Sophos MDR
Managed Detection and Response

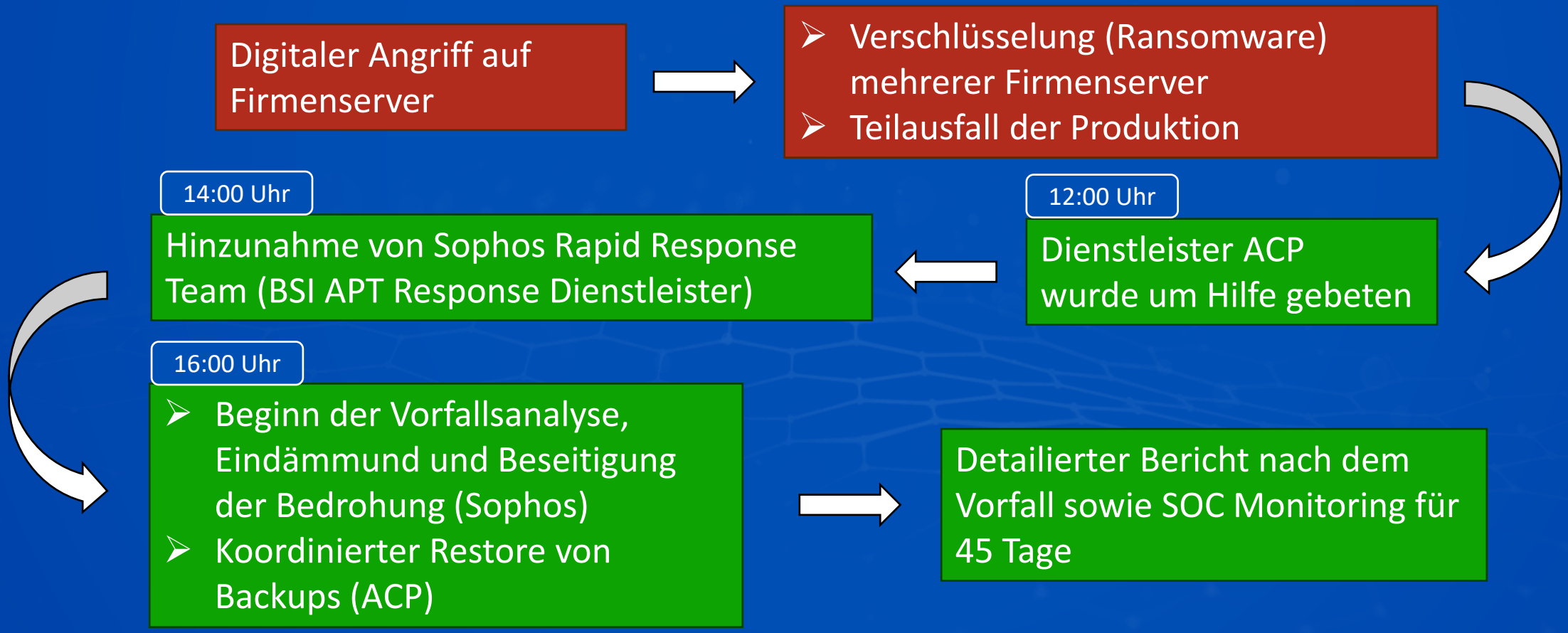
Stefan Scheck
Senior Sales Engineer - National

September 2023

SOPHOS

Cyberattacke auf Holzverarbeitungsbetrieb LKR Deggendorf

- Traditionsunternehmen mit Ca. 220 Mitarbeiter , > 60 Mio Jahresumsatz
- Vorfall am **13.09.2023** um 8.00 Uhr festgestellt



203 Mrd.€ Schaden für deutsche Unternehmen in 2021 durch Cyberangriffe[1]

84 Prozent der Unternehmen hatten Datendiebstahl, Ransomware, Sabotage[1]

6,2 Mrd.€ Investition in IT-Sicherheit 2021[2]

[1] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022
[2] https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/

SOPHOS

Die Cybersecurity Challenge

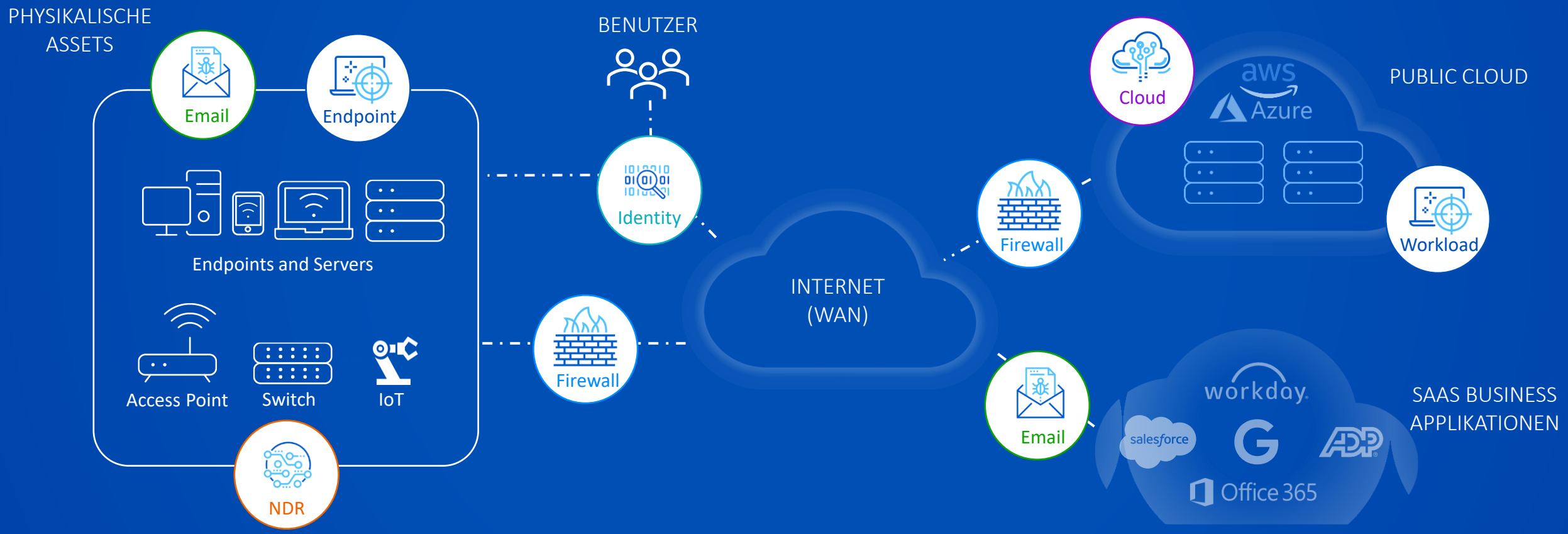
Cybersicherheit ist so komplex, so schwierig und entwickelt sich so schnell, dass die meisten Unternehmen sie alleine einfach nicht effektiv bewältigen können.

- Cyberbedrohungen nehmen an Umfang und Komplexität zu
- Cybersicherheitstools sind überaus kostspielig und komplex
- Die Einstellung und Bindung von Cybersicherheitsexperten ist zu einem Wettbewerb geworden

Dazu kommen:

- **Reaktiv**
- **Unübersichtlichkeit**
- **Inkompatibilität**

Sicherheitslösungen verteilt in der gesamten Umgebung



SOPHOS

Cybercrime as a service

Service	Preis in US $ (gesamt oder pro Nutzungszeitraum / pro Einheit)	
BankingTrojaner		
▪ Desktop-Version	1.000 - 10.000 $	bei Kauf
▪ Mobile-Version	1.000 - 10.000 $	bei Kauf
RAT	89 - 530 $	pro Monat bei Miete
(Remote Administration Tool)	Ca. 3.000 $	bei Kauf
Mining Bots	50 – 150 $	pro Monat bei Miete
Crypting	20 - 100 $	bei Kauf von einem Crypt
	360 - 500 $	bei einem Wochen-Abo mit 50 Crypts pro Tag
Spam	10 ct - 4 $	pro Spam
DDoS as a Service	80 - 1.500 $	pro Monat bei Miete
Bulletproof Hosting		
▪ Shared	5 - 50 $	pro Monat bei Miete
▪ Dedicated	50 - 700 $	pro Monat bei Miete

Abbildung 11: Übersicht krimineller Services im Darknet

Wer sagt, dass ich das wirklich brauche?

- **Cyberrisikenversicherer**
- **DSGVO**
- **NIS2**

Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

Technische und organisatorische Maßnahmen

2023

3.2.22 Endpoint Detection & Response Plattform

Der Schutz der Endgeräte (z.B. PCs, Laptops, Smartphone oder Tablets) erfordert inzwischen weit mehr als nur ein Antivirus-Programm. Moderne Lösungen (Endpoint-Detection & Response Plattformen, EDR) vereinen neueste Schutztechnologien um alle Arten von Cyber-Angriffen auf Client und Server Systemen betriebssystemübergreifend zu stoppen und die Urheber zu identifizieren. Im Gegensatz zu konventionellen Lösungen ist kein spezifisches Vorwissen, wie z. B. Signaturen oder ein erstes Opfer nötig.

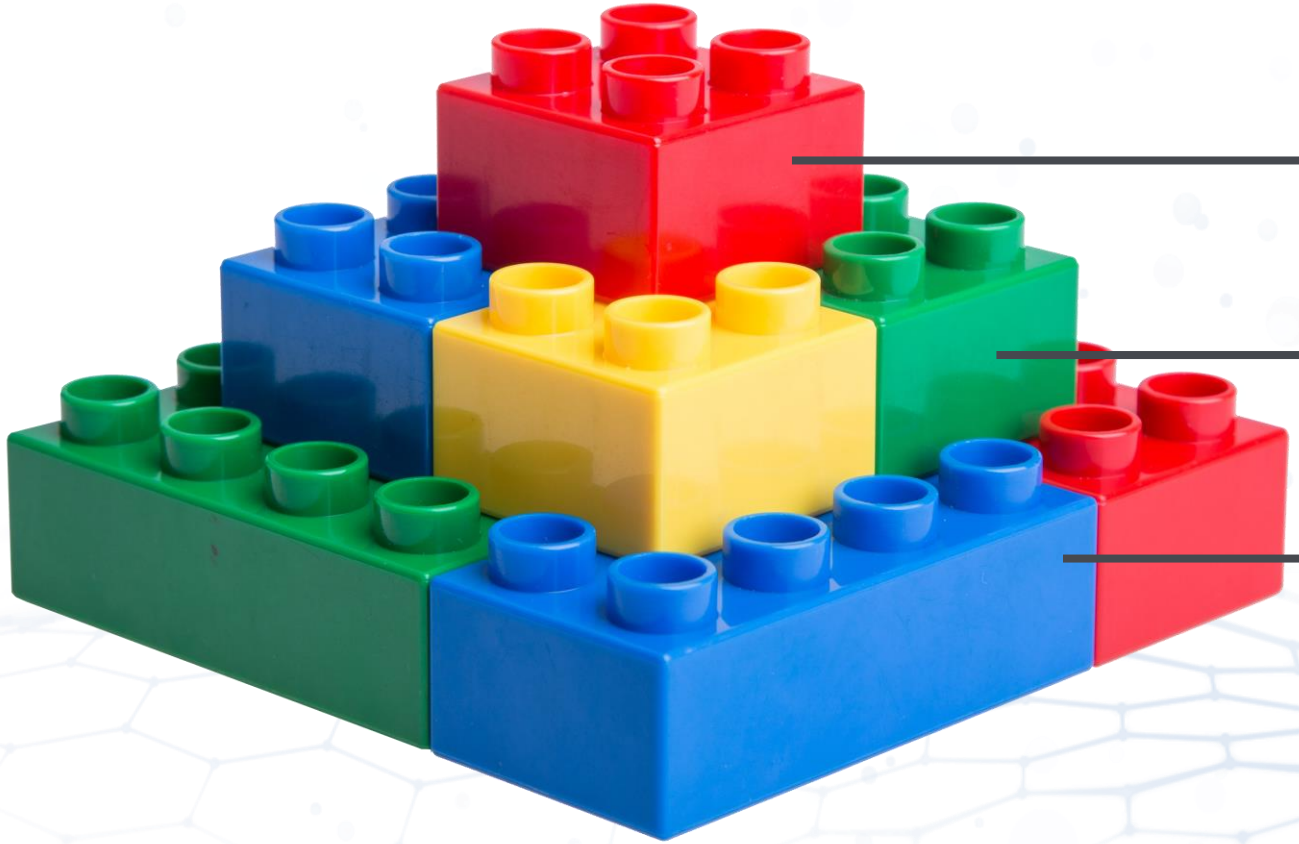
Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

- Malware
- Exploitation
- Maliziöse Scripte
- Hacker-Aktivitäten
- Missbrauch von Administrativen Werkzeugen und Tools in schädlicher Absicht

https://www.stand-der-technik-security.de/fileadmin/user_upload/2023-05_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

SOPHOS

Adaptive Cybersecurity Ecosystem - Funktionspyramide



Managed SOC | 7x24 & Experten
(Intercept X Advanced mit MDR)

Sichtbarkeit und Reaktion | Werkzeug
(Intercept X Advanced mit XDR)

Bester Endpoint-Schutz
(Intercept X Advanced)

SOPHOS

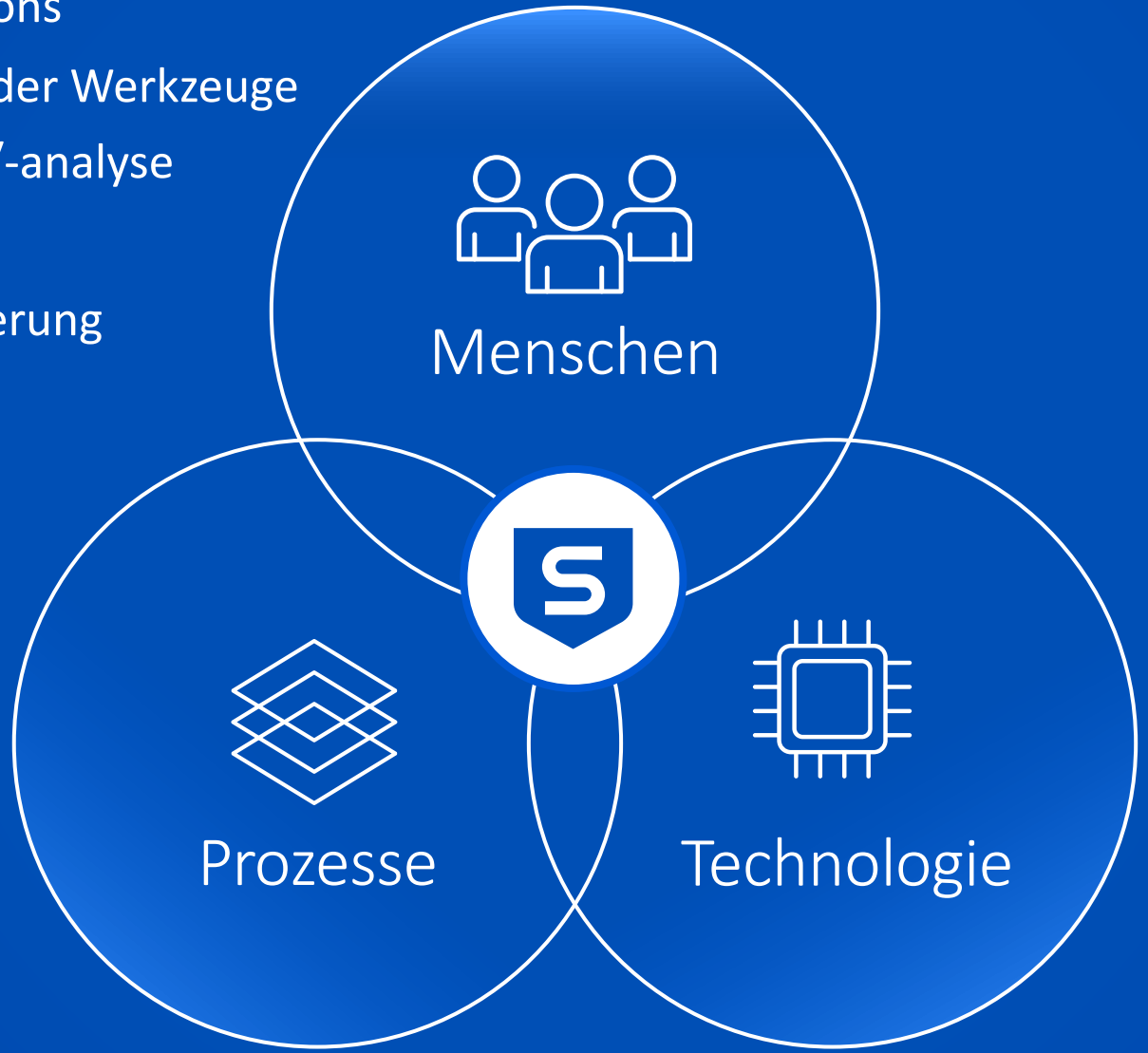
Was ist Managed Detection and Response (MDR)?

Ein vollständig verwalteter Rund-um-die-Uhr-Service der von Experten bereitgestellt wird, die darauf spezialisiert sind, Cyberangriffe zu erkennen und darauf zu reagieren, die Technologielösungen allein nicht verhindern können

Sophos MDR

24/7 Security Operations

- Aktive Bedienung der Werkzeuge
- Bedrohungssuche/-analyse
- Threat Intelligence
- Proaktive Verbesserung der Sicherheit



Vorgehen bei Vorfall

- Incident/Response
- Eindämmung
- Neutralisierung
- Wiederherstellung

Stand der Technik = XDR Ökosystem

- NextGen Schutz überall
- Telemetrie aller Quellen
- Erkennung + Korrelation
- Reaktion
- Automation

= Werkzeuge

SOPHOS

Erweiterte Telemetrie ermöglicht Sophos tiefe Einblicke

Sensoren

- Identity
- Cloud SaaS
- Firewall
- Network
- Email
- Endpoint

Data Lake

Geräte- und technologieübergreifende Aktionen
Ereigniskorrelation

Public Cloud
Ereignisse an unterschiedlichen Orten

Ungeschützte Geräte
Kommunikation von Geräten ohne XDR-Schutz

Mehrstufige Angriffe
Phishing -> Übernahme von Accounts -> Ausbreitung

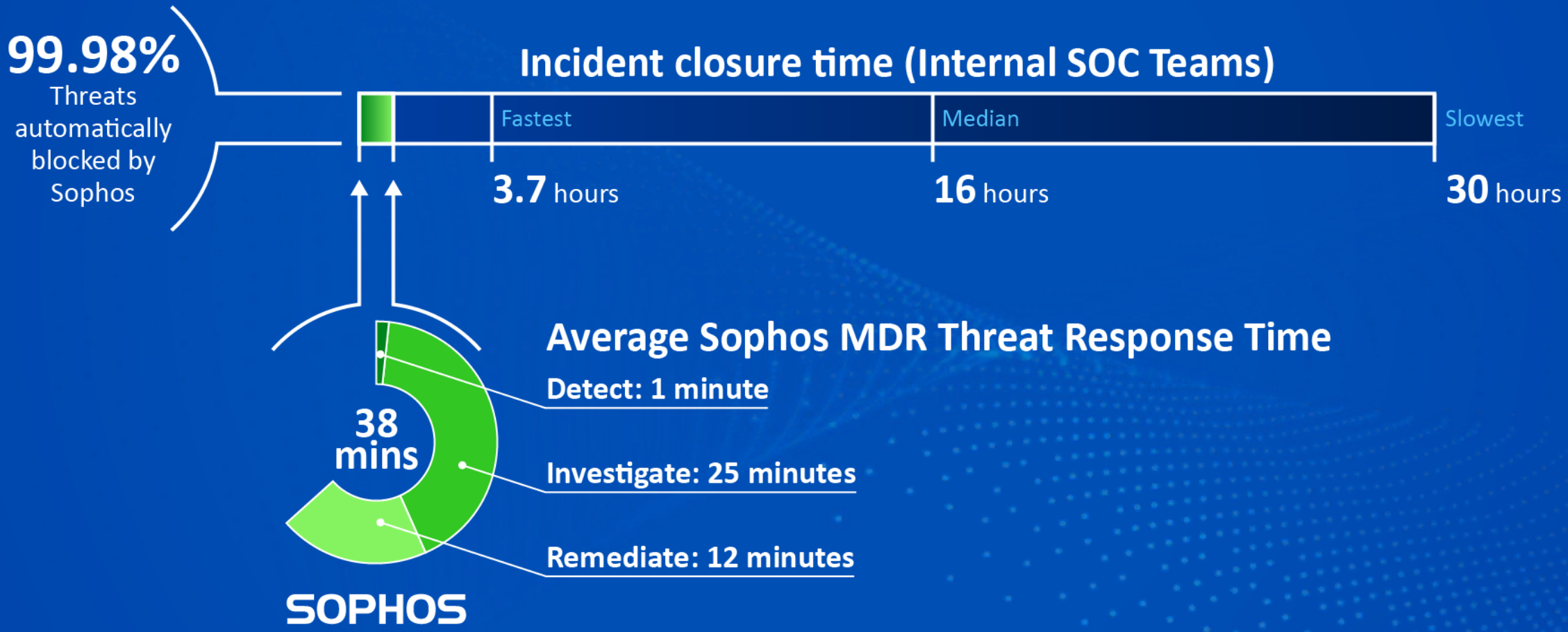
Verschlüsselter Netzwerkverkehr
Network Detection and Response (NDR)

Analyse

Aktive Bedrohungen

SOPHOS

Leading Detection and Response Times



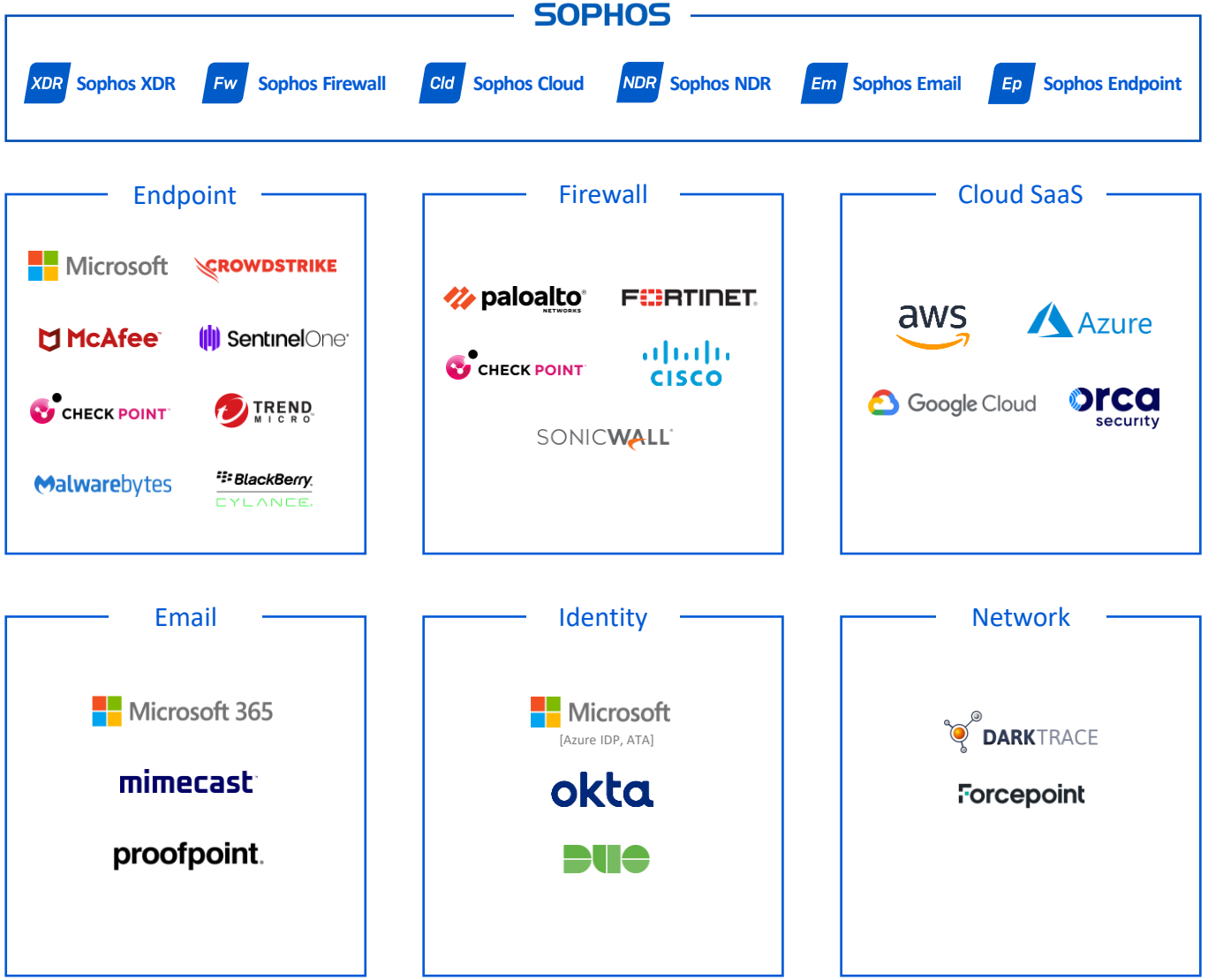
SOPHOS MDR: Offen und flexibel

MDR Sophos MDR

Kompatibel mit Ihrer Umgebung
Wir nutzen Sophos Werkzeuge, die Werkzeuge anderer Anbieter – oder eine Kombination aus beiden

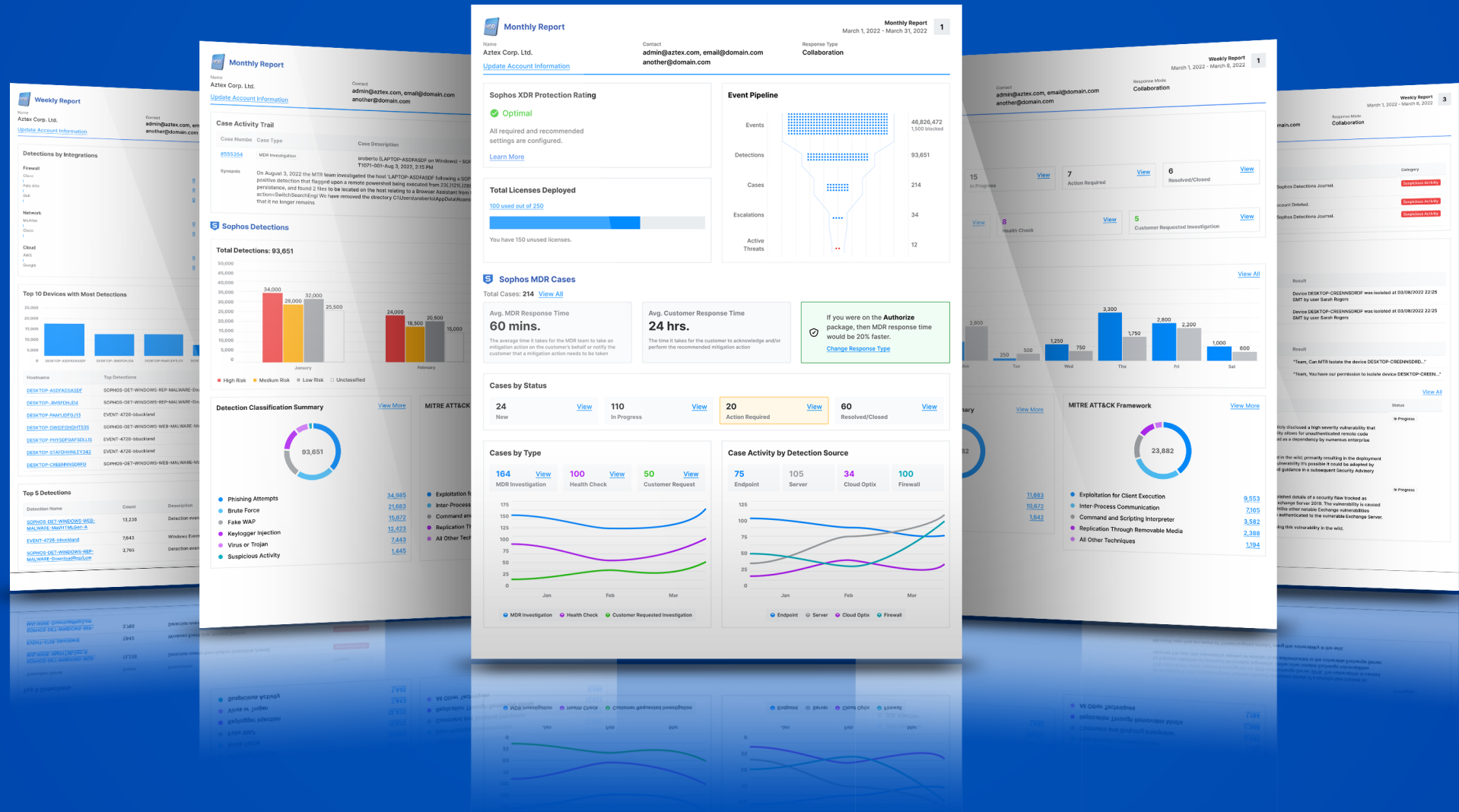
Kompatibel mit Ihren Anforderungen
Wir bieten komplettes Incident Response - oder Unterstützung für Ihr Team

Kompatibel mit Ihrem Unternehmen
Unser Team hat umfangreiche Erfahrung mit Angriffen auf Unternehmen aller Branchen



SOPHOS

Managementtaugliche Cybersecurity Reports



SOPHOS

Sophos MDR Servicestufen

	Sophos MDR	Sophos MDR Complete
24/7 Überwachung, Bedrohungserkennung und Reaktion durch Experten	✓	✓
Kompatibel mit Security-Werkzeugen anderer Hersteller	✓	✓
Wöchentliches und monatliches Reporting	✓	✓
Monatliches Briefing “Sophos MDR ThreatCast” zu aktuellen Bedrohungen	✓	✓
Sophos Account Health Check – ist Sophos XDR richtig konfiguriert?	✓	✓
Proaktive Bedrohungssuche durch Experten	✓	✓
Stoppen und Eindämmen von Bedrohungen Voraussetzung: voller Sophos XDR Agent (Schutz, Erkennung, Reaktion) oder Sophos XDR Sensor (Erkennung, Reaktion)	✓	✓
Direkter Telefon-Support bei Vorfällen	✓	✓
Vollständiges Incident-Response: komplette Neutralisierung von Bedrohungen Voraussetzung: voller Sophos XDR Agent (Schutz, Erkennung und Reaktion)		✓
Ursachenanalyse – und wie können erneute Angriffe verhindert werden?		✓
Dedizierter Ansprechpartner beim Incident Response Team		✓
Breach Protection Warranty		✓

SOPHOS

Sophos
Rapid Response

Blitzschnelle Unterstützung bei aktiven Bedrohungen durch ein weltweites Expertenteam von Spezialisten

rapidresponse@sophos.com
+49 611 711 86766

SOPHOS Produkte Lösungen Partner Support

BSI stuft Sophos als qualifizierten APT-Response-Dienstleister ein

SOPHOS PRESS RELEASE

Nach intensiver Prüfung hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Sophos in seine Liste qualifizierter Dienstleister im Bereich APT aufgenommen.

Nach einem umfangreichen Prüfverfahren gehört Sophos nun der Liste qualifizierter APT-Response-Dienstleister (**A**dvanced **P**ersistent **T**hreat, kurz APT) für KRITIS-Unternehmen an. Diese Übersicht unterstützt Betreiber kritischer Infrastrukturen dabei, ohne großen Rechercheaufwand geeignete Service-Unternehmen zu identifizieren, die in der Lage sind, getarnte Cyberattacken, die über einen längeren Zeitraum ein Netz oder System angreifen, aufzudecken und zu stoppen.

Neben der von den geprüften Unternehmen zur Verfügung gestellten Dokumentation über ihre Services steht vor allem der Praxisbezug beim Auswahlverfahren im Fokus. In einem mehrstündigen Termin beim BSI müssen zertifizierte Dienstleister anhand fiktiver Szenarien wie zum Beispiel einer Ransomware-Attacke oder einer Phishing-Kampagne zeigen, dass sie in der Lage sind, die angesprochenen Problemstellungen fach- und zielgerichtet zu lösen. Dabei achten die Experten sowohl auf das allgemeine Vorgehen des Dienstleisters als auch auf gestellte Fragen und Verarbeitung der erhaltenen Informationen.

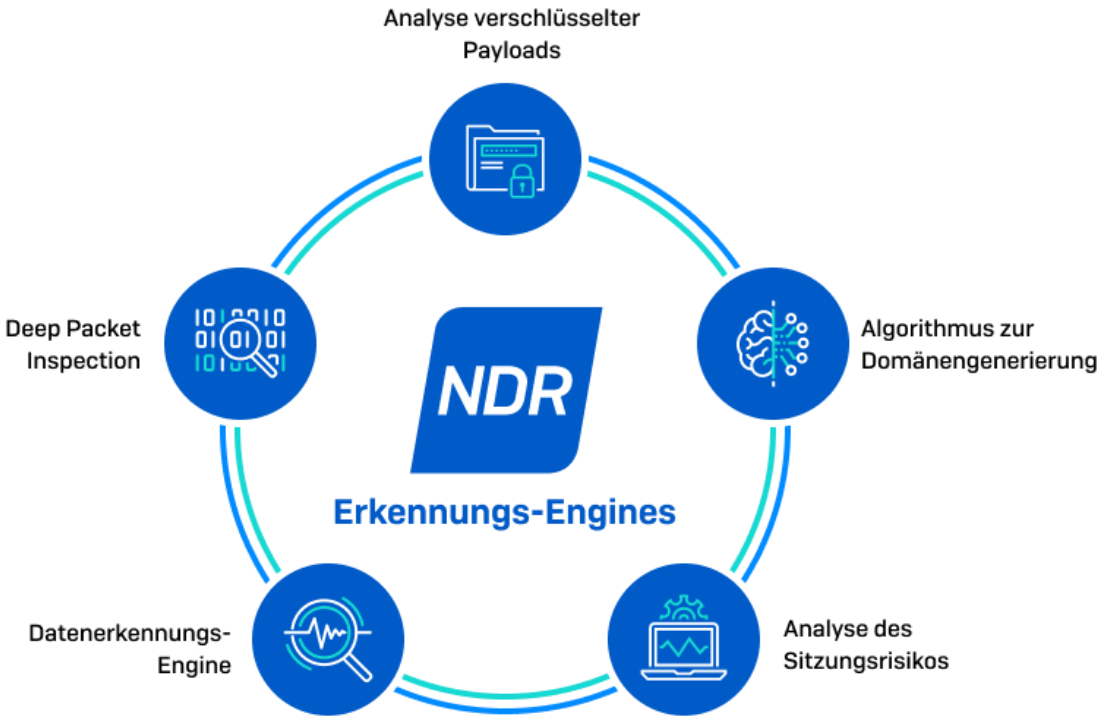
Über Sophos

Sophos ist ein weltweit führender Next-Gen-Cybersecurity-Anbieter und schützt über 500.000 Organisationen und Millionen von Kunden in mehr als 150 Ländern vor komplexen Cyberbedrohungen. Mit Threat Intelligence, KI und Machine Learning aus den SophosLabs und SophosAI bietet Sophos ein breites Portfolio modernster Produkte und Services. Diese schützen Benutzer, Netzwerke und Endpoints zuverlässig vor Malware, Exploits, Phishing und anderen Cyberangriffen. Mit Sophos Central hat Sophos eine zentrale, cloudbasierte Management-Konsole im Angebot. Sie bildet das Herzstück unseres adaptiven Cybersecurity-Ökosystems. Teil dieses Systems ist ein zentralisierter Data Lake. Er nutzt eine Vielzahl offener APIs, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung

Network Detection und Response (NDR)

NDR Einsatzszenarien

- Geräte ohne Endpointschutz
  - Industrie/Retail
    - z.B. Produktionsstraßen, IoT/OT/POS
  - Healthcare
    - z.B. Medizinische Geräte, Laborumgebungen
- Private Geräte in Firmeninfrastruktur?
- Veraltete Betriebssysteme (Telefonanlage)
- Unkontrollierte Netzwerksegmente



NDR Sensor Deployment

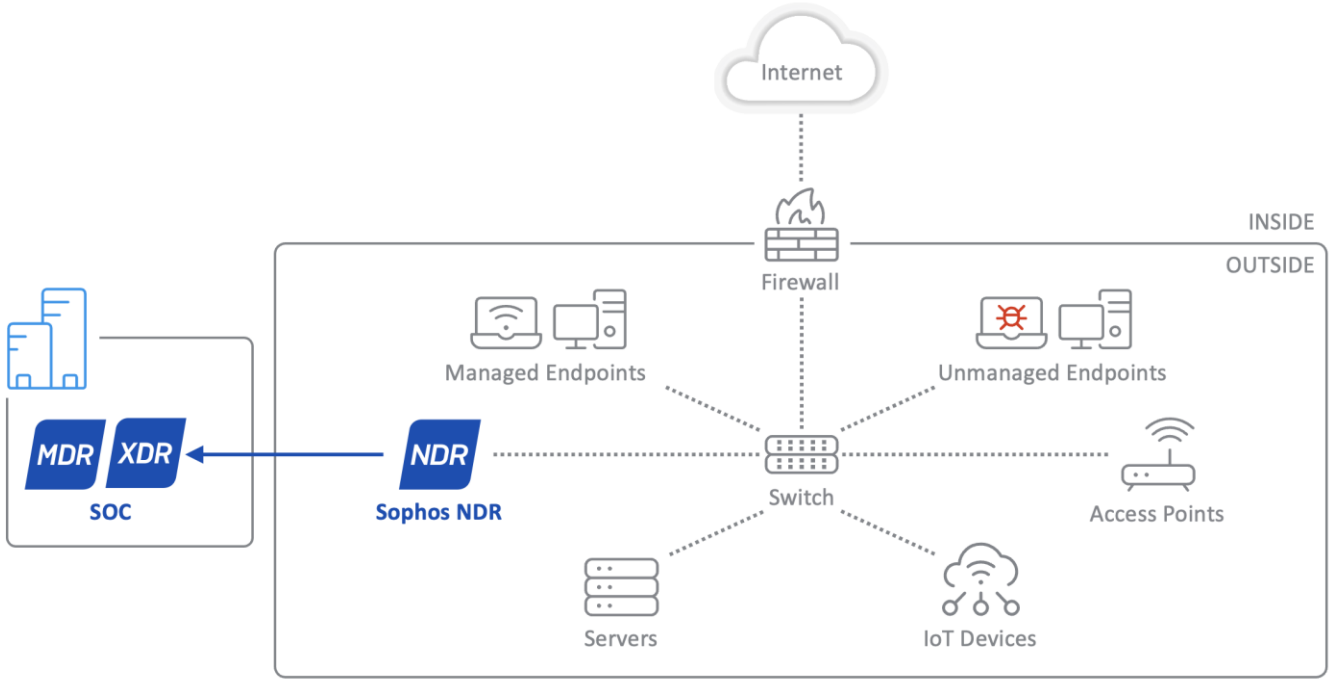
ist eine VM (Hyper-V / ESXi / *bald AWS AMI*)

hängt am Mirror Port des Switches

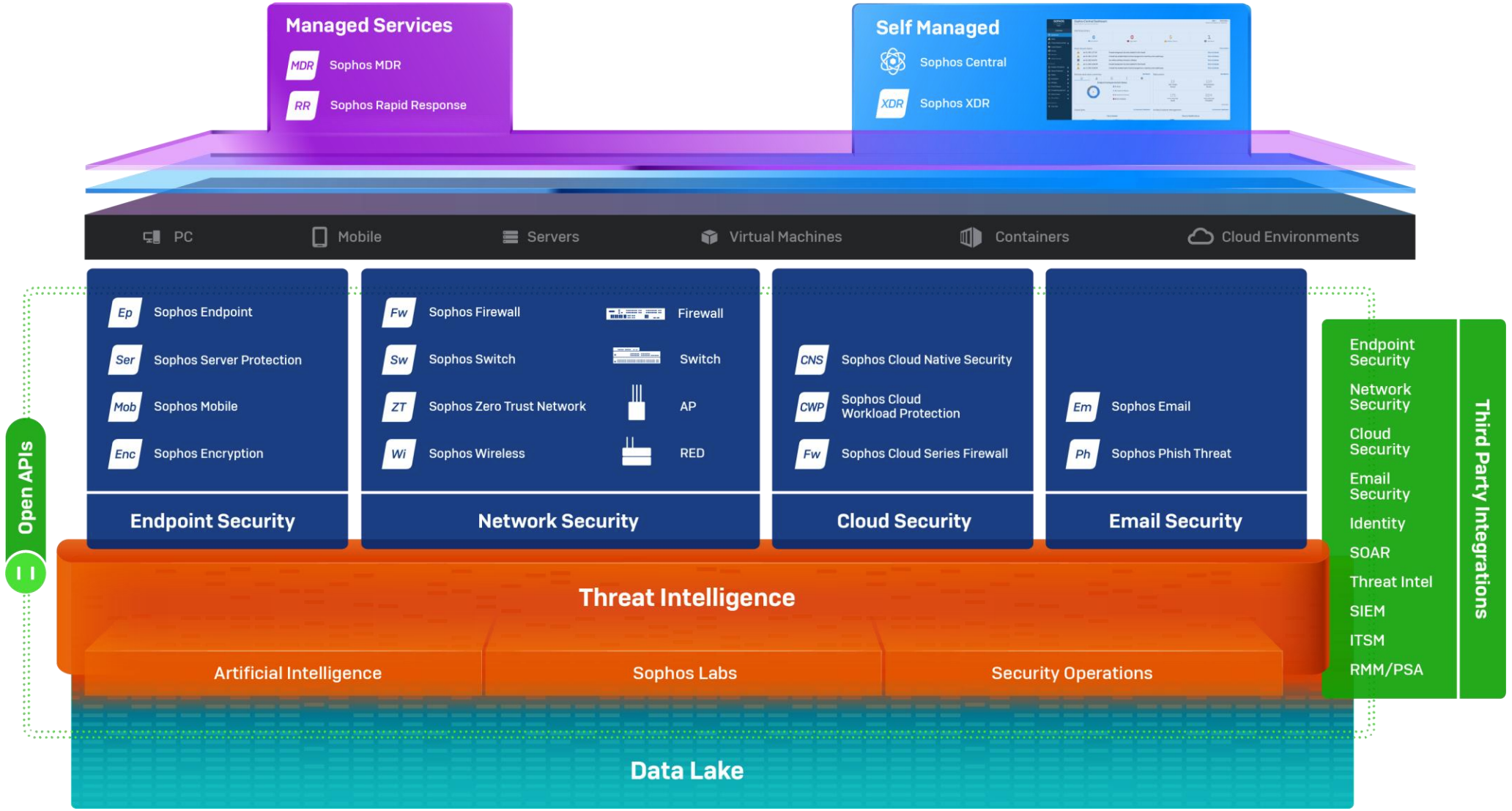
jeglicher Traffic landet gespiegelt auf der Appliance

sendet Informationen zu Sophos Central

Central GUI per Appliance Manager



Adaptive Cybersecurity Ecosystem - ACE



SOPHOS

SOPHOS

Cybersecurity delivered.