
15. BECHTLE IT-FORUM
THÜRINGEN
2024
BECHTLE
15. Mai 2024 • STEIGERWALD Stadion Erfurt
Hewlett Packard Enterprise
cisco Partner
HUAWEI
intel.

# Zukunftssichere IT-Sicherheit mit einem Managed SOC Service

Roman Schlenker
National Sales Engineer

Freitag, 3. Mai 2024

SOPHOS

# Was sind aktive Angreifer und wie gehen sie vor?

# Was sind aktive Angreifer?

Aktive Angreifer sind versierte Cyberkriminelle, die häufig umfassende Software- und Netzwerkkenntnisse besitzen. Sie verschaffen sich Zugriff auf die Systeme eines Unternehmens, entziehen sich der Erkennung und **passen ihre Techniken** kontinuierlich an. Mit manuellemHacking und KI-gestützten Methoden umgehen sie präventive Sicherheitskontrollen und führen den Angriff aus.

# Wie gehen aktive Angreifer vor?

## MEHRPHASIGE ANGRIFFE

Angriffe enden an einer anderen Stelle, als sie begonnen haben

## „LIVING OFF THE LAND“-ANGRIFFE

Es werden legitime Tools genutzt, um keinen Verdacht zu schöpfen

## UNBEKANNTE SICHERHEITSLÜCKEN

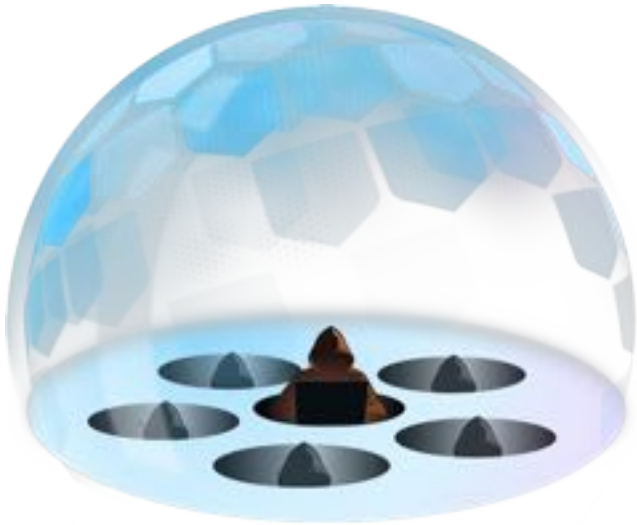
Schwachstellen oder Fehler in Software werden ausgenutzt


## MISSBRAUCH VON ZUGANGSDATEN

Der Zugriff erfolgt über legitime Zugangsdaten, statt „einzubrechen“

# Wie stoppen Sie aktive Angreifer?

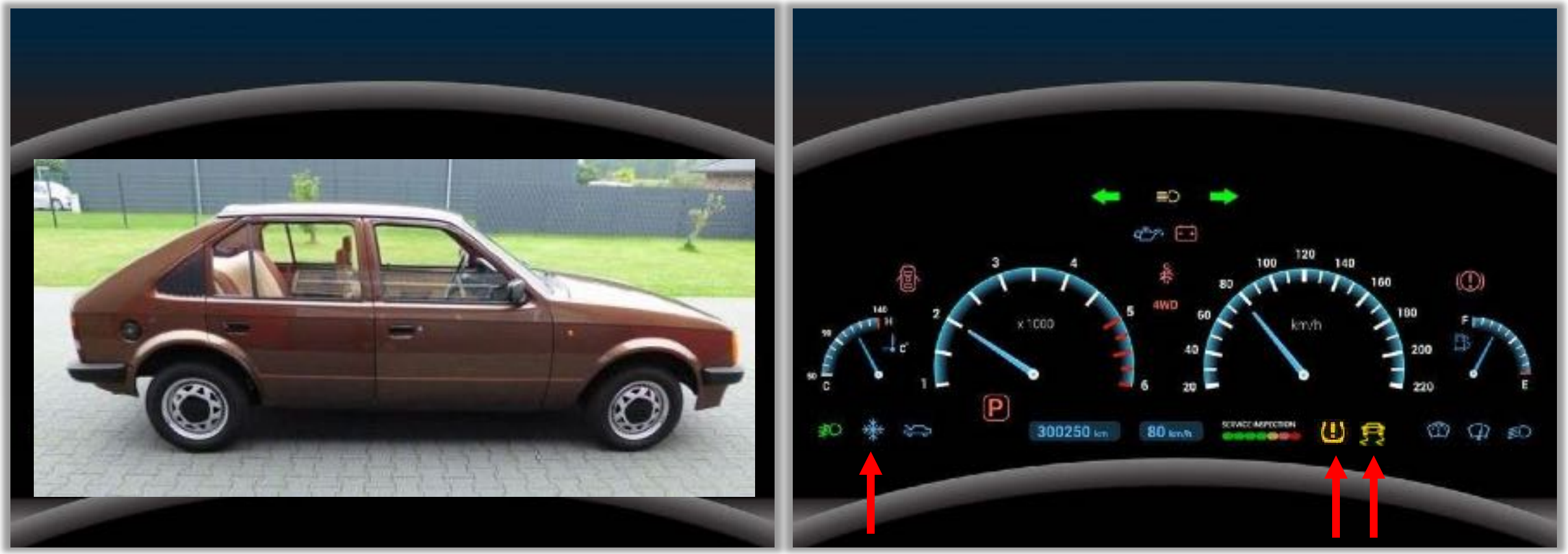
vs.



**Einzelne Produkte für einzelne Angriffe**

**Vernetzte Produkte und Services, die zusammenarbeiten**

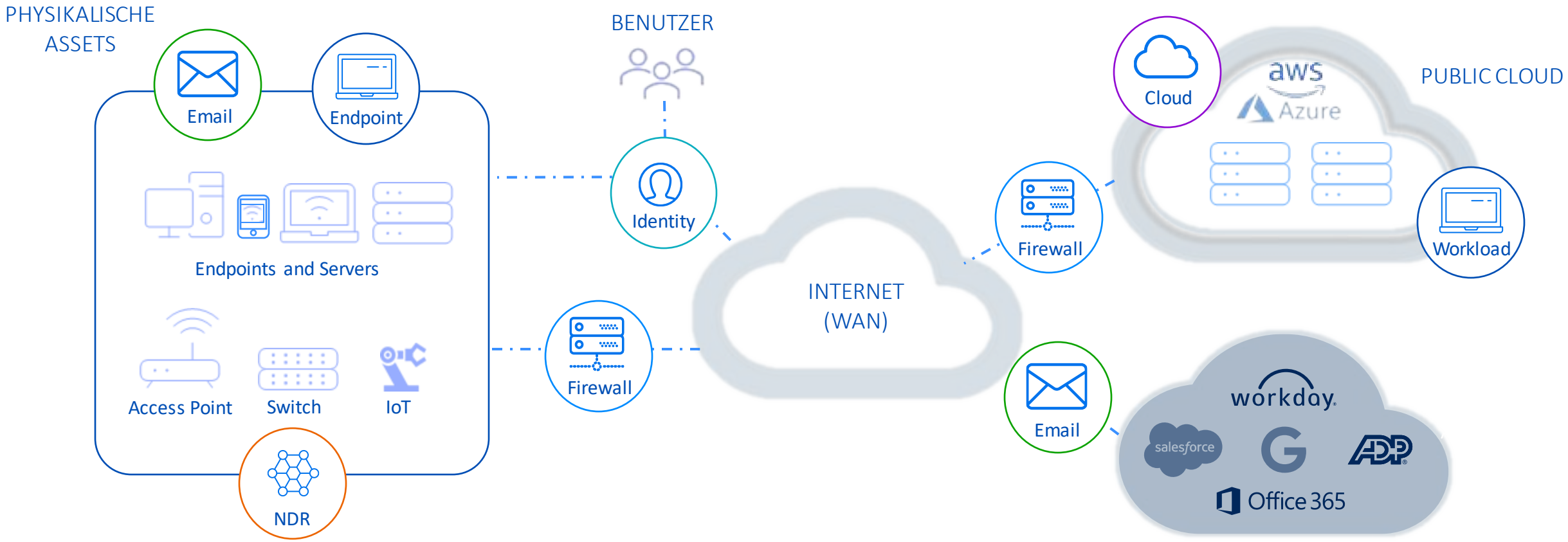
# Warum brauche ich nochmal Telemetrie?




**Und das ist nur der Bereich „Heimgebrauch“**

# Telemetrie bei den Profis

# Sicherheitslösungen verteilt in der gesamten Umgebung



# Expanding our Existing Portfolio

## SMB AND BRANCH OFFICE

**DESKTOP**

XGS 87, 87w, 107, 107w

XGS 116, 116w, 126, 126w, 136, 136w

## DISTRIBUTED EDGE

**1U RACKMOUNT**

XGS 2100, XGS 2300, XGS 3100, XGS 3300

XGS 4300, XGS 4500

## ENTERPRISE and CAMPUS EDGE

**2U RACKMOUNT**

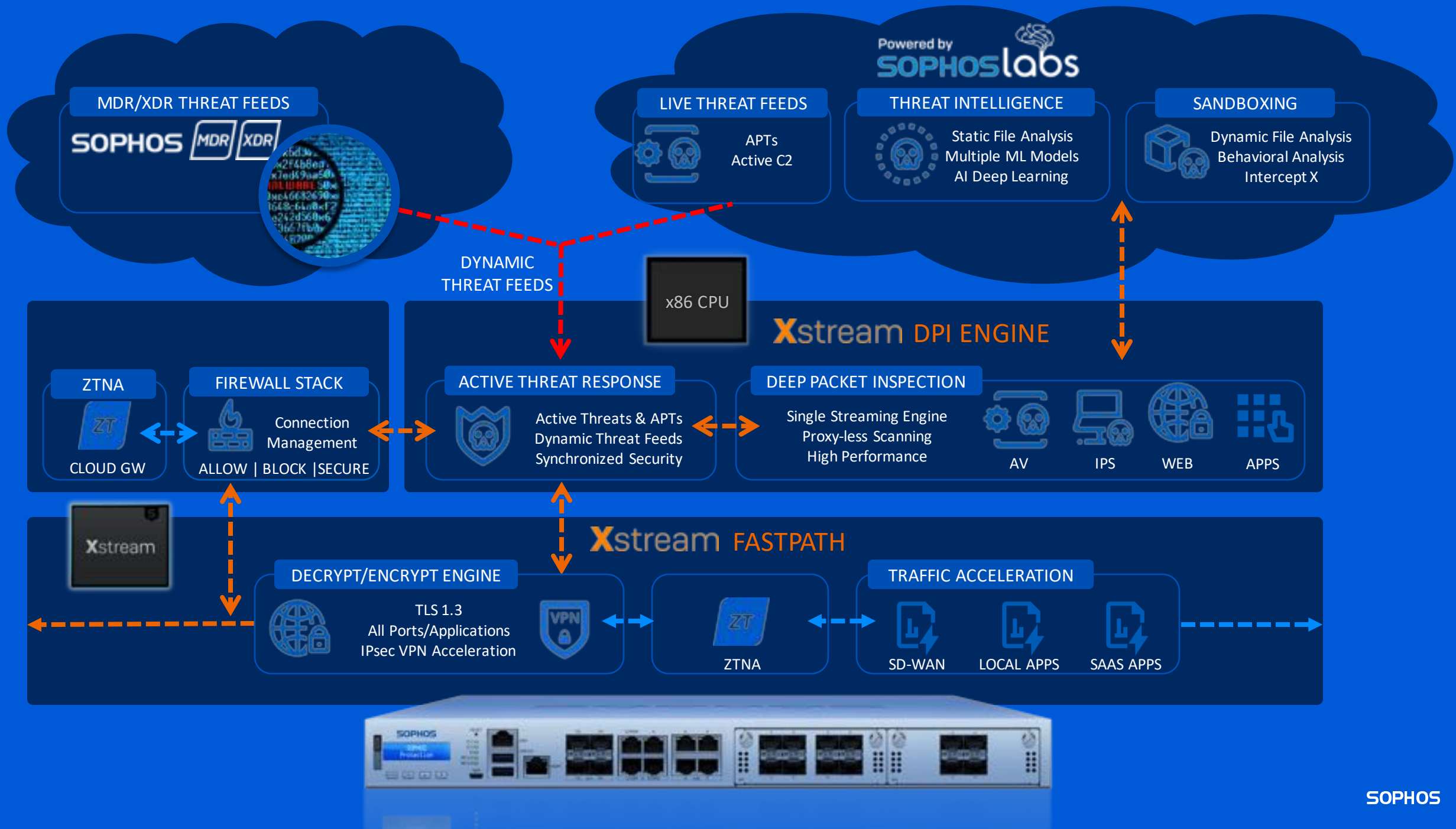
XGS 5500

XGS 6500

XGS 7500

XGS 8500

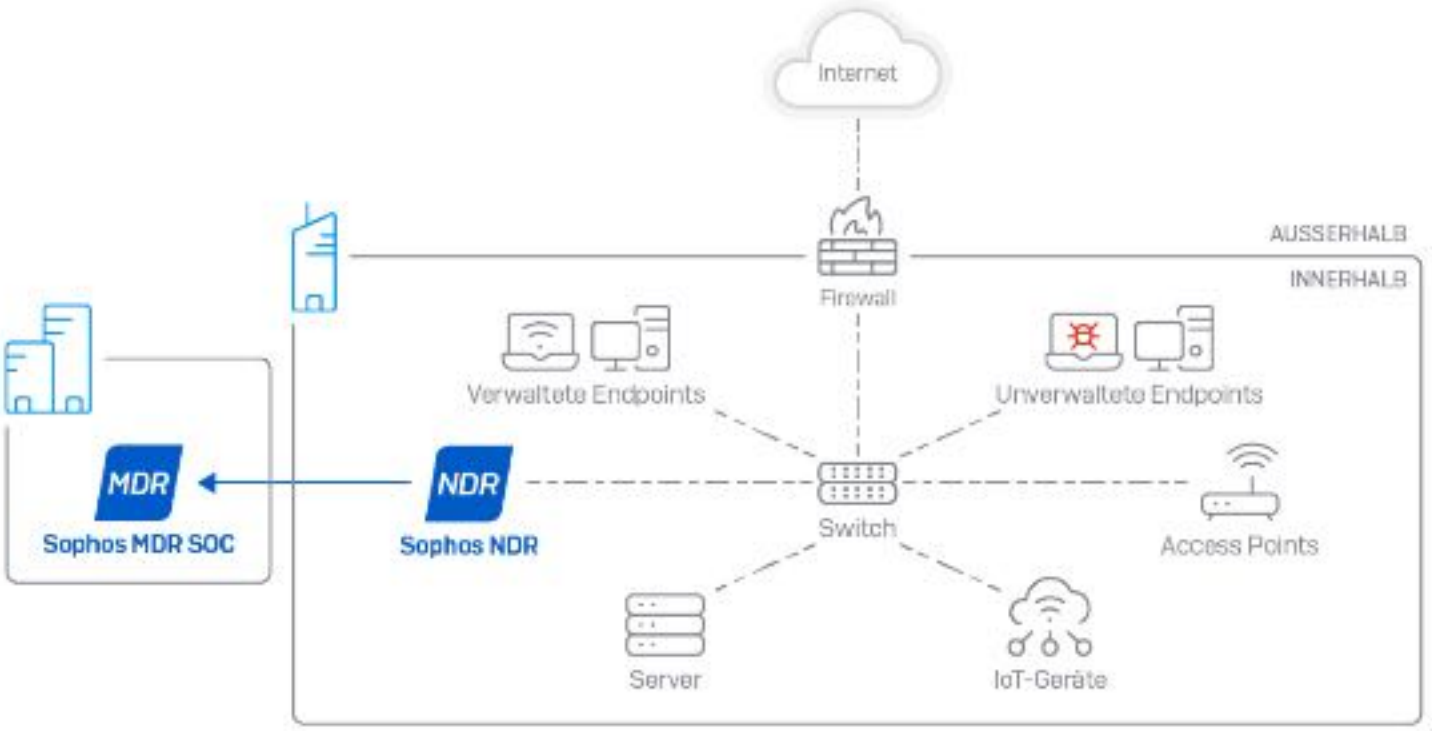
SOPHOS


MDR/XDR THREAT FEEDS
SOPHOS MDR XDR
Powered by SOPHOS labs
LIVE THREAT FEEDS
APTs
Active C2
THREAT INTELLIGENCE
Static File Analysis
Multiple ML Models
AI Deep Learning
SANDBOXING
Dynamic File Analysis
Behavioral Analysis
Intercept X
DYNAMIC
THREAT FEEDS
x86 CPU
Xstream DPI ENGINE
ZTNA
CLOUD GW
FIREWALL STACK
Connection
Management
ALLOW | BLOCK |SECURE
ACTIVE THREAT RESPONSE
Active Threats & APTs
Dynamic Threat Feeds
Synchronized Security
DEEP PACKET INSPECTION
Single Streaming Engine
Proxy-less Scanning
High Performance
AV
IPS
WEB
APPS
Xstream
Xstream FASTPATH
DECRYPT/ENCRYPT ENGINE
TLS 1.3
All Ports/Applications
IPsec VPN Acceleration
VPN
ZTNA
TRAFFIC ACCELERATION
SD-WAN
LOCAL APPS
SAAS APPS

SOPHOS

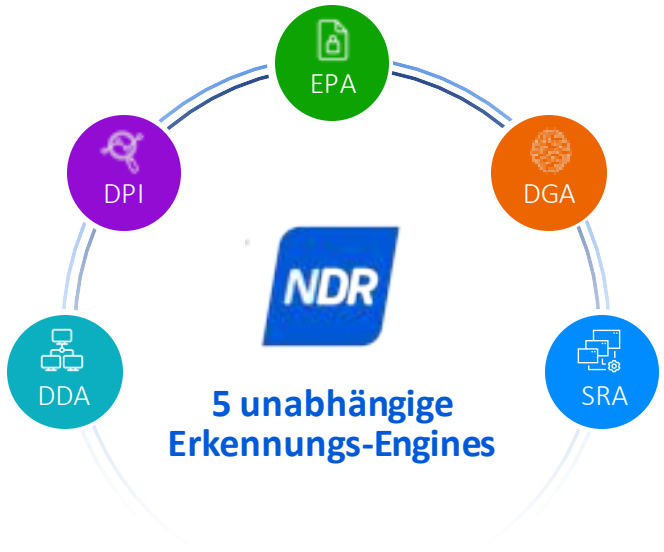
# Sophos Network Detection and Response

## Sophos NDR erkennt Angriffe selbst tief in Ihrem Netzwerk




- Überwacht den Datenverkehr mithilfe von fünf Echtzeit-Engines bis tief ins Netzwerk
- Erkennt Aktivitäten von nicht verwalteten Systemen, IoT-Geräten, nicht autorisierten Benutzern oder Assets und allen anderen Quellen des Netzwerkverkehrs

# SOPHOS NDR mit 5 unabhängigen Erkennungs-Engines in Echtzeit




**DDA** **Device Detection Analytics**

Identifiziert kommunizierende Systeme, die nicht mit Sophos geschützt sind, inkl. potentiell bösartiger Systeme

**DGA** **Domain Generation Algorithms**

Erkennt Versuche, durch die dynamische Erzeugung von Domains, die Erkennung von Command&Control-Verkehr zu umgehen

**DPI** **Deep Packet Inspection**

Erkennt sehr schnell bekannte Anzeichen für einen Angriff in verschlüsseltem und unverschlüsseltem Datenverkehr

**SRA** **Session Risk Analytics**

Analyse und Bewertung des Risikos einer Kommunikation aufgrund einer großen Menge von Merkmalen

**EPA** **Encrypted Payload Analytics**

Erkennt Zero-Day Command&Control-Kommunikation von Malware-Familien in verschlüsseltem Verkehr per Deep Learning basierend auf Metadaten

# NDR - EPA Detection Engine

CobaltStrike

QakBot

BazaLoader

Dridex

TrickBot

ZLoader

(Limb, J. (2021). *Identifying Network Applications Using Images Generated from Payload Data and Time Data. US Patent 11,159,560.* Washington, DC: U.S.)

## Encrypted Payload Analytics

Identifiziert Netzwerkverbindungen, die von Malware-Familien generiert werden, basierend auf Mustern, die in der Größe, Richtung und Ankunft der Sitzungspakete gefunden wurden.

Einzigartige Musteranalysen ermöglichen es Sophos NDR, das Vorhandensein von Malware-Familien trotz Verschlüsselung mit hoher Sicherheit zu erkennen.

EPA-Detektionen basieren auf der Form des Netzwerkflusses, bei dem es sich um eine völlig unabhängige Detektion handelt.

Patentiertes Verfahren zur Transformation und Präsentation dieser Merkmale in einem Convolutional Neural Network (CNN) zur Klassifizierung.

# Firewall vs. NDR

## Sophos Firewall

- **Einsatzszenarien**
  - Aktiver Schutz
  - Nord-Süd-Verkehr
  - TLS-Scanning „nur“ regelbasiert beim Durchgang
- **Zweck**
  - Aktiver Schutz: DPI, IPS, TLS-Inspection, Segmentierung, Web Protection, VPN,…
- **Deployment**
  - Inline im Gateway oder Bridge Modus
  - Granulares Firewall Regelwerk
  - Direkter Eingriff in den Datenverkehr

## Sophos NDR

- **Einsatzszenarien**
  - Passive Erkennung von verdächtigen Aktivitäten
  - Nord-Süd **und** Ost-West-Verkehr
  - Gesamter verschlüsselter Verkehr!
- **Zweck**
  - Sammlung von Telemetriedaten zur präzisen Erkennung und Analyse von Angriffen
- **Deployment**
  - VM am SPAN-Port des Switches
  - Keine Policy notwendig – alles wird untersucht
  - Kein aktiver Eingriff in den Datenverkehr

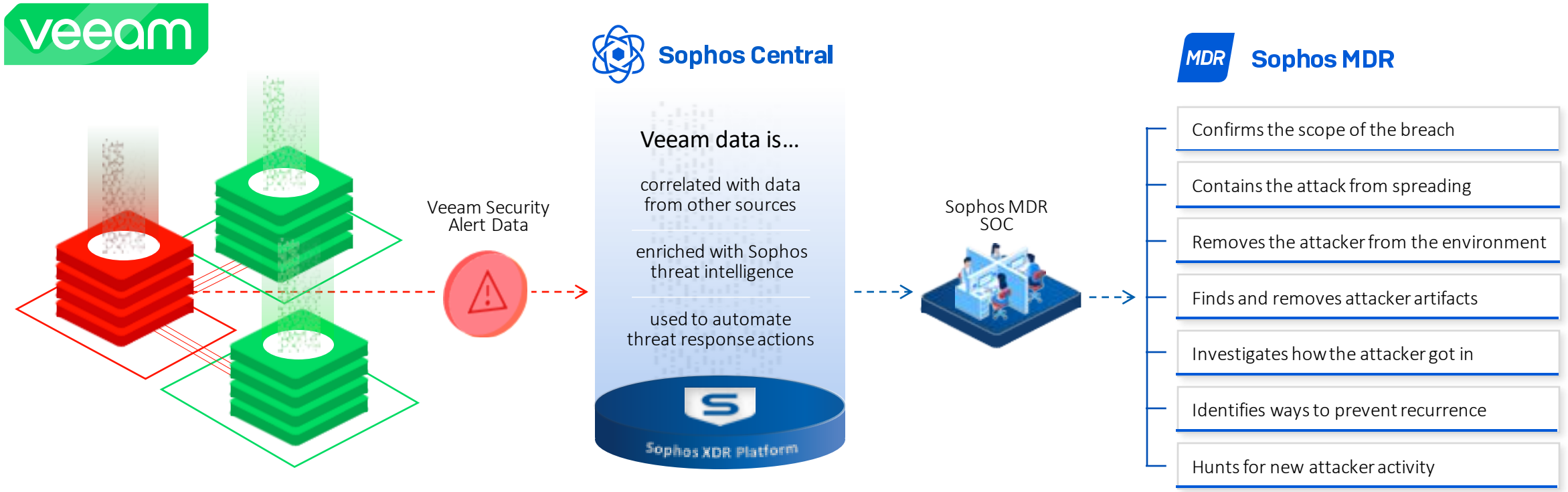
# Angriff möglichst früh stoppen

> Threat actors were able to affect the backup repositories in 75% of ransomware attacks

> Over 93% of ransomware attacks explicitly target backups

-Veeam 2023 Ransomware Trends Report

# Backup and Recovery Integration Overview



# Jede Sicherheitslösung spielt eine wichtige Rolle

## ENDPOINT

Entdeckt verdächtige Aktivitäten und Malware

## FIREWALL

Entdeckt Einbruchversuche und Ausspionieren

## IDENTITY

Entdeckt unautorisierte Zugang und Ausweitung von Privilegien

## EMAIL

Feststellen des initialen Zugangs, Versuche die Zugangsdaten zu stehlen

## CLOUD

Hinweise auf unbefugten Zugang und Versuche, Daten zu stehlen

## NETWORK

Identifikation bösartiger Geräte, ungeschützter Geräte und neuartiger Angriffe

# SOPHOS XDR & MDR: Offen und flexibel

## Telemetriequellen

SOPHOS

✓ Integrations included

- Endpoint
- Workload
- Mobile
- Cloud
- Firewall
- Email
- ZTNA
- Network

### Endpoint

✓ Included

Microsoft, CROWDSTRIKE, SentinelOne, TREND MICRO, Symantec by Broadcom (beta), BlackBerry CYLANCE (beta)

+ Others with Sophos XDR Sensor agent

### Firewall

paloalto NETWORKS, FORTINET, CHECK POINT, CISCO Meraki, SONICWALL, WatchGuard

### Network

DARKTRACE, CANARY, Secutec, Skyhigh Security

### Email

Microsoft 365 ✓ Included

Google Workspace ✓ Included

mimecast

proofpoint.

### Productivity

✓ Included

Microsoft 365

Google Workspace

### Cloud

orca security, aws

### Identity

Microsoft ✓ Included

okta, auth0, DUO, ManageEngine

### Backup and Recovery

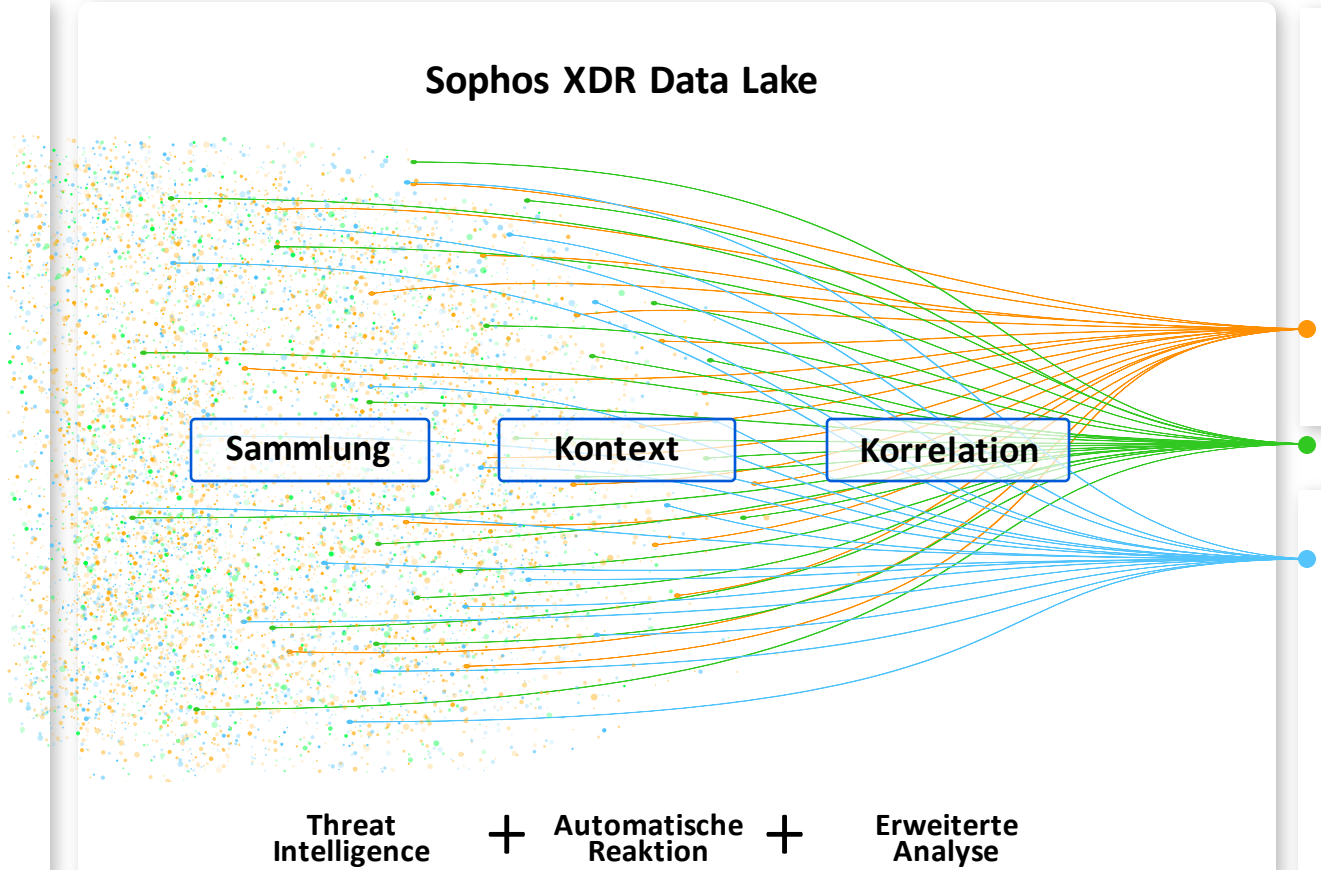
veeam

# Analyse und Reaktion – eigenes SOC oder Sophos MDR

## Telemetriequellen

- Endpoint
- Firewall
- Email
- Cloud
- NDR
- Identität
- Microsoft

## Bedrohungsanalyse und Korrelation




## Untersuchung und Reaktion

### 24/7 Managed Detection and Response Services

Sophos MDR Experten für Bedrohungssuche, Analyse und Reaktion

**38 Min** Ø Zeit bis zur Behebung

### Investigation and Response Platform für das eigene SOC

Sophos Central als zentrale Plattform für Untersuchung, Reporting und Management

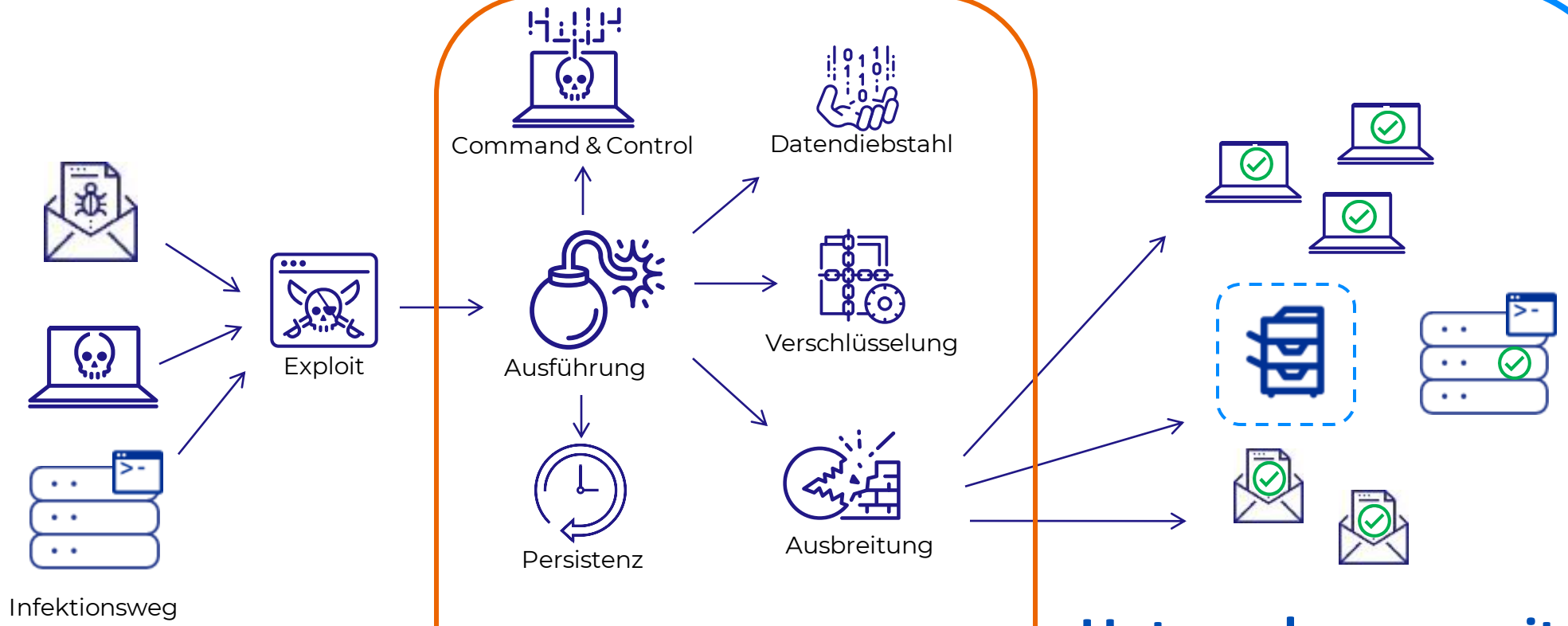
Selbst verwaltet oder zusammen mit dem Sophos MDR Team

SOPHOS

# Sophos MDR Servicestufen

| | Sophos MDR Essentials<br>(Sophos MDR for Microsoft Defender) | 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**<br>Voraussetzung: voller Sophos XDR Agent (Schutz, Erkennung, Reaktion) oder Sophos XDR Sensor (Erkennung, Reaktion) | ✓ | ✓ |
| **Direkter Telefon-Support bei Vorfällen** | ✓ | ✓ |
| **Ursachenanalyse – und wie können erneute Angriffe verhindert werden?** | | ✓ |
| **Vollständiges Incident-Response: komplette Neutralisierung von Bedrohungen**<br>Voraussetzung: voller Sophos XDR Agent (Schutz, Erkennung und Reaktion) | | ✓ |
| **Dedizierter Ansprechpartner beim Incident Response Team** | | ✓ |
| **Sophos Breach Protection Warranty** | | ✓ |

# Stoppen + Eindämmen vs. volles Incident Response




**Ursachenanalyse**

**Stoppen und Eindämmen**

**MDR Essentials**

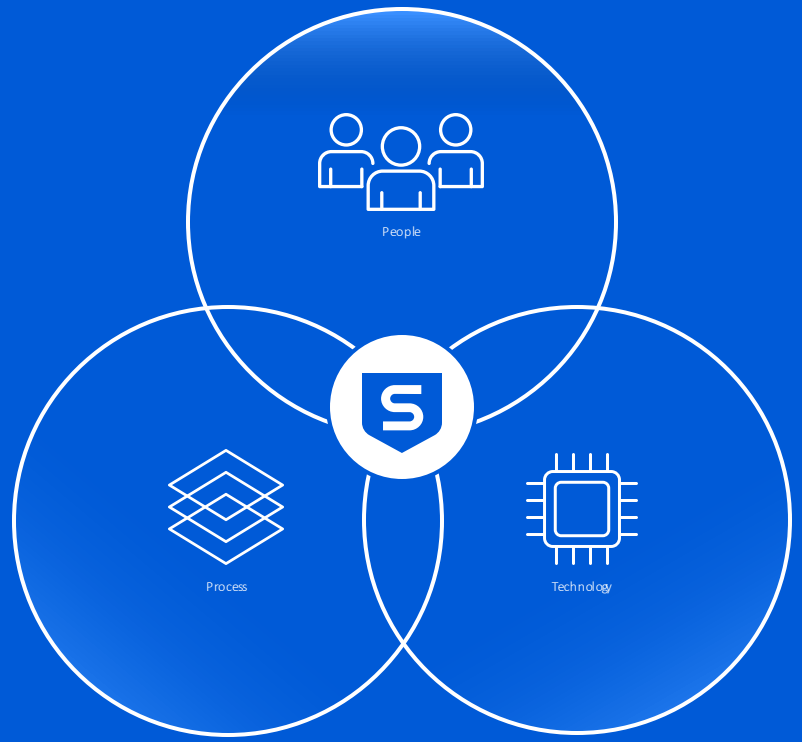
**Unternehmensweite Neutralisierung + Empfehlungen**

**MDR Complete**

SOPHOS

MANAGED DETECTION AND RESPONSE

# Das Ergebnis zählt – rundum sicher durch Cybersecurity as a Service




- **Ihr ausgelagertes Security Operations Center (SOC)**
- **24/7 Bedrohungserkennung und Reaktion**
- **Bedrohungssuche durch Experten**
- **Vollständiges Incident Response bei Angriffen**
- **Bestmögliches Ergebnis für Ihre IT-Sicherheit**

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital·Sicher·BSI·

Qualifizierte APT-Response Dienstleister

im Sinne § 3 BSIG

SOPHOS

# Weitere Informationen im Web oder hier vor Ort

**Sophos MDR**

https://www.sophos.com/de-de/products/extended-detection-and-response

**Sophos Integrations Maketplace**

https://www.sophos.com/de-de/marketplace

**Sophos Firewall**

https://www.sophos.com/de-de/products/next-gen-firewall

**Sophos NDR**

https://www.sophos.com/de-de/products/network-detection-and-response

# Vielen Dank!

Weitere Infos:
bechtle.com