

Zukunftssichere IT-Security

Michael Veit
Technology Evangelist, Sophos

SOPHOS

Fürchten Sie sich davor?



Hacker vor 5 Jahren



Hacker heute

State of Ransomware 2022



66%

der SMB wurden im letzten Jahr
mit Ransomware angegriffen



65%

der angegriffenen Unternehmen
hatten danach verschlüsselte Daten



30 Tage

hatten die Opfer keine
voll funktionsfähige IT



90%

der Opfer hatten
Einschränkungen der Produktion



\$1.7M

Schaden pro Vorfall, vor
allem durch Betriebsausfall

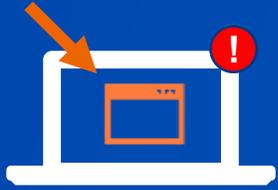
Sieht Ihr Netzwerk so aus?



✓ = verwaltet, EPP, gepatcht, aktuelles OS

..oder so?

“Tolles Tool” vom User selbst installiert



WLAN-Webcam, noch nie upgedatet



Privates älteres Android ohne Updates, ohne AV



Mitarbeiter, der auf jeden Link und Anhang klickt



Win7-Notebook “im Schrank”



“später neu starten” geklickt



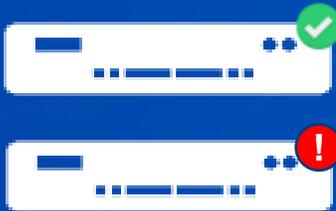
Privates Notebook



Server2003/2008 mit alter Software



Reboot erst im nächsten Wartungsfenster



Drucker/Scanner/Kopierer mit Windows Embedded ohne AV und Updates



Entwickler-Workstation mit vielen Scan-Ausnahmen



Maschinensteuerung mit NT 4.0/Win2000



! = unsicher

✓ = verwaltet, EPP, gepatcht, aktuelles OS

..oder so?

“Tolles Tool” vom User selbst installiert

WLAN-Webcam, noch nie upgedatet

Privates älteres Android ohne Updates, ohne AV

Mitarbeiter, der auf jeden Link und Anhang klickt

Win7-Notebook “im Schrank”

..dann brauchen Sie

XDR

Privates Notebook

Server2003/2008 mit alter Software

Reboots im nächsten Wartungsfenster

Drucker/Scanner/Kopierer mit Windows Embedded ohne AV und Updates

Maschinensteuerung mit NT 4.0/Win2000

Entwickler-Workstation mit vielen Scan-Ausnahmen

! = unsicher

✓ = verwaltet, EPP, gepatcht, aktuelles OS

Was ist Sophos XDR (eXtended Detection and Response)?

- Beste proaktive Schutztechnologien
- Erfassung, Analyse und Korrelation aller Technologien: Endpoint, Firewall, Cloud, Email, Netzwerk, Identität..
- Aussagefähigkeit
 - Cyberangriff?
 - Datenabfluss / Compliance-Verstoß?
 - Zustand der IT?
- Bei einem Vorfall: Fähigkeit zur Reaktion
- Automation - z.B. automatische Isolation unsicherer Systeme



EDR / XDR = „Stand der Technik“

Wer sagt, dass ich das brauche?

- Cyberrisiken-Versicherer
- Geschäftspartner, Zulieferer
- Compliance (DSGVO, SOX, PCI)

- Während eines Vorfalls... - jeder!
„Wäre es schon dagewesen!“

Bundesverband IT-Sicherheit e.V.



IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

technischer und organisatorischer Maßnahmen

2021

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?

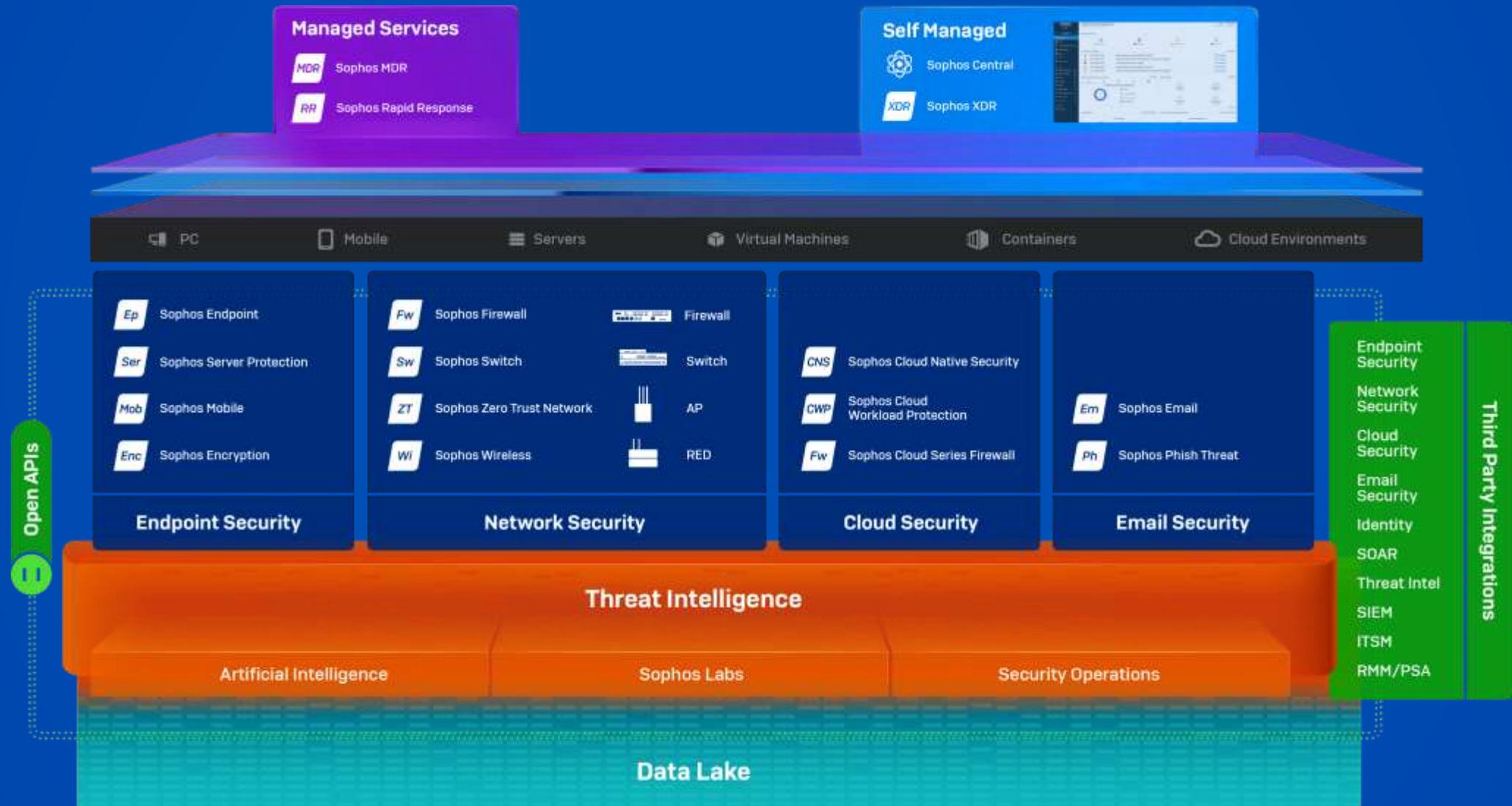
- Malware
- Exploitation
- Maliziöse Scripte
- Hacker-Aktivitäten
- Missbrauch von Administrativen Werkzeugen und Tools in schädlicher Absicht

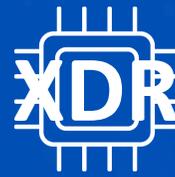
Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

EDR-Plattformen kombinieren wirksame Detektions- und Präventionstechniken, um die Kompromittierung von Clients und Servern, auch über Computer und Betriebssystemgrenzen hinweg, zu verhindern und sogar aktive Angreifer in Computernetzen zu enttarnen.

https://www.stand-der-technik-security.de/fileadmin/user_upload/2021-09_TeleTrust-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

SOPHOS Adaptive Cybersecurity Ecosystem - XDR





Technologie

Alle Jahre wieder Ende Dezember...

**CHRISTOPHEIT
Bedenschutzmatte 4 mm**
Art.-Nr. 10029552
ab 11,99

Extra tiefer Einstieg

Heimtrainer Ergometer „AX 3000“
Magnet-Brems-System, Schwungradmasse: ca. 8 kg, Widerstandseinstellung: 24-stufig, Trainingsprogramme: 21, Je Stück.
Art.-Nr. 100302785

-61%
uVP 599,-
229,-
24 Monate* à 10,45
Grundbetrag für Abrechnung 229,00

Heimtrainer „HT3“
Magnet-Brems-System, Schwungradmasse: ca. 10 kg, Widerstandseinstellung: 9-stufig, Trainingsprogramme: 0, Je Stück.
Art.-Nr. 100004020

-58%
uVP 599,-
249,-
inkl. Versandkostenzuschlag 9,95
24 Monate* à 11,78
Grundbetrag für Abrechnung 249,00

Vibrationsplatte „Vibro 3000“
Leistungsstufen: 22, Schwingungsbreite: 0-5 mm, Trainingsprogramme: 4, Je Stück.
Art.-Nr. 100271403

-56%
uVP 299,-
129,-

Inkl. Transportrollen & Trainingsbänder

Über 40 Übungsmöglichkeiten

Bauchtrainer „Total Exerciser TE 1“
Widerstand ergibt sich durch das eigene Körpergewicht und den 5-fach verstellbaren Steigungswinkel, Je Stück.
Art.-Nr. 100183943

-40%
uVP 249,-
149,-
inkl. Versandkostenzuschlag 9,95

HAMMER

Klassisches Rudern durch Ausleger-Arme

Rudergerät „Rower Cobra“
17-stufiges und verstellbares Zylinder-Brems-System, 3-fach höhenverstellbare Kutschuhlen für individuelle Trainingspositionen, Kugelgelagertes Komfortsitz, verstellbar für vierst. Körperproben, Je Stück.
Art.-Nr. 100018667

-37%
uVP 399,95
249,-
24 Monate* à 11,34
Grundbetrag für Abrechnung 249,00

Rudergerät „Cobra XTR Plus II“
16-stufiges Magnet-Brems-System, Schwungradmasse: ca. 8 kg, Trainingsprogramme: 10, Je Stück.
Art.-Nr. 100328529

-36%
uVP 749,-
479,-
36 Monate* à 14,89
Grundbetrag für Abrechnung 479,00

AB-Roller
Je Stück.
Art.-Nr. 100254131

-40%
uVP 19,99
11,99

Fitnessmatte 10 mm
Je Stück.
Art.-Nr. 100254133

-40%
uVP 24,99
14,99

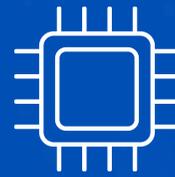
Jetzt NEU mit integriertem Puls-Empfänger

Crosstrainer „EL 5000 Pro“
Magnetbremse-System, Schwungradmasse: ca. 10 kg, Widerstandseinstellung: 24-stufig, Trainingsprogramme: 10, Je Stück.
Art.-Nr. 100328501

-52%
uVP 629,-
299,-
inkl. Versandkostenzuschlag 29,95
30 Monate* à 12,13
Grundbetrag für Abrechnung 299,00

Eine Lösung kaufen reicht nicht mehr





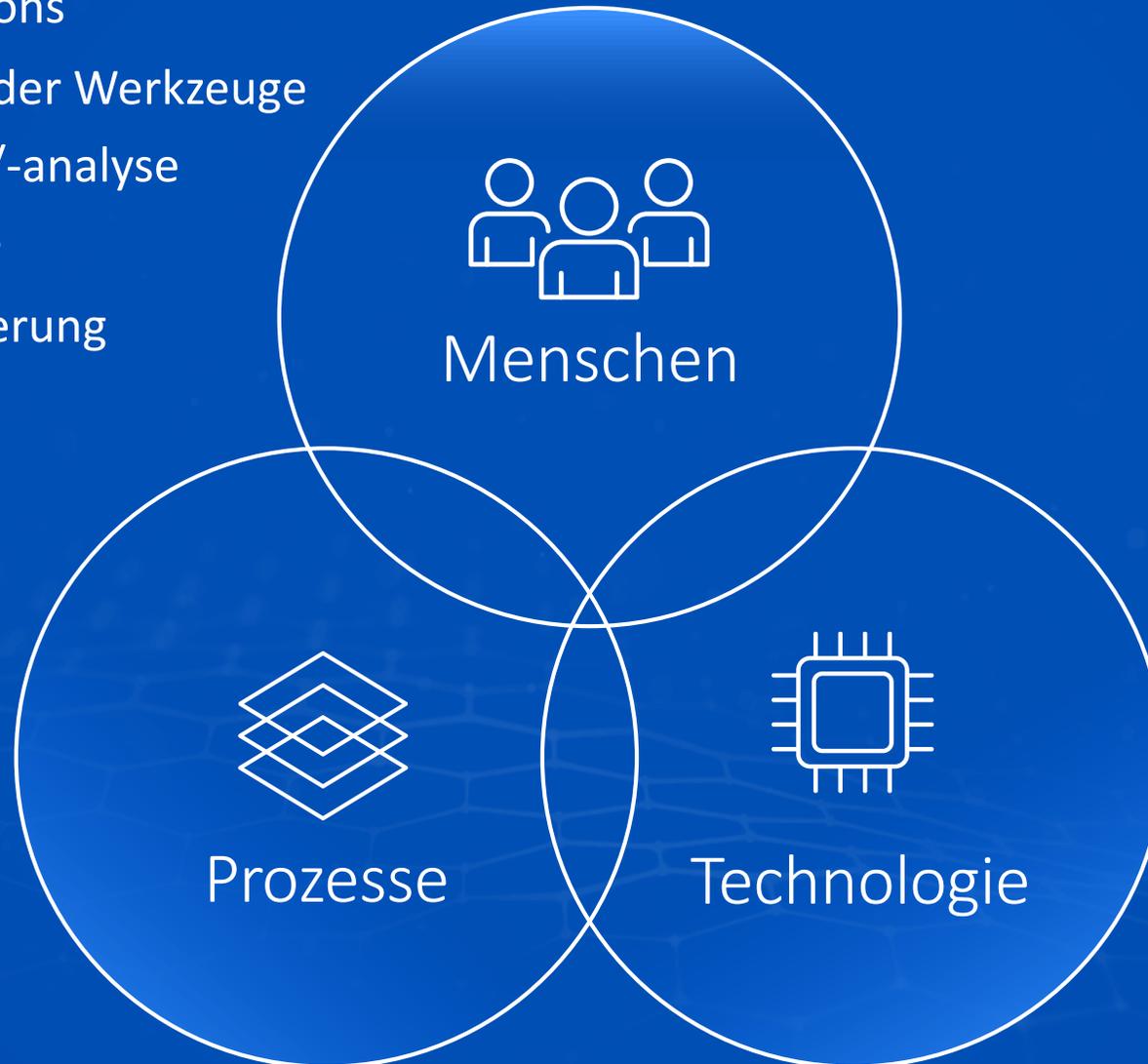
Technologie

24/7 Security Operations

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

Vorgehen bei Vorfall

- Incident/Response
- Eindämmung
- Neutralisierung



Stand der Technik =
XDR Ökosystem

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

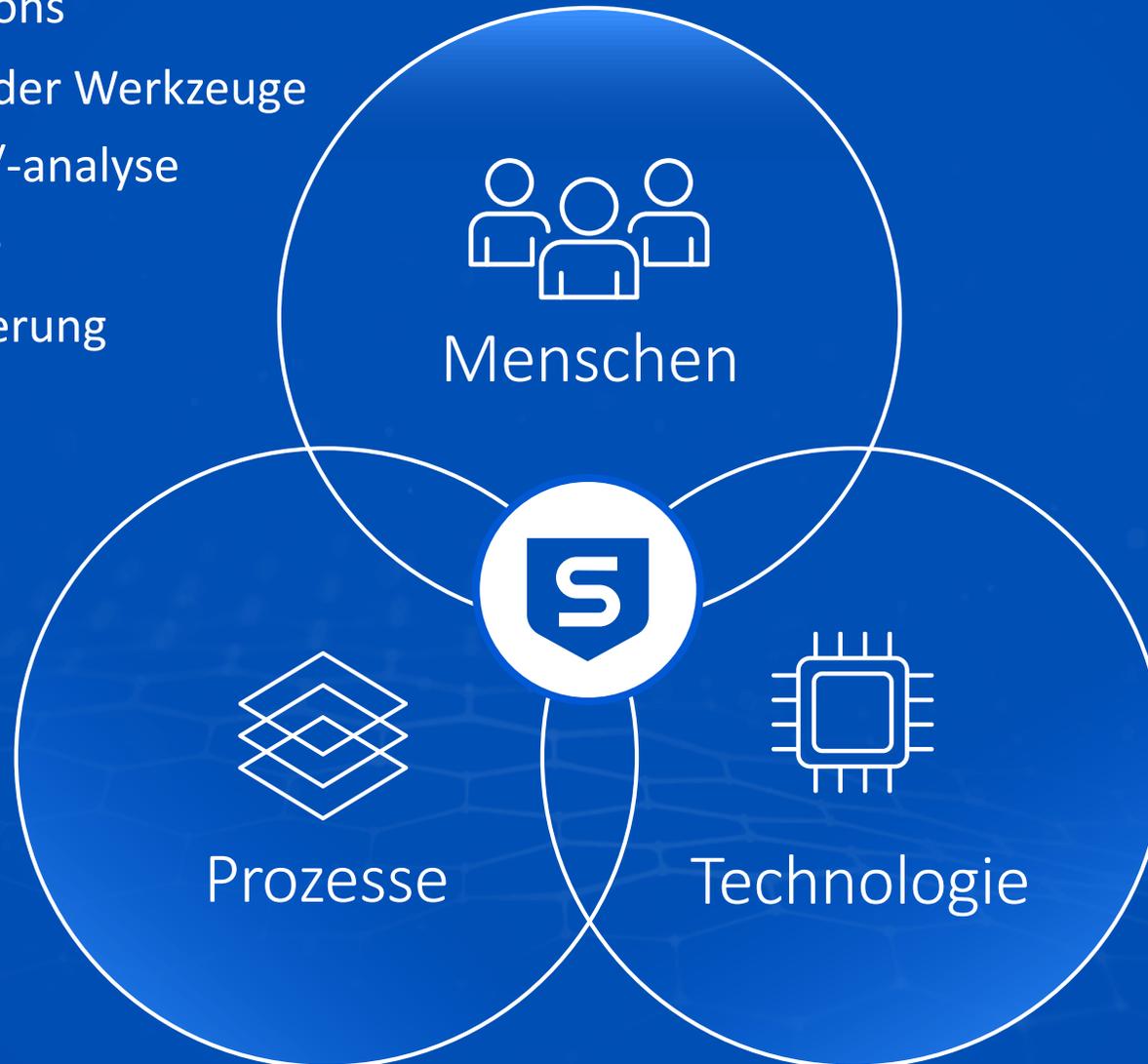
Sophos MDR

24/7 Security Operations

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

Vorgehen bei Vorfall

- Incident/Response
- Eindämmung
- Neutralisierung



Stand der Technik =
XDR Ökosystem

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

Nächste Schritte:

Halle 7, Stand 328

Sophos Adaptive Ecosystem (ACE)

Mit einer Kombination von Automatisierung und menschlichen Experten bietet das Sophos Adaptive Cybersecurity Ecosystem (ACE) leistungsstarken Schutz, der kontinuierlich dazulernt und sich verbessert.

➤ <https://www.sophos.com/de-de/content/adaptive-cybersecurity-ecosystem>



Sophos XDR - eXtended Detection and Response

Erkennen und analysieren Sie Bedrohungen lückenlos – mit Endpoint-, Server-, Firewall-, Email und weiteren Datenquellen.

➤ <https://www.sophos.com/de-de/products/endpoint-antivirus/xdr.aspx>



Sophos Managed Detection Response

24/7 Managed Detection and Response mit aktiver Bekämpfung von Bedrohungen durch ein Expertenteam, als Fully-Managed-Service

➤ Mehr Infos: <https://www.sophos.com/de-de/products/managed-threat-response.aspx>

