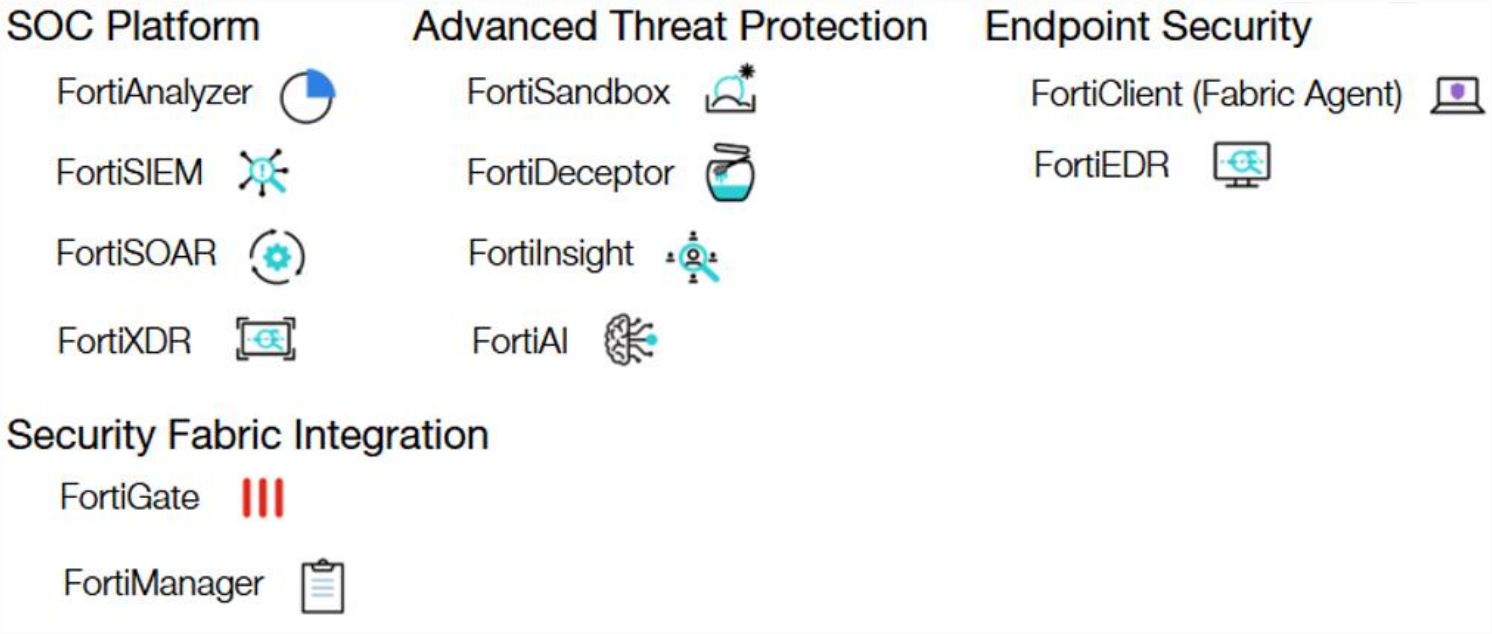
Welche Herausforderungen lösen SecOps?

- Verbesserung der Sichtbarkeit und Kontrolle
- Entlastung des SOC/Security Teams
- Schnelle, automatisierte Erkennung & Reaktion
- Verhinderung der Störung des Geschäftsbetriebs
- Wachsende Regulatorien integrieren

Security Operations Lösungen bei Fortinet umfassen:

- Künstliche Intelligenz (KI)
- Integration und Automatisierung
- Erweiterte Erkennung und Reaktion auf Bedrohungen
- Zentrale Überwachung und Optimisierung

Einordnung von SecOps



Fortinet Fabric Management Center

1. SOC Plattform:
   - Centralized Management
   - Security Fabric Analytics
2. Advanced Threat Protection
   - Security Automation and Orchestration
3. Endpoint Security
   - Detection and Response for Endpoints

Die umfangreichste Plattform der Cybersecurity

Secure Networking

FortiGate
NGFW with ASIC acceleration and industry leading Convergence

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

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

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

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

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

FortiRecorder
Secure NVR with smart AI analysis and centralized visibility

FGaaS
Hardware as a service for FortiGate

FortiSwitch
Protected Ethernet connectivity via Secure Networking convergence with FortiGate

FortiManager
Centralized management of your Fortinet security infrastructure

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

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

FortiFone
Robust IP phones and softclient to stay connected from anywhere

FortiCamera
Physical security with intelligent motion detection in any light condition

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

Resources

Product Matrix
Specifications for top selling models

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

FortiOS
The Heart of the Fortinet Security Fabric

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

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

FortiCare
Support and mitigation services

Unified SASE

SASE

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

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

FortiProxy
Enforce internet compliance and granular application control

FortiCASB
Prevent misconfigurations of SaaS apps and meet compliance

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

FortiSASE
Cloud-delivered Security Services Edge

FortiMonitor
SaaS based DEM platform, performance monitoring

CLOUD

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

FortiWeb
Prevent web application attacks against critical web assets

FortiGSLB
Ensure business continuity during unexpected network downtime

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

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

FortiADC
Application-aware intelligence for distribution of application traffic

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

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

AI-Powered FortiGuard Security

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

Security Operations

FortiAnalyzer
Security Fabric log management, monitoring and response

FortiSIEM
Enterprise-wide monitoring, threat detection, and response

FortiEDR/XDR
Automated endpoint protection and correlated incident response

FortiSOAR
Automated security operations, investigation, and response

FortiNDR
AI-driven analysis to detect and respond to threats

SOCaaS
Continuous security monitoring, incident triage, and escalation

IR Services
Rapid detection, containment, and recovery of cyberattacks

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

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

FortiGuest
Access management solution for temporary access to guests and visitors

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

FortiDLP
Endpoint DLP and Insider Risk management

FortiMail
AI-powered, protection against email-borne threats

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

FortiToken
Cloud/HW/Mobile MFA provide passwordless adaptive authentication

FortiAuthenticator
Centralized identity and access management solution

FortiGuard MDR Service
Managed threat detection, investigation, and response

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

FortiPAM
Privileged identity and access management, and session monitoring

FortiTester
Network performance testing and breach attack simulation (BAS)

FortiDevSec
Orchestrated and automated continuous application security testing

FortiDAST
Automated black-box dynamic application security testing

FortiScanner Cloud
Cyber Asset Attack Surface Management Service

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

infinigate

QUICK QUIZ

infinigate

Wie viel Zeit für Erkennung und Behebung braucht man durchschnittlich mit SecOps?

a) 15 Tage

b) 14 Stunden

c) Weniger als 1 Stunde

Vorfälle in 10 Minuten statt 18,5 Stunden beheben

Vor SecOps

... bis zur Erkennung

... um zu begrenzen

... für Abhilfe

... zum Untersuchen

Nach SecOps

Source: Enterprise Strategy Group, 1. ESG Research, SOC Modernization Survey, January 2025. Fortinet Inc. All Rights Reserved

FortiAnalyzer

SIEM light:

speziell optimiert für Fortinet-Produkte, versteht aber auch Logs anderer Hersteller (z. B. Linux, Cisco)

Datenkorrelation:

sammelt, analysiert und verknüpft Logs aus der gesamten Infrastruktur.

KI-Unterstützung:

hilft beim Erkennen von Mustern und Anomalien.

Threat Intelligence:

Reichert interne Daten mit „Indicators of Compromise“ (IoCs) aus den FortiGuard Labs an.

Compliance & Reporting:

Stellt aussagekräftige Reports bereit, die regulatorische Anforderungen unterstützen.

Use Case:

Ideal für Organisationen, die einen Überblick über Sicherheitsereignisse brauchen, ohne gleich ein „großes“ SIEM einzuführen.

FortiDeceptor

Deception-Technologie:

Lockt Angreifer in eine künstliche, aber echt wirkende Umgebung.

Früherkennung:

Erkennt Angriffe, sobald sich ein Eindringling in der Falle bewegt – noch bevor er produktive Systeme erreicht.

Täuschungs-Assets:

Erstellt realistische Köder (Server, Datenbanken, Endpoints), die für Angreifer wie echte Ziele aussehen.

Visibilität:

Gibt Security-Teams frühzeitige Warnungen und detaillierte Informationen über das Vorgehen der Angreifer.

Automatisierung:

Kann auf erkannte Bedrohungen automatisiert reagieren (z. B. Angreifer isolieren).

Use Case:

Ideal, um unbekannte oder besonders ausgefeilte Angriffe (Zero-Day, APTs) sichtbar zu machen.

Fazit

- Kein Projekt, sondern ein Prozess
- Automatisierung & KI entlasten Teams
- Schneller reagieren – resilienter werden
- Viele Unternehmen sind schon auf dem Weg
- Früh starten heißt: Angreifern voraus sein

Gibt es Fragen zu weiteren Lösungen, wollt Ihr mehr in die Tiefe gehen oder sollen wir Euch bei Euren Projekten unterstützen?

Sprecht mich und mein Team gern an!

P.S.: In Q4 haben wir eine FortiDeceptor Promo!

Julia Seifert

Business Development Manager

T.: +49 (0) 40 – 23 73 01- 244

Mail: julia.seifert@infinigate.de

https://www.linkedin.com/in/julia-seifert-a97156106/

Vielen Dank für die Aufmerksamkeit!