
SOPHOS
PARTNER 2026
EXPERIENCE

SOPHOS

# Sophos Workspace Protection

# (M)ein typischer Arbeitstag?

Hybrides und von unterwegs Arbeiten heißt: Ich bin online!

**Kooperieren**

**Erstellen**

**Beraten**

**Kommunizieren**

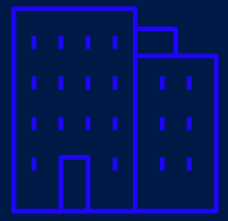
Und die meisten Tätigkeiten finden im Browser statt?

# WER arbeitet von WO, auf WELCHE Art und Weise?


PRIVATE ANWENDUNGEN


SaaS ANWENDUNGEN

GENERELLES WEB



# Sophos Workspace Protection

Alle erforderlichen Schutzfunktionen in einer einzigen, einfachen und kostengünstigen Lösung integriert

## Protected Browser

## ZTNA

## DNS Protection

## EMS

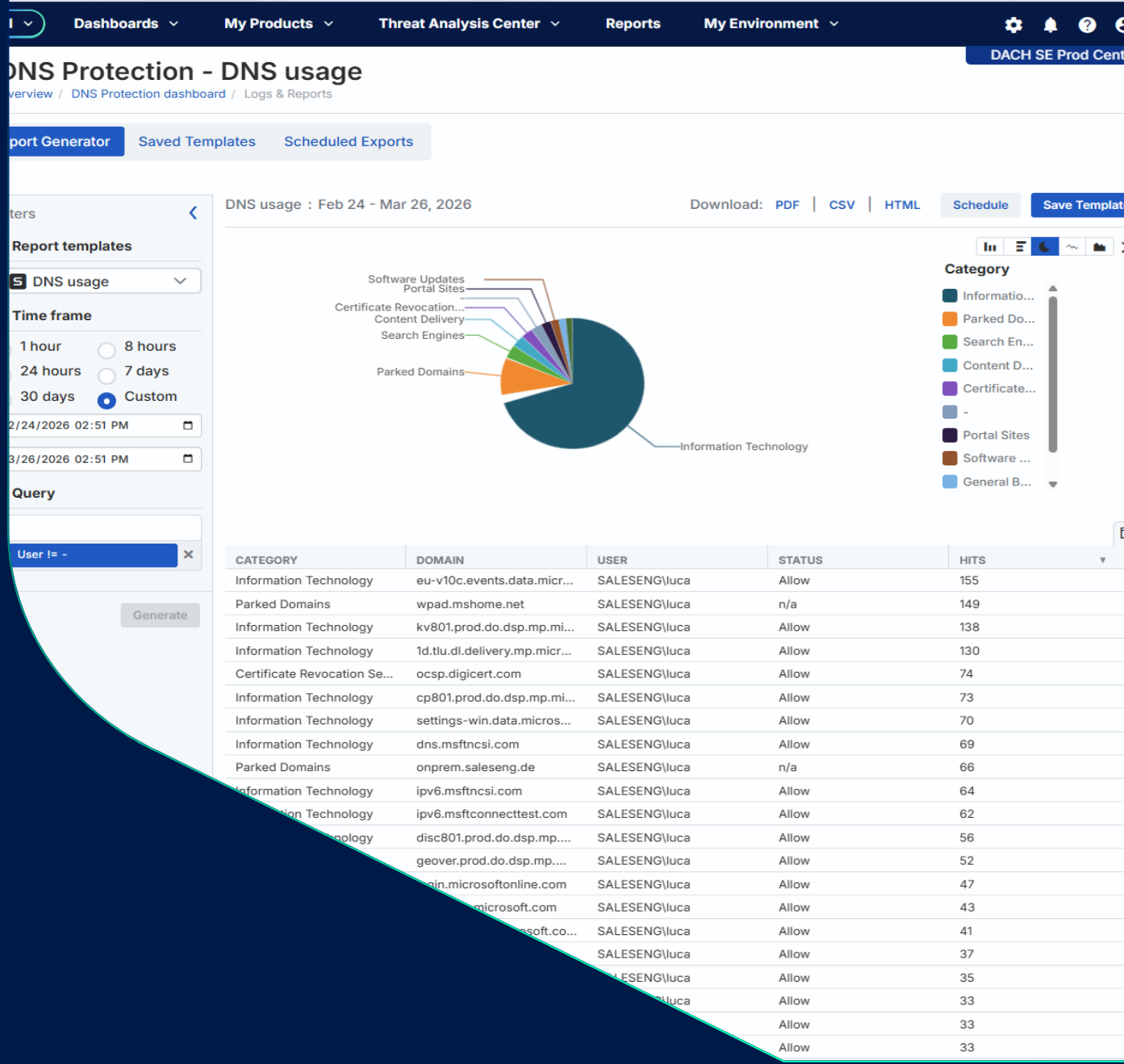
Bereitstellen oder nur das nutzen, was gebraucht wird

## Sophos Workspace Protection

# Sophos DNS Protection

# Sophos DNS Protection

- Sophos DNS Protection unterstützt DNS over HTTPS (DoH)
- Regulieren von DNS-Anfragen
- Performantes Blocken
  - Kein Filtertreiber benötigt
- Anwendbar auf alle Applikationen und nicht nur HTTP/S (wie z.B. ein Proxy)
  - Blockieren von GenAI im Browser **und** Apps
- Verfügbar in Sophos Firewall & Workspace Protection




SOPHOS

PARTNER 2026 EXPERIENCE

# DNS Protection im Endpoint vs. Sophos Firewall

## DNS Protection auf der Sophos Firewall

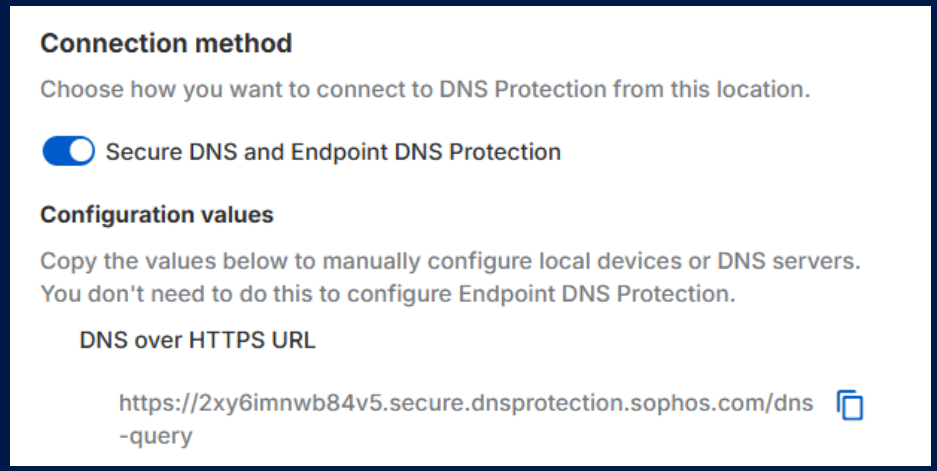
- Konfiguration im DHCP-Server
- Erfordert keine Konfiguration auf einem Client selbst
- Block Page Zertifikat ist Optional
- Geeignet für BYOD-Netzwerke (z.B. Gäste)
- Standort basiertes Reporting

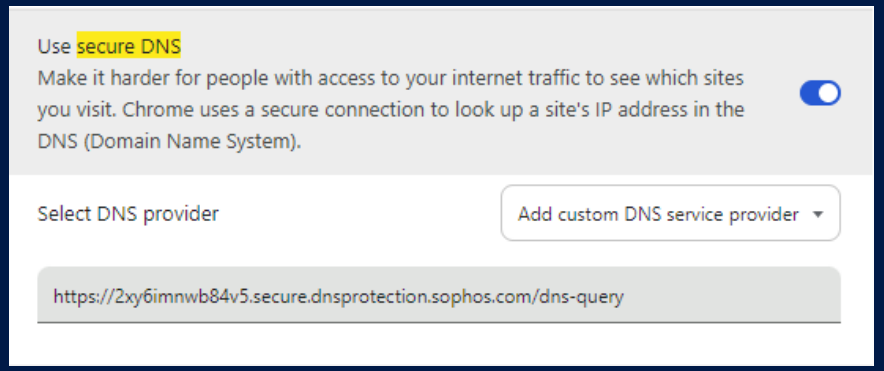
## DNS Protection im Sophos Endpoint

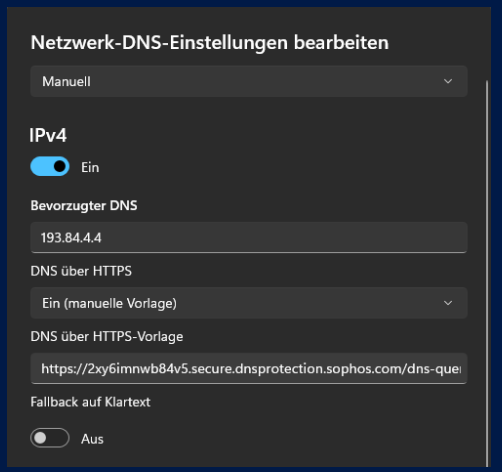
- DoH Setting und Block Page Zertifikat werden vom Sophos Endpoint ausgerollt
- User können diese Einstellung nicht verändern (Always On)
- Hinter der Firewall und im Homeoffice aktiv
- User basiertes Reporting

# Auch ohne Sophos Endpoint!

- DoH wird von Betriebssystemen und Browser unterstützt
- Pro Sophos DNS „Location“ werden eigene DoH Links generiert
  - Locations beinhalten Control&Block Entscheidungen
- DoH Einstellungen sind zentral verwaltbar, z.B.
  - Microsoft Intune
  - GPOs
  - Management Tools

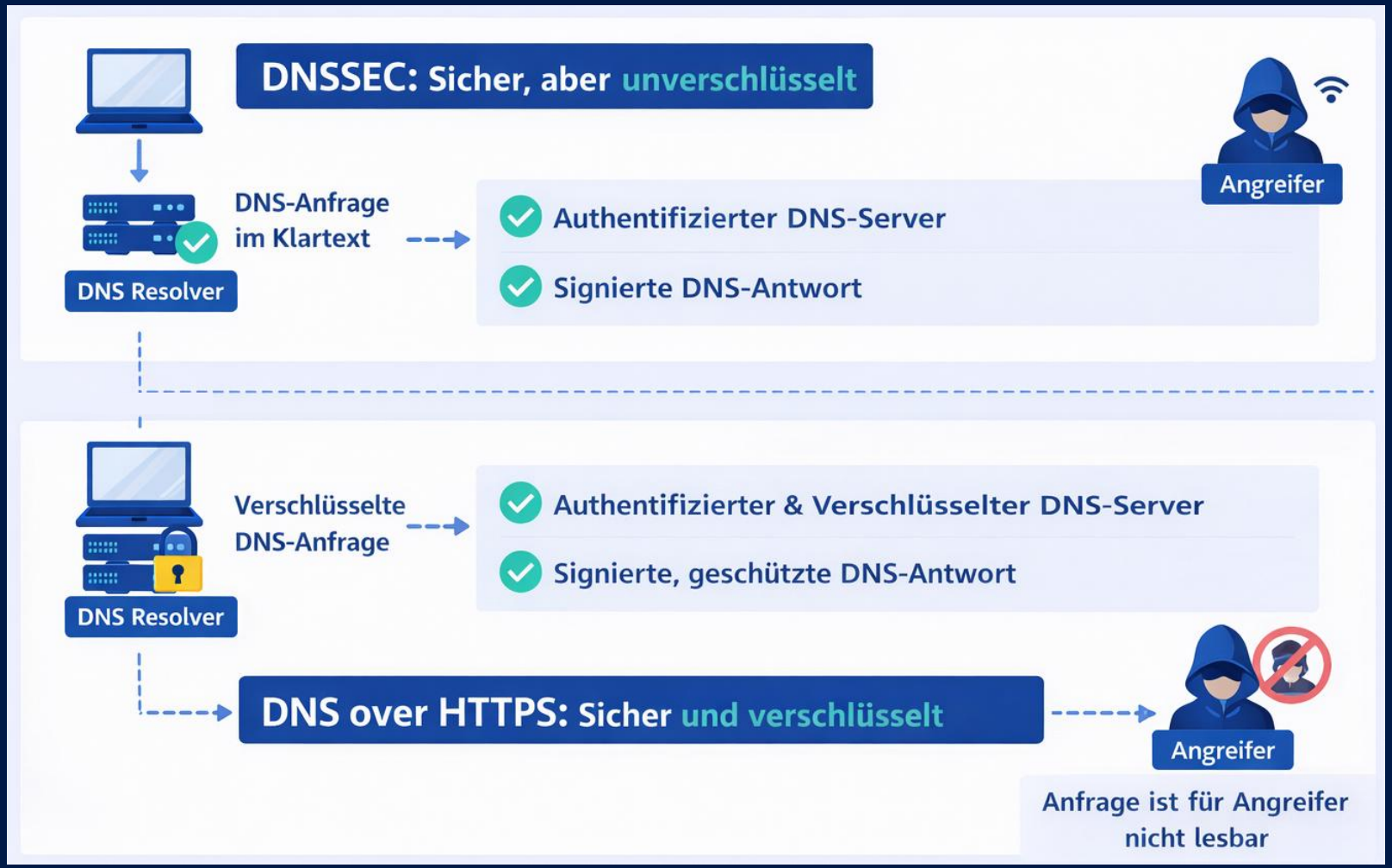


# Warum eigentlich DoH?

# Warum eigentlich DoH?



## Sophos Workspace Protection

# Sophos Protected Browser

# Was sind die TOP 5 Anforderungen von Endkunden?

### Data Control (im Browser)

Ich möchte vermeiden, dass sensitive Daten einfach außerhalb meines Unternehmens gelangen

### Fernwartung & Fernzugriff ohne Device Trust

Ich möchte eigenen Mitarbeitenden und externen Parteien unkompliziert Fernzugriff gestatten

### Web Protection (unmanaged)

Ich möchte Web-Security durchsetzen – auch auf Geräten, die nicht zu meiner Organisation gehören.

### Web Control

Ich möchte festlegen, wie Web-Applikationen genutzt werden – nicht nur, ob sie erreichbar sind.

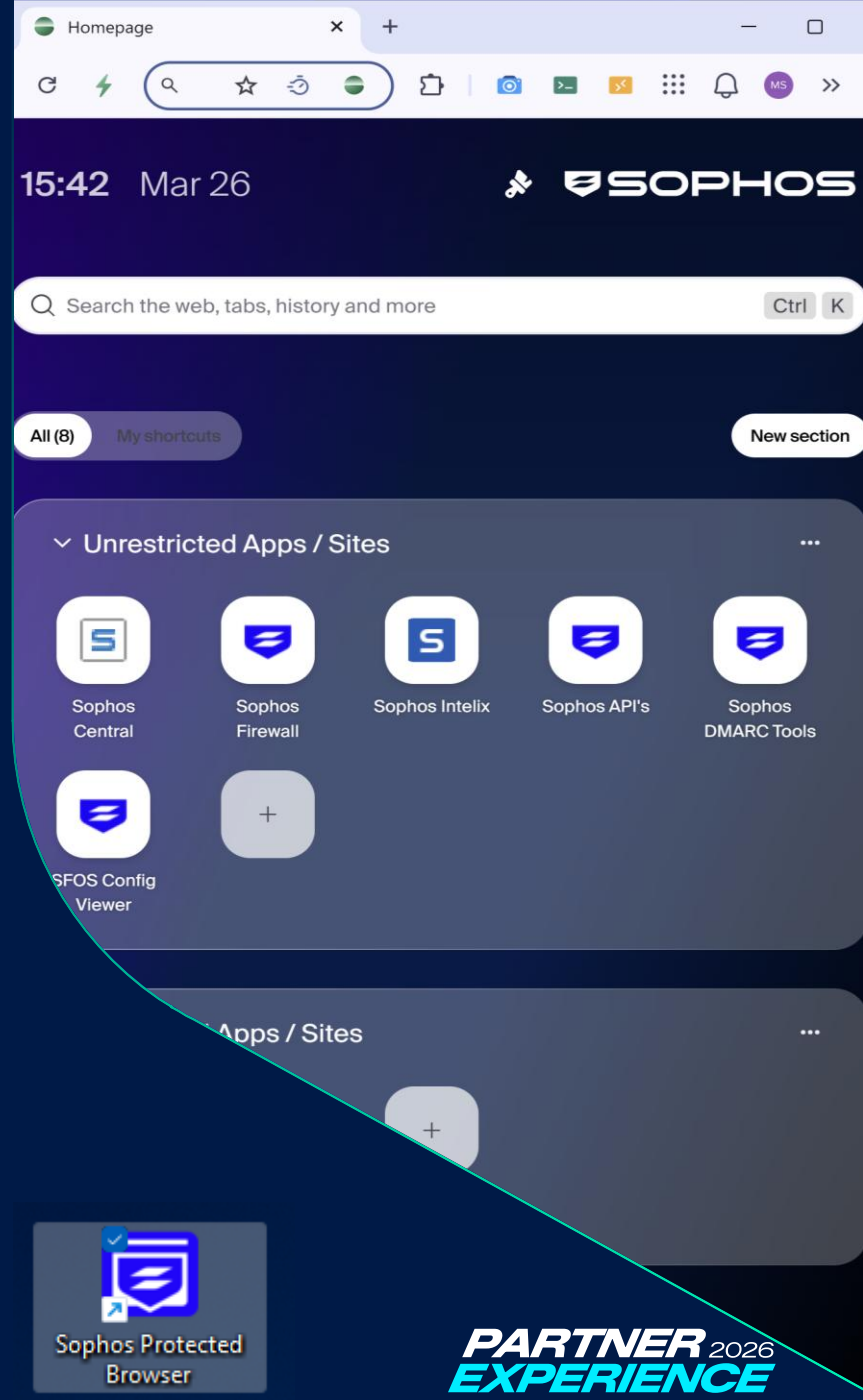
### EntraID Conditional Access

Ich möchte kontrollieren können, welche Gruppen/Benutzer auf meine Web Apps mit meinen Spielregeln zugreifen können

# Was ist ein Protected Browser?

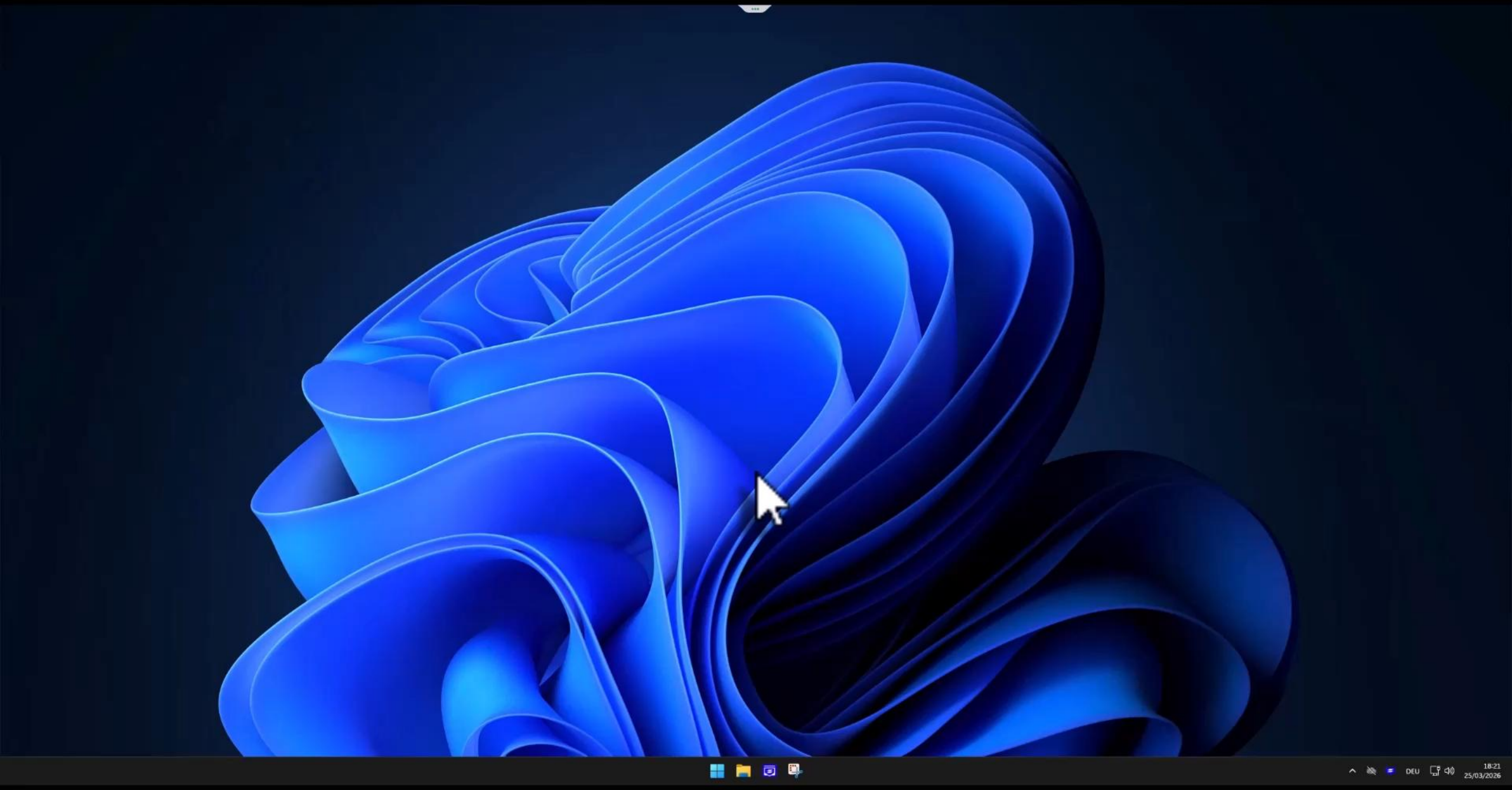
**„Ein Browser wie jeder andere – nur vollständig kontrolliert, abgesichert und zentral gesteuert.“**

- Auf Chromium basierender Browser
- Über Sophos Central verwaltet inklusive Reporting
- Inklusive Webfilter Möglichkeiten
  - CA-Rollout frei
- Integrierter RDP&SSH Client für Sophos ZTNA
- Data Control um Screenshots, Copy/Paste zu kontrollieren
- Unterstützt EntraID Conditional Access

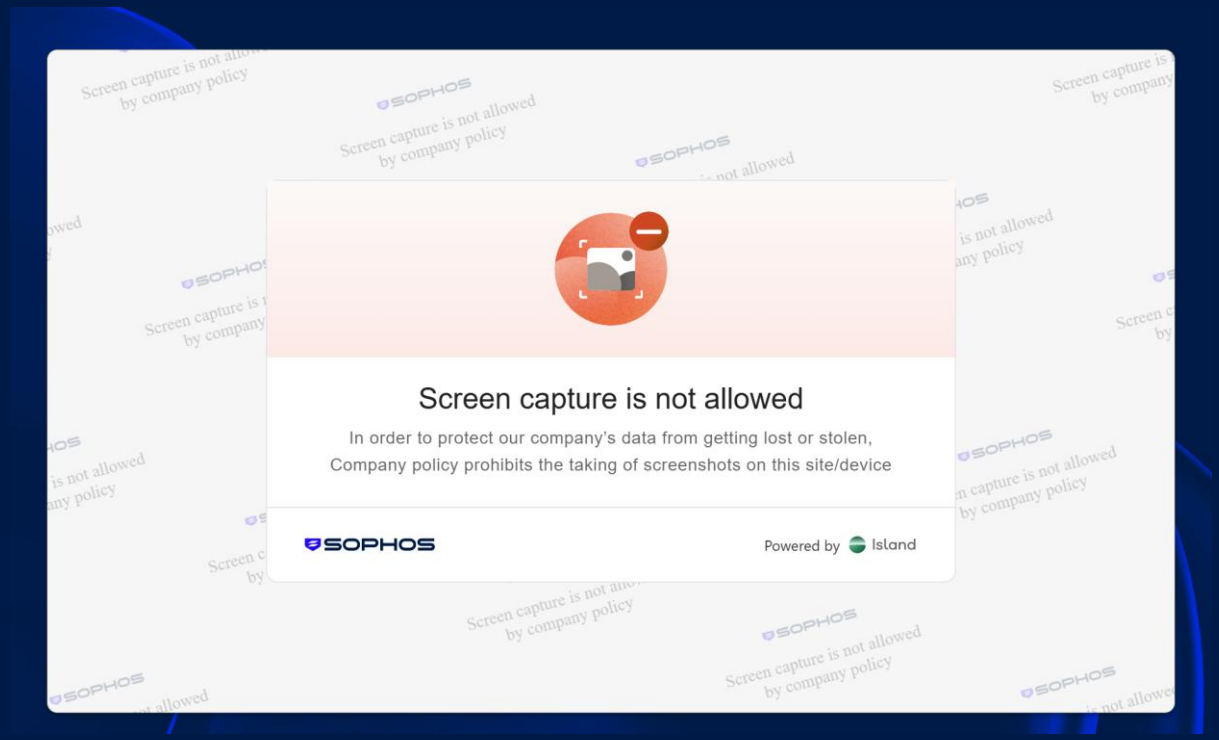


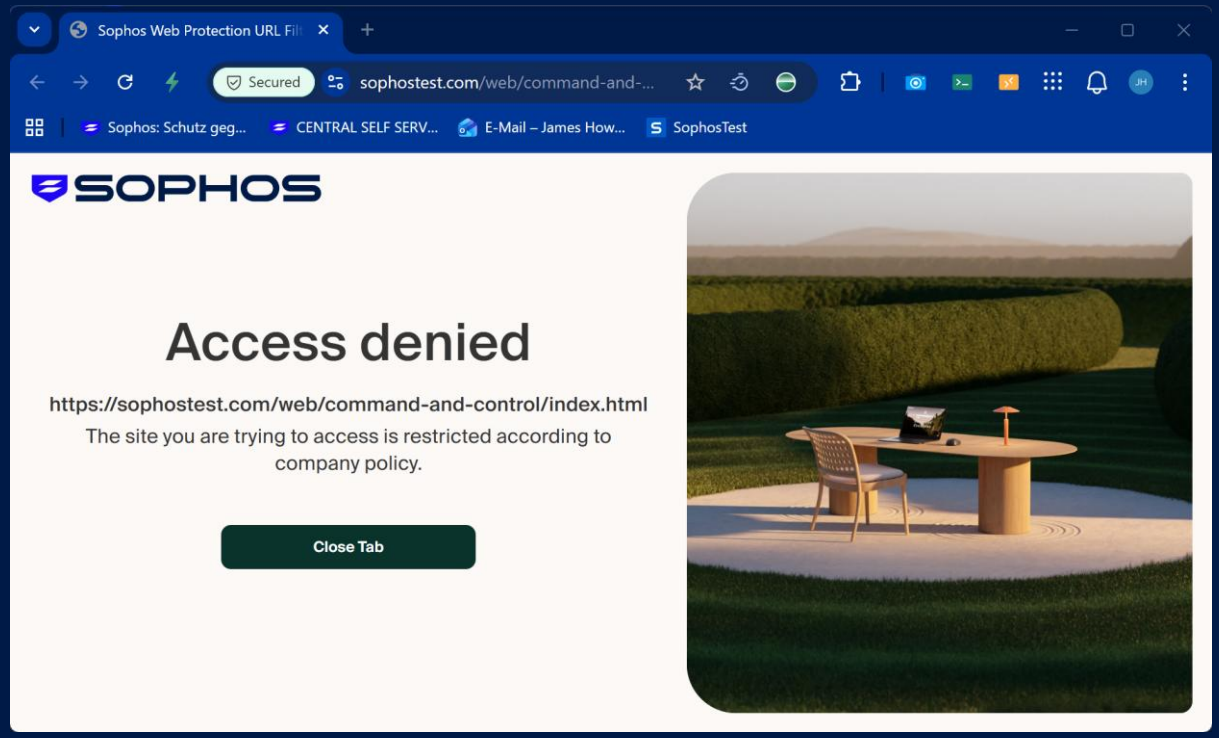

SOPHOS

PARTNER EXPERIENCE 2026


DEU
18:21
25/03/2026

# Richtlinien durchsetzen – Block Pages



# Protected Browser – Dashboard

SOPHOS AI Dashboards My Products Threat Analysis Center Reports My Environment

Frieder Kettel

## Protected Browser - Logs & reports

Overview / Protected Browser / Logs & reports

- Protected Browser
- Dashboard
- Logs & reports
- Web policy
- Policy objects
- Settings

Report generator | Saved templates | Scheduled exports

Filters

**Report templates**

Web Usage

**Time frame**

1 hour | 8 hours | 24 hours | 7 days | 30 days | Custom

03/19/2026 09:58 AM

03/26/2026 09:58 AM

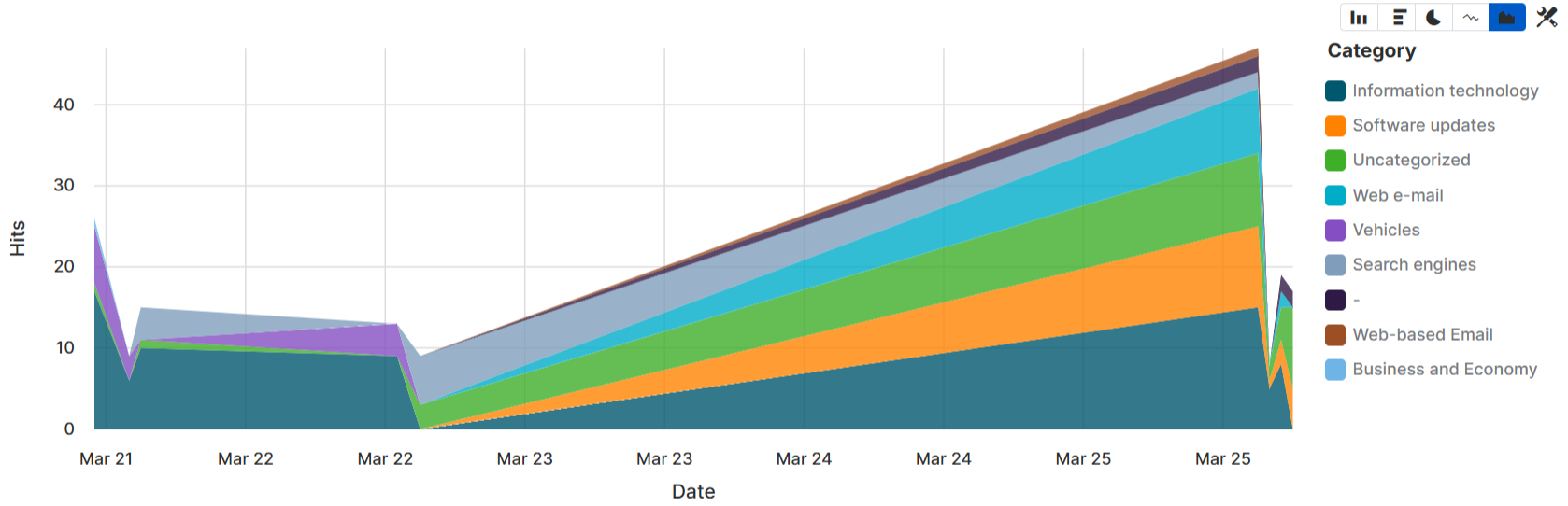
**Query**

OS User != GREEN\Frieder.Kettel

Generate

Web Usage : Mar 19 - 26, 2026

Download: PDF | CSV | HTML Schedule Save Template




Showing up to 10,000 results sorted by **Hits**

| Date | Status | User | OS User | Local IP | Category | Domain | URL |
|---|---|---|---|---|---|---|---|
| Mar 25, 2026 3:00 PM | Allowed | lab@kep4.de | AzureAD\JamesHowl... | 192.168.12.21 | Software updates | www.sophos.com | https://v |
| Mar 25, 2026 3:00 PM | Allowed | lab@kep4.de | AzureAD\JamesHowl... | 192.168.12.21 | Information technolo... | outlook.cloud.micros... | https://c |
| Mar 25, 2026 5:00 PM | Allowed | lab@kep4.de | AzureAD\JamesHowl... | 192.168.12.21 | Information technolo... | outlook.cloud.micros... | https://c |
| Mar 25, 2026 6:00 PM | Approved | lab@kep4.de | AzureAD\JamesHowl... | 192.168.12.21 | Uncategorized | island.apps.homepage | https://i |

# Welche Lösung für welches Enkundenszenario?

| Commercial | Midmarket | Enterprise |
| --- | --- | --- |

Workspace Protection + EP + FW
= Maximaler Schutz

Workspace Protection mit Endpoint Protection = Synchronized Security
oder
Workspace Protection Standalone = maximal kompatibel mit 3rd Party EP + FW

Workspace Protection +
Protected Browser + DNS only
= Enterprise kompatibel

# Die drei wichtigsten Vorteile der Sophos Workspace Protection

| | |
|---|---|
| **Architektur & Betrieb** | • Cloud Native, no Backhauling<br>• Kein Full-Agent-Zwang<br>• Schnelles Rollout (auch für externe User) |
| **Security-Mehrwert** | • Reduziert Angriffsfläche im Browser (Hauptangriffsrisiko)<br>• Verhindert Credential Theft & Session Hijacking<br>• Schutz vor Zero-Day-Web-Angriffen |
| **Business Impact** | • Weniger Vorfälle durch Web-Angriffe<br>• Schnellere Absicherung von Partnern, Externen & BYOD<br>• Ideal für M&A- oder Übergangsszenarien |


SOPHOS
PARTNER 2026
EXPERIENCE

# Sophos XDR/MDR & ITDR mit Microsoft 365 Daten

Referent 1 & Referent 2

SOPHOS

PARTNER 2026 EXPERIENCE

# Agenda

- Sophos für jeden M365 Plan
- Wertvolle Microsoft Telemetrie
- Gefahrenquelle Identity
- Aber bitte mit SOC

# Sophos nutzt Microsoft Telemetriequellen jedes Plans

MICROSOFT 365 LICENSING

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

## Management Activity

*Sophos Plattform Erkennungen*

- Sophos-eigene Erkennungsregeln für Rohhdaten
- Verarbeitet M365/EntraID-Auditprotokolle
- Für ALLE M365-Pläne verfügbar
- Ausgangspunkt für > 90% der Sophos MDR MS Cases

## Microsoft Graph Security

*Von Microsoft generierte Sicherheitsmeldungen*

- Sophos verarbeitet Meldungen von Microsoft Sicherheitslösungen
- Sophos bewertet und gruppiert Meldungen und reichert diese mit Sophos-Erkenntnissen an
- Qualität der Meldungen abhängig von M365-Plan, MS E5 liefert beste Meldungen

# Microsoft Management Activity Rohdaten - Sophos Erkennungen

## Welche Daten liefert Microsoft?

- Konfigurationsänderungen an Mandanten und Apps
- Anmeldeereignisse
- Dateizugriffe/-sharing
- [illegible]

## Was erkennt Sophos daraus?

- Verdächtige Änderung der Kontokonfiguration
- Verdächtiges Anmeldeverhalten
- Erstellung verdächtiger Postfachregeln
- Ungewöhnliche Dateifreigaben
- Indikatoren für Kontoübernahme
- Mögliches Business Email Compromise (BEC)

# Top Microsoft Management Activity Erkennungen

Erkennungen, die 2025 zur Erzeugung von Cases geführt haben

| # | Erkennung | Typ | % aller Erkennungen |
|---|---|---|---|
| 1 | SAAS-M365-inbox-SpecialCharacterInboxRuleName | Inbox Rule with Special Characters in Name | 21.4% |
| 2 | SAAS-M365-credstuffing-NodeFetch-AzureCLI-ValidSession | Credential Stuffing via NodeFetch / Azure CLI (Valid Session) | 20.3% |
| 3 | SAAS-M365-inbox-SixCharactersOrLessRuleName-DeleteAndMarkAsRead | Inbox Rule with Short Name (Delete & Mark as Read) | 20.1% |
| 4 | SAAS-M365-aitm-AxiosUserAgent-OfficeHome | AiTM Phishing via Axios User Agent (Office Home) | 9.5% |
| 5 | SAAS-M365-aitm-multipleOSandUserAgentsInSession | AiTM Session with Multiple OS / User Agents | 9.4% |
| 6 | SAAS-M365-inbox-MoveToConversationHistoryFolder | Inbox Rule Moving Mail to Conversation History | 7.6% |
| | Weitere Erkennungen | | 11.7% |

Quelle: Sophos MDR Ops

# Microsoft Graph Security - Meldungen von Security Produkten

## Beispiele für Microsoft Graph Security Meldungen

- Defender for Endpoint Bedrohungen (BP, E3, E5)
- Entra ID Identitätsrisiken und Impossible Travel (E5)
- Verdächtige Active Directory-Ereignisse (E5)
- Email Phishing- und Malware-Interaktionen (E3, E5)
-
-

## Was macht Sophos damit?

- Sophos bewertet und gruppiert Microsoft-Meldungen
- Sophos reichert Microsoft-Meldungen mit Sophos-Erkenntnissen an
-
-

# Microsoft Graph Security Erkennungen je nach M365 Plan

| Security Produkt \ M365 Plan | M365 Business Premium | M365 E3 | M365 E5 |
|---|---|---|---|
| **365 Defender / Defender for Office 365** | Eingeschränkt | Eingeschränkt | Vollständig |
| **Microsoft Entra ID - Identity Protection** | Eingeschränkt | Eingeschränkt | Vollständig |
| **Microsoft Defender for Endpoint** | Eingeschränkt[1] | Eingeschränkt[2] | Vollständig |
| **Microsoft Defender for Cloud Apps (CASB)** | Nein | Nein | Vollständig |
| **Microsoft Defender for Identity (on-prem AD)** | Nein | Nein | Vollständig |
| **Microsoft Defender for Cloud (Azure)[3]** | Nein | Nein | Nein |
| **Microsoft Purview - Data Loss Prevention** | Eingeschränkt | Eingeschränkt | Vollständig |
| **Microsoft Purview - Insider Risk Management** | Nein | Nein | Vollständig[4] |

[1] Defender for Business ist in Business Premium enthalten.
[2] Defender for Endpoint P1 (kein EDR).
[3] Separates Azure-Abonnement; nicht in M365-Bundles enthalten.
[4] E5 Compliance- oder eigenständiges Add-on.
*Quelle: Microsoft Graph Security API v1.0 - Alerts and Incidents providers (learn.microsoft.com)*

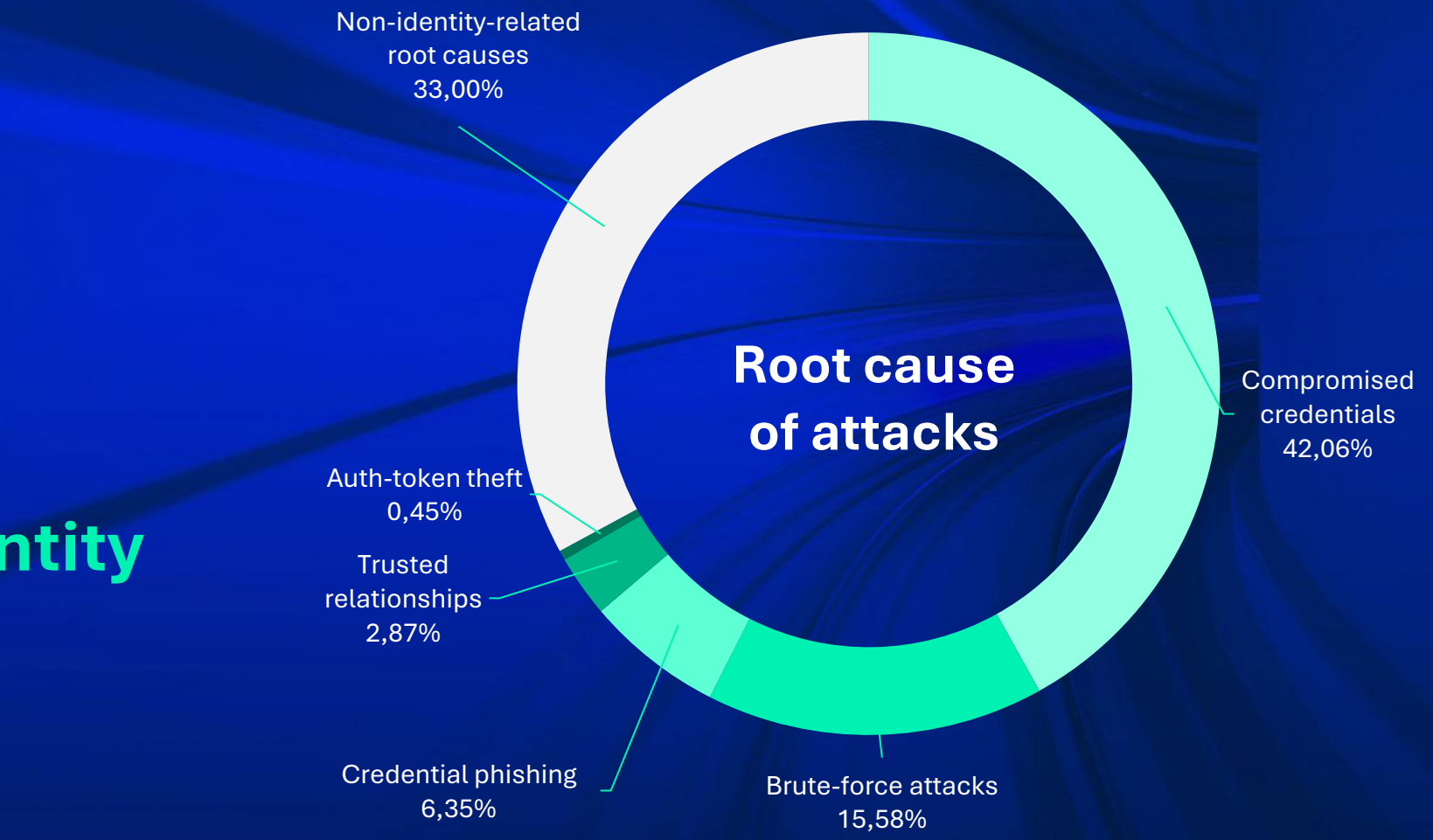
# Top Graph Security Erkennungen

Erkennungen, die 2025 zur Erzeugung von Cases geführt haben

| # | Detection | Provider | % |
|---|---|---|---|
| 1 | Leaked Credentials | Entra ID Identity Protection | 38.8% |
| 2 | Compromised User Account (Attack Activity Analysis) | Defender for Office 365 | 6.3% |
| 3 | User Clicked Through to Potentially Malicious URL | Defender for Office 365 | 5.4% |
| 4 | Suspicious Network Connection over EFS Remote Protocol | Defender for Endpoint | 3.7% |
| 5 | Phishing Document | Defender for Office 365 | 3.0% |
| 6 | Attempt to Turn Off Defender AV Protection | Defender for Endpoint | 2.7% |
| 7 | Impossible Travel Activity | Entra ID Identity Protection | 2.4% |
| | Weitere Erkennungen | | 37.7% |

Quelle: Sophos MDR Ops

# 67%
# of incidents started with compromised identity




Source: Sophos 2026 Active Adversary Report

SOPHOS

PARTNER 2026 EXPERIENCE

# Gefahrenquelle Identität - Sophos ITDR

Ganzheitlicher Ansatz, das Identitätsrisiko in der Organisation zu reduzieren

### Reduziert die Identity Angriffsfläche

Kontinuierlicher Scan von Microsoft Entra ID nach Identity Sicherheitslücken und Fehlkonfigurationen

### Minimiert das Risiko kompromittierter Zugangsdaten

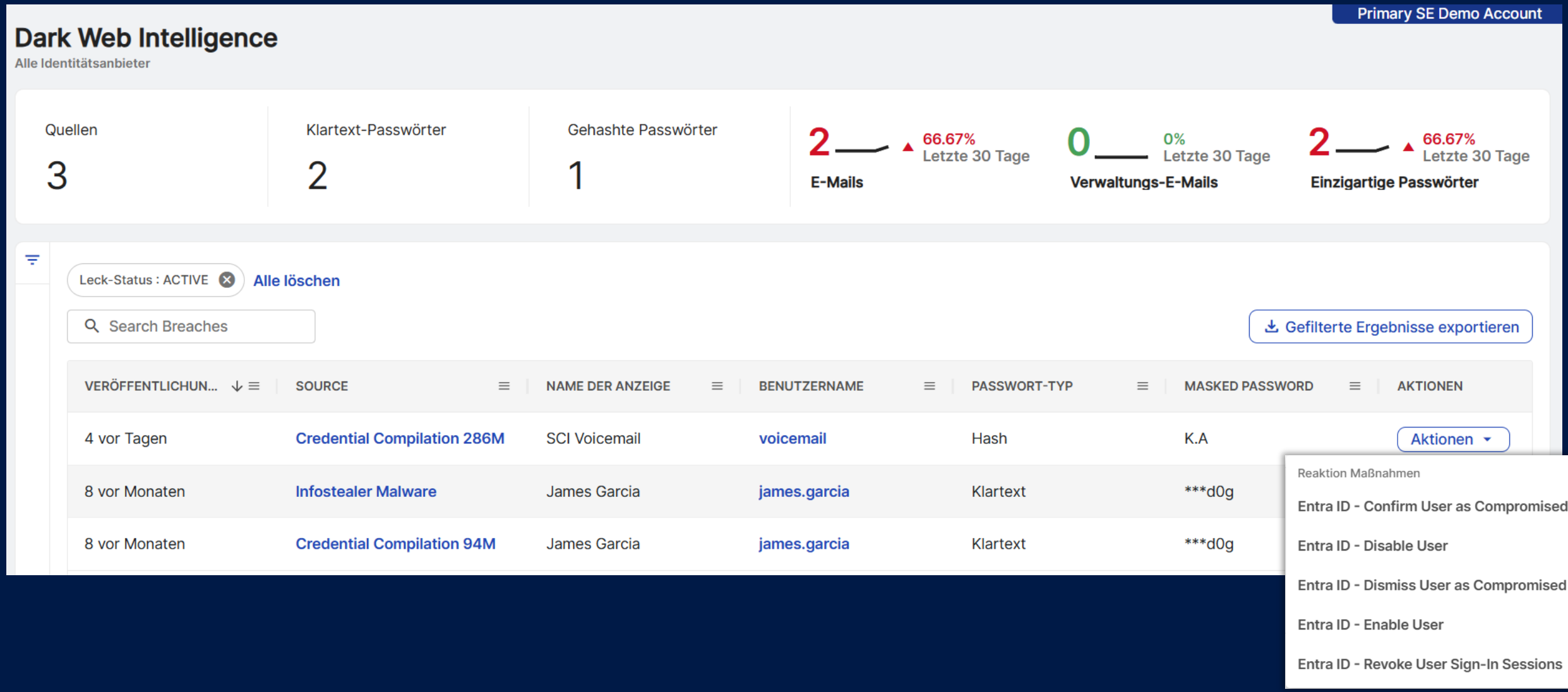
Benachrichtigung, wenn Zugangsdaten im Darknet auftauchen

### Identifiziert riskantes Nutzerverhalten

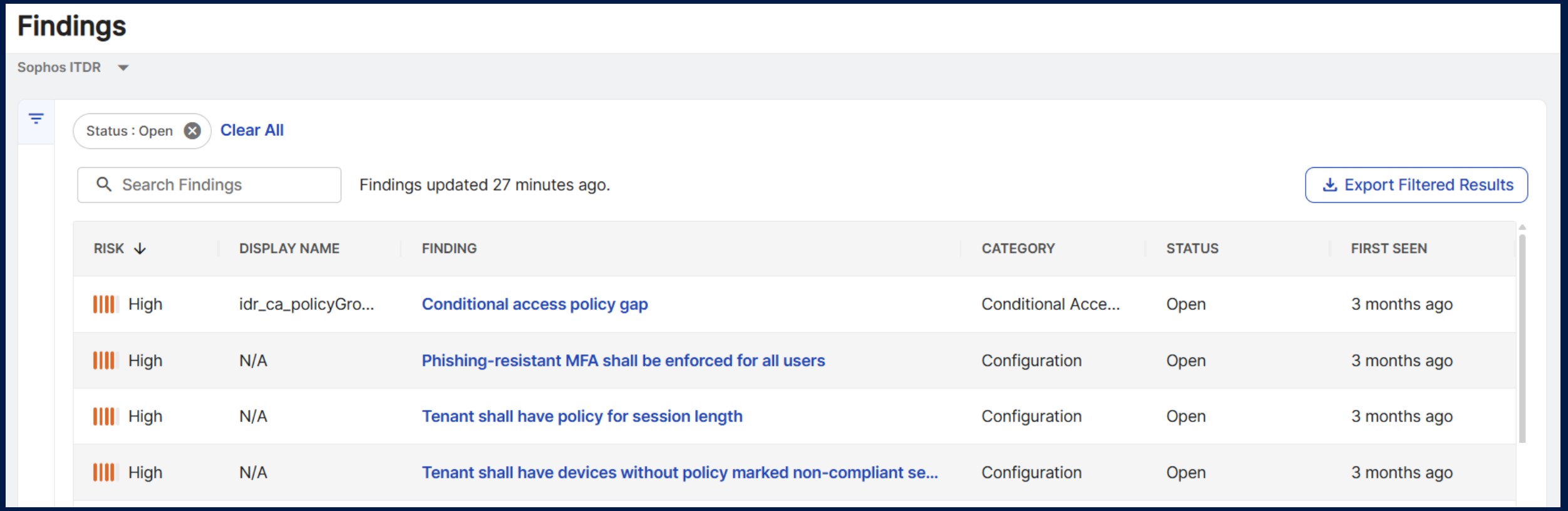
Monitoring und Alarmierung bei ungewöhnlichen Benutzeraktivtäten

**Sophos ITDR Add-on zu Sophos XDR und Sophos MDR**

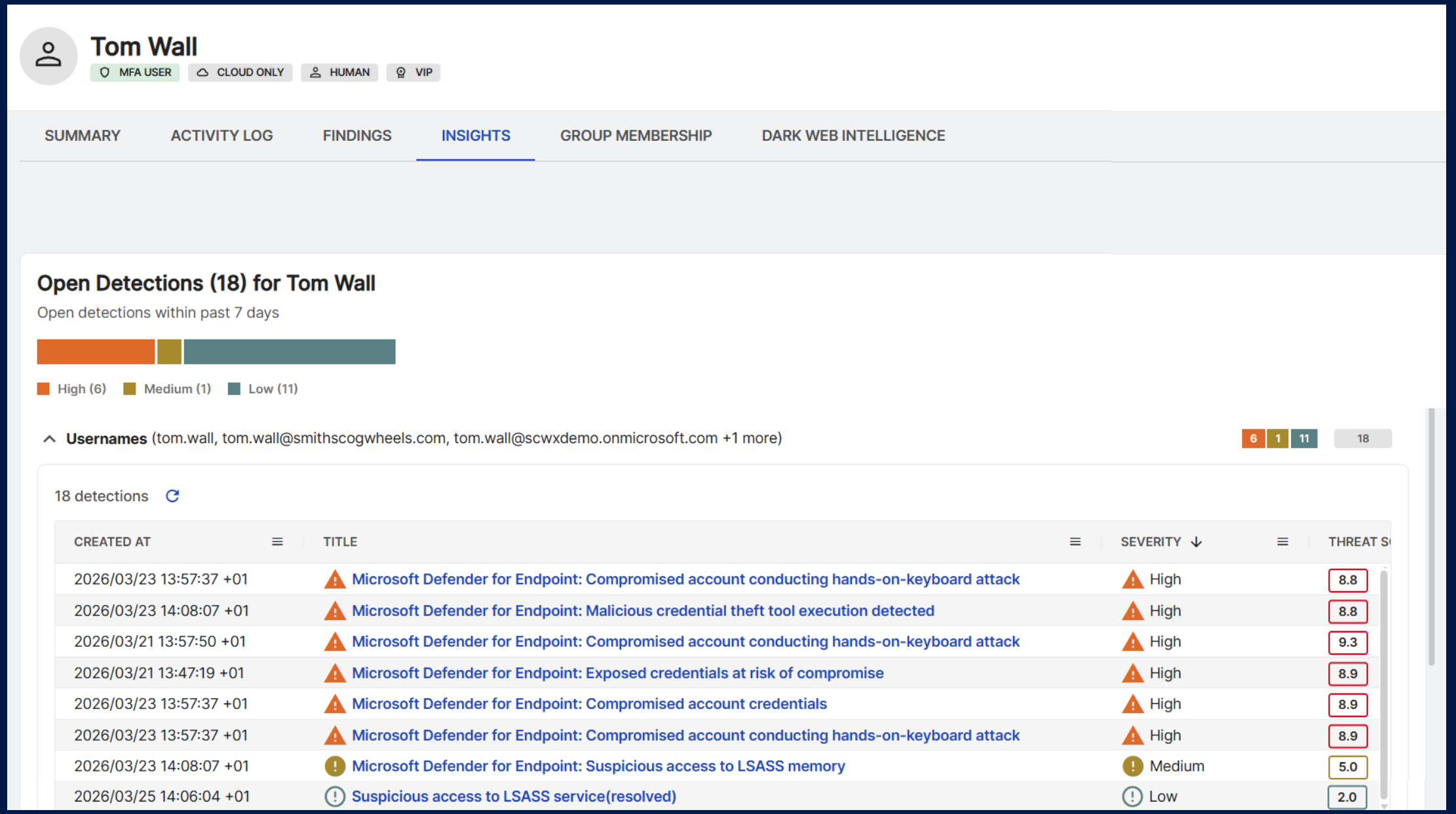
# ITDR – Zugangsdaten in Password-Leaks



# ITDR – Unsichere Identity-Konfiguration



# ITDR – Verdächtiges Benutzerverhalten + Reaktion



# Ein SOC wird benötigt

- In keinem M365 Plan ist Dienstleistung beinhaltet
- Reine Schutztechnologien reichen nicht mehr
- Angriffe starten zu 90% außerhalb der Geschäftszeiten
- Ein SOC Team wird 24/7 benötigt
  - Kunden SOC
  - Partner SOC
  - Sophos MDR

# Sophos MDR Essentials = Sophos MDR for Microsoft Defender

Korrelation von Microsoft Telemetrie mit Daten anderer Security-Lösungen

Integration in Sophos XDR/MDR ohne Zusatzkosten

Microsoft Certified Security Operations Analysts

Sophos Erkennungen für jeden M365 Business Plan

MS Defender muss nicht ersetzt werden

Reaktionsmöglichkeiten für Analysten in Microsoft 365

# 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**

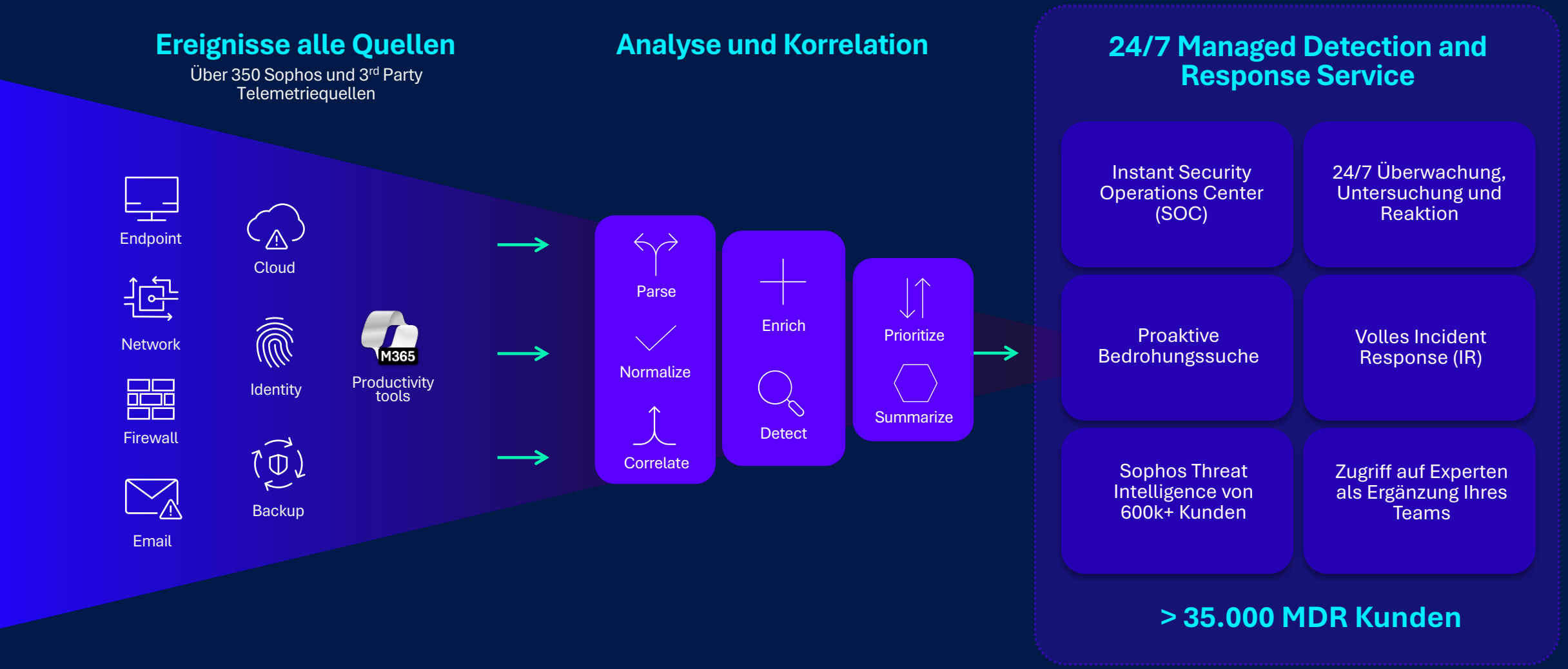
## Microsoft Sicherheitswerkzeuge

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

# Sophos XDR+MDR nutzt alle Telemetrie im Unternehmen



# Nächste Schritte

**Microsoft API Anbindungen aktivieren**

- Graph Security API V2
- Management Activity API
- M365 Response Actions

**MDR Best Practices für Microsoft**

- Windows Server Security
- Windows Event Logging
- M365 und Entra ID

**ITDR zum proaktiven Identity-Schutz**

- Erkennung von geleakten Zugangsdaten
- Erkennung von Fehlkonfigurationen im EntraID
- Erkennung von Angreiferverhalten


SOPHOS
PARTNER 2026
EXPERIENCE

SOPHOS

# Die neue Sophos SecOps Plattform:

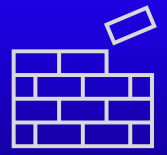
## XDR, MDR & Next Gen SIEM vereint

# Sophos Active Adversary Report 2026

Erkenntnis

## Mangel an Telemetriedaten erschwert die Arbeit der Verteidiger

**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.

# Woher kommen die Daten?

## Sophos XDR

### Sophos Ecosystem

- Sophos Endpoint
- Sophos Firewall
- Sophos ITDR
- Sophos Email
- Sophos NDR

### Integrations (60+)

- 3rd Party Endpoint
- + XDR Sensor
- 3rd Party Backup
- 3rd Party Identity
- 3rd Party Email
- 3rd Party Firewall
- 3rd Party Productivity
- 3rd Party Network
- 3rd Party Cloud

Events

## Sophos XDR powered by Secureworks

### Sophos Ecosystem

- Sophos Endpoint
- Sophos Firewall
- Sophos ITDR
- Sophos Email
- Sophos NDR

### Integrations (350+)


Custom Integration

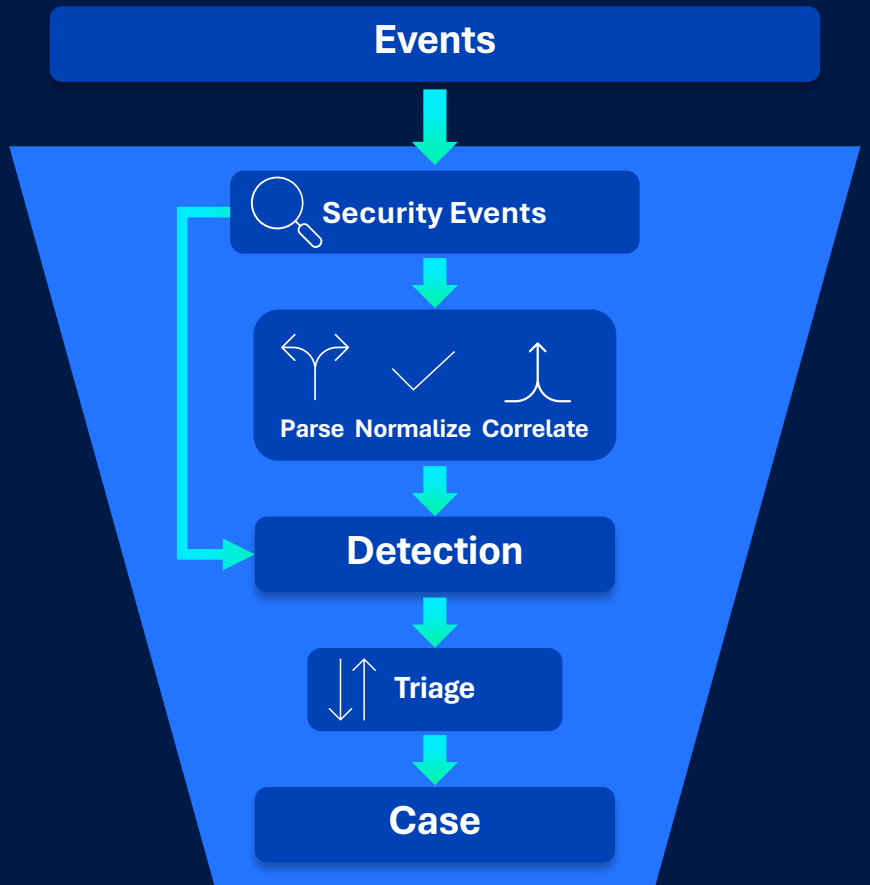
Events

Any

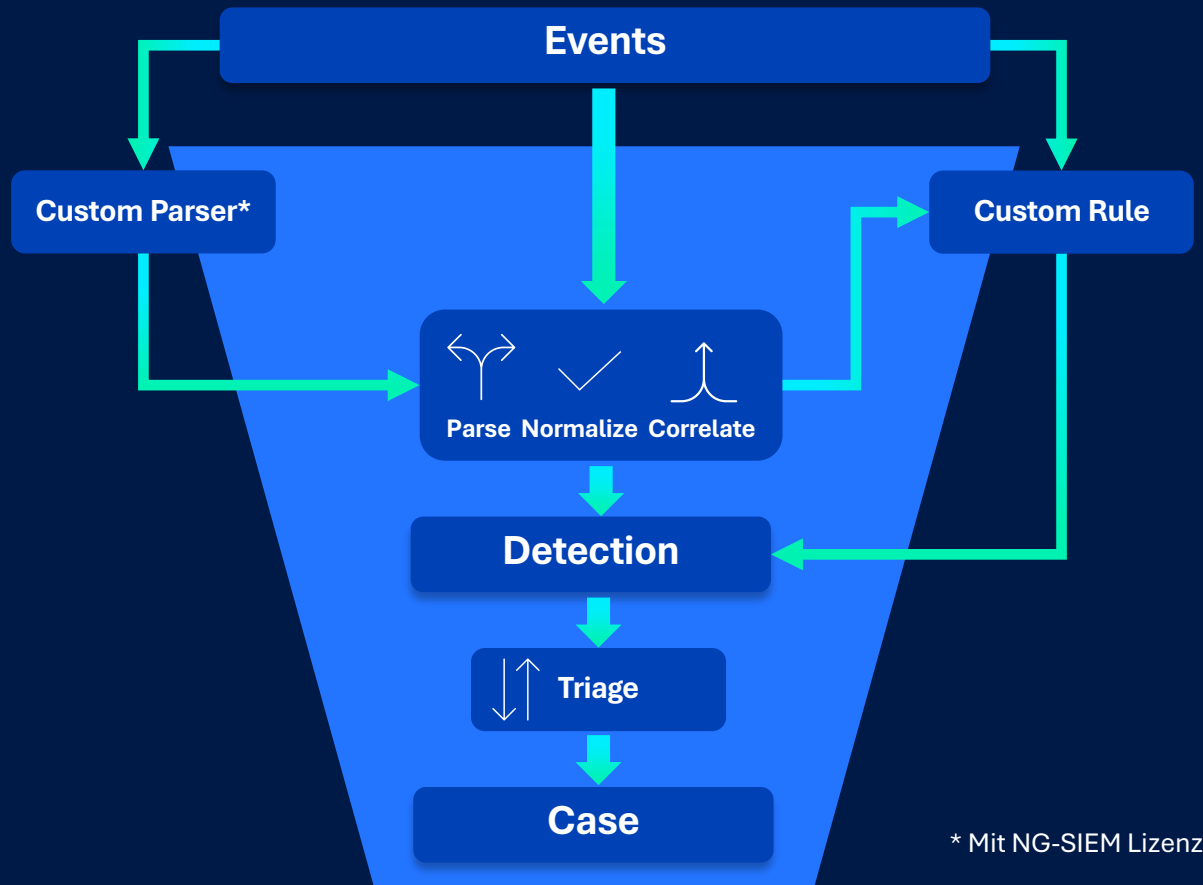
- NG-SIEM License
- Custom Parser

# Verarbeitung von Events

## Sophos XDR

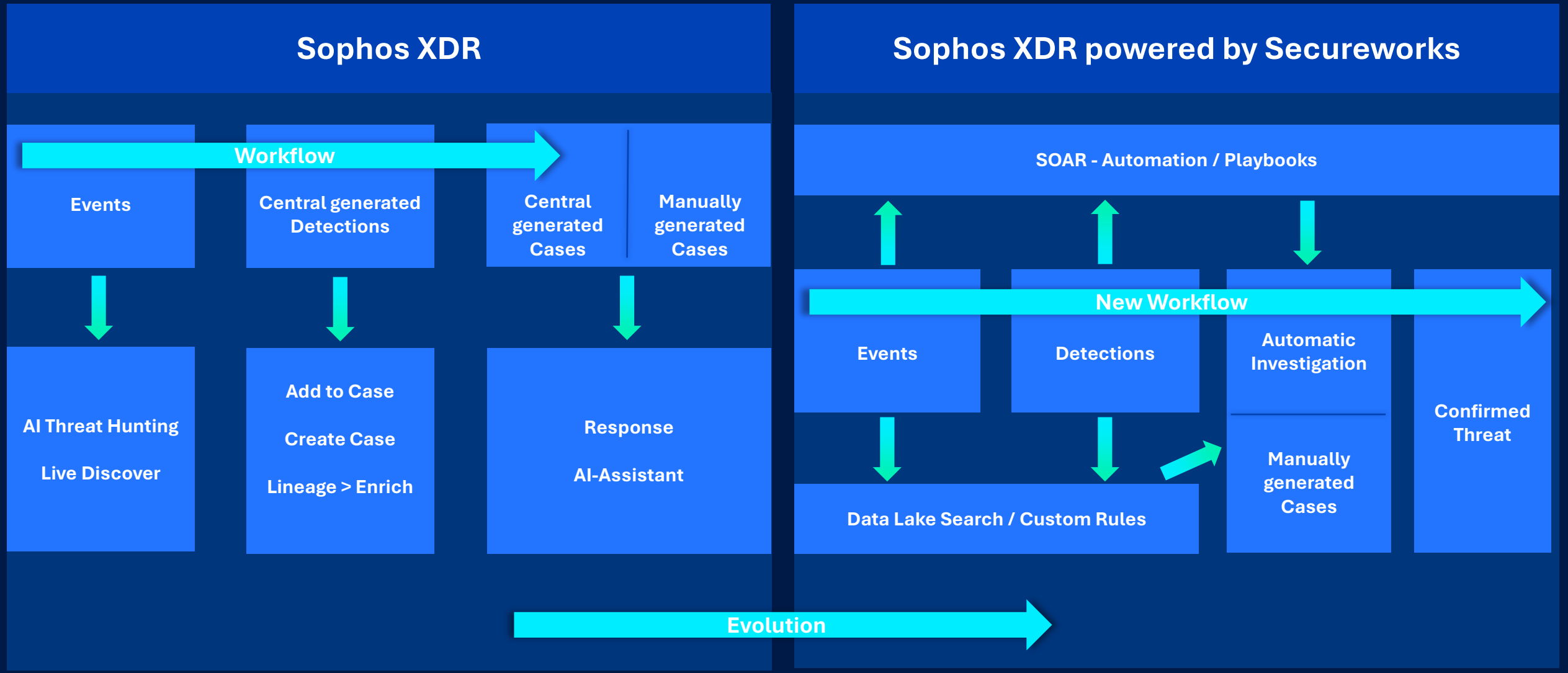



## Sophos XDR powered by Secureworks




* Mit NG-SIEM Lizenz

# Analysten Workflow



Security Operations

DETECT
Dashboard
Cases
Detections
Rules

INVESTIGATE
Data Lake Search

CONFIGURE
Automations
Threat Analysis Center Classic

See a snapshot of your security protection

# XDR Overview

**Event pipeline** Last 30 days

| 753k | 278 | 6 | 0 |
|---|---|---|---|
| Total Events | Total detections | Total cases | Confirmed security threats |
| ▼ -23.95% | ▼ -24.25% | ▲ 50% | 0% |
| | 43 Critical, 40 High | | |

**Total cases** Last 30 days Include closed cases

| 0 | 5 | 1 |
|---|---|---|
| Critical | High | Medium |

| PRIORITY | Date Created | TYPE | Case # | NAM | | | DETECTIONS |
|---|---|---|---|---|---|---|---|
| Medium | 2026/04/28 04:31:05 +... | Security Investigation | INV00049 | Adn | | | 9 |
| High | 2026/04/27 14:47:33 +... | Security Investigation | INV00048 | 202 | | 0-4c65-... | 8 |
| High | 2026/04/21 19:01:37 +02 | Security Investigation | INV00045 | 202 | | | 40 |
| High | 2026/04/15 17:23:38 +02 | Security Investigation | INV00044 | 202 | | | 48 |
| High | 2026/04/15 03:43:37 +... | Security Investigation | INV00043 | 202 | | 0-4c65-... | 1 |
| High | 2026/04/02 17:53:47 +... | Security Investigation | INV00042 | RK Test Case | Open | Randy Kersey | 1 |

| | |
|---|---|
| Status: | Suspended |
| Assignee: | Open |
| Priority: | Active |
| Type: | Awaiting Action |
| Close Reason: | Closed: Confirmed Security Incident |
| ID: | Closed: Authorized Activity |
| Created By: | Closed: Threat Mitigated |
| Created: | Closed: Not Vulnerable |
| Updated By: | Closed: False Positive Alert |
| Updated: | Closed: Inconclusive |
| Archived: | Closed: Informational |

# XDR in der Praxis

## Server in der Produktion

*Für die meisten Organisation die wichtigsten Systeme im gesamten Unternehmen*

- Events auf diesen Systemen werden als kritisch gemeldet
- Eingehende Kommunikation auf Port XY werden als kritisch gemeldet (z.B. RDP)
- Detektionen für individuelle Applikationen*

## Notebooks der Geschäftsführung

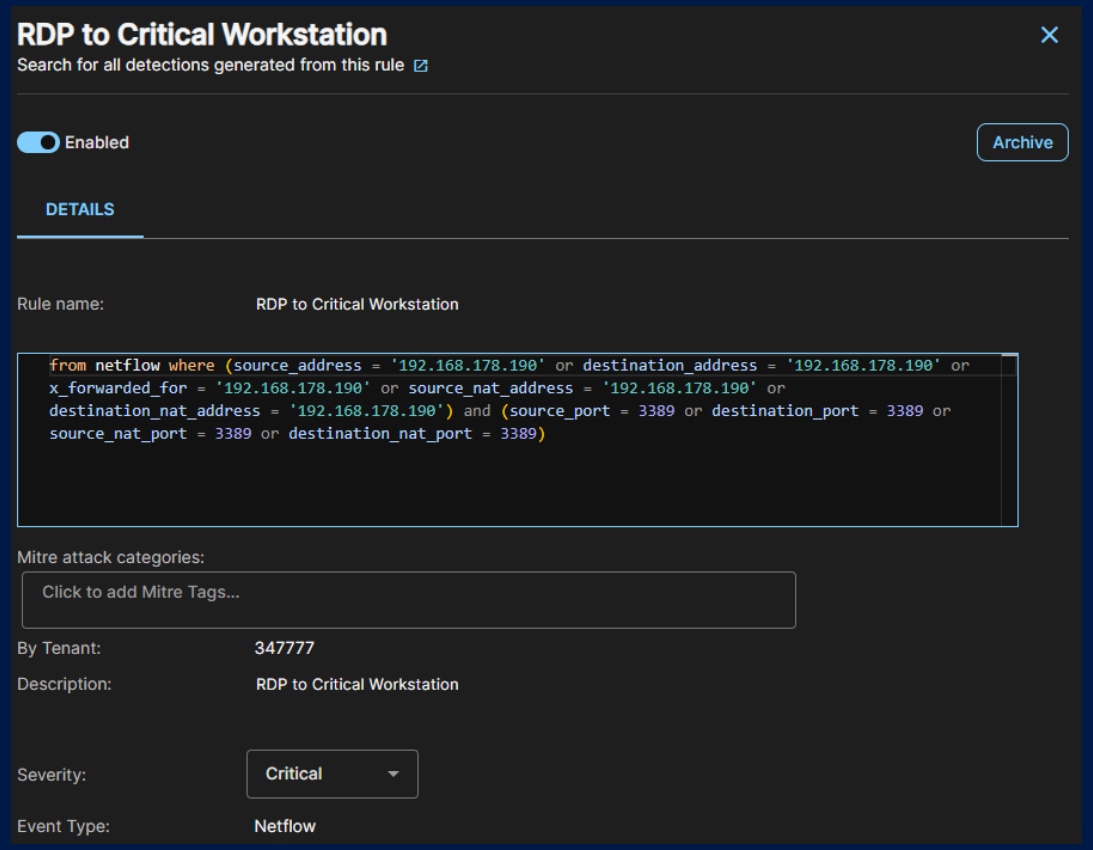
*Für Cyberkriminelle sind Geschäftsführung und Prokuristen attraktive Ziele*

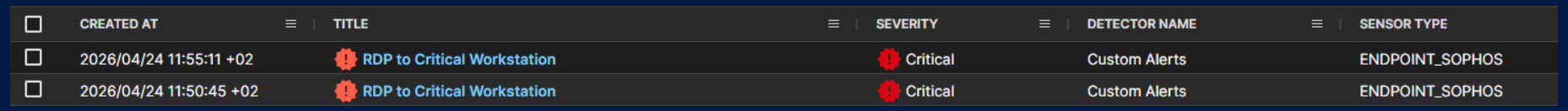
- Alle Events der Email Security Lösung für VIP-Benutzer werden als kritisch gemeldet
- PowerShell mit Bypass oder Encoding werden als kritisch gemeldet
- Protokollierung der Anmeldeversuche mit Benutzerkonto eines Mitglieds der Geschäftsführung

* Benötigt Custom Parser

# Custom Rules

- Frei definierbare Regeln auf Basis normalisierter Ereignisdaten
- Individuell anpassbare und maßgeschneiderte Erkennungen.
- Ermöglichen es, eigenes Business-Wissen in die Erkennungslogik einfließen zu lassen
- Dienen nicht der Repriorisierung bestehender Meldungen, sondern ergänzen diese.

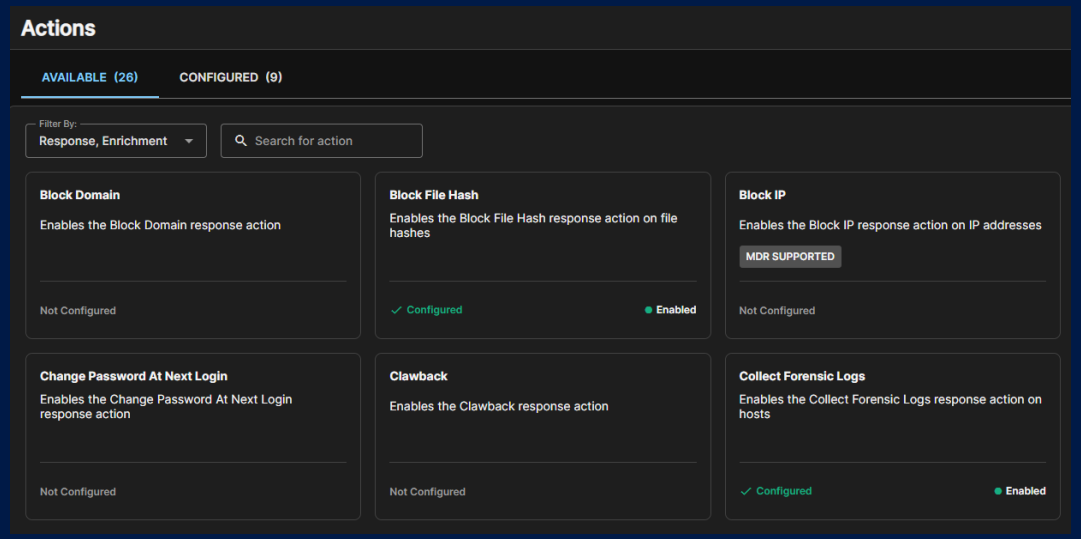



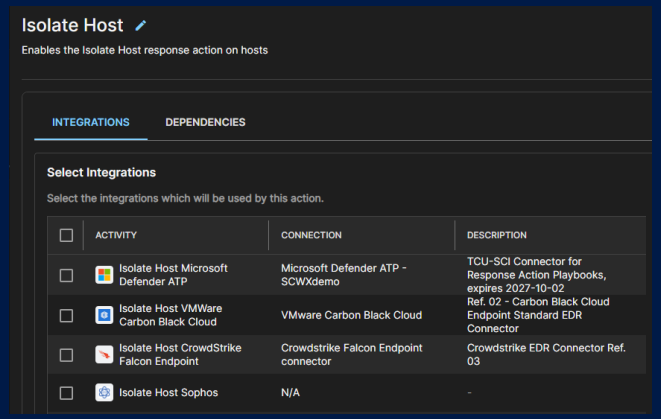
# SOAR

- Security Orchestration, Automation and Response
- Orchestrierung und Automatisierung sicherheitsrelevanter Abläufe
- Schnellere und konsistente Incident Response
- Automatisierte Eindämmung von Bedrohungen
- Bereitstellung von Actions und Playbooks
- Unterstützung von Drittanbieterlösungen

# Automatisierung

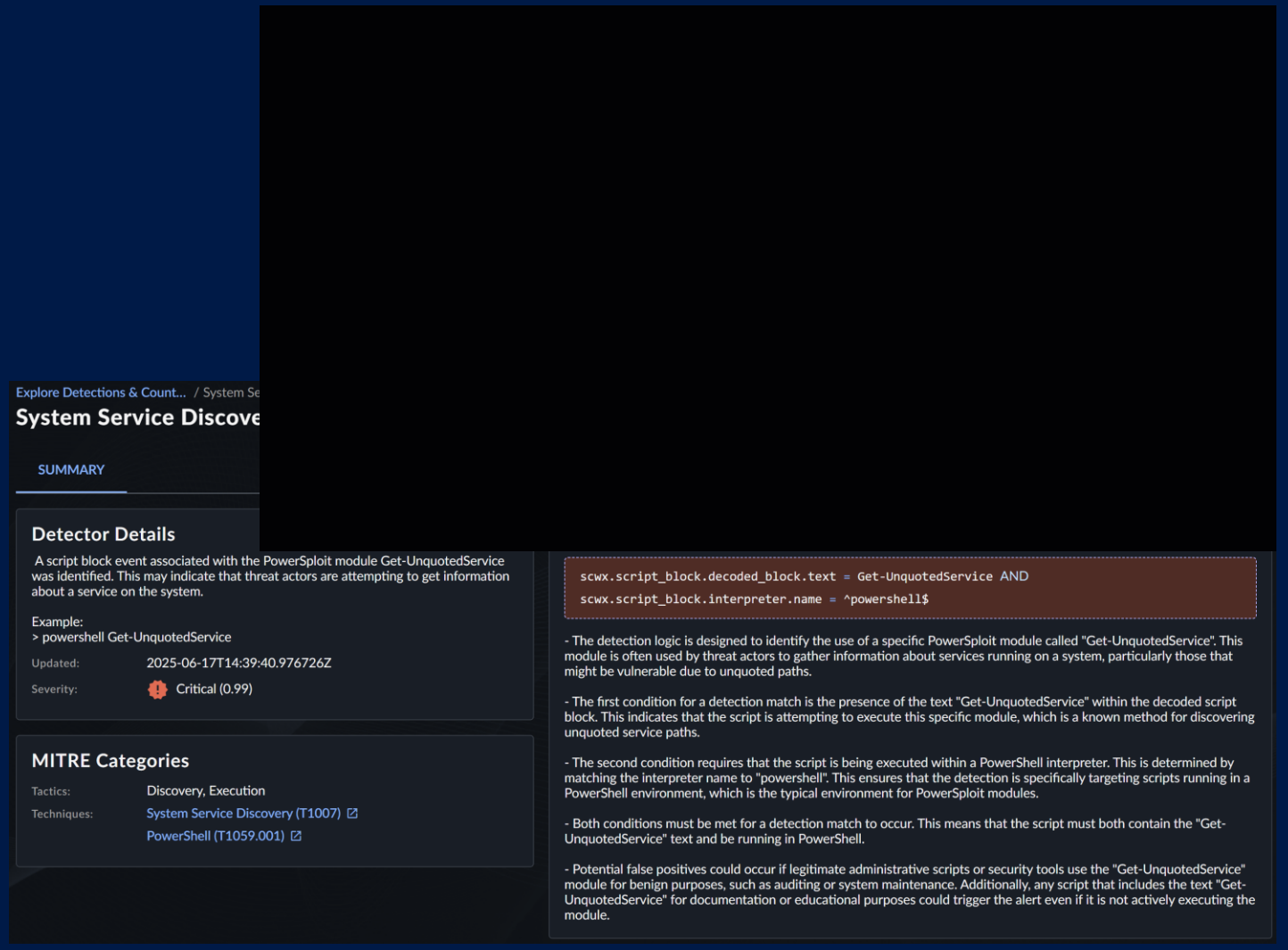
- Actions
  - Technologie unabhängige Response Actions
  - nahtlos in den Triage- und Case-Workflow eingebettet
  - z.B. Isolate Host Endpunkttechnologie unabhängig
- Playbooks
  - Automatisierte Interaktionen mit der XDR-Plattform und externen Systemen (via API)
  - Ermöglicht:
    - Datenanreicherung von Cases
    - Response Actions auf externen Systemen
    - Vollautomatisierte Prozesse
    - Einbettung in externe Workflows via Ticketingsysteme
    - Erweiterte Reaktionsketten über mehrere Systeme
    - Anbindung an externe KI-Modelle (Public / Private)



# Detector Explorer

- Ermöglicht es die Liste der Detektoren und Gegenmaßnahmen zu durchsuchen
- Bietet Details zu Erkennungslogik sowie zugehörigen MITRE-Taktiken und -Techniken.



# Löst Sophos endlich das SIEM Thema

- Audit
- langfristige Datenaufbewahrung.
- proprietäre Datenquellen
- erweiterte Funktionen

# XDR & Next Generation SIEM

**XDR konzentriert sich zu 100 % auf Threat Detection & Response.**
**Mit NG-SIEM sind auch Compliance-Anforderungen abgedeckt.**

## XDR

- Bedrohungsprävention
- Anreicherung von Alarmen
- Native Endpoint Visibilität
- Native Response
- Native Integrationen
- Anpassungen
- Threat Detection, Investigation & Response
- Verwaltung und Aufbewahrung von Sicherheitsprotokollen
- Erweiterte Abfragemöglichkeiten
- SOAR

## NG-SIEM

- Compliance
- Richtlinienüberwachung
- Beliebige Telemetrie
- Protokollverwaltung
- Protokollaufbewahrung

SOPHOS

# Ausblick – Next Generation SIEM

- **Einbindung beliebiger Daten**
  - aus Logdaten, die nicht durch bestehende native Integrationen abgedeckt sind
  - Legacy Lösungen, IoT, etc.
  - Customer Rules können auf beliebigen Daten erstellt werden
- **Custom Parser**
  - Generische Events können strukturiert und in ein passendes Schema (z. B. Auth, Filemod, Netflow, HTTP) transformiert werden
  - Alle regulären XDR-Funktionen inkl. Detection Engine sind darauf anwendbar


SOPHOS

## Ihr SOC + Unsere Plattform

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

## Ihr SOC + Unser SOC

MSP

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

## Unser SOC = Ihr SOC

Reseller

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

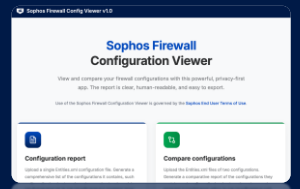

SOPHOS
PARTNER 2026
EXPERIENCE


# Sophos Firewall

**Name**
Title, Company
Date

# Sophos Firewall

## Sophos Firewall v22.0 GA

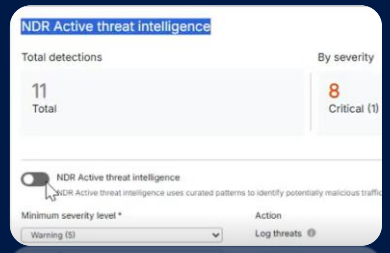

### Secure by Design

- Firewall Health Check
- XDR Linux Sensor zum Schutz der Firewall
- Neue Control Plane + Neuer Kernel
- Neue Anti-Malware Engine

### Verbessertes Networking & höhere Skalierbarkeit

### Firewall Config Studio

## Sophos Firewall v22 MR1


### NDR Active Threat Intelligence

- Erkennen potenziell bösartigen Datenverkehrs & aktiver Angreifer

### NDR-E für Virtual und Cloud

- NDR Essential für virtuelle & Cloud Firewalls

### Sophos Central Audit Log Verbesserungen

# The First MDR/XDR-Optimized Firewall

with purpose-built active threat detection and response capabilities

SOC

MDR

XDR

SOPHOS X-OPS

APTs
Active C2s

3rd PARTIES

Domains
Bad IPs
IPS

NEW

SOPHOS NDR

NDR

AI Analysis
of TLS & DNS

SOPHOS DNS

DNS
Protection


SOPHOS vCISO

Threat Intel
and
Fortification

SECURE BY DESIGN

Proactively monitored by Sophos
Containerized OS
Hardened access
Over-the-Air updates

ADVANCED AI DETECTIONS

Multiple AI threat intel sources:
MDR | XDR | NDR | EDR
- Sophos or Third Party -
Direct feeds to the Firewall

ACTIVE THREAT RESPONSE

Auto response to active threats
with Synchronized Security and
Lateral Movement Protection

# Sophos Firewall V22.0 MR1


- **Secure by Design Improvements**
  - Mehr Telemetrie für bessere Sichtbarkeit
- **NDR Active Threat Intelligence**
  - Erkennen potenziell bösartigen Datenverkehrs & aktiver Angreifer
- **NDR-E for Virtual and Cloud**
  - NDR Essential verfügbar für virtuelle & Cloud Firewalls
- **Sophos Connect 2.0 für MacOS**
  - SSLVPN Support für OVPN
    - [Coming Soon] Provisioning File Support
    - [Coming Soon] Apple Sillicon Support
    - [Coming Soon] Entra ID Support
- **Entra ID Conditional Access Support for Sophos Connect VPN**

SOPHOS

# NDR Active Threat Intelligence

## v20

**Sophos X-OPs**

SophosLabs Threat Intel Datenbank mit >1 Mio. Bedrohungen

**Sophos MDR/XDR**

Von Analysten identifizierte Bedrohungen & IOCs

## v21

**Third-Party**

Unabhängige Threat Intelligence Quellen von Drittanbietern

## v21.5

**Sophos NDR Essentials**

Sophos NDR KI-Modelle analysieren Domains & TLS-Traffic auf Bedrohungen

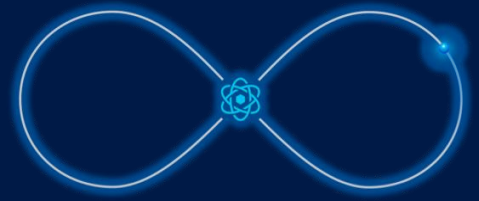
## v22.1

NEW

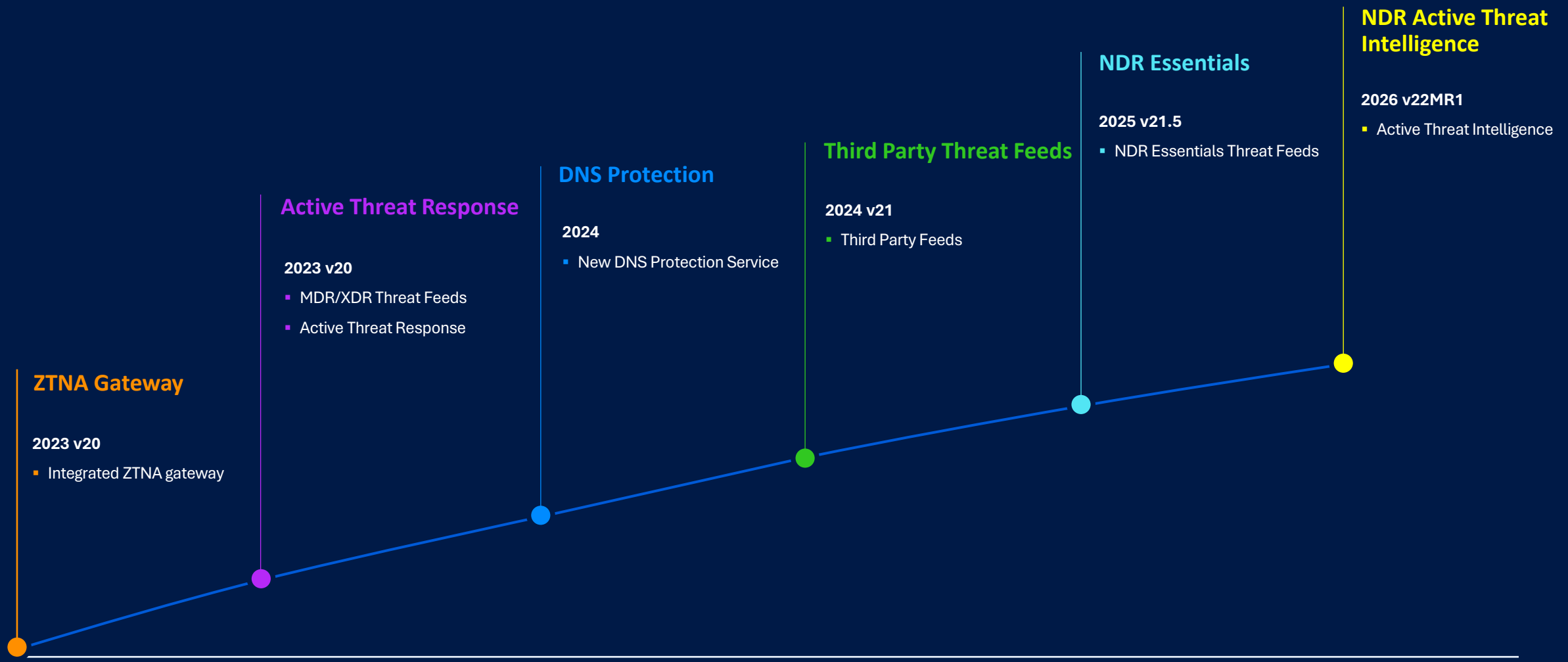
**NDR Active Threat Intelligence**

Optimierte iSensor-Muster für die Erkennung von bösartigem Traffic & aktiven Angreifern

Active Threat Response
erweitert Synchronized Security



# Steigende Wertstellung von Xstream Protection



# NDR Active Threat Intelligence Beispiel Erkennungen

## Living-off-the-Land-Angriff

Ein vertrauenswürdiges Tool wie Certutil wird missbraucht, um Malware heimlich herunterzuladen

Erkennt den Download einer ausführbaren Datei

## Kompromittiertes Gerät

Ein infizierter Rechner startet SSH-Scanning wie beim NoaBot-Botnet

Erkennt eine SSH-Verbindung, die auf ein kompromittierten Host hinweist

## Malware „callhome“

Verdächtiger HTTP-Traffic über den DNS-Standardport

Erkennt eine GET-Anfrage an ein Remote-System mit einem Webserver, der auf dem DNS-Standardport lauscht

## Heimliche Daten-Exfiltration

Tools wie “Finger” leaken Daten unauffällig oder tarnen Malware als Bilder

Erkennt Datenabfluss von Windows-Hosts über das Finger-Tool – Hinweis auf einen kompromittierten Host in der Kundenumgebung

# Control center

XGS118 (SFOS 22.0.1 MR-1-Build478) X115027KGYMMV96

Search

MONITOR & ANALYZE
- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics
- Firewall health check

PROTECT
- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Active threat response

CONFIGURE
- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication
- System services

SYSTEM
- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

## System

Performance | Services | Interfaces | VPN

| | |
|---|---|
| 0/0 RED | 0/0 Wireless APs |
| 0 Connected remote users | 0 Live users |
| 18% CPU | 51% Memory |
| 460KB/s Bandwidth | 68 Sessions |
| 0% Decryption capacity | 0 Decrypt sessions |

High availability: Not configured

Managed by Sophos Central

Zero Trust Network Access: Not configured Free eval

DNS Protection: Not configured

Running for 17 day(s), 19 hour(s), 5 minute(s)

## Firewall health check

Total 31

19 61% Compliant | 12 Noncompliant

Noncompliant policies by policy severity: 6/17 High | 5/11 Medium | 1/3 Low

## Traffic insight

Web activity (1 max | 1 avg)

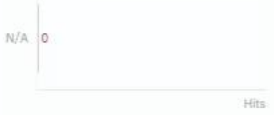

Cloud applications


Allowed app categories


Network attacks


Allowed web categories


Blocked app categories




## User & device insights

Security Heartbeat®

| 0 At risk | 0 Missing | 0 Warnings | 0 Connected |
|---|---|---|---|

Synchronized Application Control™

| 22 New | 2 Categorized | 368 Total |
|---|---|---|

Zero-day protection

| 0 Recent | 6 Incidents | 8 Scanned |
|---|---|---|

UTQ

0 Accounts at risk

SSL/TLS connections

| 78% Of traffic | 0% Decrypted | 0 Failed |
|---|---|---|

## Active threat response

MDR threat feeds — Status: On; Blocked/Monitored: 0

NDR Essentials — Status: On; Monitored: 0

Sophos X-Ops — Status: On; Blocked/Monitored: 0

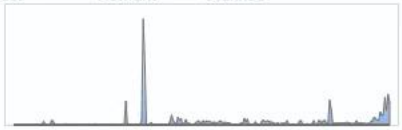
Third-party threat feeds

| Threat feeds | Sync status | Blocked/Monitored |
|---|---|---|
| AbuseURlhaus | Success | 0 |
| RecentURLHaus | Success | 0 |
| ipthreat | Success | 0 |

Click on widgets to open details

## Active firewall rules

| 0 WAF | 1 User | 5 Network | 6 Scanned |
|---|---|---|---|



| 3 Unused | 3 Disabled | 0 Changed | 0 New |
|---|---|---|---|

## Reports

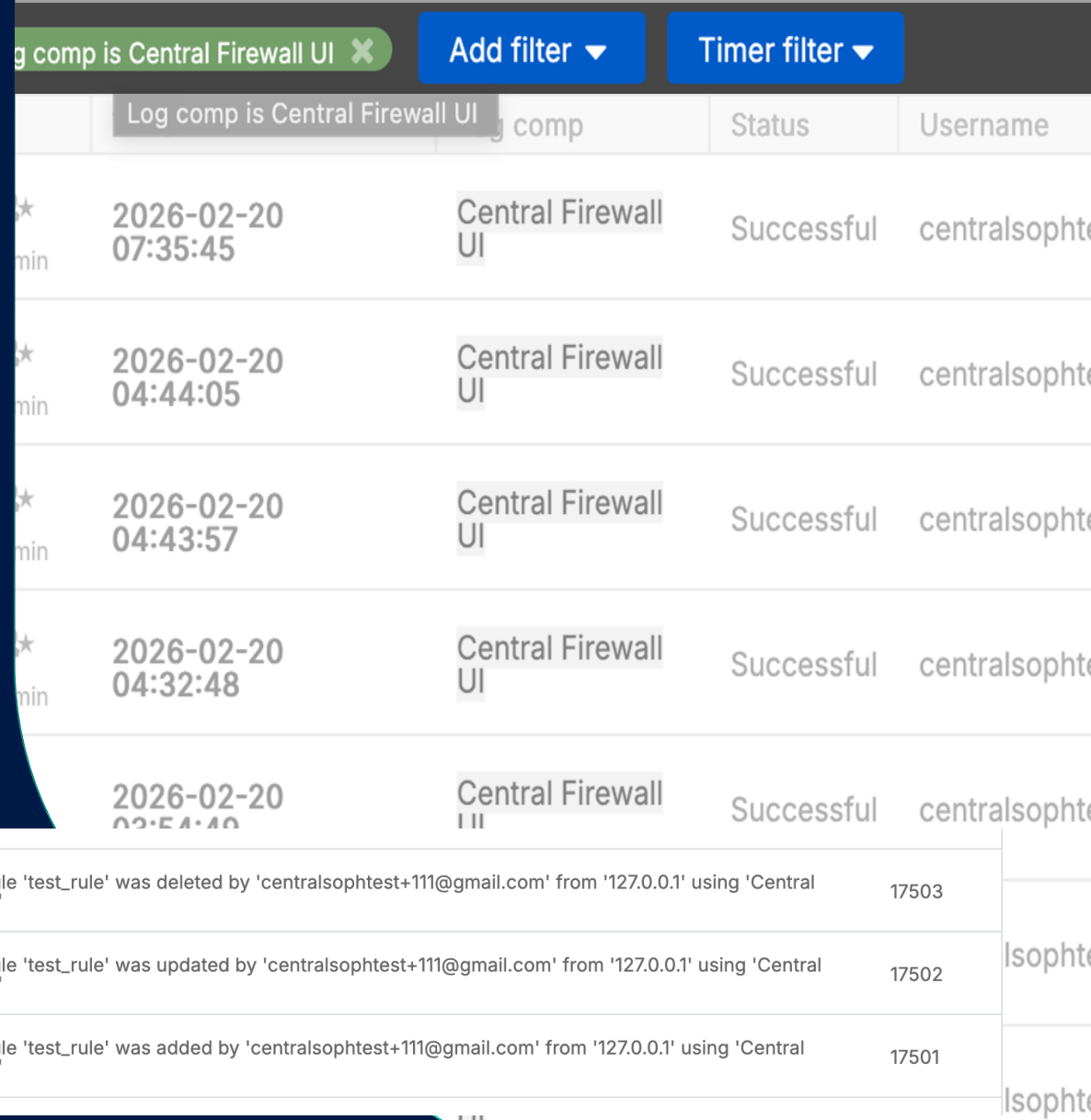
- 11 Yesterday — Risky apps seen
- 0 Yesterday — Objectionable websites seen
- 0 bytes Yesterday — Used by top 10 web users
- 0 Yesterday — Intrusion attacks

## Messages

Alert — 5m ago
The Let's Encrypt terms of service have changed. To accept the new terms of service, go ...

# Central SSO Verbesserungen

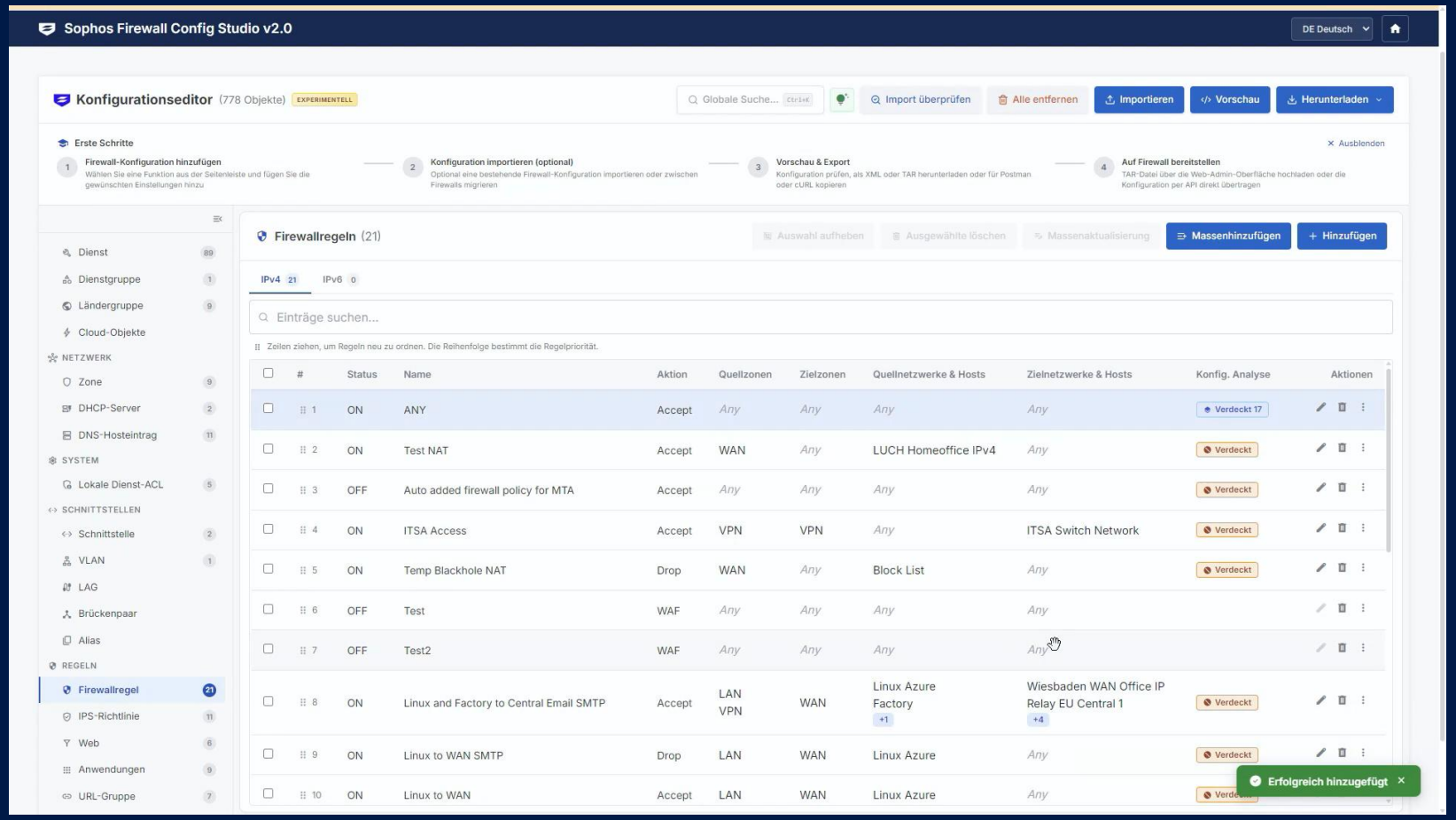
- Compliance Verbesserungen
- Ersetzt “admin_central_sa” mit Central Benutzername
- Sichtbar in:
  - SFOS Logviewer
  - Central Firewall Reporting
- Partner Dashboard Support




| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Admin | 2026-02-20 03:54:49 | Central Firewall UI | Successful | centralsophtest+111@gmail.com | 127.0.0.1 | Firewall Rule 'test_rule' was deleted by 'centralsophtest+111@gmail.com' from '127.0.0.1' using 'Central Firewall UI' | 17503 |
| Admin | 2026-02-20 03:54:11 | Central Firewall UI | Successful | centralsophtest+111@gmail.com | 127.0.0.1 | Firewall Rule 'test_rule' was updated by 'centralsophtest+111@gmail.com' from '127.0.0.1' using 'Central Firewall UI' | 17502 |
| Admin | 2026-02-20 03:53:19 | Central Firewall UI | Successful | centralsophtest+111@gmail.com | 127.0.0.1 | Firewall Rule 'test_rule' was added by 'centralsophtest+111@gmail.com' from '127.0.0.1' using 'Central Firewall UI' | 17501 |

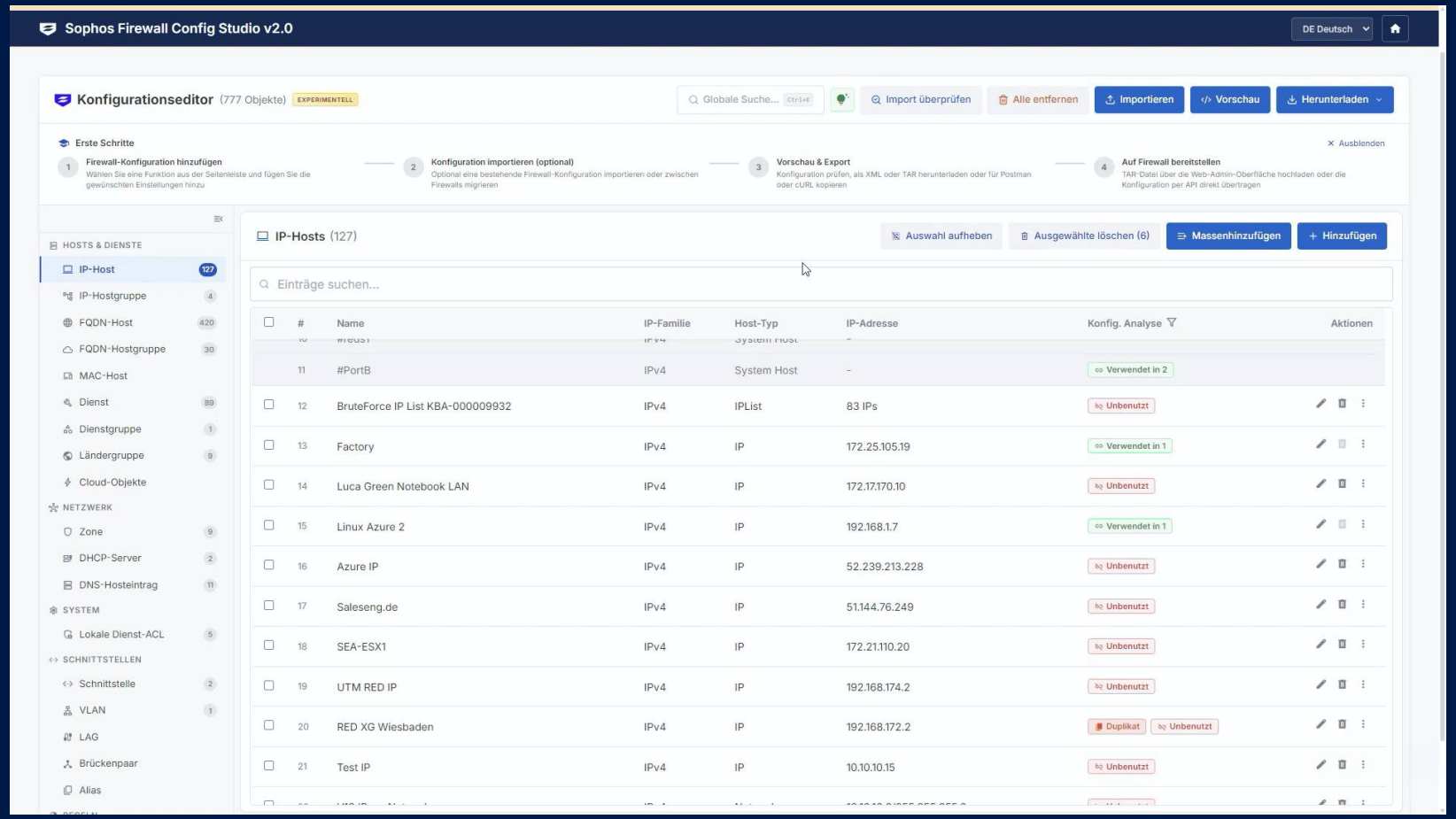
# Firewall Config Studio

- Human-Readable Config Report
- Revisionen vergleichen und Dokumentation anlegen
- Neue Objekte erstellen
- Mass Changes (z.B. Alle Firewall Regeln gleichzeitig anpassen)
- Firewall Rule Shadowing – Duplicated Objects
- CSV und JSON Import (z.B. M365 Objekte)
- Partner Templates aktuell halten



# Firewall Config Studio

- Human-Readable Config Report
- Revisionen vergleichen und Dokumentation anlegen
- Neue Objekte erstellen
- Mass Changes (z.B. Alle Firewall Regeln gleichzeitig anpassen)
- Firewall Rule Shadowing – Duplicated Objects
- CSV und JSON Import (z.B. M365 Objekte)
- Partner Templates aktuell halten



# VPN als Herausforderung

# Sophos Annual Threat Report

## Akira and Fog

In terms of actual incidents, the Akira ransomware-as-a-service led the pack in 2024, ultimately stepping in to fill the void left by LockBit. Initially seen in 2022, Akira attacks ramped up in late 2023. The group and its affiliates were steadily active throughout 2024, spiking in August when Akira accounted for 17% of the ransomware detections reported by Sophos customers—doubling from its position in the first two quarters of the year. By year's end, it still accounted for 9% of ransomware detection reports.

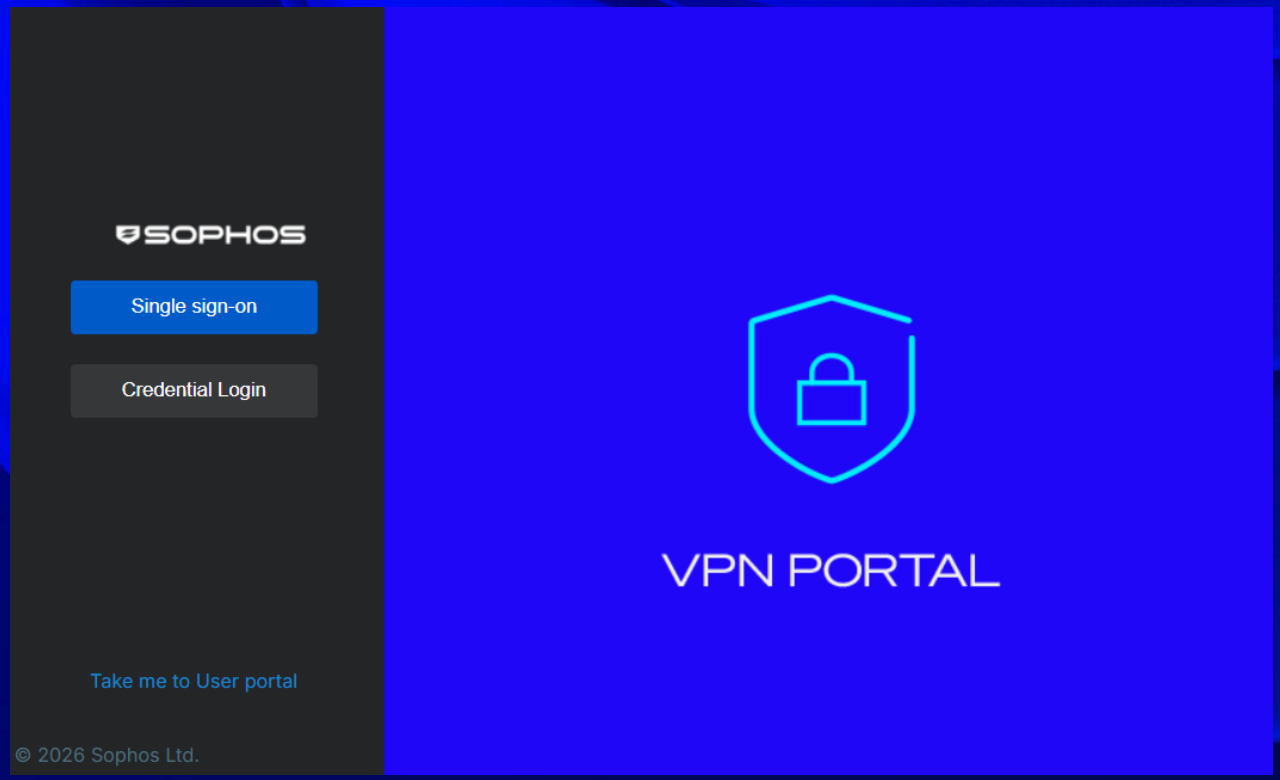
Notably, Sophos observed affiliates tied to Akira also deploying other ransomware variants, including Fog, Frag and Megazord. These attackers (such as those in STAC5881) typically focused on exploiting VPNs for initial access. Typically, Akira's targets had VPNs with no multifactor authentication, or had misconfigured VPN gateways that allowed the attackers to gain access with stolen credentials or brute force attacks.

While Akira remains active, Fog ransomware has occasionally been used as a replacement by affiliates previously connected to Akira, which accounts for its position in third among the top 15 ransomware families encountered in MDR and IR incidents.

https://www.sophos.com/en-us/blog/the-sophos-annual-threat-report-appendix-most-frequently-encountered-malware-and-abused-software

# VPN Herausforderungen

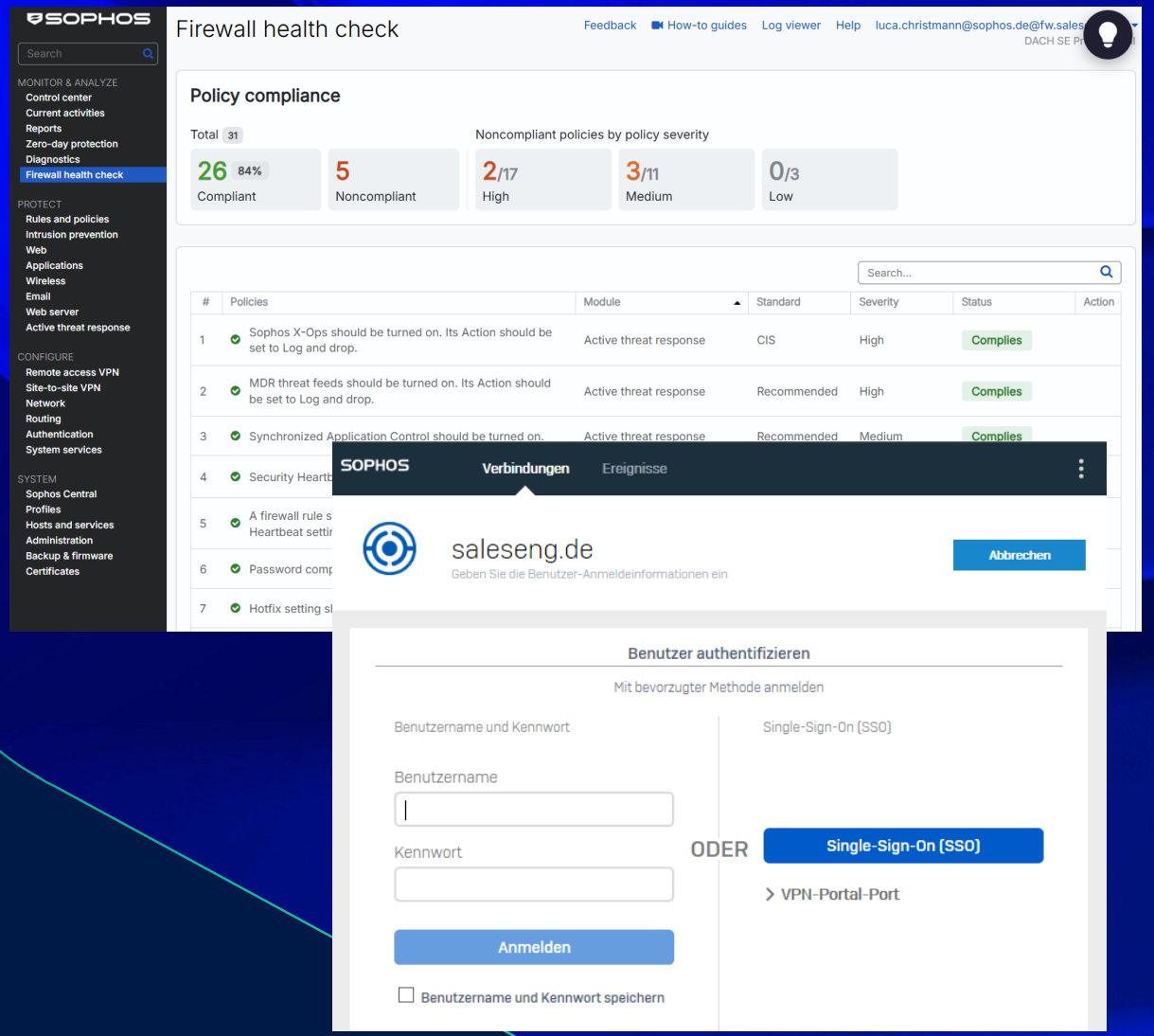
- Credentials im Internet & VPN Konfiguration gestohlen (Phishing)
- Kein Multifaktor für VPN & Brute Force gegen VPN / AD
- VPN Software auf unsicheren Geräten
- Schwachstellen / CVEs/ Bugs in der VPN Software oder Gateway




| | Time | Log comp | Status | Username | Src IP | Auth client | Auth mechanism | Message |
|---|---|---|---|---|---|---|---|---|
| Authentication | 2026-03-12 15:32:23 | VPN Portal Authentication | Failed | cfadmin | 93.152.221.42 | N/A | Local,AD,AD | User cfadmin failed to login to VPN portal through Local,AD,AD authentication mechanism because of wrong credentials |
| Authentication | 2026-03-12 15:32:18 | VPN Portal Authentication | Failed | https | 85.11.187.44 | N/A | Local,AD,AD | User https failed to login to VPN portal through Local,AD,AD authentication mechanism because of wrong credentials |
| Authentication | 2026-03-12 15:32:05 | VPN Portal Authentication | Failed | admin | 85.11.187.24 | N/A | Local,AD,AD | User admin failed to login to VPN portal through Local,AD,AD authentication mechanism because of wrong credentials |
| Authentication | 2026-03-12 15:32:02 | VPN Portal Authentication | Failed | est | 216.162.44.30 | N/A | Local,AD,AD | User est failed to login to VPN portal through Local,AD,AD authentication mechanism because of wrong credentials |
| Authentication | 2026-03-12 15:32:00 | VPN Portal Authentication | Failed | backup | 85.11.187.12 | N/A | Local,AD,AD | User backup failed to login to VPN portal through Local,AD,AD authentication mechanism because of wrong credentials |
| Authentication | 2026-03-12 15:31:56 | VPN Portal Authentication | Failed | tomls | 93.152.221.10 | N/A | Local,AD,AD | User tomls failed to login to VPN portal through Local,AD,AD authentication mechanism because of wrong credentials |

# Was kann ich tun?

- Firewall Best Practises & Hardening
  - Keine unnötigen Ports offen haben
  - Firewall Health Check 100% erreichen
- Login Security – Grundrauschen reduzieren
  - Nach fehlerhaften Login - IP sperren
- 3rd Party Feed
  - Blockieren von bekannten WAN IPs
- Sophos Endpoint & Sophos Connect
  - Synchronized Security aktivieren
- MFA (Entra ID)
  - Conditional Access
  - Multi Factor Support in Sophos Connect
- Dark Web Monitoring (ITDR)




SOPHOS
DEFEAT CYBERATTACKS