KHZG-Erfahrungsberichte

Martin Weiß
Senior Sales Engineer Public

SOPHOS

Krankenhauszukunftsgesetz - Fördertatbestände

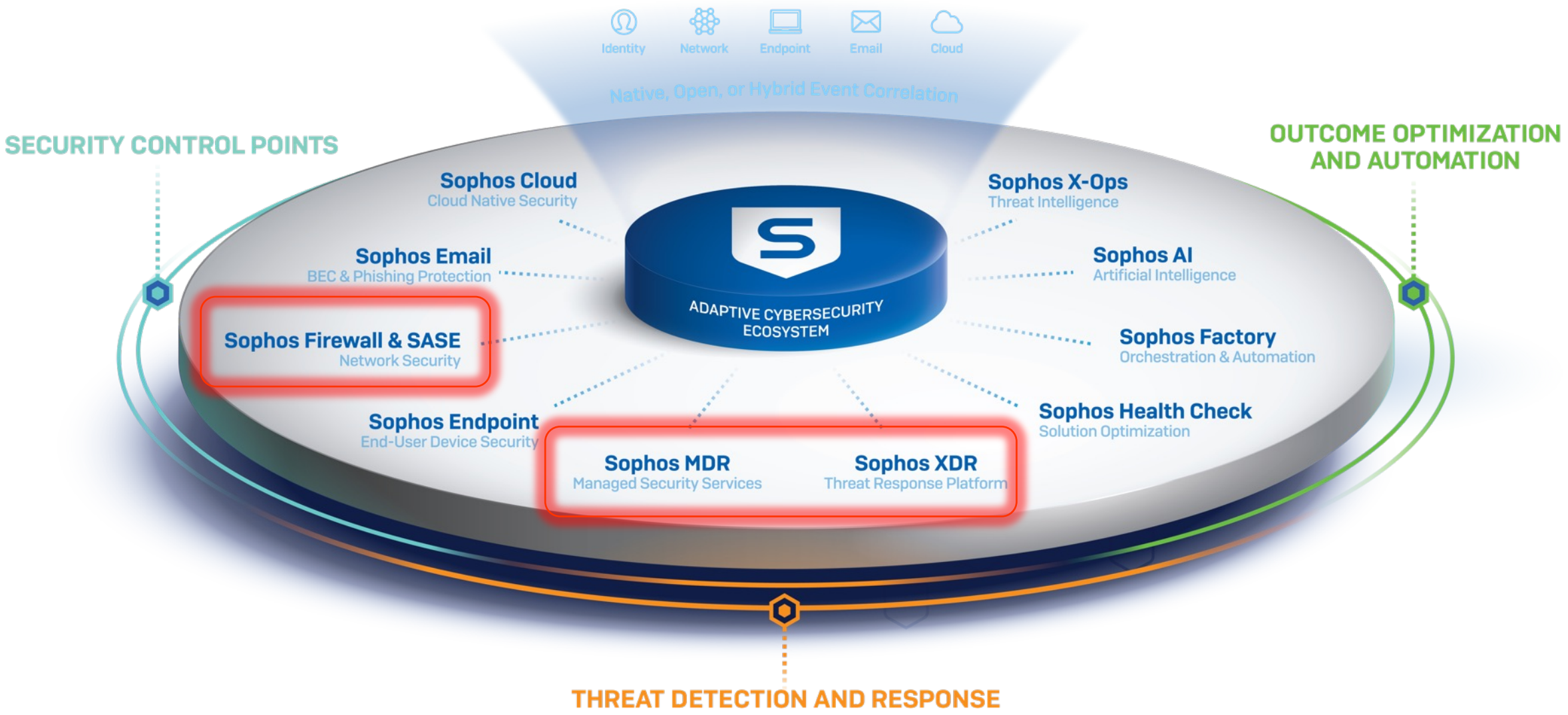
- 01: Notaufnahme
- 02: Patientenportal
- 03: Pflege- und Behandlungsdokumentation
- 04: Entscheidungsunterstützung
- 05: Medikationsmanagement
- 06: Krankenhausinterner digitaler Leistungsprozess
- 07: Leistungsabstimmung und Cloud-Computingsysteme
- 08: Versorgungsnachweissystem Betten
- 09: Telemedizinische Netzwerke
- 10: IT- und Cybersicherheit
- 11: Anpassung von Patientenzimmern bei Epidemien

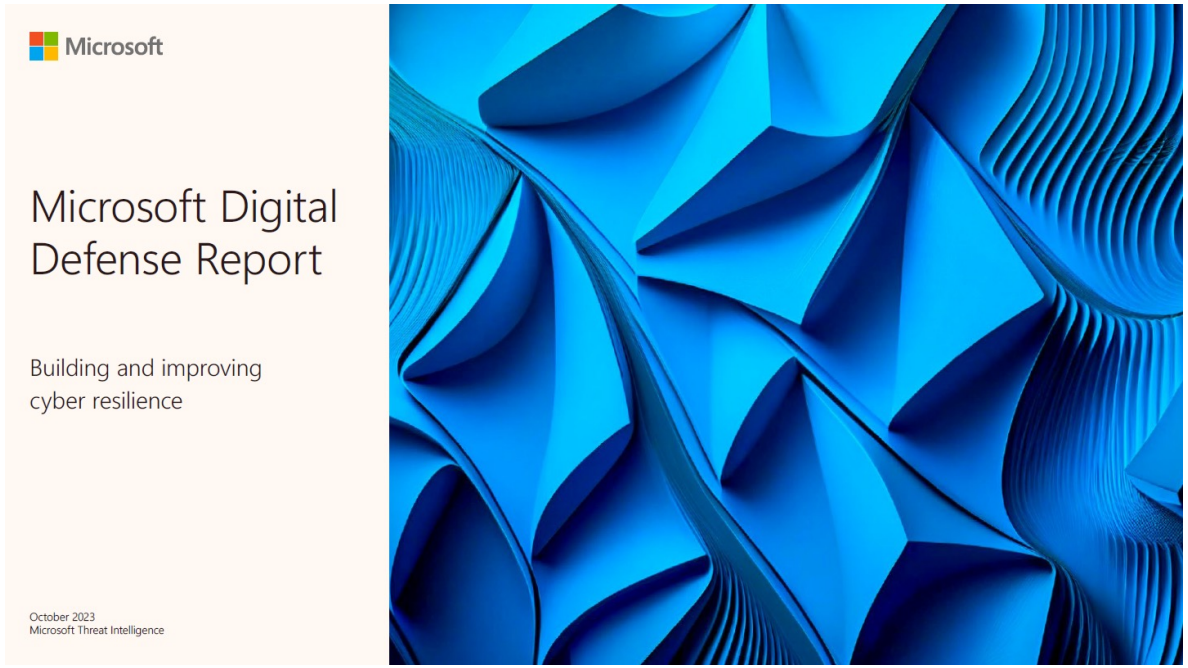
SOPHOS

Krankenhauszukunftsgesetz (KHZG/KHZF)

- Maßnahmen müssen Stand der Technik entsprechen
- Schutz von Netzwerken, Zonierung, VPN, IDS/IPS, ZTNA
- Interoperabilität muss gewährleistet sein
- Systeme zur Detektion von Informationssicherheits-Vorfällen (u. a. SOC & MDR) werden explizit gefördert
- Steigerung und Aufrechterhaltung der Awareness gegenüber Informationssicherheits-Vorfällen

Optimale Sicherheit für Ihre Organisation





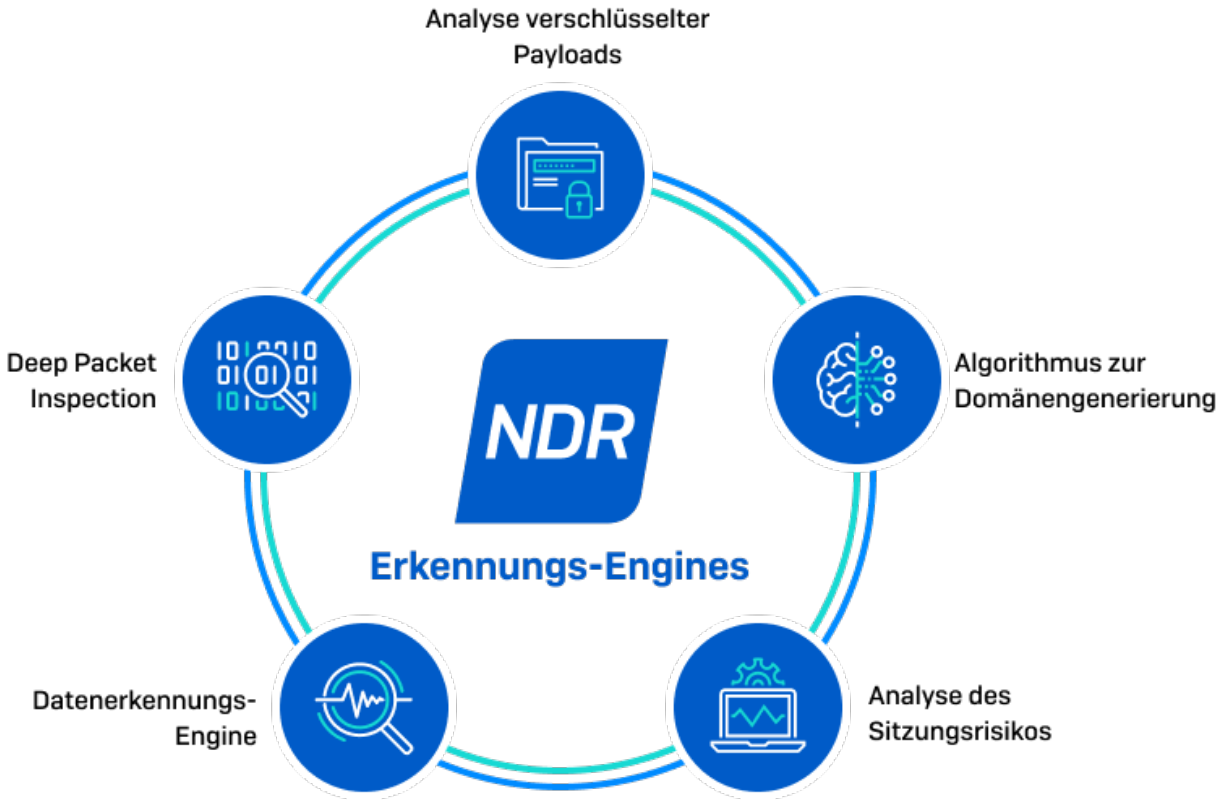
„80-90% aller erfolgreichen Ransomware-Angriffe starten von nicht-verwalteten Geräten“

„70% aller Organisationen, die Opfer von interaktiven Angriffen mit Ransomware waren, hatten weniger als 500 Mitarbeiter “

https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Network Detection and Response

- Fremde und unbekannte Geräte
- Angriffe auf IoT/OT
- Lieferkettenangriffe
- Insider-Bedrohungen
- Versuchter Zugriff mit deaktivierten Accounts
- Datenexfiltration via DNS oder Remote-Sitzungen

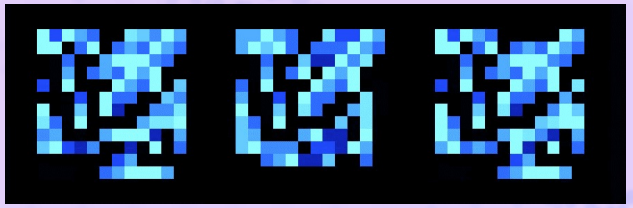


Sophos NDR

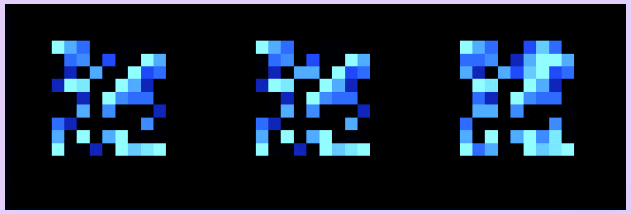
Encrypted Packet Analysis

Malware Flow Images

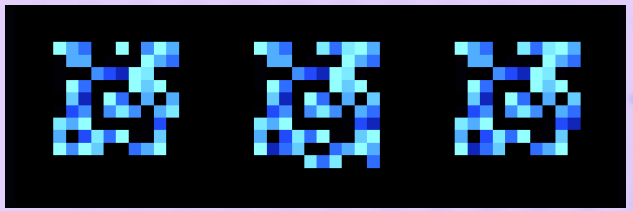
CobaltStrike



QakBot

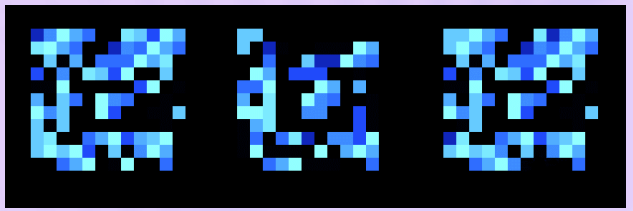


BazaLoader

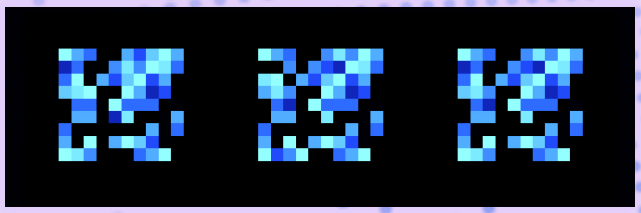


Dridex

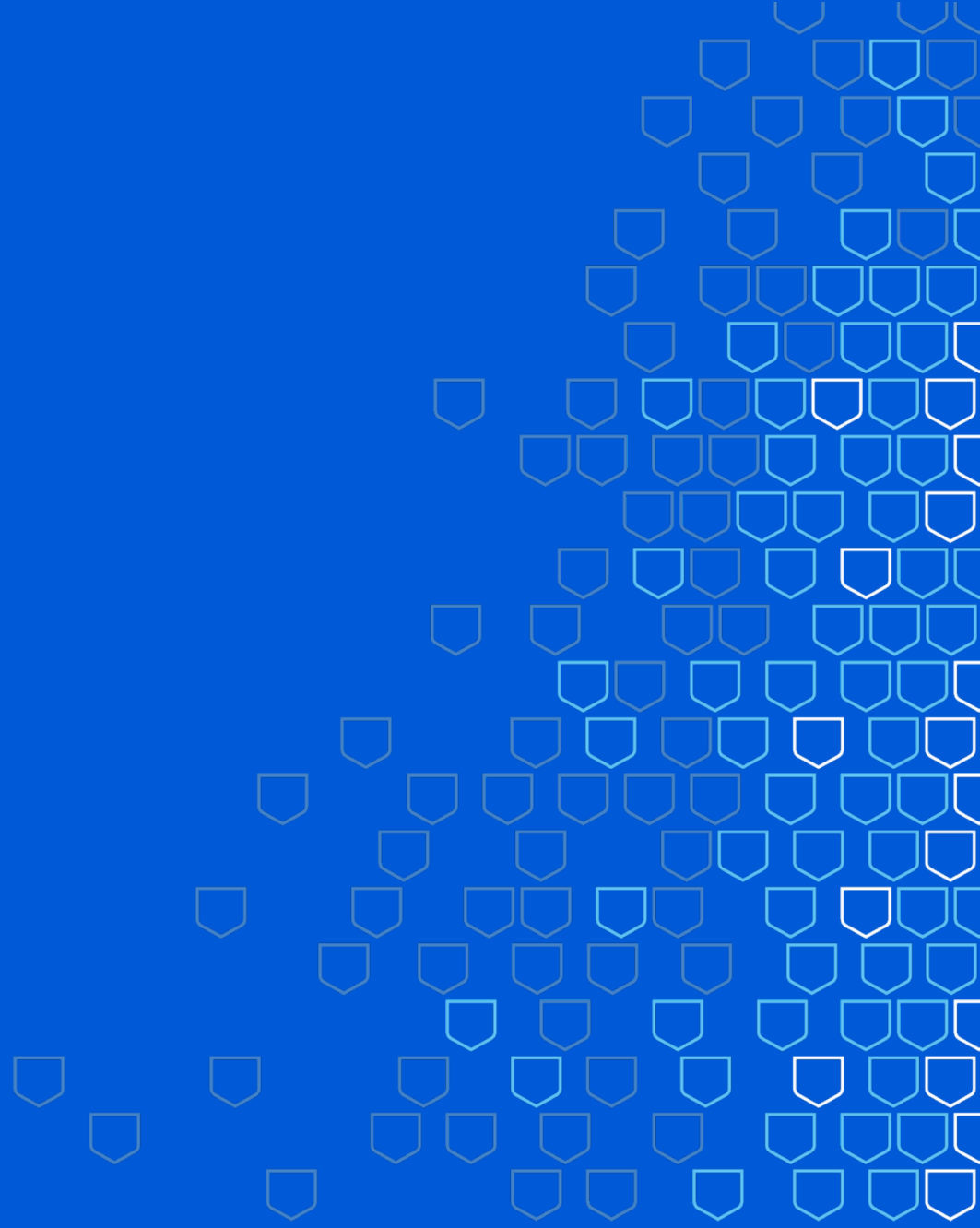
TrickBot



ZLoader

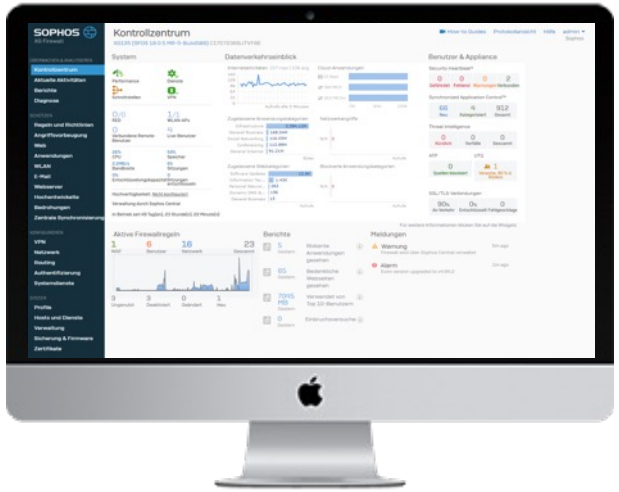


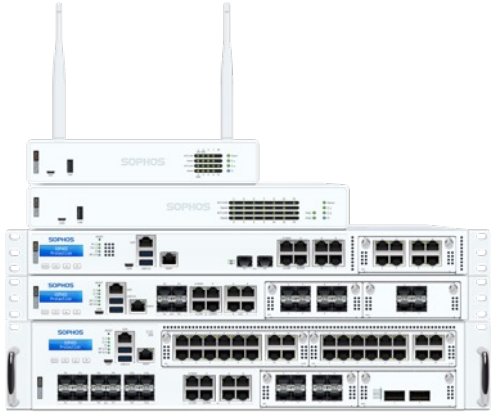
Sophos Firewall

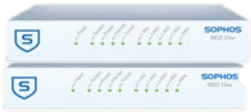


SOPHOS

Sophos Firewall







Azure

aws

Einfaches Management

Sofortige Sichtbarkeit

Kompletter Schutz

Synchronized Security

Maximale Performance

Zentrales Management

Flexible Deployment Optionen

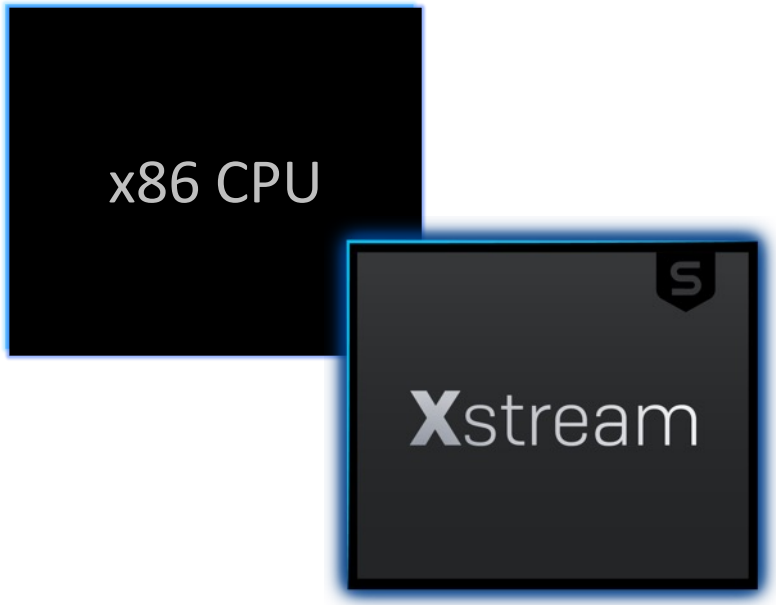
XGS Series Appliance

Software oder Virtual Appliance

Public Cloud (AWS/Azure)

Architektur

Sophos XGS Hardware Beschleunigung



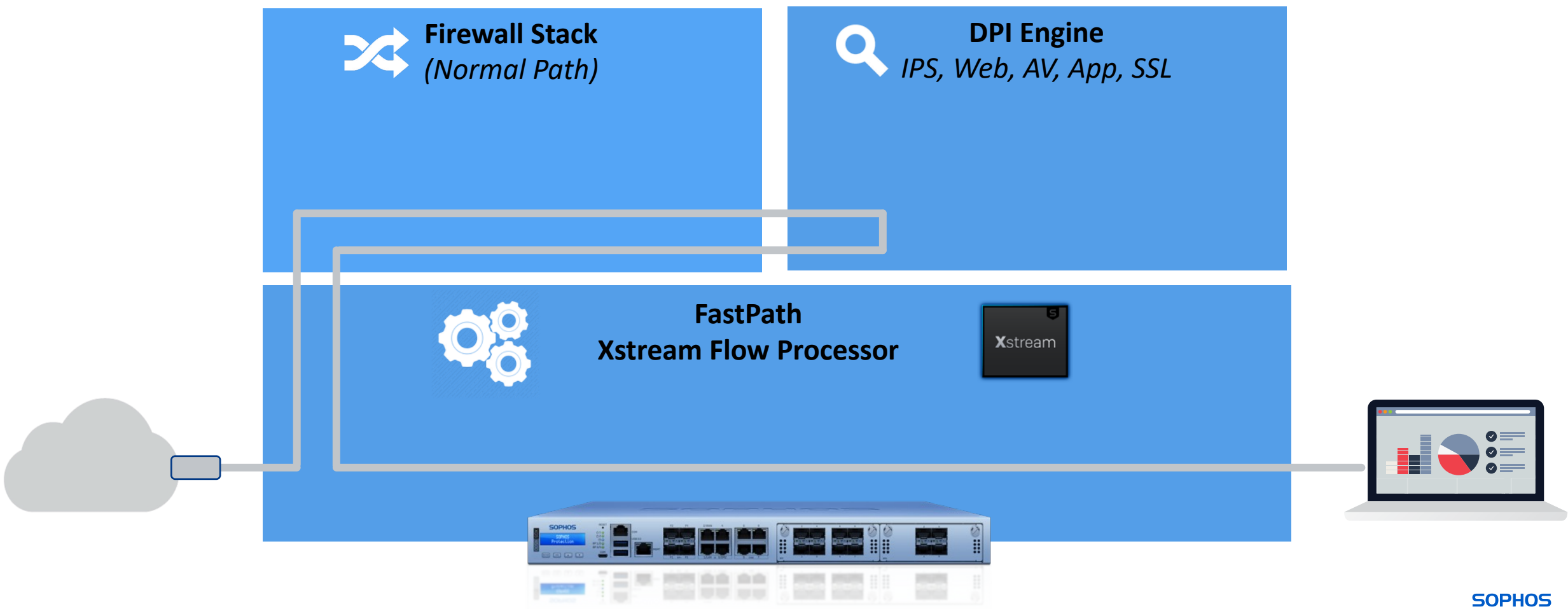
Neue Dual Prozessor Architektur
x86 CPU plus Sophos eigener
Xstream Flow Processor

x86 CPU (AMD)
Routing, Connection Management,
Deep Packet Inspection, TLS Inspection

Xstream Flow Processor (Marvell NPU)
Xstream Hardware FastPath
IPsec Beschleunigung

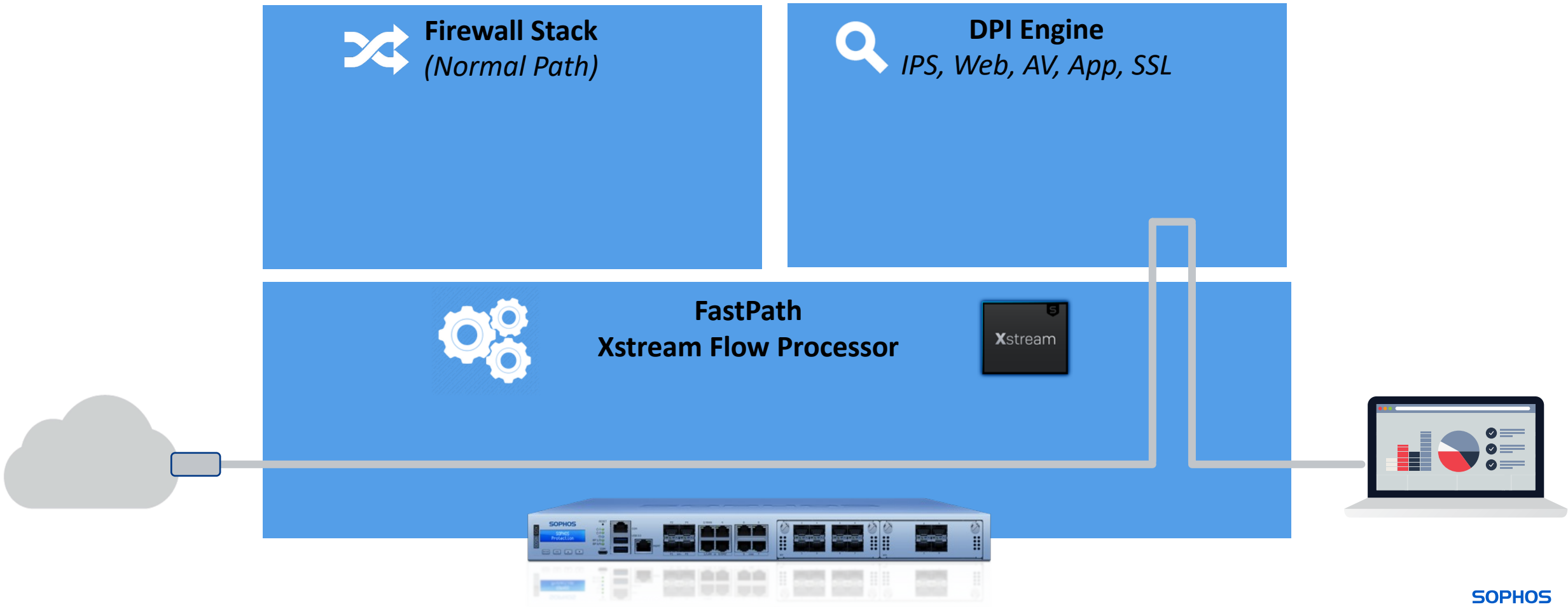
Meeting Webinar

Schritt 1) Initiale Übermittlung von Paketen an Kernel & DPI Engine über SlowPath



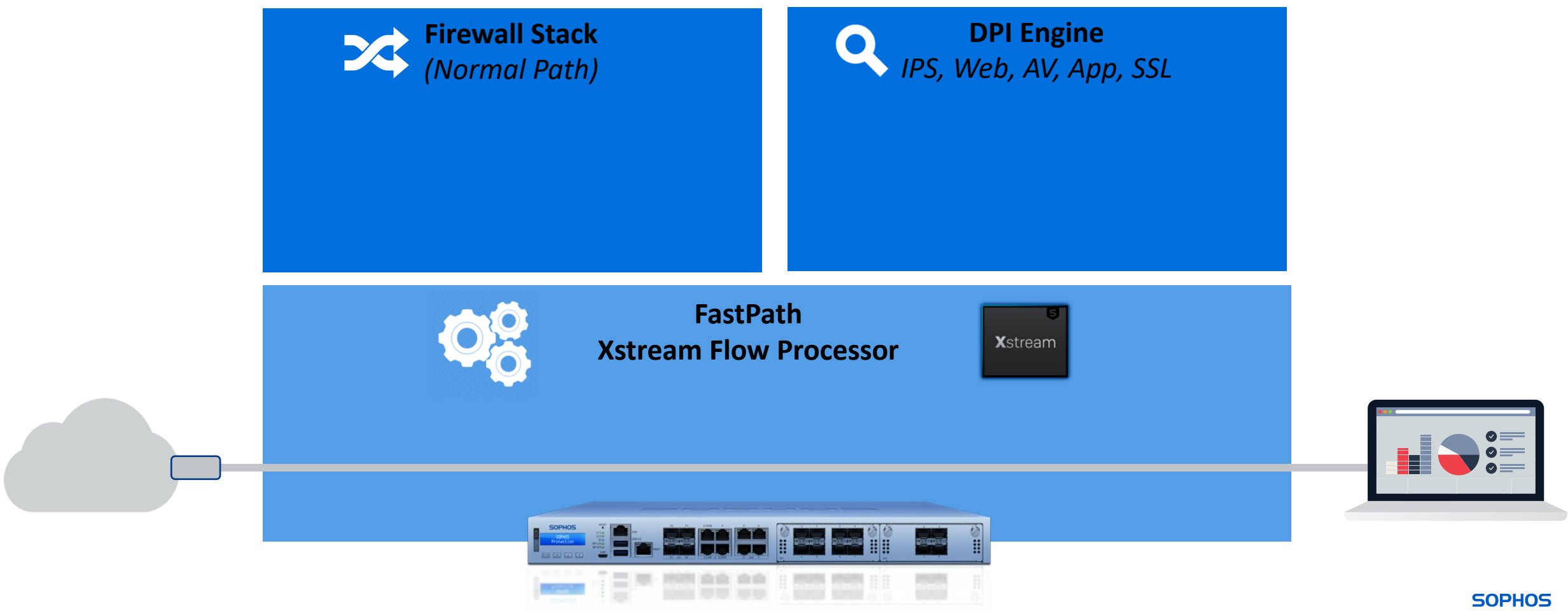
Meeting Webinar

Schritt 2) Die Firewall übergibt den Datenfluss an die DPI-Engine zur Sicherheitsüberprüfung



Meeting Webinar

Schritt 3) Wenn der Datenstrom als sicher eingestuft wird, kann die DPI-Engine an den Xstream-Flow-Prozessor übergeben werden



Zonenkonzept

Zonenkonzept

Zone Clients

- Client-Netz - .20
- VLAN31 - .31
- VLAN32 - .32
- VLAN33 - .33
- VLAN34 - .34

Zone Medizin Geräte

- VLAN82 - .82
- VLAN83 - .83

Zone KIS / PACS

- VLAN50 - .50

Zone Server

- Server-Netz - .40

Zone WAN

- Telekom - .100

Zone WAN

- Vodafone - .200

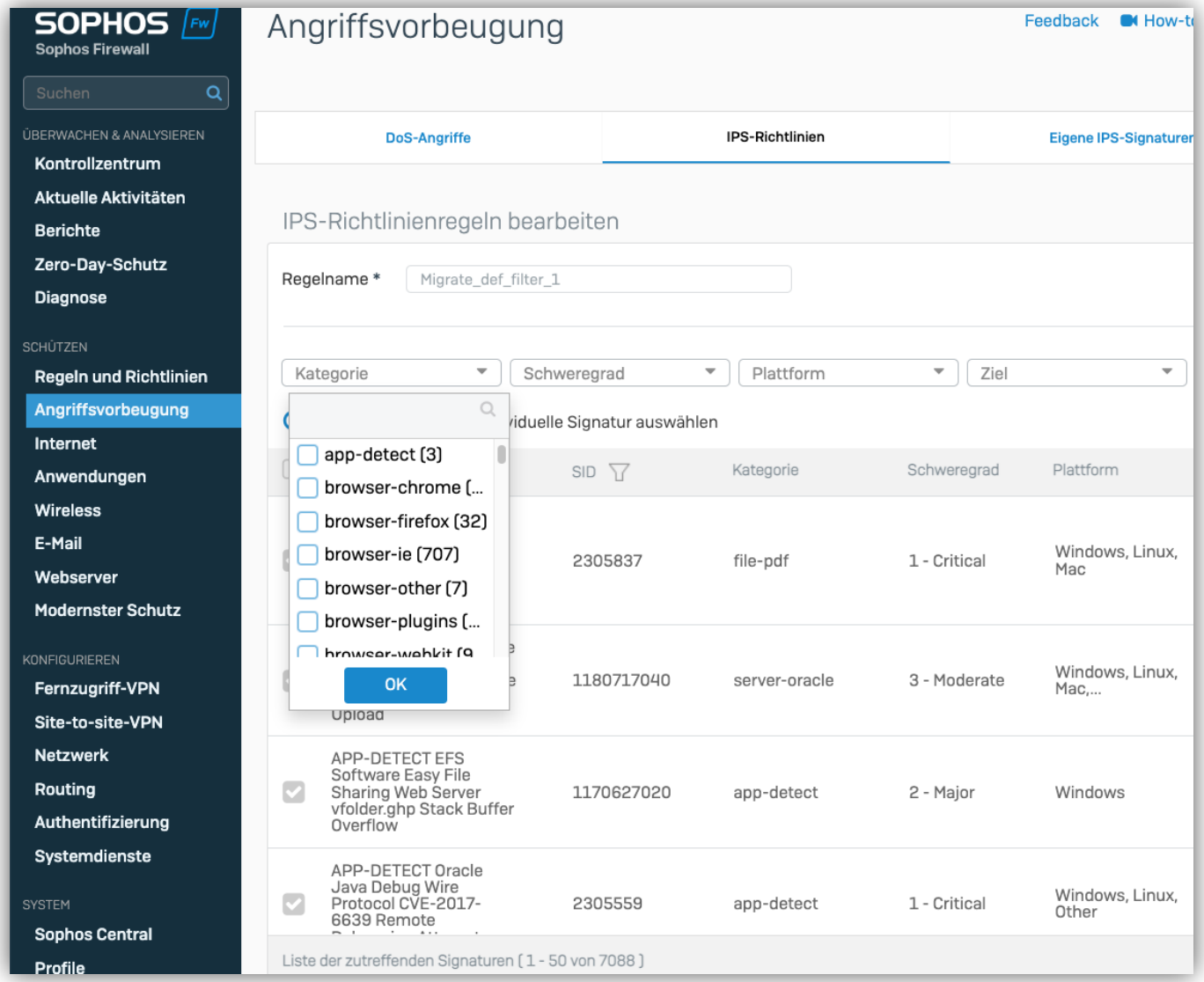
Intrusion Prevention System (IPS)

Wie funktioniert es?

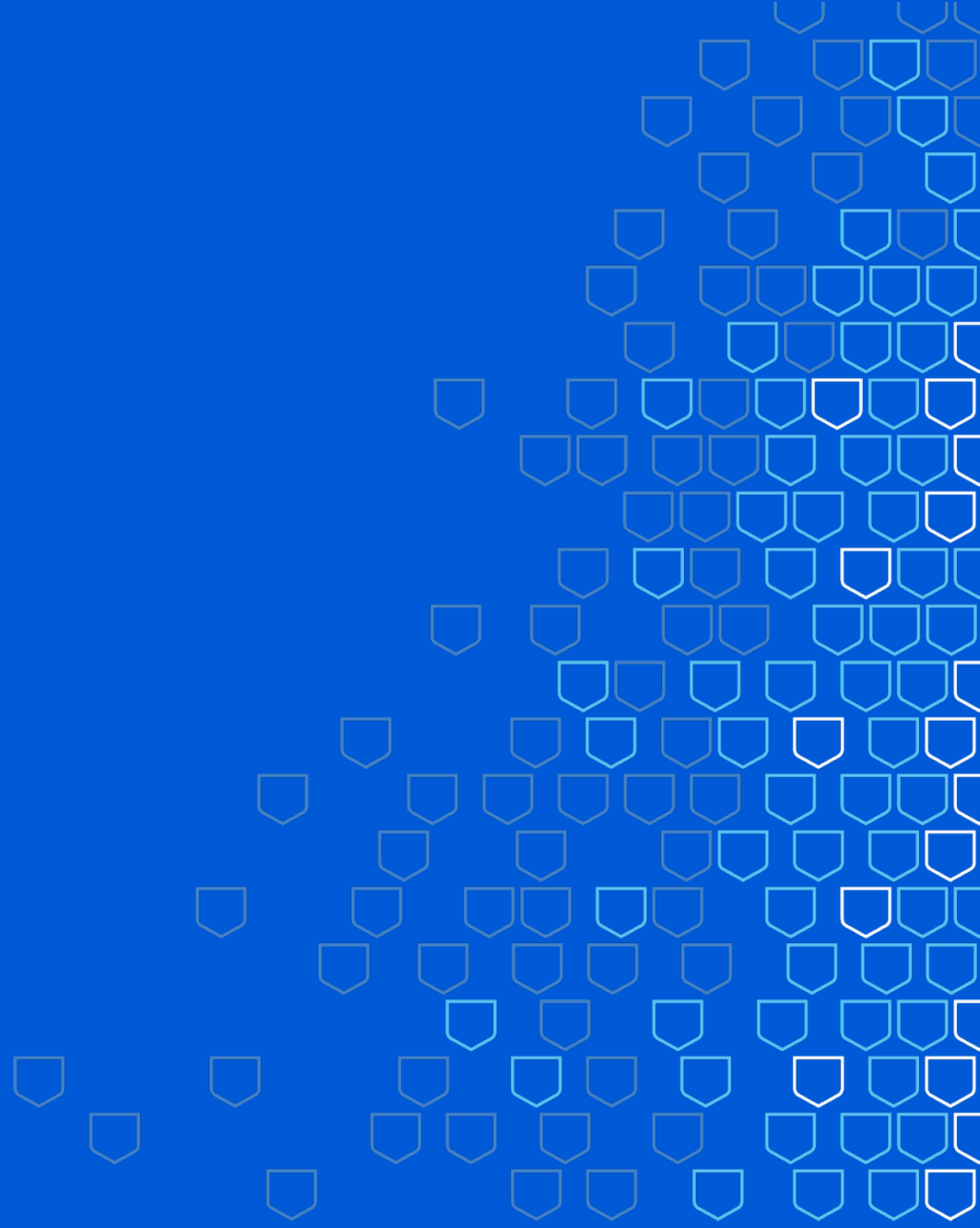
- Untersucht den Netzwerkverkehr auf Anzeichen von Exploits
- Kann Angriffe auf Betriebssysteme, Netzwerk-Stacks, Server, Endpunkte, Browser, Anwendungen und mehr erkennen

Features

- Höchste Sicherheitseffektivität und Leistung
- Von den SophosLabs erstellte und kuratierte Signaturen zusammen mit Cisco Talos-Signaturen
- Empfohlen von den NSS Labs
- Granulare Kategorien erleichtern die Feinabstimmung von Leistung/Schutz



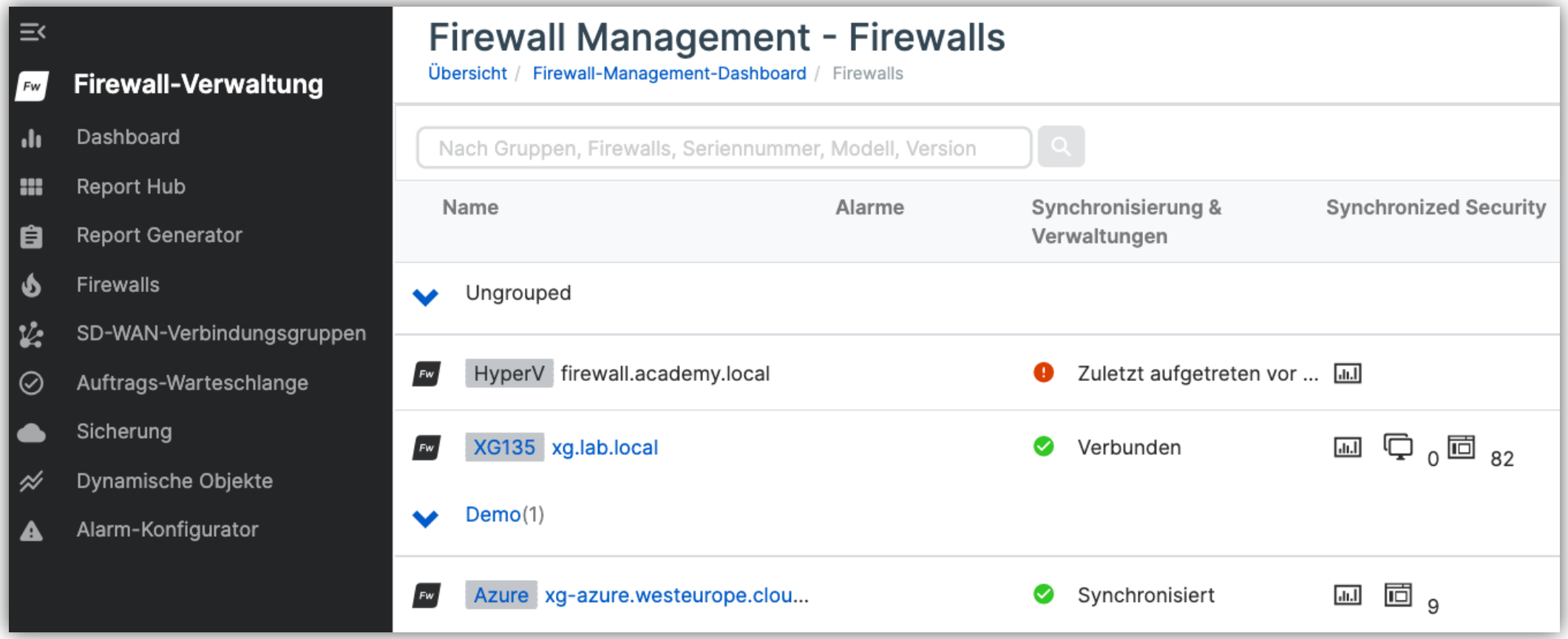
Central Management



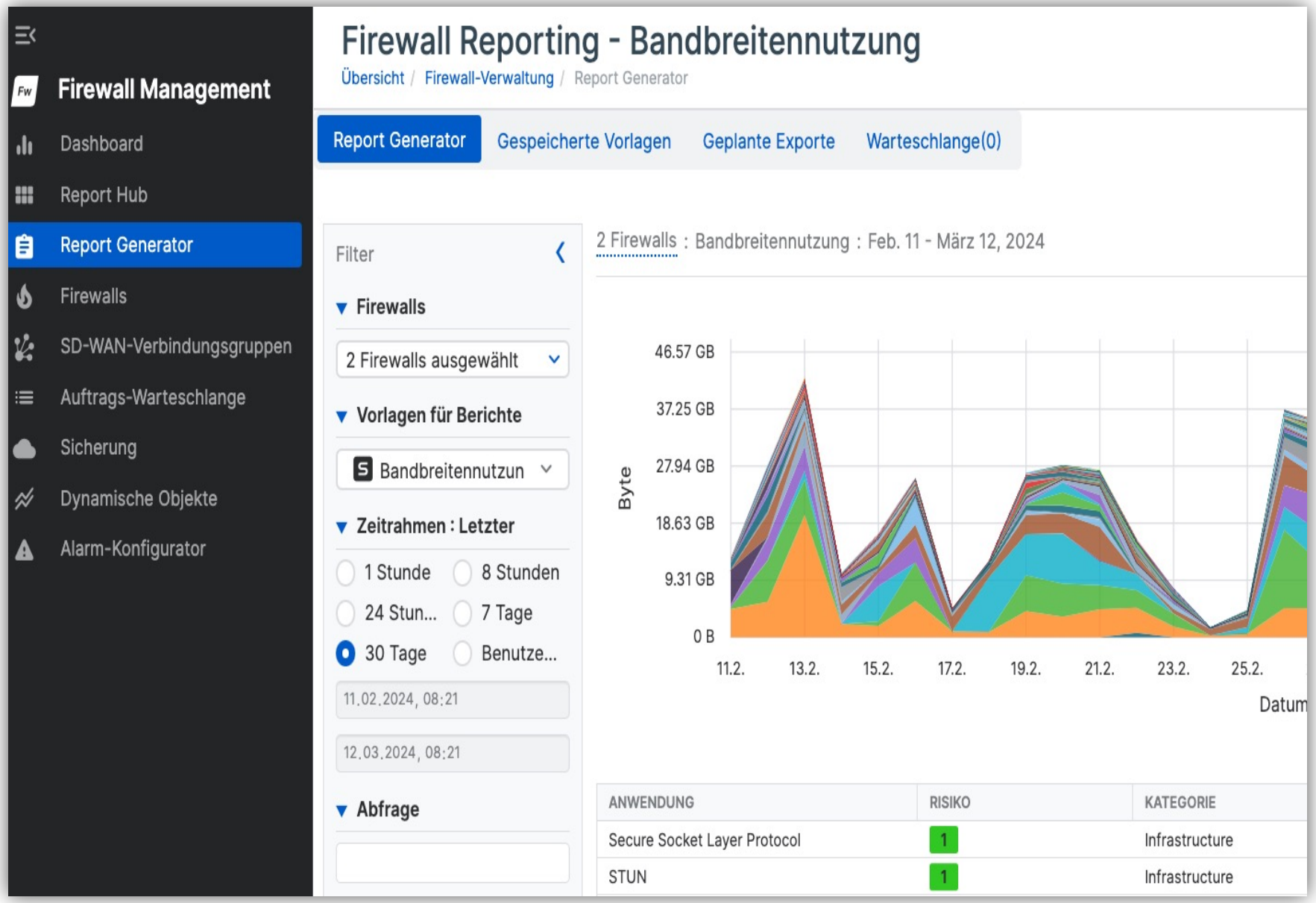
SOPHOS

Central Management

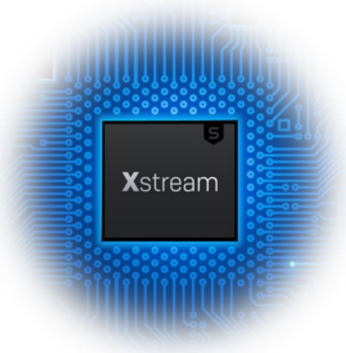
- Erstellung von Firewall Gruppen (inkl. Policy)
- Definition von globalen Objekten



Reporting


Firewall Management
Dashboard
Report Hub
Report Generator
Firewalls
SD-WAN-Verbindungsgruppen
Auftrags-Warteschlange
Sicherung
Dynamische Objekte
Alarm-Konfigurator
Firewall Reporting - Bandbreitennutzung
Übersicht / Firewall-Verwaltung / Report Generator
Report Generator
Gespeicherte Vorlagen
Geplante Exporte
Warteschlange(0)
Filter
Firewalls
2 Firewalls ausgewählt
Vorlagen für Berichte
Bandbreitennutzun
Zeitrahmen : Letzter
1 Stunde
8 Stunden
24 Stun...
7 Tage
30 Tage
Benutze...
11.02.2024, 08:21
12.03.2024, 08:21
Abfrage
2 Firewalls : Bandbreitennutzung : Feb. 11 - März 12, 2024
46.57 GB
37.25 GB
27.94 GB
18.63 GB
9.31 GB
0 B
Byte
11.2.
13.2.
15.2.
17.2.
19.2.
21.2.
23.2.
25.2.
Datum
ANWENDUNG
RISIKO
KATEGORIE
Secure Socket Layer Protocol
1
Infrastructure
STUN
1
Infrastructure

Mehrwerte in der Sophos Firewall



- Synchronized Security
- Zone Based Firewalling
- IKEv2 und Route based VPN
- Enterprise NAT
- SD-WAN policy-based routing
- Sophos Connect
- Next Generation IPS
- Xstream Architecture
- Light Touch Deployment
- Central Integration

Systeme zur Angriffserkennung (SzA) - Whitepaper

Systeme zur Angriffserkennung (SzA)

Diese Sophos-Lösungen unterstützen Sie beim Erfüllen der BSI-Anforderung

Nach einer Neuerung im deutschen BSI-Gesetz (BSIG) und im Energiewirtschaftsgesetz (EnWG) müssen Betreiber Kritischer Infrastrukturen sowie Betreiber von Energieversorgungsnetzen in Deutschland gegenüber dem BSI so genannte Systeme zur Angriffserkennung (SzA) vorweisen können. Dieses Dokument bietet eine Übersicht, wie Sophos-Lösungen bei der Umsetzung der Anforderung unterstützen können.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
Grundsätzliche Anforderungen					
MUSS	Die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen MÜSSEN geschaffen werden.	✓	alle	MDR	Die technischen Sophos-Lösungen sowie der Sophos MDR-Service können in die Strukturen und Abläufe der Organisation eingebunden werden.
MUSS	Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten MÜSSEN fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.	✓	alle	MDR	Die Sophos X-Ops und Sophos Labs liefern den Sophos-Lösungen sowie dem Sophos MDR-Team kontinuierlich Informationen über aktuelle Angriffsszenarien.
MUSS	Alle zur effektiven Angriffserkennung erforderliche Hard- und Software MUSS durchgängig auf einem aktuellen Stand gehalten werden.	✓	alle	MDR	Sophos-Lösungen ermöglichen ein automatisiertes Aktualisieren der Hard- und Software-Komponenten.
MUSS	Die Signaturen von Detektionssystemen MÜSSEN immer aktuell sein.	✓	alle		Die Aktualisierung der Signaturen von Detektionstechnologien in Sophos-Lösungen erfolgt automatisch.
MUSS	Alle relevanten Systeme MÜSSEN so konfiguriert sein, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt werden können, sofern keine schwerwiegenden Gründe dagegensprechen.	✓	alle	MDR, Professional Services	Auf Endpoints und im Netzwerk werden Angriffe erkannt und gestoppt, die versuchen, Schwachstellen auszunutzen. Die Konfiguration sowie deren Überprüfung kann durch Sophos Professional Services und Sophos MDR unterstützt werden.

SOPHOS

Die nächsten Schritte

Entscheidungsvorlage für IT-Leiter und Geschäftsführer

Jetzt downloaden

Podcast

Cybersecurity für kritische Infrastrukturen – was KRITIS-Unternehmen aus gesetzlicher Sicht beachten müssen mit Rechtsanwalt Andreas Daum, LL.M. (LSE) von Noerr Partnerschaftsgesellschaft mbB.

Zum Podcast

IT-Sicherheitsgesetz und Kritis

Das neue IT-Sicherheitsgesetz 2.0 betrifft nicht nur KRITIS-Betreiber in Deutschland, sondern auch deren Lieferanten in anderen Ländern. Weitere Informationen erhalten Sie auf unserer Webseite.

sophos.de/it-sicherheitsgesetz

Kontakt

Wenn Sie Fragen haben oder Unterstützung benötigen, ist Ihr Sophos-Ansprechpartner gerne für Sie da und hilft Ihnen weiter.

gesundheitswesen@sophos.de

SOPHOS