
SOPHOS
PARTNER 2026
EXPERIENCE

SOPHOS

Co-managed SOC

Wir sind uns einig:

Cyberbedrohung ist real und Unternehmen können sich nicht dagegen selbst wehren

IT Fachkräftemangel

Es gibt generell zu wenig IT Fachpersonal, geschweige denn Cyber Security Spezialisten

Fachkenntnis

Angriffserkennung und Abwehr verlangt tiefe Kenntnis der Materie und der notwendigen Tools, die im IT-Arbeitsalltag untergehen

KI Verstärkungseffekt

Privat gehostete KI Modelle ohne ethische Grenzen, aber auch nicht ausgereifte Kontrollen bei den etablierten Anbietern erlauben auch nicht-versierten Angreifern, Schaden anzurichten

Identitätsdiebstahl

Seit etwa 5 Jahren konstanter Anstieg der Identitätsbedrohungen, mit der Folge, dass 2025 in 67% aller Angriffsversuche, dieser Weg der Ursprung ist. Unternehmen haben noch keine phishing-resistente Agenda

Geschwindigkeit

Die durchschnittliche Verweildauer der Angreifer ist etwa bei drei Tagen, was extrem schnelles Handeln erfordert, wenn man bedenkt, dass mehr als 80% der Angriffe Freitagnacht bis Sonntagnacht erfolgen.

Regularien Ignoranz

Trotz DSGVO, NIS 2, KRITIS und älteren Regularien der Industrie und Wirtschaft, bleiben eine Vielzahl von Unternehmen noch auf einem erschreckend schlechten Cyber-Abwehr-Niveau

Ein SOC muss her

Zusammen lösen wir das Problem	• IT des Kunden kann sich wieder auf Kernaufgaben konzentrieren
24 / 7	• Die meisten Angriffe finden ausserhalb der Bürozeiten statt
Nachricht oder Eingriff	• Sensible Bereiche können unterschiedlich behandelt werden
Langfristige Beziehung	• Ein Service hat eine andere Wertstellung

SOPHOS CENTRAL PLATFORM

Managed by Customers | Managed by Partners | Managed by Sophos

SERVICES

MANAGED SERVICES

- MDR
- Incident Response
- Vulnerability Management
- Professional Services

ADVISORY SERVICES

- Penetration Testing
- Security Assessments
- Red Team Exercises
- Incident Readiness

THREAT PREVENTION AND CONTROLS

CONTROLS

- Endpoint
- Firewall
- Identity
- Email
- Network
- Web Browser

INTEGRATIONS

350+ Third Party Integrations

SECURITY OPERATIONS

- XDR
- SIEM
- EDR
- ITDR
- NDR
- SOAR

THREAT INTELLIGENCE

SOPHOS X-OPS

- Adversary Tracking
- Threat Research
- Breach Forensics
- Malware Analysis
- Industry Collaboration

AI, AUTOMATION & ENGINEERING

- Adaptive Attack Protection
- Critical Attack Warning
- Security Analytics
- Detection Logic
- Threat Protection

DATA LAKE

AI-ASSISTED & AGENTIC WORKFLOWS

Your SOC + Our SOC

Co-managed / MSP / MSSP

- Erweitern Sie Ihr Security Team mit Sophos Experten
- Erweitern Sie Servicezeiten und Leistungsumfang
- Bedienen Sie mehr Kunden mit MDR

Our SOC = Your SOC

Reseller

- Bieten Sie Ihren Kunden ein Instant SOC an
- Sophos Experten überwachen und reagieren 24/7
- Erhöhen Sie die Marge ohne zusätzliches Personal

Your SOC + Our Platform

SOC-Anbieter

- Steigern Sie die Effizienz Ihrer Analysten mit einer erstklassigen XDR-Plattform
- Automatisierte Prävention und Reaktion reduzieren den Arbeitsaufwand
- Nutzen Sie Sophos Incident Response bei Bedarf

Converged Platform

Erweitern Sie Ihr Security Team mit Sophos Experten

Erweitern Sie Servicezeiten und Leistungsumfang

Bedienen Sie mehr Kunden mit MDR

SOAR - Automation z.B. Integration in ein Ticketsystem

Umfangreichere SOC Services durch Playbooks und unlimitierte Integration

Erfüllung von Compliance und SIEM Anforderungen

Steigern Sie die Effizienz Ihrer Analysten mit einer erstklassigen XDR-Plattform

Automatisierte Prävention und Reaktion reduzieren den Arbeitsaufwand

Nutzen Sie Sophos Incident Response bei Bedarf

Wie viel Service?

- Termed
  - Endkunde ist Lizenznehmer
  - Co-managed wird vorher angemeldet
  - Partner kann autorisierte Kontakte übernehmen

- MSP
  - Partner ist der Lizenznehmer unter dem MSP Flex Programm
  - Co-managed quasi eingebaut
    - Entscheidung, wie viel der MDR Kommunikation zum Kunden kommt, liegt beim Partner
    - Autorisierte Kontakte per default beim Partner

SOC während der Bürozeiten	24/7 SOC	Zero Trust Upgrade
Alerting	Response	Prozess-Integration
Security Audit	Pentest	Risiko Analyse
Tech Integration	Onboarding	Angriffsflächen-reduktion
Auswertung	GF Berichte	SOAR
Compliance Audit	Passkey Implementierung	Playbooks

Prävention vs. Detection & Response

- Phishing-resistente Authentifizierung reduziert die Angriffsfläche nachhaltig
- Prävention stoppt Bedrohungen frühzeitig, meist automatisch, was Notwendigkeit für manuelle Investigation reduziert
- Detection & Response, wenn Angriffe an präventiven Maßnahmen vorbeikommen und SOC Analysen und Gegenmaßnahmen notwendig sind
- Prävention ist stark unterschätzt, es ist nur schwer messbar – Erfolg bedeutet: “nichts passiert”

Ökonomischer Einfluss von Prävention

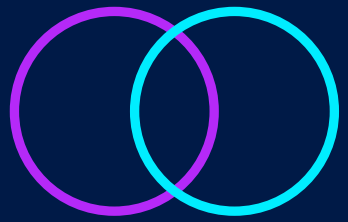
- Wirksame Prävention reduziert die Anzahl der Vorfälle, die untersucht werden müssen, und spart dadurch Zeit und Ressourcen
- Selbst kleine Sicherheitsvorfälle (z. B. der Diebstahl von Zugangsdaten) können ohne Prävention schnell zu aufwendigen und kostspieligen Untersuchungen eskalieren.
- Prävention ermöglicht es, Sicherheitsprozesse zu skalieren, ohne den Personalaufwand oder die Kosten proportional erhöhen zu müssen.

SOC Effizienz

- Ticket Anzahl ist kein adäquates Mittel, um SOC-Performance zu messen
- Focus auf
  - Mean Time to Triage
  - Mean Time to Resolution
  - Root Cause Analysis (RCA), um Prävention zu stärken und Wiederholungsfälle zu reduzieren

Kein SOC = keine Option

- Your SOC + Our SOC
  - CO-managed term/MSP



- Your SOC = Our SOC
  - Sell through

- Your SOC + Our Platform
  - XDR + Partner SOC


SOPHOS
PARTNER 2026
EXPERIENCE

SOPHOS

Winning with Sophos Sales

Agenda

- Channel First mit Direct Touch
- Sales Teams & Ressourcen
- Projektverlauf & Projekt-Qualifizierung
- Sales Tools zur Lead-Generierung
- Zusammenfassung

Channel First mit Direct Touch

Channel First

Seit vielen Jahren ist unsere Strategie und unser Versprechen an Sie: **100 % Channel First**

Wir unterstützen alle unsere Channel-Partner bei Projekten, egal welches Partner-Level sie haben.

Direct Touch

Wir interagieren mit Kunden & Interessenten, ohne die Verkaufstransaktion selbst durchzuführen. Die Transaktion wird immer über unsere Channel-Partner durchgeführt.

SOPHOS CENTRAL PLATFORM

Managed by Customers | Managed by Partners | Managed by Sophos

SERVICES

MANAGED SERVICES

- MDR
- Incident Response
- Vulnerability Management
- Professional Services

ADVISORY SERVICES

- Penetration Testing
- Security Assessments
- Red Team Exercises
- Incident Readiness

THREAT PREVENTION AND CONTROLS

CONTROLS

- Endpoint
- Firewall
- Identity
- Email
- Network
- Web Browser

INTEGRATIONS

350+ Third Party Integrations

SECURITY OPERATIONS

- XDR
- SIEM
- EDR
- ITDR
- NDR
- SOAR

THREAT INTELLIGENCE

SOPHOS X-OPS

- Adversary Tracking
- Threat Research
- Breach Forensics
- Malware Analysis
- Industry Collaboration

AI, AUTOMATION & ENGINEERING

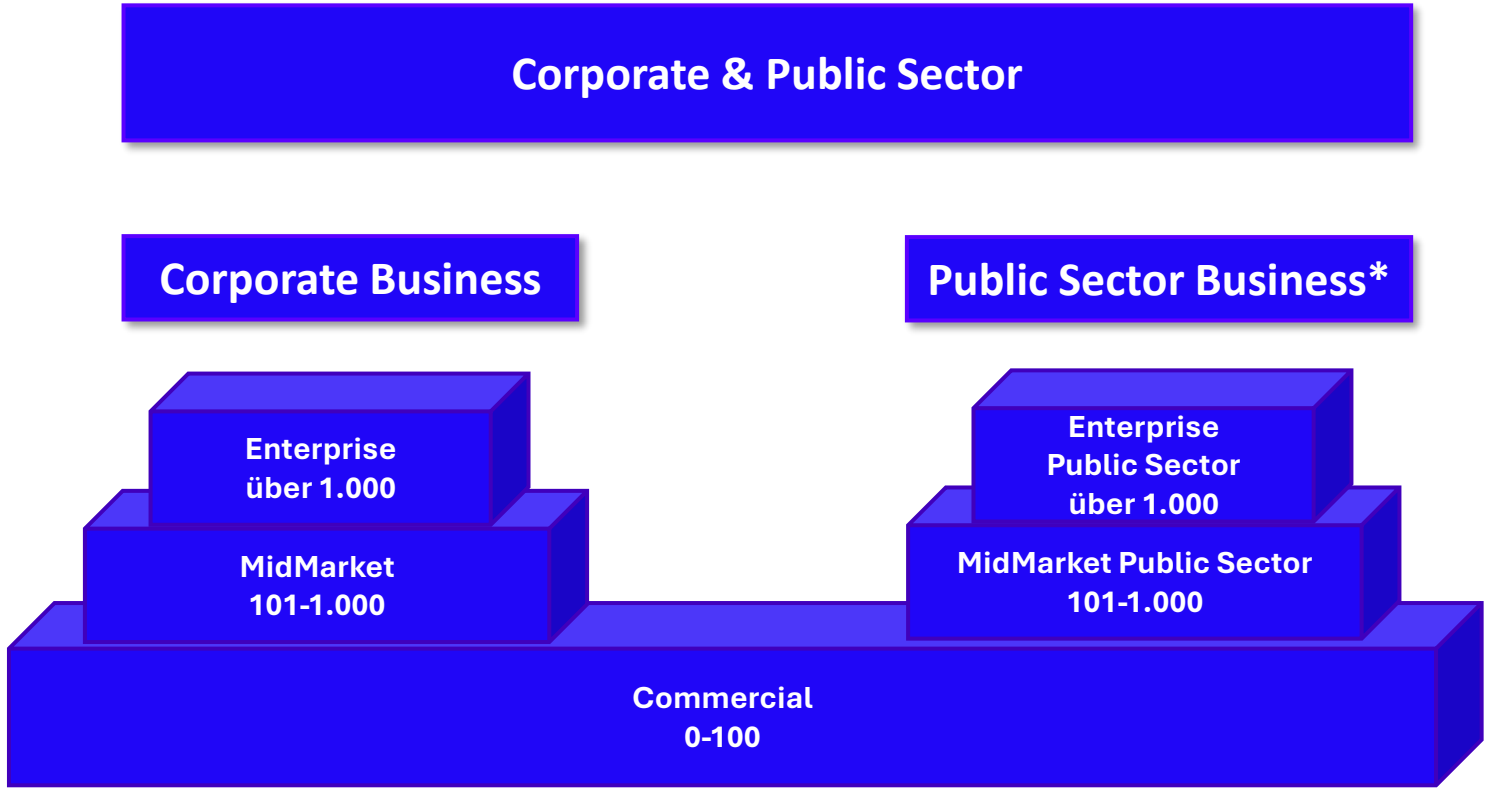
- Adaptive Attack Protection
- Critical Attack Warning
- Security Analytics
- Detection Logic
- Threat Protection

DATA LAKE

AI-ASSISTED & AGENTIC WORKFLOWS

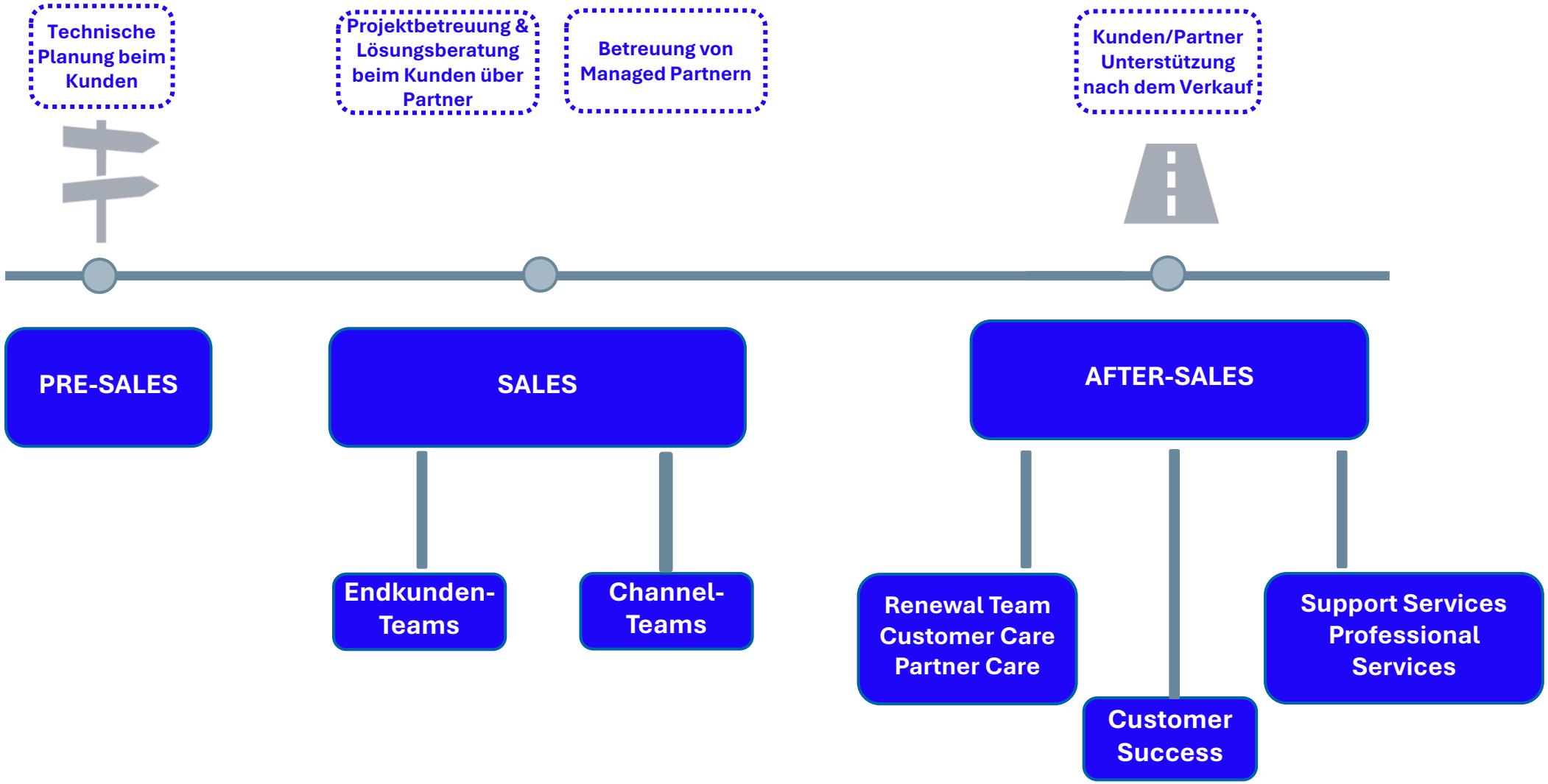
Sales Teams & Ressourcen

Sophos Sales: Endkunden Teams



- Public Sector Business Deutschland: Behörden/Gesundheitswesen/Non-Profit/Schulen & Universitäten
- In der Schweiz und in Österreich haben wir kein dediziertes Public Sector Team. Alle Endkunden Teams betreuen Corporate und Public Sector Kunden

Sophos Lifecycle



PRE-SALES

Sophos Sales Engineering Team
Unterstützung bei gemeinsamen Projekten

- Technische Projektunterstützung
  - Voraussetzungen: Deal Registration, qualifizierte Opportunity
  - Anfragen zu Pre-Sales Unterstützung ausschließlich über die Endkunden Teams

- Sales Engineers liefern technische Tiefe über das gesamte Sophos-Portfolio
  - Wichtig: Voraussetzung für eine Pre-Sales-Anfrage ist eine vorab klar definierte Zielsetzung inklusive der Inhalte, die präsentiert werden sollen.

- Kostenloser Pre-Sales-Helpdesk: Ausschreibungen, Wireless-Planungen, Migrationen & Firewall-Sizing

- Partner-Enablement: bei Managed Partner

- Partner-Enablement: bei Distribution Managed Partner übernehmen unsere Distributoren

Sophos Endkunden Teams
Unterstützung bei gemeinsamen Projekten

SALES

- Projekt-Support für alle Partner – unabhängig vom Partner-Level
- Qualifizierung von Projektmeldungen (Deal Registrations)
- Identifikation & Aktivierung von Cross- und Upselling-Potenzialen
- Bearbeitung von Kundenanfragen & vorqualifizierten Leads
- Positionierung unserer Lösungen & überzeugende Sales-Argumentation
- Unterstützung in Preisverhandlungen & Projektkonditionen
- Einbindung von Pre-Sales Engineers in Projekten
- Wettbewerbskompetenz
- Gemeinsame virtuelle und vor Ort Termine bei Ihren Kunden mit/ohne Sales Engineers
- Unterstützung bei Call-Out Days zur Neukundengenerierung
- Präsenz & Vorträge auf Hausmessen

Sophos Endkunden Teams
Unterstützung bei Public Sector Kunden

SALES

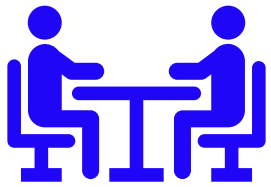
- Branchenspezifischer Vertikal-Vertrieb
  - Health-Care / Non-Profit: Kirche & Wohlfahrt, Gesundheitswesen
  - EDU: Forschung & Lehre: Schulen, Hochschulen, Universitäten, Forschungseinrichtungen
  - GOV: Bund/Land/Kommunen: Öffentliche Einrichtungen der Verwaltung
- Expertise bei Ausschreibungen
  - Eigene Juristin / Bid Manager: Unterstützung bei komplexen Ausschreibungen (National und EU-weit)
  - Erstellung von eigenen Leistungsbeschreibungen zur pro-aktiven Unterstützung und Beratung von Ausschreibungen

Sales-Expertise in der Central Region

Endkunden Segment / Sales Teams	E-Mail-Verteiler
Commercial Team Betreuung nach Unternehmensgröße des Endkunden Unternehmensgröße: 1-100 Mitarbeiter Länder: Deutschland, Österreich, Schweiz und Osteuropa	SmallBusinessSalesDE@sophos.de
MidMarket Team Betreuung nach Unternehmensgröße des Endkunden Unternehmensgröße: 101-1.000 Mitarbeiter Länder: Deutschland, Österreich, Schweiz und Osteuropa	Deutschland: MidMarketSalesDE@sophos.de Österreich: Sales@sophos.at Schweiz: projekte@sophos.ch
Enterprise Team Betreuung nach Unternehmensgröße des Endkunden Unternehmensgröße: über 1.000 Mitarbeiter Länder: Deutschland, Österreich, Schweiz	EnterpriseSalesDE@sophos.de
Public Sector Team Betreuung nach Unternehmensgröße & Sektoren* Unternehmensgröße: über 100 Mitarbeiter Länder: Deutschland	PublicSalesDEsophos.de

Projektverlauf, Projektmeldung & Projekt-Qualifizierung

Projektverlauf in der Praxis



Partner & Kunde besprechen Projekt

SOPHOS PARTNERS

Partner meldet Projekt im Portal

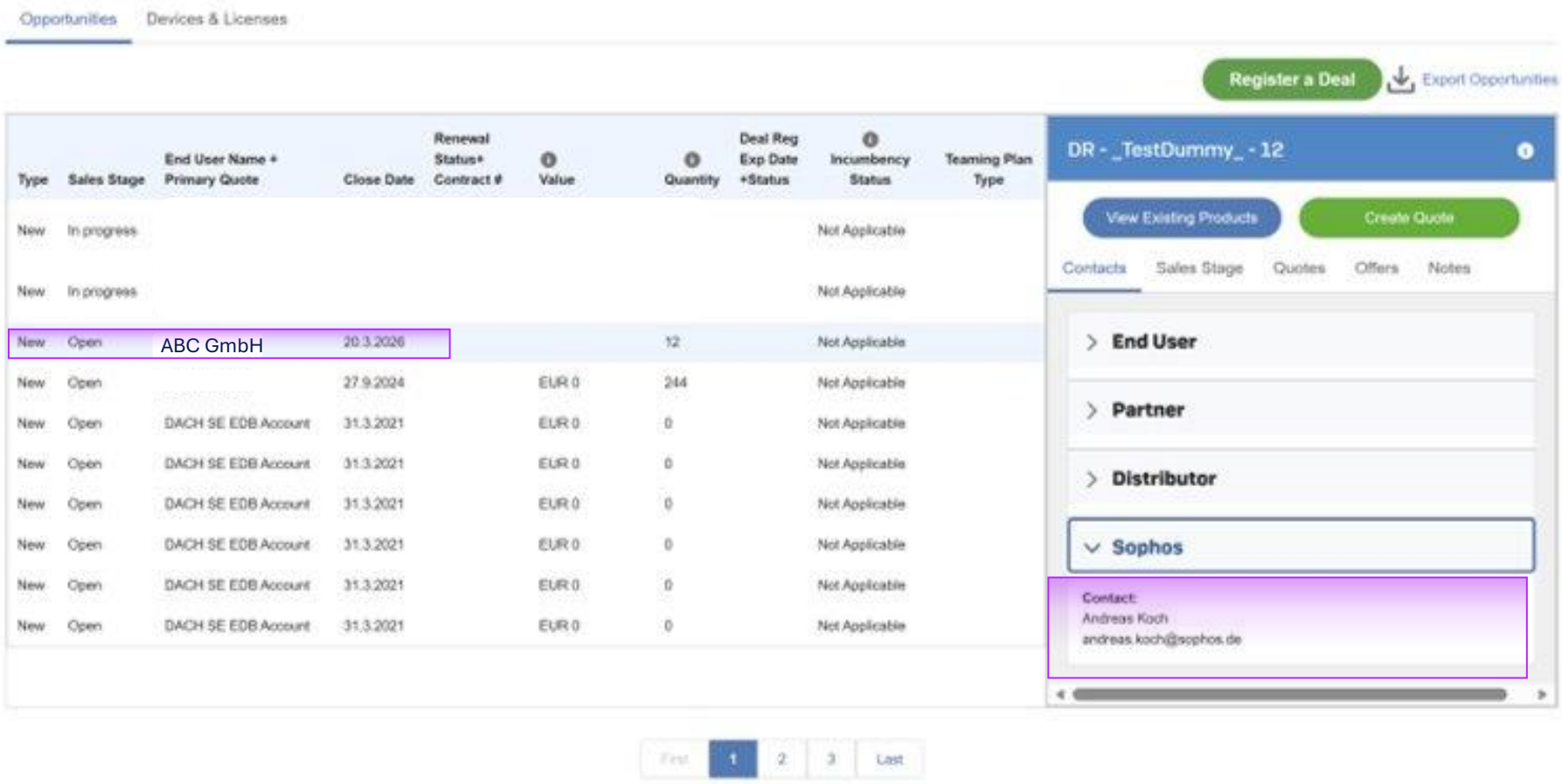
Projekt wird von Sophos geprüft

Austausch zwischen Partner und Endkunden-betreuer

Opportunity Management im Partner Portal

Im **Partner Portal** unter der Rubrik **Vertrieb** finden Sie im **Opportunity & Device Manager** die Übersicht Ihrer Opportunities

Opportunity Management im Partner Portal



In jeder **Opportunity** im **Partner Portal** ist unter **Contacts** ersichtlich, welcher **Endkunden Ansprechpartner** bei **Sophos** für den Account zuständig ist

SOPHOS

PARTNER 2026 EXPERIENCE

Projekt-Qualifizierung

- Frühzeitige Einbindung der Endkunden Teams
- Qualifizierung ist Entscheidend !
  - Klärung von Bedarf & Nutzen
  - Ressourcen richtig einsetzen
  - Risiken früh erkennen
  - Priorisierung ermöglichen
- Sie haben alle Informationen -> gemeinsamen Kundentermin
- Sie haben diese nicht -> wir qualifizieren gemeinsam im Kundentermin
- Kernprojektdaten:
  - Ziel, Zeitplan, Wettbewerb
  - Art der Unterstützung: technisch, vertrieblich
  - Gemeinsame Aktivitäten: Kundentermin virtuell / vor Ort, Demo, POC

Sales Tools zur Lead-Generierung

kostenfrei zur Umsatzsteigerung bei Ihren Kunden

SOPHOS

PARTNER 2026 EXPERIENCE

Sales Tools zur Lead Generierung

SE Health Checkups

- **Zielgruppe:** Sophos Bestandskunden (Sophos Endpoint, Sophos EDR oder Sophos XDR)
- **Hauptziel:** Überprüfung der Sophos-Security-Umgebung des Kunden und offensichtliche Bereiche für Verbesserungen zu identifizieren.
- **Benefit:** Überblick über Best Practices zur Konfiguration der Sophos-Lösungen sowie weitere Empfehlungen.

Threat Profile

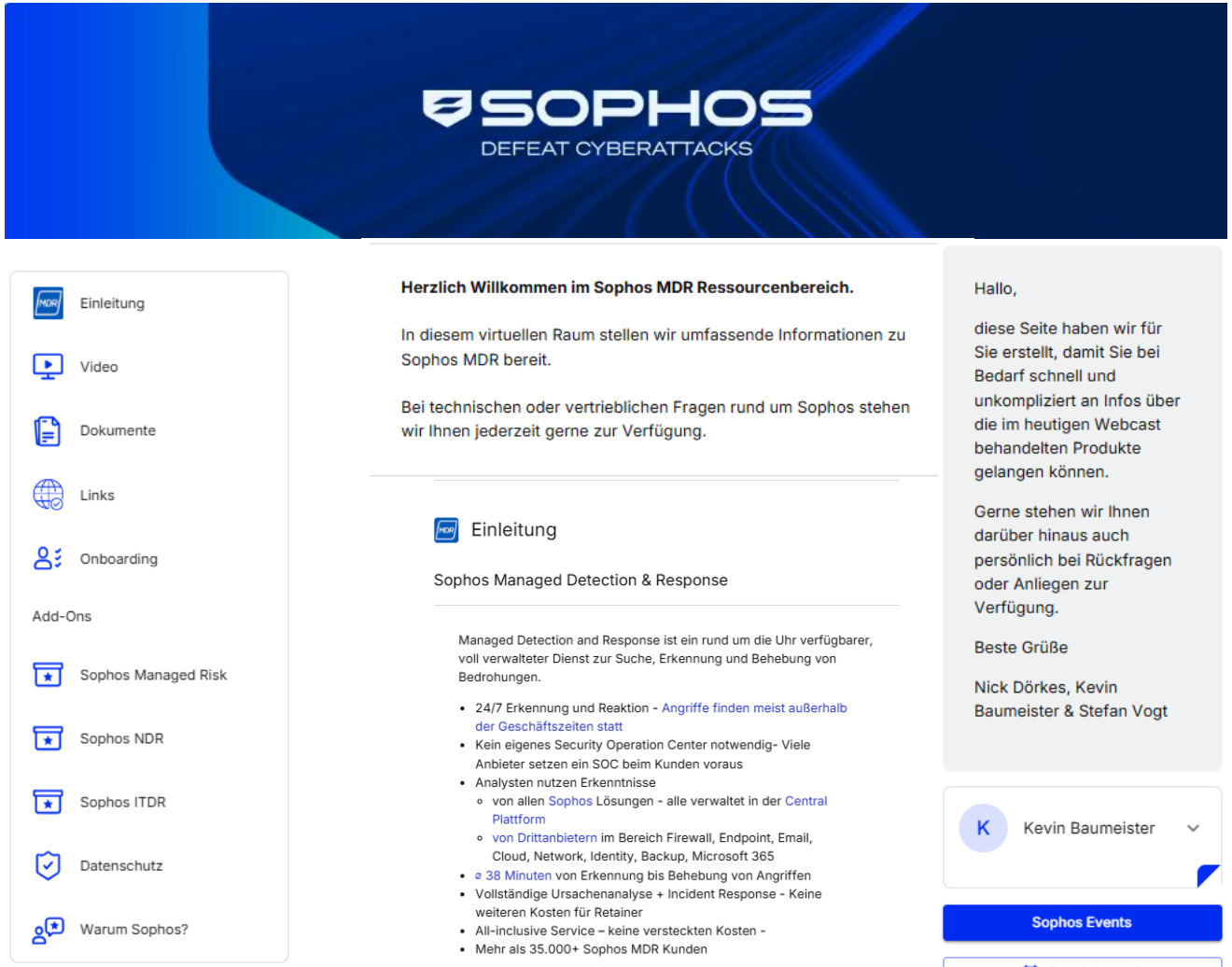
- **Zielgruppe:** Interessenten, die keine Sophos Lösung im Einsatz haben
- **Hauptziel:** Zugangsdaten in Datenleaks, verwundbare, aus dem Internet erreichbare Systeme, Email-Adressen in Datenleaks, Verdächtige Domains, DMARC-Bewertung der primären Email-Domain
- **Benefit:**
  - Kostenloser Sicherheitsstatus aus Angreifer Sicht
  - Erkenntnisse zu Schwachstellen
  - Datenlecks & Domains
  - starker Door-Opener für Advisory & MDR/NDR/Managed Risk

Proof of Value (POV)

- **Zielgruppe:** Interessenten und Bestandskunden (Cross Sell)
- **Hauptziel:** Den echten Mehrwert von Sophos-Lösungen in der eigenen Umgebung sichtbar machen – anhand realer Bedrohungen, Daten und Betriebsabläufe.
- **Benefit:**
  - Klare Erfolgskennzahlen: Risikoreduktion, Detection-Qualität, Effizienz im Betrieb
  - Geführte Implementierung durch Sophos-Experten – sicher & nicht-invasiv
  - Reale Validierung: Test gegen echte Bedrohungen in den Kunden Umgebung
  - Executive-Report mit Ergebnissen, Risiken & klaren Handlungsempfehlungen
  - Nahtloser Übergang in den Produktivbetrieb möglich

Digital Sales Room

- Personalisierter digitaler Raum für Sophos Kunden, Interessenten und Partner
- Zentrale Bereitstellung aller relevanten Informationen zum Verkaufs- oder Evaluierungsprozess
- Sicheres personalisiertes Online-Portal für gemeinsame Nutzung von Inhalten, Dokumenten, Analysen und Projekt-Schritten



Wir sind für Sie da

- Sprechen Sie unsere Endkunden Teams an, gemeinsam holen wir das Beste aus Ihren Projekten heraus
- Wir arbeiten im Schulterschluss mit Ihnen
- Wir ergänzen uns und teilen unsere Fachkompetenz miteinander
- Wir sind mit unseren Endkunden Teams in allen Regionen des DACH-Markts vertreten
- Wir sind Ihr verlängerter Arm beim Endkunden


SOPHOS
PARTNER 2026
EXPERIENCE

SOPHOS

Maximum Security & Maximum Marge mit MDR und Add-Ons

SOPHOS CENTRAL PLATFORM

Managed by Customers | Managed by Partners | Managed by Sophos

SERVICES

MANAGED SERVICES

- MDR
- Incident Response
- Vulnerability Management
- Professional Services

ADVISORY SERVICES

- Penetration Testing
- Security Assessments
- Red Team Exercises
- Incident Readiness

THREAT PREVENTION AND CONTROLS

CONTROLS

- Endpoint
- Firewall
- Identity
- Email
- Network
- Web Browser

INTEGRATIONS

350+ Third Party Integrations

SECURITY OPERATIONS

- XDR
- SIEM
- EDR
- ITDR
- NDR
- SOAR

THREAT INTELLIGENCE

SOPHOS X-OPS

- Adversary Tracking
- Threat Research
- Breach Forensics
- Malware Analysis
- Industry Collaboration

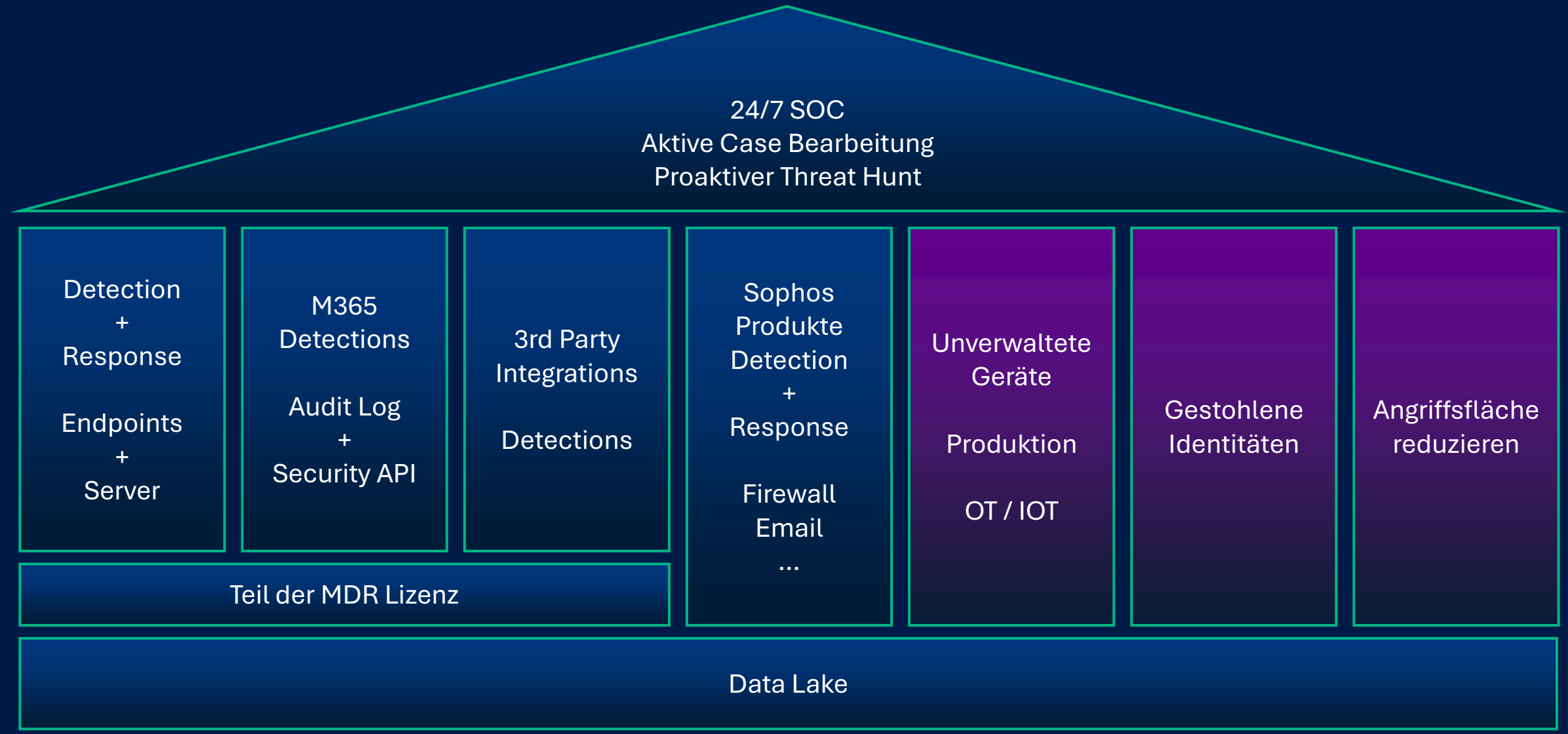
AI, AUTOMATION & ENGINEERING

- Adaptive Attack Protection
- Critical Attack Warning
- Security Analytics
- Detection Logic
- Threat Protection

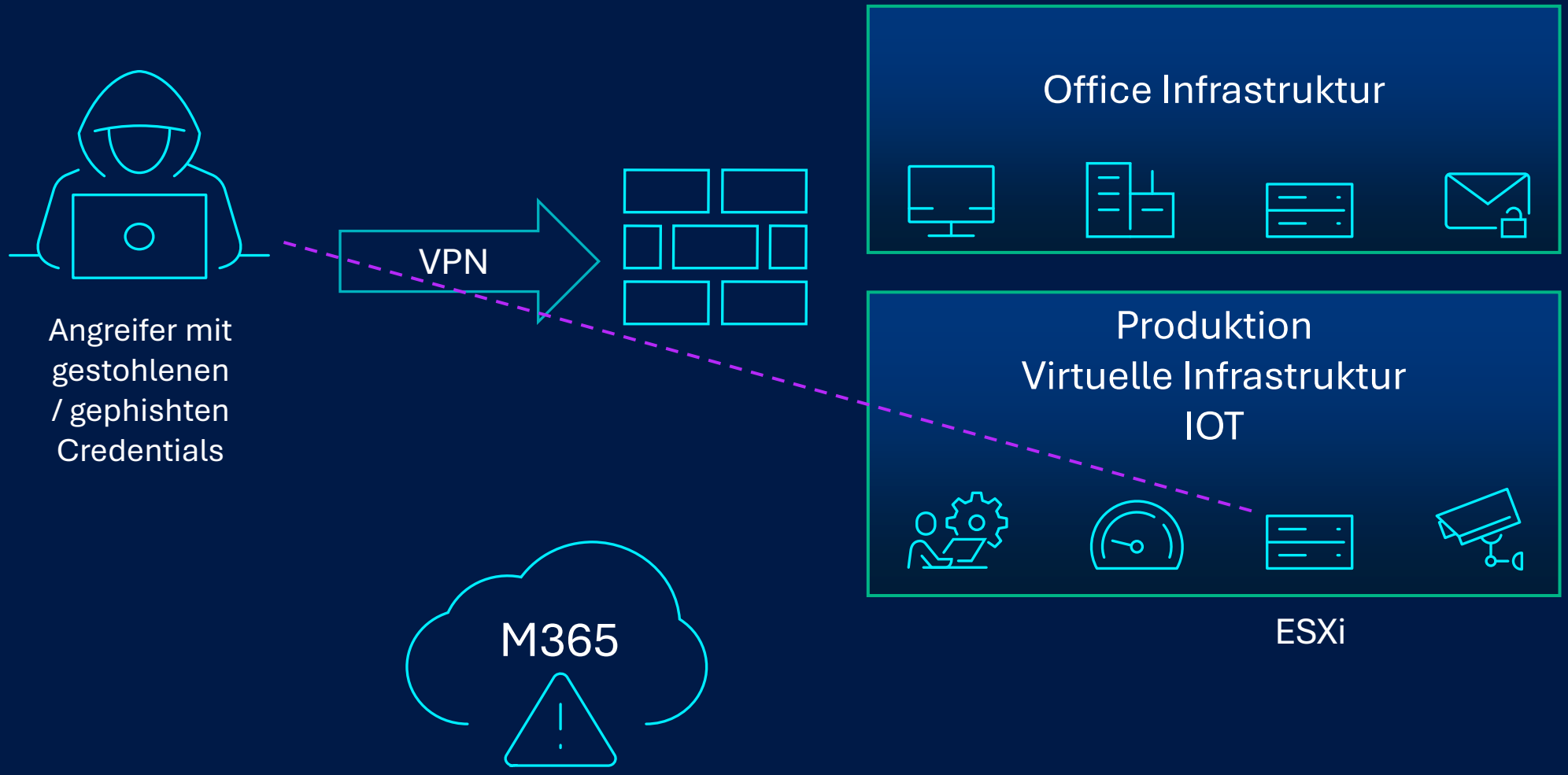
DATA LAKE

AI-ASSISTED & AGENTIC WORKFLOWS

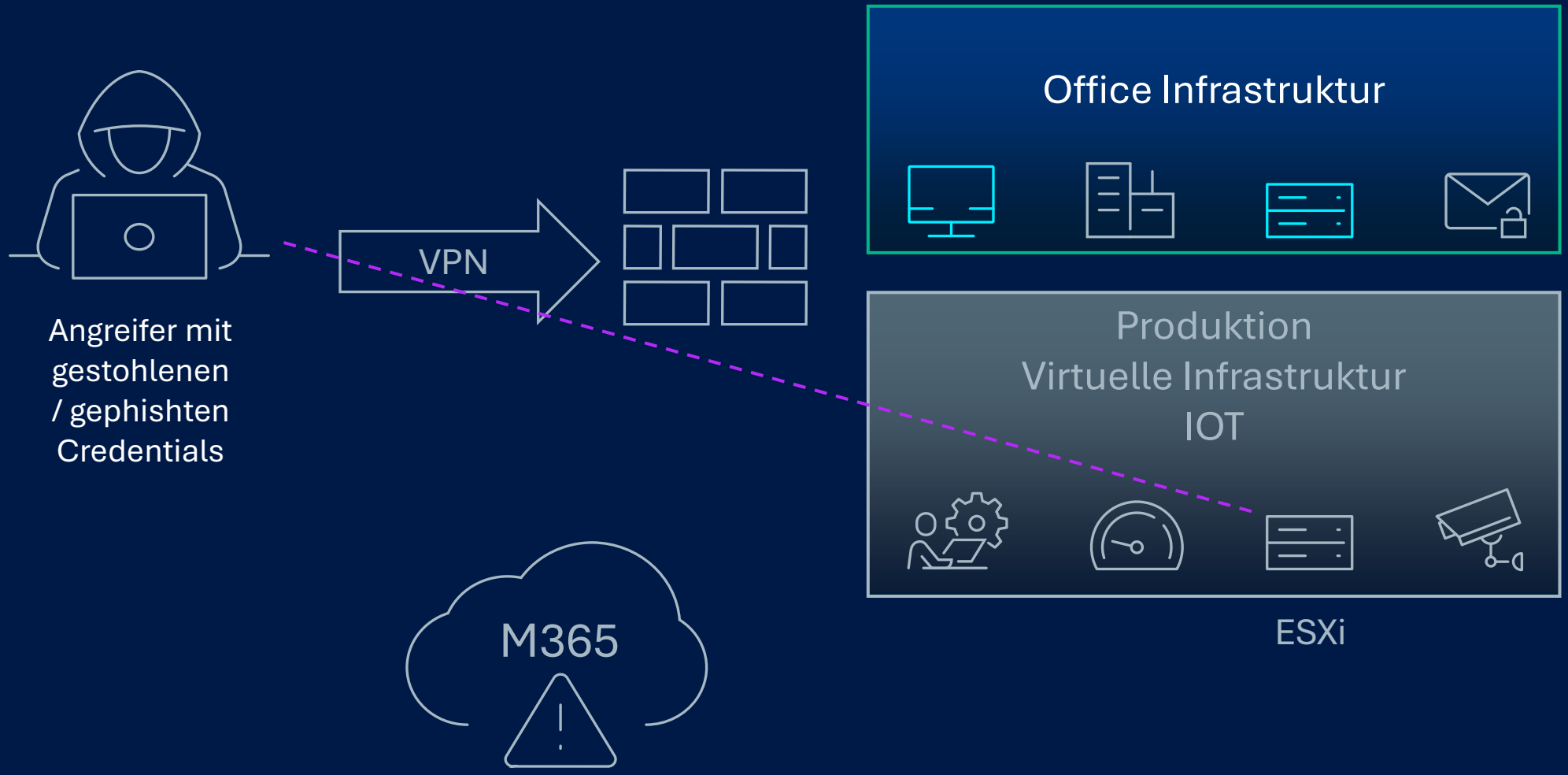
MDR – das reicht?



67% der aktuellen Angriffe*



Sichtbarkeit ohne zusätzliche* Telemetrie



Active Adversary Report 2026

https://www.sophos.com/de-de/blog/2026-sophos-active-adversary-report

- **Die durchschnittliche Verweildauer sank auf drei Tage.** Dies ist auf mehr Effizienz der Angreifer, aber auch die schnellere Reaktion der Verteidiger zurückzuführen. Der Rückgang ist in MDR-Umgebungen besonders auffällig.
- Angreifer gelangen immer schneller zur Active Directory (AD). Hat es der feindliche Akteur ins Innere der Organisation geschafft, **braucht er nur 3,4 Stunden, um den AD-Server zu erreichen**.
- Ransomware-Angriffe finden hauptsächlich außerhalb der Geschäftszeiten statt. **88 Prozent der Attacken fanden zu den Schließzeiten der Unternehmen statt**, ebenso wie 65 Prozent der Datenexfiltration.
- Ein **Mangel an Telemetrie untergräbt die Verteidigung** zusätzlich. Die Anzahl fehlender Protokolle aufgrund von Problemen bei der Datenspeicherung hat sich im Vergleich zum Vorjahr verdoppelt. Dieser Anstieg ist vor allem auf Firewalls zurückzuführen, bei denen die Standardeinstellung für die Log-Dateien nur sieben Tage und in einigen Fällen sogar nur 24 Stunden betrug.
- Die Multifaktor-Authentifizierung ist bei vielen Unternehmen immer noch nicht als wichtiges Sicherheitselement angekommen. **In 59 Prozent der Fälle mangelte es an MFA** und erleichtert so den Missbrauch gestohlener und kompromittierter Zugangsdaten.

Realität - Konfigurationsarmut

- M365 Integrationen sind nur bei 50% der Kunden aktiviert
- Für Active Directory Integration fehlt den allermeisten Installationen die notwendigen Security Events
- Nicht genug Kunden haben 3rd Party Integrations aktiviert
- Zu viele Unternehmen nutzen weiterhin kein MFA bzw. kein phishing-resistentes MFA

- Allein das zu korrigieren ist eine bezahlbare Service Leistung

Sophos MDR Analysten profitieren von allen M365 Lizenzen

MICROSOFT 365 LIZENZEN

M365 BUSINESS BASIC | M365 BUSINESS STANDARD | OFFICE 365 E1 | OFFICE 365 E3 | ENTRA ID P1 | ENTRA ID P2 | DEFENDER FOR ENDPOINT P1/P2 | M365 BUSINESS PREMIUM | M365 E3 | M365 E5

ORGANISATIONEN NUTZT

MS Produktivitätswerkzeuge

Office 365 Werkzeuge inkl. Word, Excel, PowerPoint, Teams, Outlook, OneDrive

SOPHOS MDR

- Nutzt **Microsoft-Telemetrie** zur **Erkennung** menschlich gesteuerter Angriffe
- Sophos-Analysten können in Microsoft 365 **Gegenmaßnahmen** ausführen
- **Proprietäre Sophos-Regeln** auf Basis von Microsoft-Management-Ereignissen

ORGANISATIONEN NUTZT

Microsoft Entra ID

Entra ID standalone oder Teil eines Bundles

SOPHOS MDR

- Nutzt **Microsoft Entra ID Telemetrie** zur Erkennung von Angriffen
- Sophos-Analysten können direkt im **Entra-ID Gegenmaßnahmen** ausführen
- **Sophos ITDR** erkennt **zusätzlich** Entra ID **Fehlkonfigurationen**, verdächtiges **Anmeldeverhalten** sowie gestohlene u. **geleakte Zugangsdaten**

ORGANISATIONEN NUTZT

Microsoft Sicherheitswerkzeuge

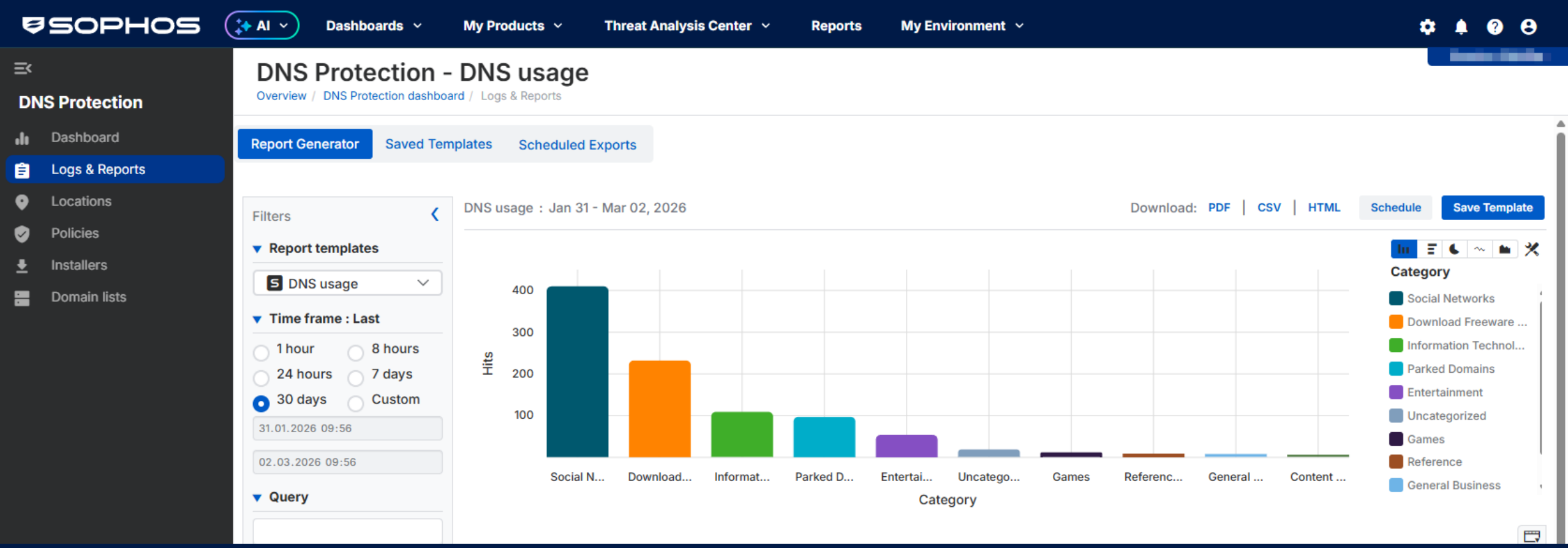
Microsoft Defender für Endpoint, Cloud Apps und Identity.

SOPHOS MDR

- Nutzt Alarme von **Microsoft Sicherheitswerkzeugen** zur Erkennung von Angriffen
- **Filtert** Alarme und **korreliert** sie mit **Sophos-Telemetrie** und **anderen Quellen**
- **Ergänzt interne Teams** durch MS-zertifizierte **Analysten** mit maßgeschneiderten **Playbooks** für Microsoft-Umgebungen

EXPERIENCE

Workspace Protection Trial – DNS Protection

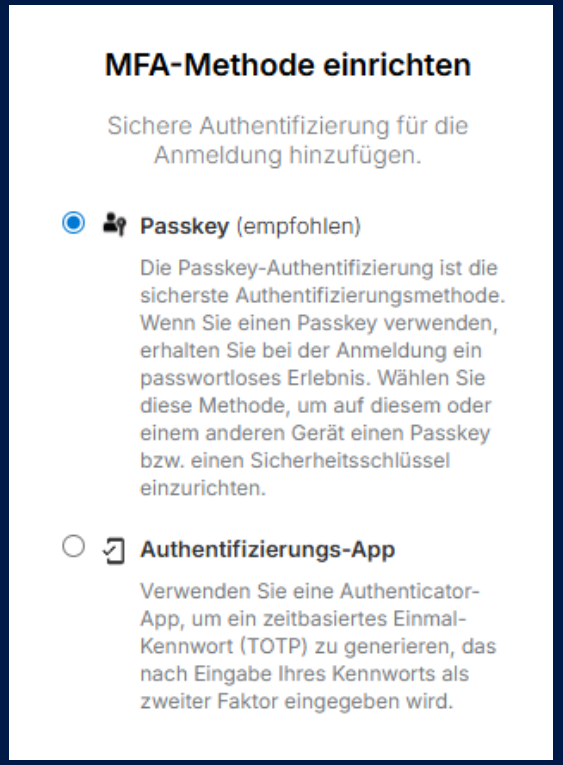


EXPERIENCE

Erste Schritte, bevor man Passkeys implementieren kann

NIS 2, DSGVO, ISO 27001, TISAX, PCI-DSS, HIPAA, SOC 2, C5, SOX, ...

- Response – sofortige Aktion
  - Kontrolle über kompromittierte Konten – Sophos XDR / MDR / ITDR
  - C2 Verbindungen blockieren – Sophos XDR / MDR + Sophos Firewall
- Conditional Access - Microsoft Entra ID P1 oder höher
- Kompromittierte Zugangsdaten finden - Sophos ITDR
- M365 / AD User Setup verifizieren - Sophos ITDR
- Zutrittskontrolle - Sophos Workspace Protection
- Kontrolle der Arbeitsumgebung - Sophos Endpoint / XDR / MDR
- Kommunikation unverwalteter Geräte prüfen – Sophos NDR
- Angriffsfläche reduzieren – Sophos Managed Risk



EXPERIENCE


SOPHOS


SOPHOS
PARTNER 2026
EXPERIENCE

SOPHOS

Projekte gewinnen mit MDR enabled Firewall

SOPHOS CENTRAL PLATFORM

Managed by Customers | Managed by Partners | Managed by Sophos

SERVICES

MANAGED SERVICES

- MDR
- Incident Response
- Vulnerability Management
- Professional Services

ADVISORY SERVICES

- Penetration Testing
- Security Assessments
- Red Team Exercises
- Incident Readiness

THREAT PREVENTION AND CONTROLS

CONTROLS

- Endpoint
- Firewall
- Identity
- Email
- Network
- Web Browser

INTEGRATIONS

350+ Third Party Integrations

SECURITY OPERATIONS

- XDR
- SIEM
- EDR
- ITDR
- NDR
- SOAR

THREAT INTELLIGENCE

SOPHOS X-OPS

- Adversary Tracking
- Threat Research
- Breach Forensics
- Malware Analysis
- Industry Collaboration

AI, AUTOMATION & ENGINEERING

- Adaptive Attack Protection
- Critical Attack Warning
- Security Analytics
- Detection Logic
- Threat Protection

DATA LAKE

AI-ASSISTED & AGENTIC WORKFLOWS

Flexibel im Einsatz – immer gleiche Software

XGS Series
hardware appliances

Virtual or Software
appliance

Public Cloud

Xstream Protection – ein Bundle für alles

EMPFEHLUNG

	Standard Protection	Xstream Protection
Base License	✓	✓
Network Protection	✓	✓
Web Protection	✓	✓
DNS Protection (für Firewalls)		✓
Zero-Day Protection		✓
Central Orchestration		✓
MDR and 3rd Party Threat Feeds		✓
NDR Essentials Protection		✓
Enhanced Support	✓	✓
XGS Series Appliance 	✓	✓

Ideal für Installationen ohne TLS Decrypt.

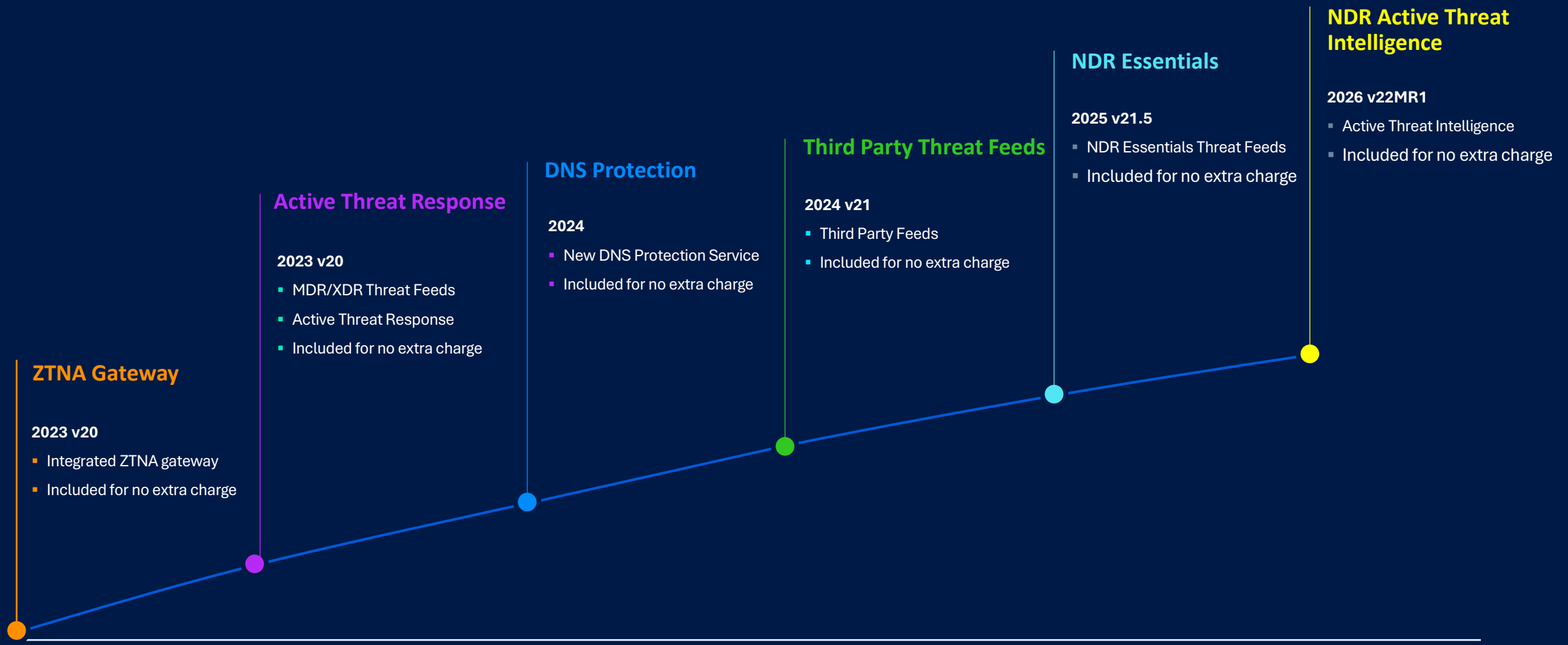
Ideal für Installationen ohne TLS Decrypt.

XDR / MDR Integration

Minimum Lizenz für Mgmt und Updates

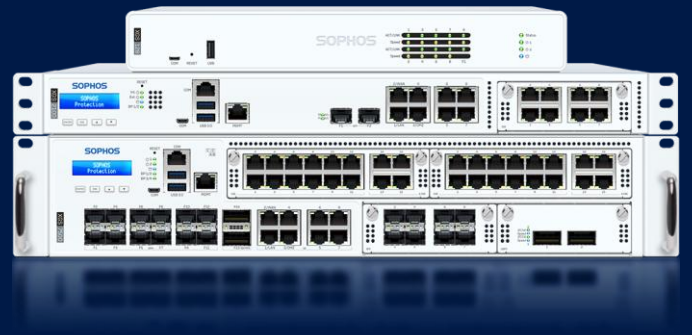
EXPERIENCE

Steigende Wertstellung von Xstream Protection



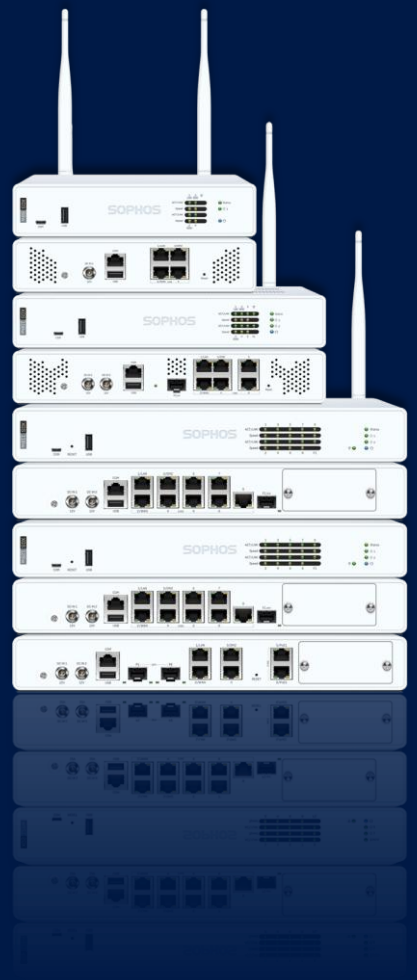
Sophos Firewall auf den Punkt

- Central Partner Dashboard
  - Einfache Verwaltung über viele Kunden – ohne extra Kosten
  - Alternativ auch mit MSP Lizenzen
  - Skalierbar
- Sophos MDR enabled Firewall
  - Advanced Threat Response
  - Synchronized Security
  - Authentifizerung über Synchronized Security
- Eingebaute Sandbox mit Sophos Intelix
- Central Firewall Reporting – 30 Tage in Xstream eingebaut
- Active-Passive HA ohne Notwendigkeit der Lizenzierung der 2. Box
- Integration in SOC Services wie Sophos MDR



Flexible Firewall für alle KMU-Projekte

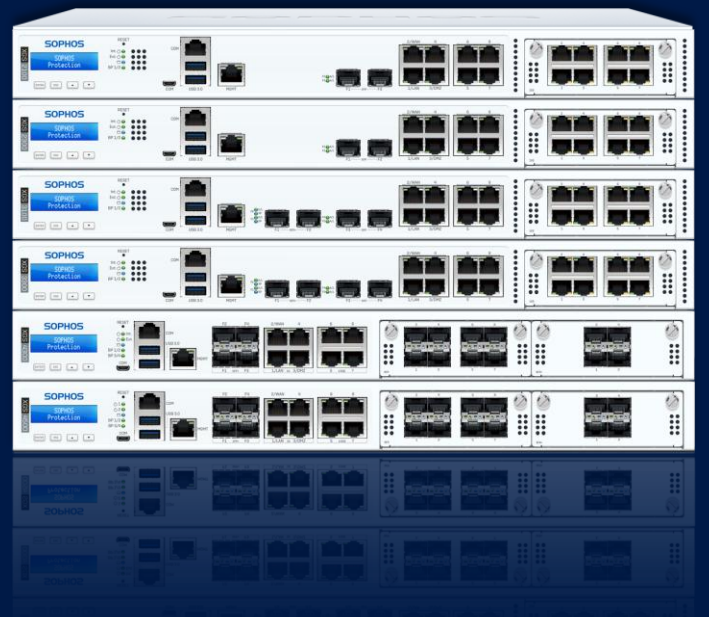
- Performante Hardware Modellpalette – Ablöse des in die Tage gekommenen Mitbewerbs
- Zusammen mit **EP100** ein Preis-Leistungshammer, VPN inklusive
- Wireless und Switch auf der gleichen Plattform
  - Hoch integriertes Partner Management
- Neukunden Promo macht es preislich extrem attraktiv



EXPERIENCE

MDR enabled Firewall für alle Mittelstands-Projekte

- SD-WAN integriert
  - Anbindung aller Standorte **ohne Aufpreis**
- VPN oder Workspace Protection
  - Unterstützung zum Wechsel nach Zero Trust
  - Hybrid Working
  - Phishing Resistenz
- Service Unterstützung und Wartungsverträge mit Central Partner Dashboard



Sichere Firewall für alle Projekte großer Unternehmen

- Performance für größere Installationen
- Kein zusätzliches Training notwendig
  - Gleiche Konfiguration und Administration von Sophos Firewall über alle Modelle hinweg
- Flexible Anbindung vieler Außenstellen mit Zero Touch Deployment
  - Wahl zwischen **SD-RED** oder **XGS 88/108**
  - Full Tunnel oder lokaler Internet Breakout

EXPERIENCE

Platform Security

Sophos Firewall | Secure by Design

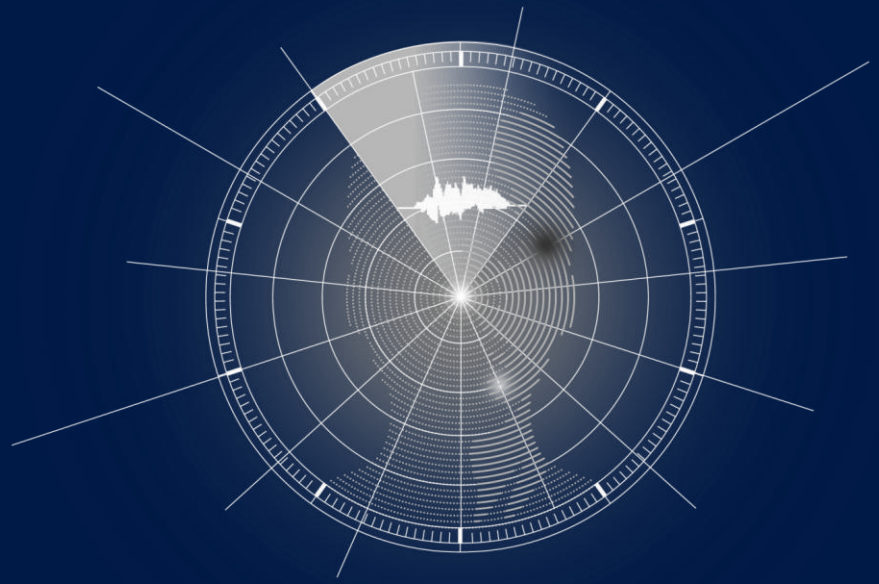
Sichere Firewall

- CISA Secure by Design Initiative
  - Sophos verfolgt alle Punkte dieser Initiative, um Sicherheit der Plattform zu erhöhen
- Backup sind doppelt gesichert in Sophos Central
  - Backup Passwort plus zweiter Schlüssel (SSMK)
- Hotfixes werden automatisch ausgerollt
  - Sophos adressiert automatisch alle sicherheitsrelevanten Themen
  - Ohne **zusätzliche Wartungsfenster** oder **Aufpreis**
- Keine unbezahlten Stunden zum Debugging und Firmware-Wechsel wegen Sicherheitslücken

MDR enabled Firewall

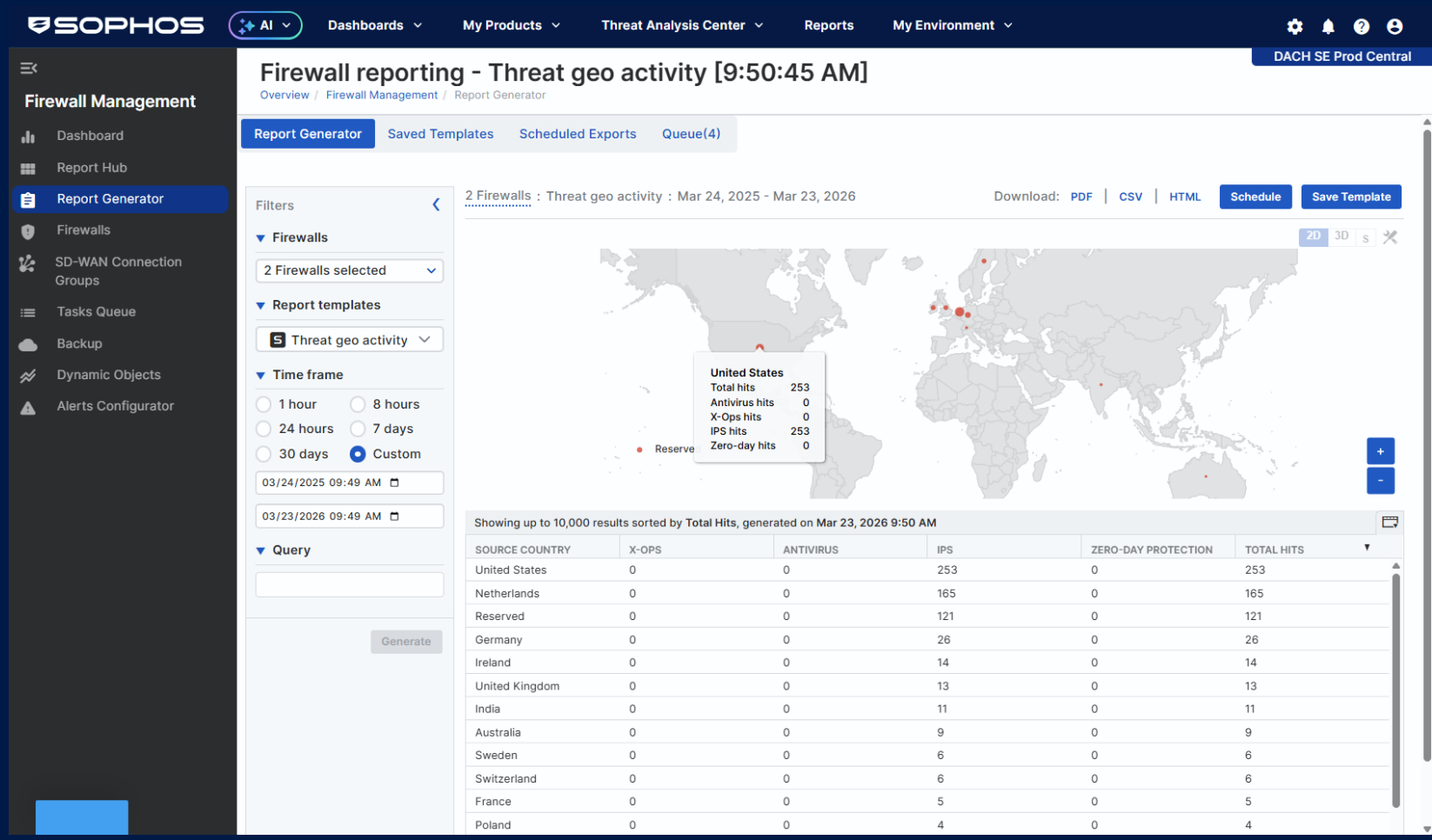
MDR Enabled Firewall - Active Threat Response

- **Echtzeit Threat Feeds** (IP-Adressen, Domains, URLs) direkt an die Kunden-Firewall senden
  - Betrieb durch Sophos, **Partner** oder Kunde
- Über 50% der MDR Kunden nutzen Sophos Firewall
- Nahtlose Integration mit Sophos MDR und Sophos XDR
- Flexibles Servicemodell: Kunde oder Partner oder Sophos
- Keine Konfiguration notwendig



Central Firewall Reporting

- Automatische Reports für Abteilungs-/Firmenführung
  - Z.B. für MSP Service Nachweis
- Datenhaltung bis zu einem Jahr
- Stapelbare Lizenzen
- Konfigurationsfreie Integration in Sophos XDR und MDR
- Keine On-Premise Installation notwendig, reduziert den Aufwand für Datenspeicherung
- Nahtloser RMA Übergang
- Compliance



Data Storage Estimation Tool

https://www.sophos.com/en-us/products/next-gen-firewall/central-reporting/sizing-tool

EXPERIENCE

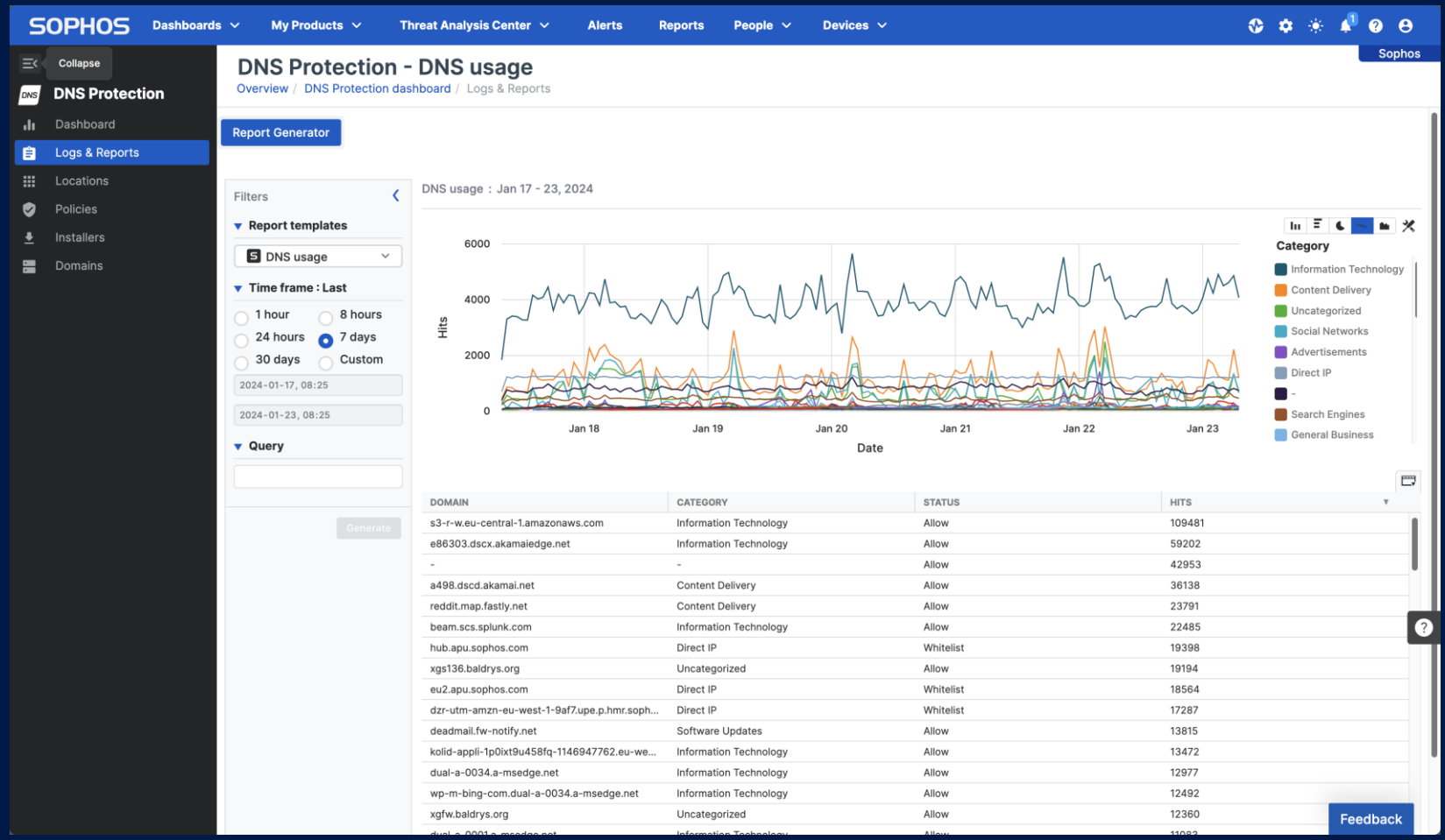
Transparenz ohne Entschlüsselung

NDR Essentials und DNS Protection

- Die Analyse von TLS-Verschlüsslung stellt Kunden vor Herausforderungen
  - Datenschutz / Betriebsrat
  - Technische Herausforderung (Ausrollen von Zertifikaten und Ausnahmen wie Online-Banking)
- NDR Essentials und DNS Protection in Sophos Firewall bieten Schutz ohne die Komplexität des Aufbrechens der Verschlüsselung
- Patentierte Technologie in NDR Essentials, um Verkehr zu analysieren, ohne Mehraufwand
- Einer der größten Internet Datenbank der Welt (Sophos SXL) in DNS Protection, um Gäste- und Benutzerzugriff zu regulieren

DNS Protection - Service Modell

- Analyse des Verkehrs
  - Unkategorisiert
  - Parked Domains
  - AI
  - Zeitfresser
- Implementation
  - Universelle Service Modelle
  - Ideal mit Workspace Protection
  - Ideal für Hybrides Arbeiten
  - Compliance + Reports

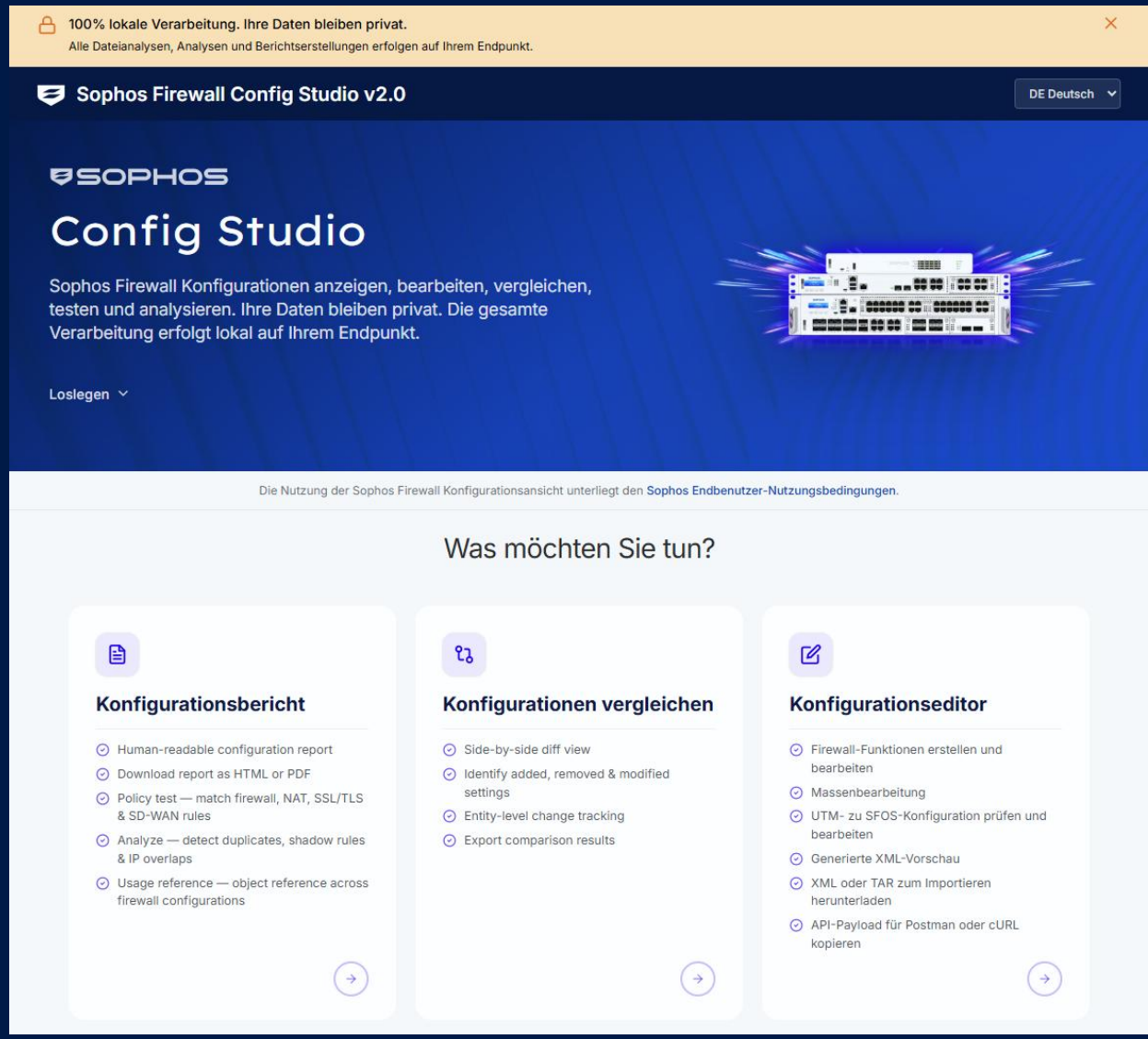


EXPERIENCE

Extras

Firewall Config Studio

- Kostenfrei für Partner und Kunden / Keine Anmeldung
- Kein anderer Hersteller bietet diesen Service an
- Für MSP und Service Partner geeignet, um seine Arbeit schnell zu dokumentieren
- Unterstützt die Technik beim modernisieren der Firewall Konfiguration
- Kann für Projektgeschäft genutzt werden



EXPERIENCE


SOPHOS
DEFEAT CYBERATTACKS