

 SOPHOS

PARTNER 2026
EXPERIENCE



Sophos Workspace Protection

(M)ein typischer Arbeitstag?

Hybrides und von unterwegs Arbeiten heißt: Ich bin online!

Kooperieren



Erstellen



Beraten

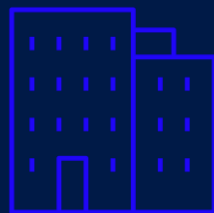


Kommunizieren



Und die meisten Tätigkeiten finden im Browser statt?

WER arbeitet von WO, auf WELCHE Art und Weise?



Sophos Workspace Protection

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

Protected Browser



ZTNA



DNS Protection



EMS



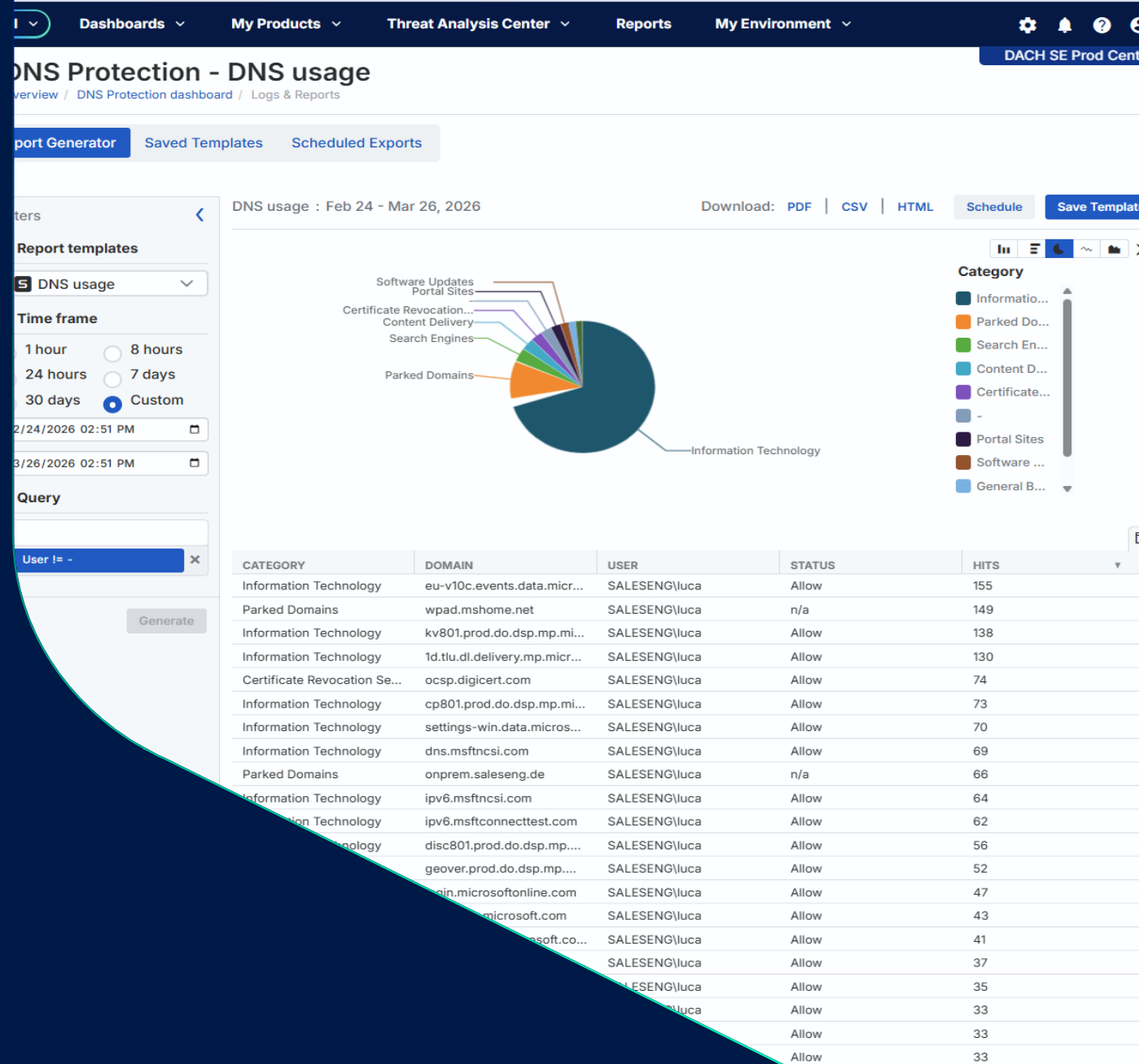
← Bereitstellen oder nur das nutzen, was gebraucht wird →

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



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

Connection method

Choose how you want to connect to DNS Protection from this location.

Secure DNS and Endpoint DNS Protection

Configuration values

Copy the values below to manually configure local devices or DNS servers. You don't need to do this to configure Endpoint DNS Protection.

DNS over HTTPS URL

<https://2xy6imnwb84v5.secure.dnsprotection.sophos.com/dns-query> 

Use **secure DNS**

Make it harder for people with access to your internet traffic to see which sites you visit. Chrome uses a secure connection to look up a site's IP address in the DNS (Domain Name System).

Select DNS provider

Netzwerk-DNS-Einstellungen bearbeiten

Manuell

IPv4 Ein

Bevorzugter DNS

DNS über HTTPS

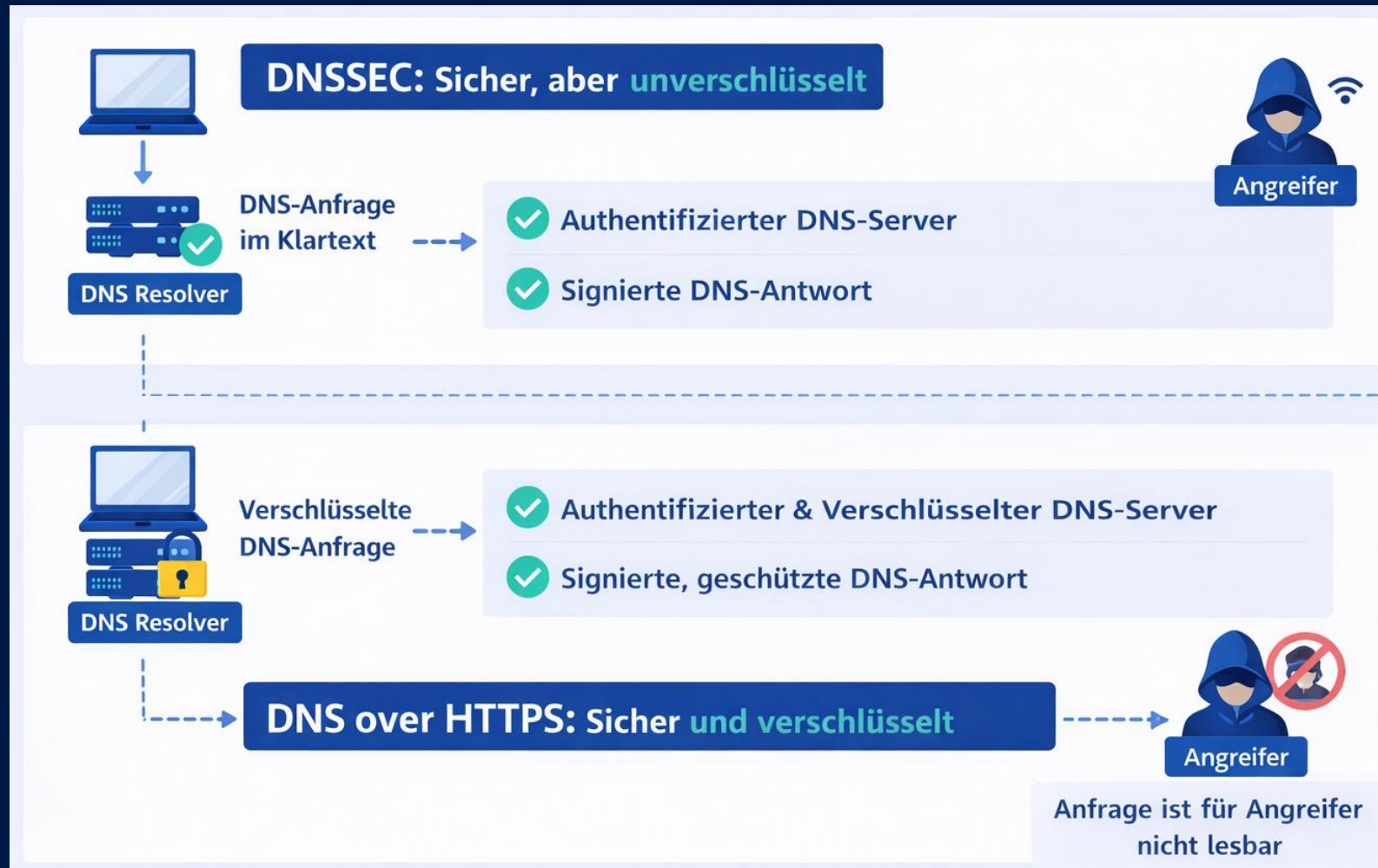
DNS über HTTPS-Vorlage

Fallback auf Klartext Aus

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.

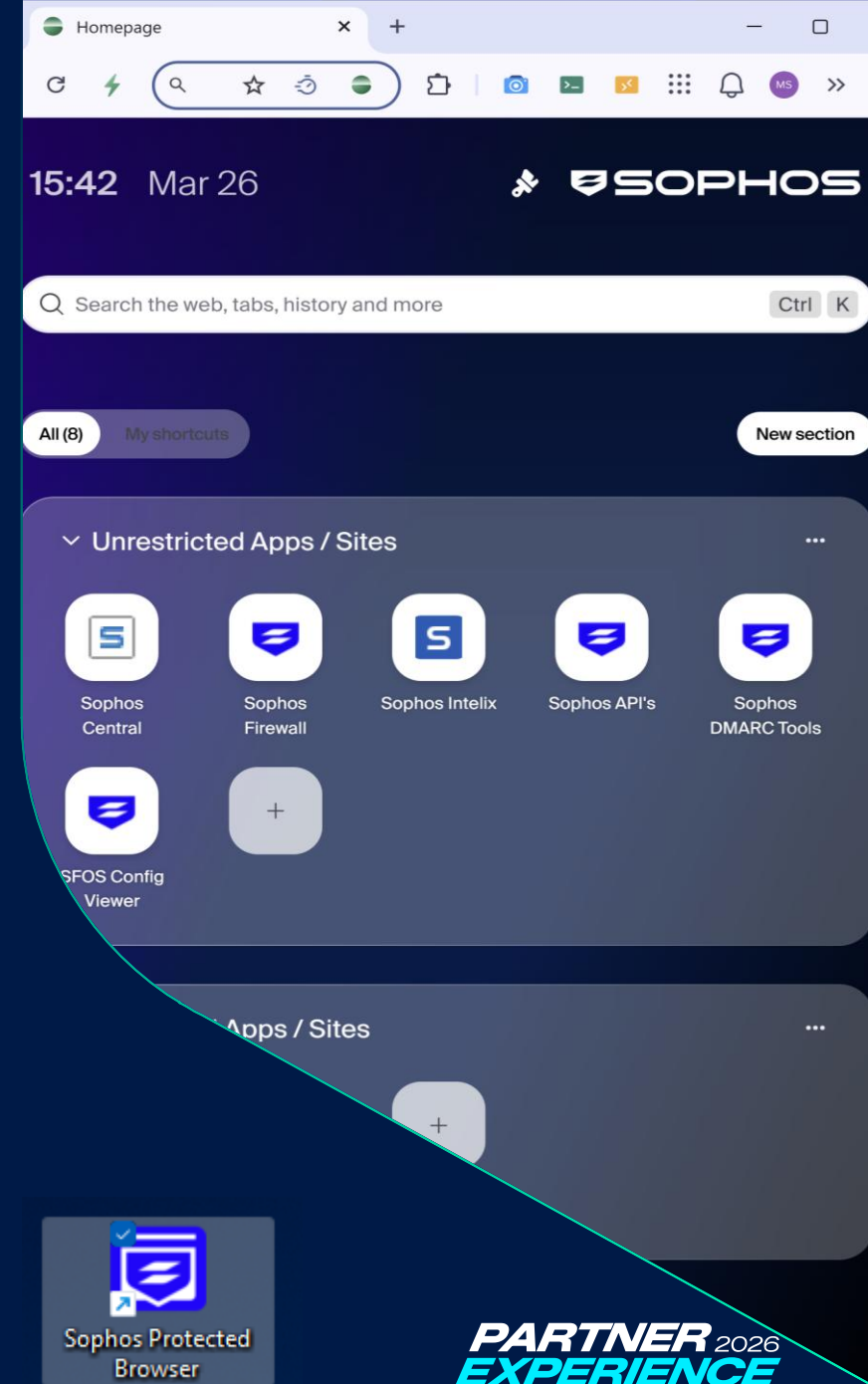
EntraID Conditional Access

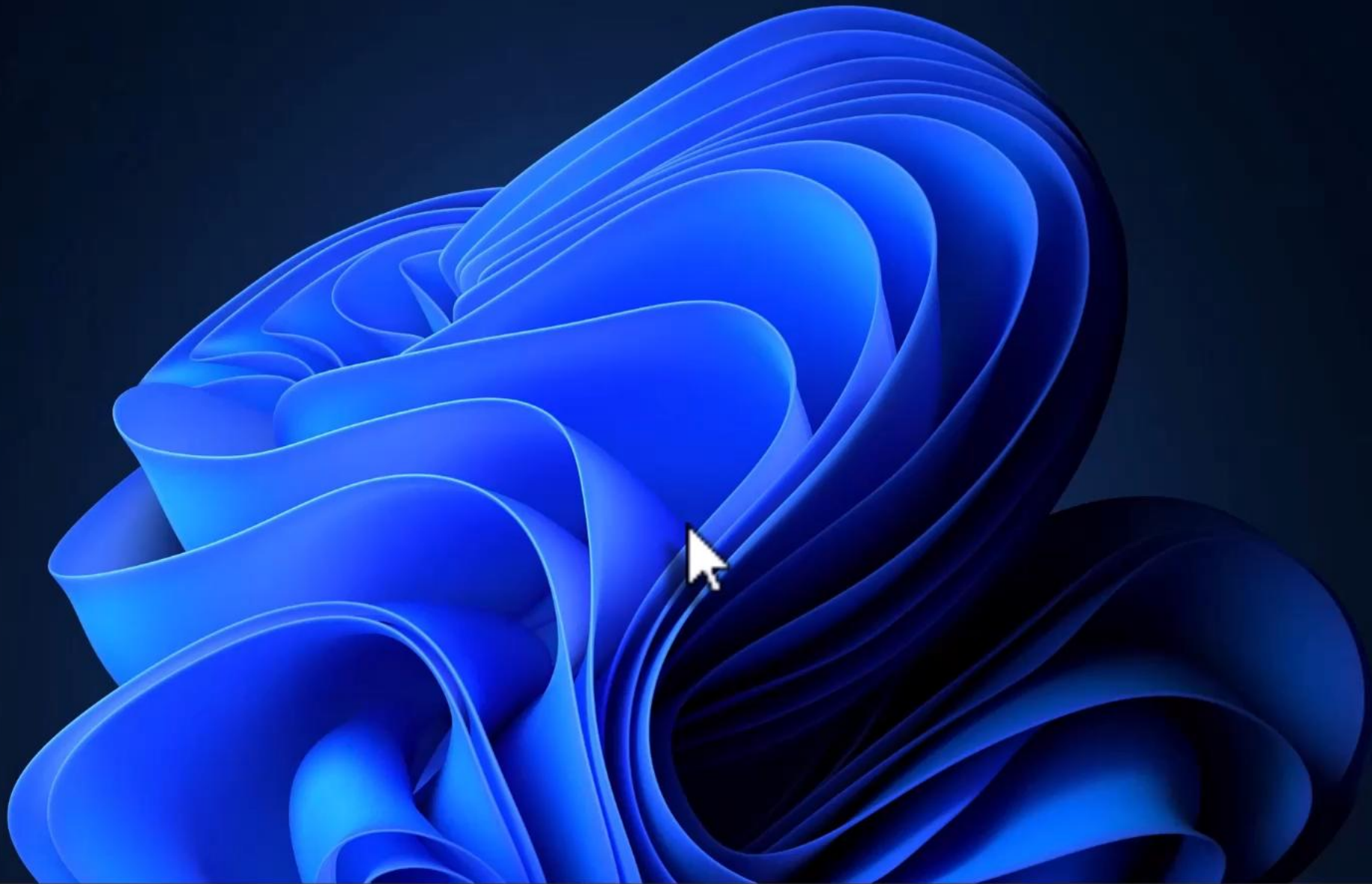
Ich möchte kontrollieren können, welche Gruppen/Benutzer auf meine Web Apps mit meinen Spielregeln zugreifen können

Was ist ein Protected Browser?

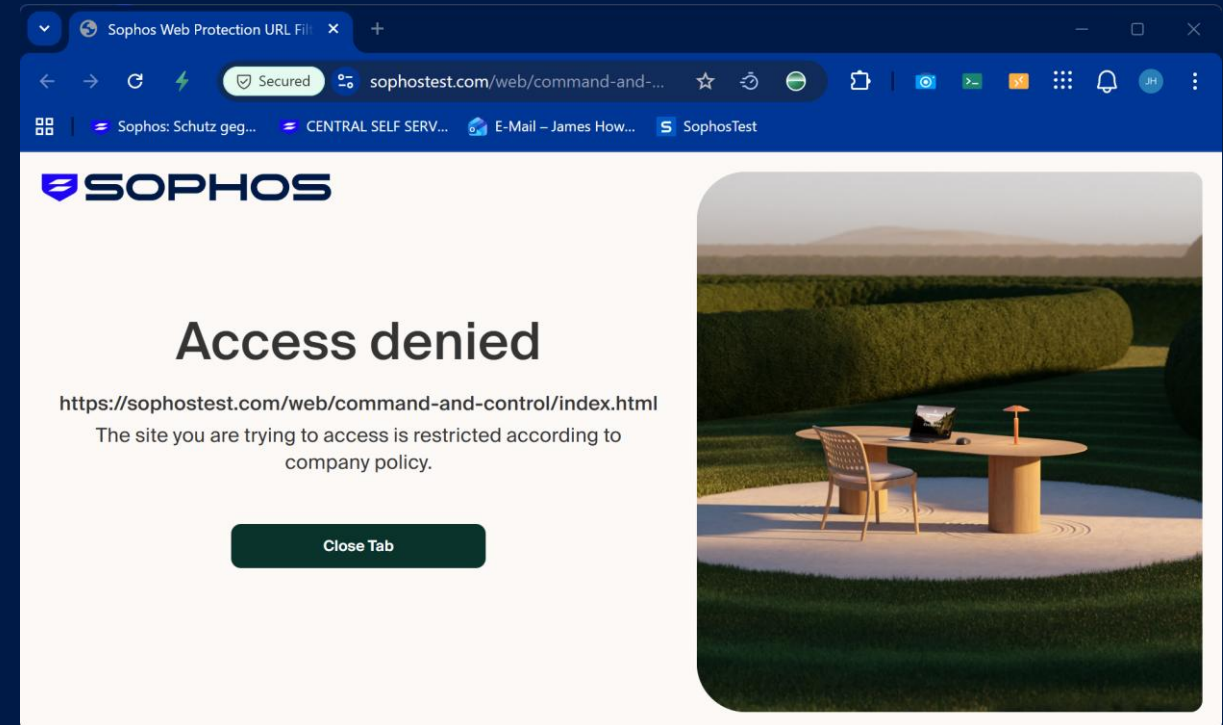
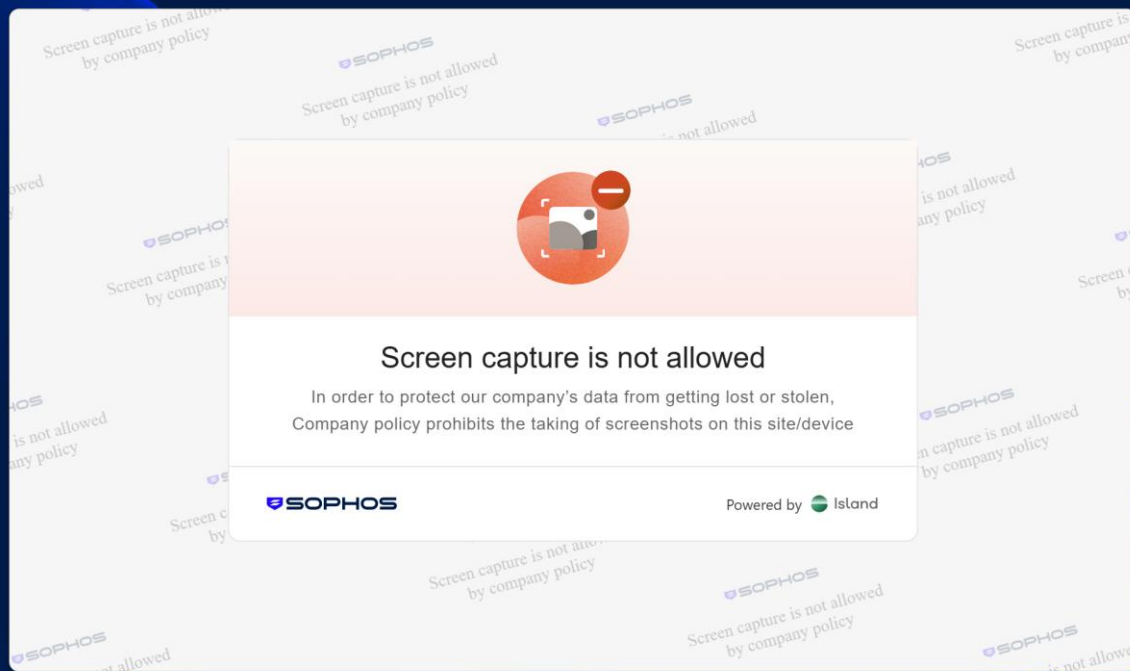
„Ein Browser wie jeder andere – nur vollständig kontrolliert, abgesichert und zentral gesteuert.“

- 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





Richtlinien durchsetzen – Block Pages



Protected Browser – Dashboard



Protected Browser

Dashboard

Logs & reports

Web policy

Policy objects

Settings

Protected Browser - Logs & reports

Overview / Protected Browser / Logs & reports

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

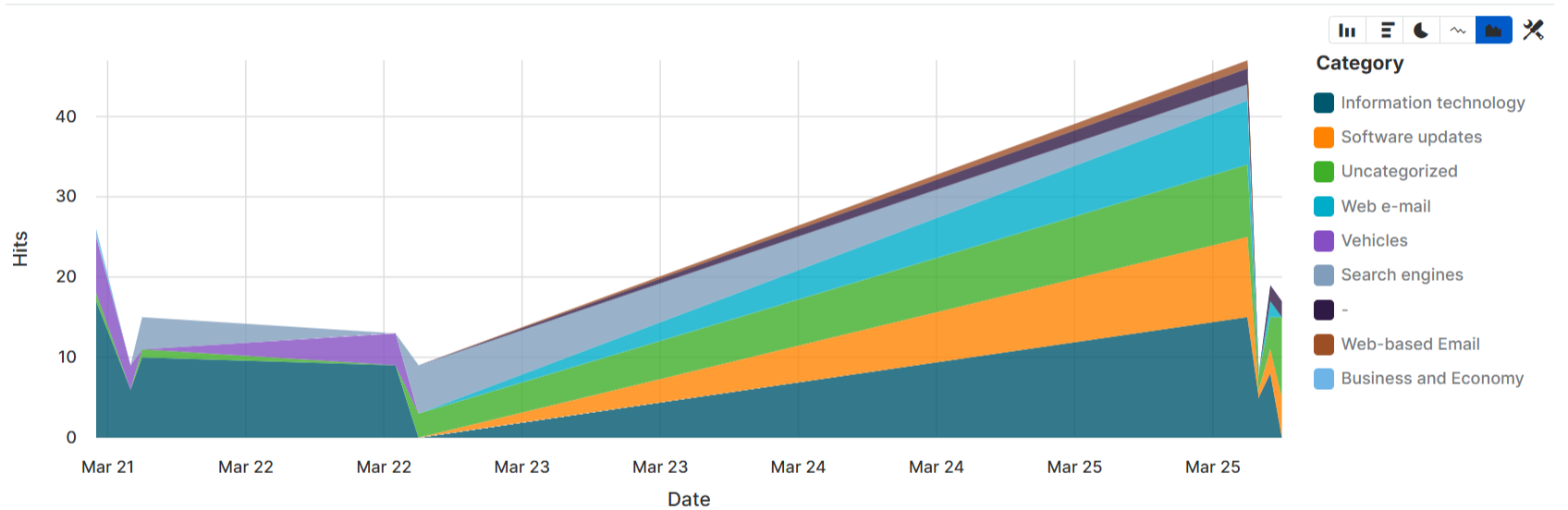
Generate

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
- Kein Full-Agent-Zwang
- Schnelles Rollout (auch für externe User)

Security-Mehrwert

- Reduziert Angriffsfläche im Browser (Hauptangriffsrisiko)
- Verhindert Credential Theft & Session Hijacking
- Schutz vor Zero-Day-Web-Angriffen

Business Impact

- Weniger Vorfälle durch Web-Angriffe
- Schnellere Absicherung von Partnern, Externen & BYOD
- Ideal für M&A- oder Übergangsszenarien

 SOPHOS

PARTNER 2026
EXPERIENCE

Sophos XDR/MDR & ITDR mit Microsoft 365 Daten

Referent 1 & Referent 2

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 Rohdaten
- 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
-

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%

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.

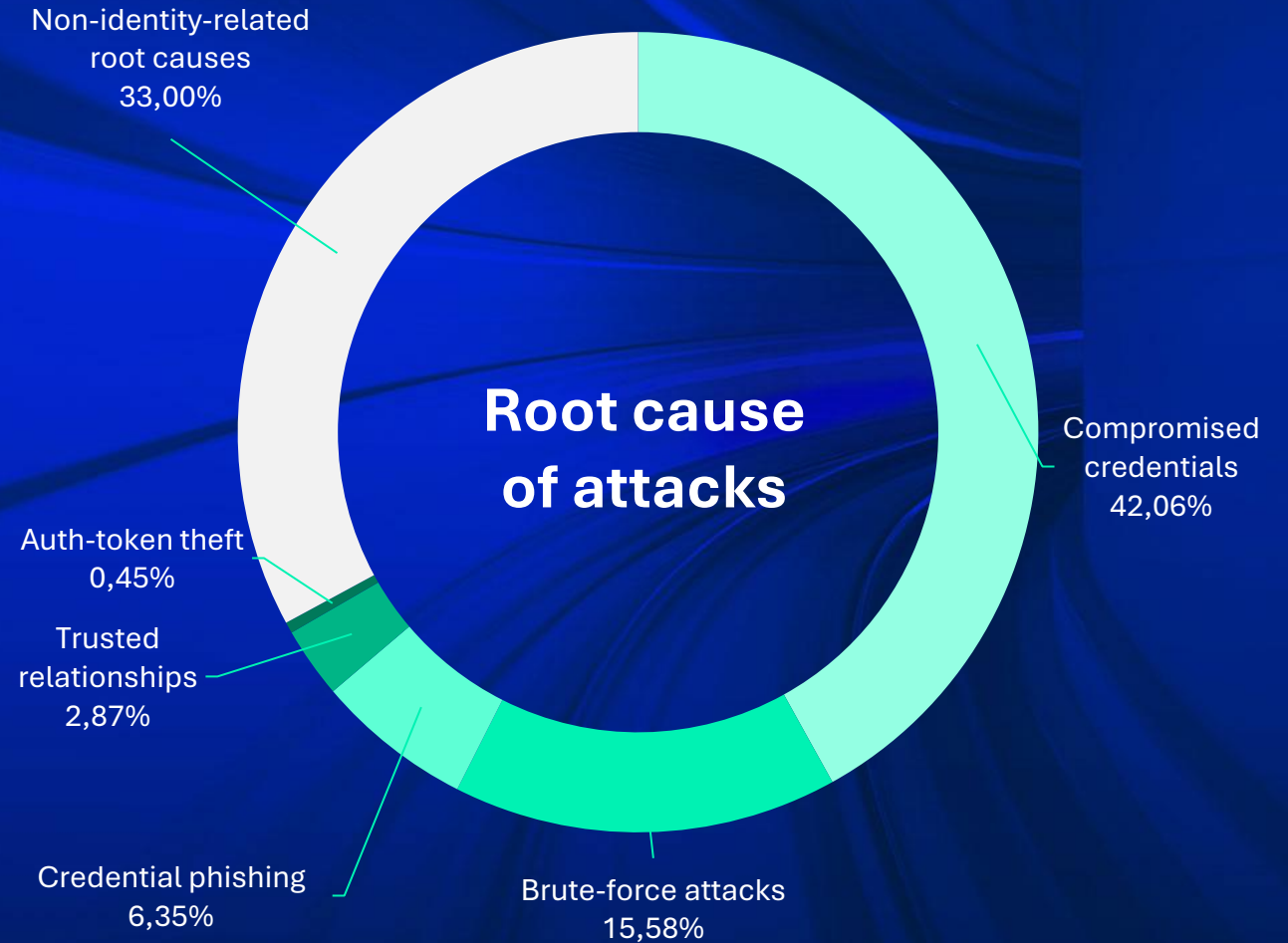
Quelle: Microsoft Graph Security API v1.0 - Alerts and Incidents providers (learn.microsoft.com)

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%

67%
of incidents
started with
compromised identity



Source: Sophos 2026 Active Adversary Report

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
Benutzeraktivitäten

Sophos ITDR Add-on zu Sophos XDR und Sophos MDR

ITDR – Zugangsdaten in Password-Leaks

Primary SE Demo Account

Dark Web Intelligence

Alle Identitätsanbieter

Quellen

3

Klartext-Passwörter

2

Gehashte Passwörter

1

2

E-Mails

▲ 66.67%
Letzte 30 Tage

0

Verwaltungs-E-Mails

0%
Letzte 30 Tage

2

Einzigartige Passwörter

▲ 66.67%
Letzte 30 Tage



Leck-Status : ACTIVE

Alle löschen

Search Breaches

Gefilterte Ergebnisse exportieren

VERÖFFENTLICHUN...	SOURCE	NAME DER ANZEIGE	BENUTZERNAME	PASSWORT-TYP	MASKED PASSWORD	AKTIONEN
4 vor Tagen	Credential Compilation 286M	SCI Voicemail	voicemail	Hash	K.A	Aktionen
8 vor Monaten	Infostealer Malware	James Garcia	james.garcia	Klartext	***d0g	
8 vor Monaten	Credential Compilation 94M	James Garcia	james.garcia	Klartext	***d0g	

- Reaktion Maßnahmen
- Entra ID - Confirm User as Compromised
- Entra ID - Disable User
- Entra ID - Dismiss User as Compromised
- Entra ID - Enable User
- Entra ID - Revoke User Sign-In Sessions

ITDR – Unsichere Identity-Konfiguration





Findings

Sophos ITDR


Status : Open ✕ [Clear All](#)

Findings updated 27 minutes ago.

[Export Filtered Results](#)

RISK ↓	DISPLAY NAME	FINDING	CATEGORY	STATUS	FIRST SEEN
 High	idr_ca_policyGro...	Conditional access policy gap	Conditional Acce...	Open	3 months ago
 High	N/A	Phishing-resistant MFA shall be enforced for all users	Configuration	Open	3 months ago
 High	N/A	Tenant shall have policy for session length	Configuration	Open	3 months ago
 High	N/A	Tenant shall have devices without policy marked non-compliant se...	Configuration	Open	3 months ago


ITDR – Verdächtiges Benutzerverhalten + Reaktion

 **Tom Wall**
MFA USER CLOUD ONLY HUMAN VIP

SUMMARY ACTIVITY LOG FINDINGS **INSIGHTS** GROUP MEMBERSHIP DARK WEB INTELLIGENCE

Open Detections (18) for Tom Wall

















Open detections within past 7 days



High (6) Medium (1) Low (11)

^ **Username** (tom.wall, tom.wall@smithscogwheels.com, tom.wall@scwxdemo.onmicrosoft.com +1 more) 6 1 11 18

18 detections [↻](#)

CREATED AT	TITLE	SEVERITY ↓	THREAT S
2026/03/23 13:57:37 +01	 Microsoft Defender for Endpoint: Compromised account conducting hands-on-keyboard attack	 High	8.8
2026/03/23 14:08:07 +01	 Microsoft Defender for Endpoint: Malicious credential theft tool execution detected	 High	8.8
2026/03/21 13:57:50 +01	 Microsoft Defender for Endpoint: Compromised account conducting hands-on-keyboard attack	 High	9.3
2026/03/21 13:47:19 +01	 Microsoft Defender for Endpoint: Exposed credentials at risk of compromise	 High	8.9
2026/03/23 13:57:37 +01	 Microsoft Defender for Endpoint: Compromised account credentials	 High	8.9
2026/03/23 13:57:37 +01	 Microsoft Defender for Endpoint: Compromised account conducting hands-on-keyboard attack	 High	8.9
2026/03/23 14:08:07 +01	 Microsoft Defender for Endpoint: Suspicious access to LSASS memory	 Medium	5.0
2026/03/25 14:06:04 +01	 Suspicious access to LSASS service(resolved)	 Low	2.0

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

Ereignisse alle Quellen

Über 350 Sophos und 3rd Party Telemetriequellen



Endpoint



Cloud



Network



Firewall



Email



Identity



Backup



Productivity tools

Analyse und Korrelation



Parse

Normalize

Correlate



Enrich

Detect



Prioritize

Summarize

24/7 Managed Detection and Response Service

Instant Security Operations Center (SOC)

24/7 Überwachung, Untersuchung und Reaktion

Proaktive Bedrohungssuche

Volles Incident Response (IR)

Sophos Threat Intelligence von 600k+ Kunden

Zugriff auf Experten als Ergänzung Ihres Teams

> 35.000 MDR Kunden

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

[My Products](#) ^

★ [Free Trials](#)

 SOPHOS

PARTNER 2026
EXPERIENCE



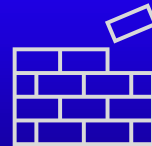
**Die neue Sophos SecOps
Plattform:
XDR, MDR & Next Gen SIEM vereint**

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

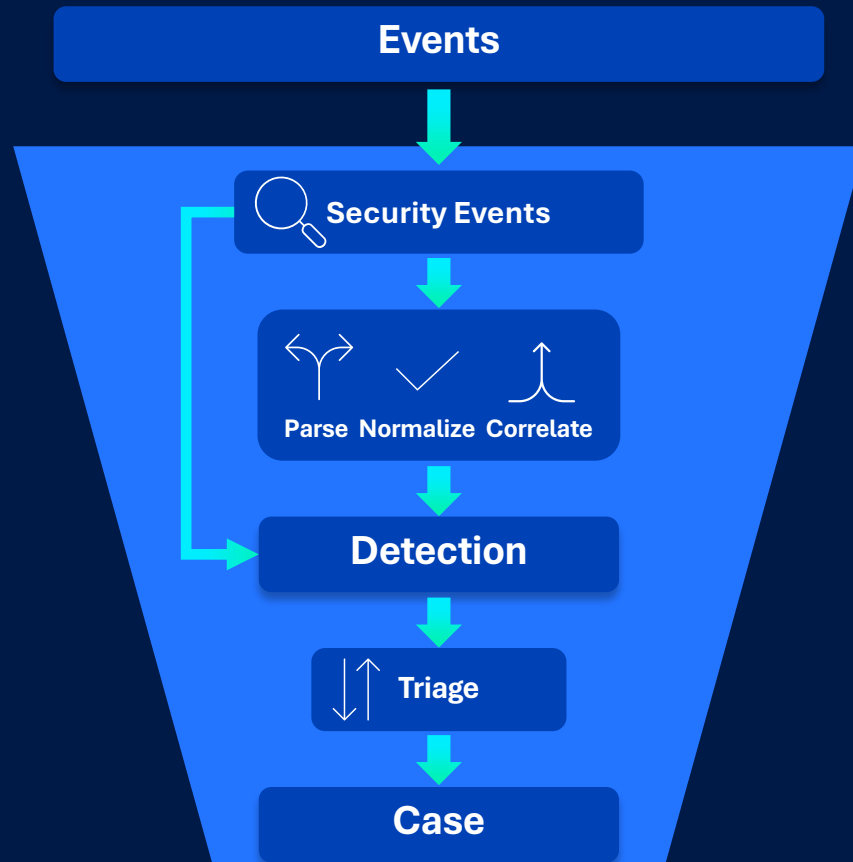
Any

NG-SIEM License

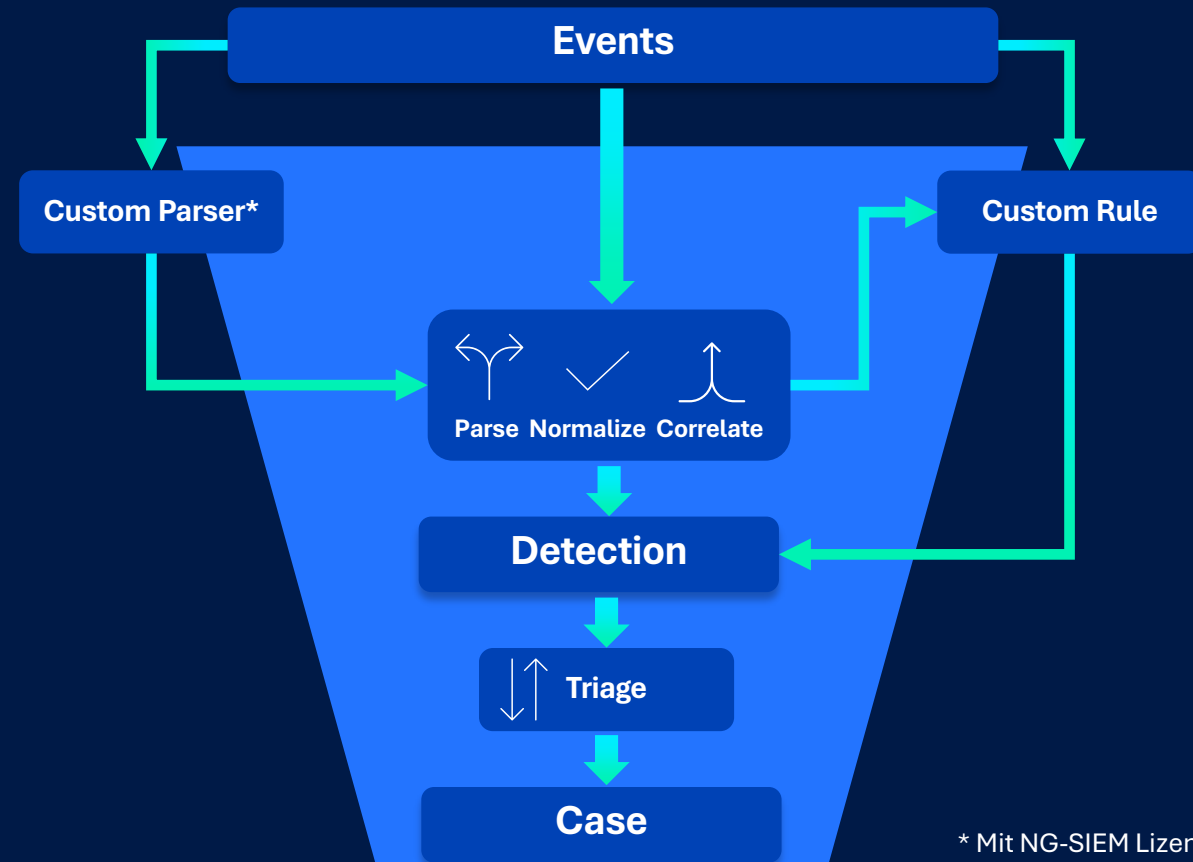
Custom Parser

Verarbeitung von Events

Sophos XDR



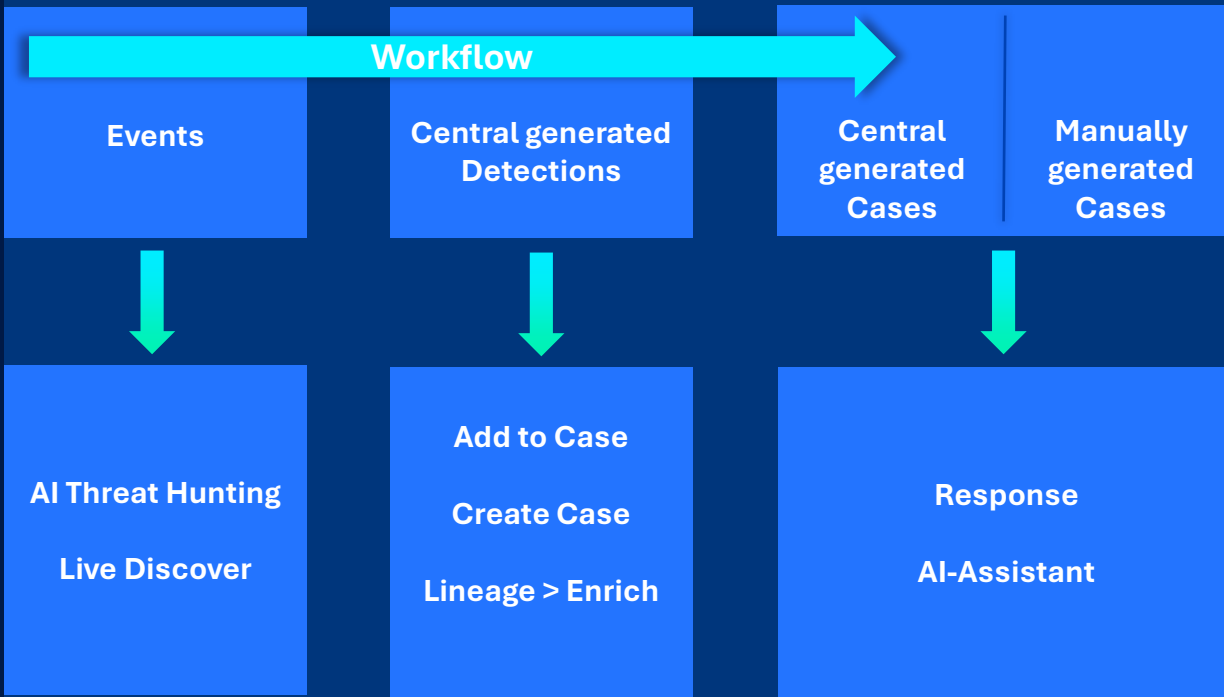
Sophos XDR powered by Secureworks



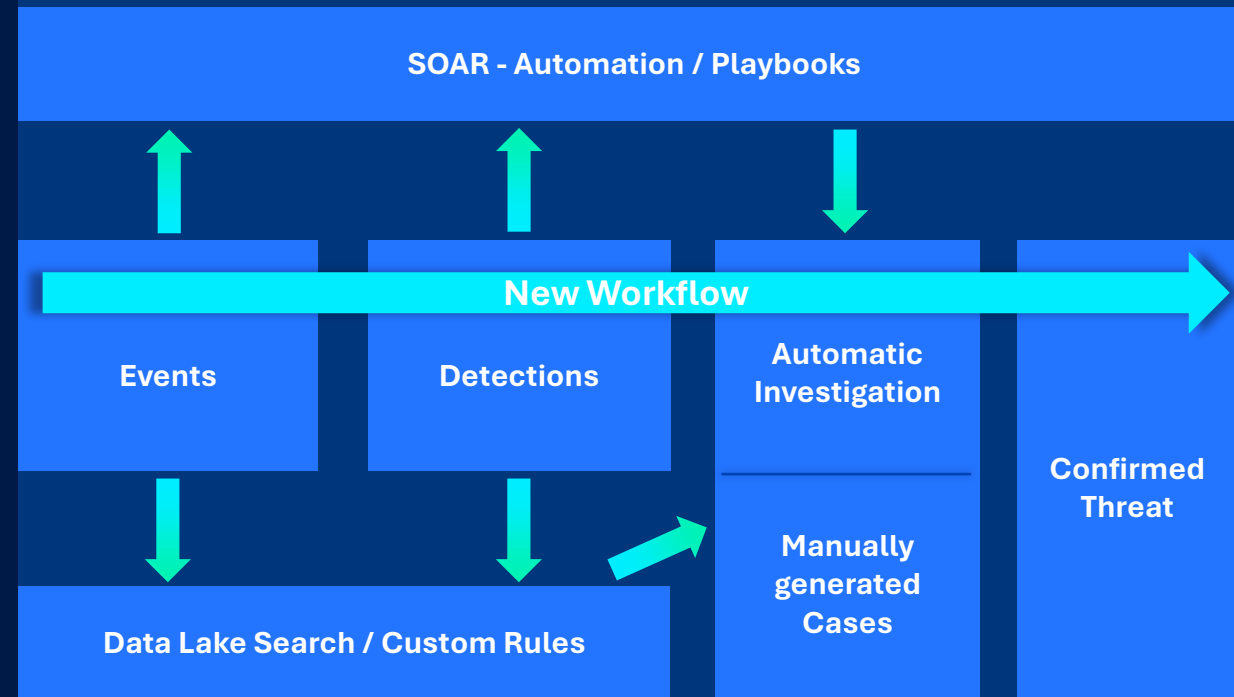
* Mit NG-SIEM Lizenz

Analysten Workflow

Sophos XDR



Sophos XDR powered by Secureworks



Evolution

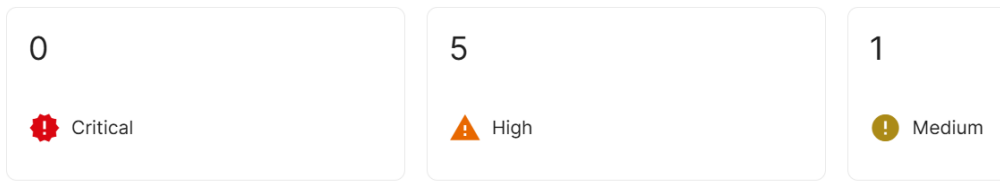
See a snapshot of your security protection

XDR Overview

Event pipeline Last 30 days



Total cases Last 30 days Include closed cases



PRIORITY	Date Created	TYPE	Case #	NAME	ID	DETECTIONS
● Medium	2026/04/28 04:31:05 +...	Security Investigation	INV00049	Adn		9
▲ High	2026/04/27 14:47:33 +...	Security Investigation	INV00048	202		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		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

Custom Rules

<input type="checkbox"/>	TIMESTAMP	SUMMARY	TYPE
<input type="checkbox"/>	2026/04/24 11:50:14 +02	Netflow 192.168.178.190:3389 - 192.168.178.90:52233 TCP	NET
<input type="checkbox"/>	2026/04/24 11:50:05 +02	Netflow 192.168.178.190:3389 - 192.168.178.90:56427 TCP	NET



- 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.

RDP to Critical Workstation

Search for all detections generated from this rule [🔍](#)

Enabled Archive

DETAILS

Rule name: RDP to Critical Workstation

```
from netflow where (source_address = '192.168.178.190' or destination_address = '192.168.178.190' or x_forwarded_for = '192.168.178.190' or source_nat_address = '192.168.178.190' or destination_nat_address = '192.168.178.190') and (source_port = 3389 or destination_port = 3389 or source_nat_port = 3389 or destination_nat_port = 3389)
```

Mitre attack categories:

By Tenant: 347777

Description: RDP to Critical Workstation

Severity: Critical

Event Type: Netflow



<input type="checkbox"/>	CREATED AT	TITLE	SEVERITY	DETECTOR NAME	SENSOR TYPE
<input type="checkbox"/>	2026/04/24 11:55:11 +02	RDP to Critical Workstation	Critical	Custom Alerts	ENDPOINT_SOPHOS
<input type="checkbox"/>	2026/04/24 11:50:45 +02	RDP to Critical Workstation	Critical	Custom Alerts	ENDPOINT_SOPHOS

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)

Actions

AVAILABLE (26) CONFIGURED (9)

Filter By: Response, Enrichment Search for action

- Block Domain**
Enables the Block Domain response action
Not Configured
- Block File Hash**
Enables the Block File Hash response action on file hashes
Configured Enabled
- Block IP**
Enables the Block IP response action on IP addresses
MDR SUPPORTED
Not Configured
- Change Password At Next Login**
Enables the Change Password At Next Login response action
Not Configured
- Clawback**
Enables the Clawback response action
Not Configured
- Collect Forensic Logs**
Enables the Collect Forensic Logs response action on hosts
Configured Enabled

Isolate Host

Enables the Isolate Host response action on hosts

INTEGRATIONS DEPENDENCIES

Select Integrations

Select the integrations which will be used by this action.

<input type="checkbox"/>	ACTIVITY	CONNECTION	DESCRIPTION
<input type="checkbox"/>	Isolate Host Microsoft Defender ATP	Microsoft Defender ATP - SCWXdemo	TCU-SCI Connector for Response Action Playbooks, expires 2027-10-02
<input type="checkbox"/>	Isolate Host VMware Carbon Black Cloud	VMware Carbon Black Cloud	Ref. 02 - Carbon Black Cloud Endpoint Standard EDR Connector
<input type="checkbox"/>	Isolate Host CrowdStrike Falcon Endpoint	CrowdStrike Falcon Endpoint connector	CrowdStrike EDR Connector Ref. 03
<input type="checkbox"/>	Isolate Host Sophos	N/A	-

Detector Explorer

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

Explore Detections & Count... / System Se
System Service Discover

SUMMARY

Detector Details

A script block event associated with the PowerSploit module Get-UnquotedService was identified. This may indicate that threat actors are attempting to get information about a service on the system.

Example:
> powershell Get-UnquotedService

Updated: 2025-06-17T14:39:40.976726Z

Severity:  Critical (0.99)

MITRE Categories

Tactics: Discovery, Execution

Techniques: System Service Discovery (T1007) [🔗](#)
PowerShell (T1059.001) [🔗](#)

```
scwx.script_block.decoded_block.text = Get-UnquotedService AND  
scwx.script_block.interpreter.name = ^powershell$
```

- The detection logic is designed to identify the use of a specific PowerSploit module called "Get-UnquotedService". This module is often used by threat actors to gather information about services running on a system, particularly those that might be vulnerable due to unquoted paths.

- The first condition for a detection match is the presence of the text "Get-UnquotedService" within the decoded script block. This indicates that the script is attempting to execute this specific module, which is a known method for discovering unquoted service paths.

- The second condition requires that the script is being executed within a PowerShell interpreter. This is determined by matching the interpreter name to "powershell". This ensures that the detection is specifically targeting scripts running in a PowerShell environment, which is the typical environment for PowerSploit modules.

- Both conditions must be met for a detection match to occur. This means that the script must both contain the "Get-UnquotedService" text and be running in PowerShell.

- Potential false positives could occur if legitimate administrative scripts or security tools use the "Get-UnquotedService" module for benign purposes, such as auditing or system maintenance. Additionally, any script that includes the text "Get-UnquotedService" for documentation or educational purposes could trigger the alert even if it is not actively executing the module.

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

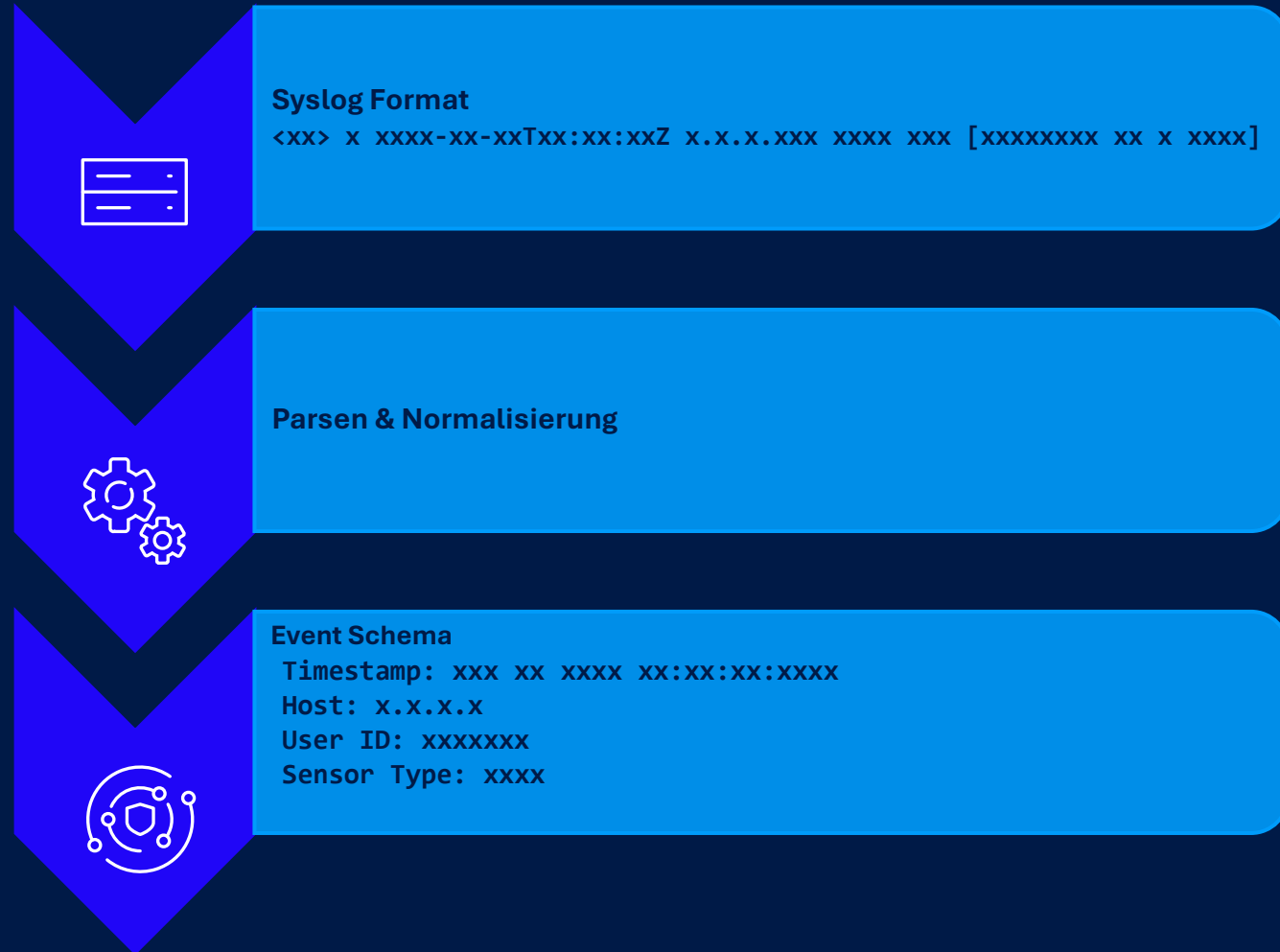
Ausblick – Next Generation SIEM

- **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





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



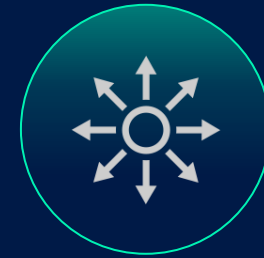
Erweitern Sie Ihr Security Team mit Sophos Experten



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

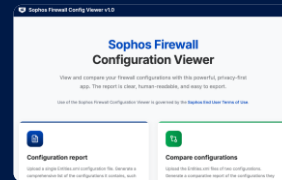
Date

Sophos Firewall

Sophos Firewall v22.0 GA

Secure by Design
Automatic hotfix patches
Secure backups
Hardened portals
Remote monitoring

New in Sophos Firewall v22
Firewall Health Check
Next-gen Xstream Architecture
XDR Linux Sensor for proactive monitoring
New anti-malware engine
Secure updates



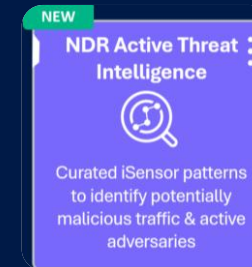
Secure by Design

- 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

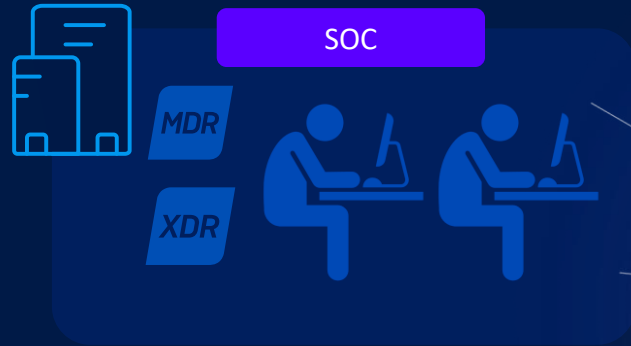
NDR-E für Virtual und Cloud

- NDR Essential für virtuelle & Cloud Firewalls

Sophos Central Audit Log Verbesserungen

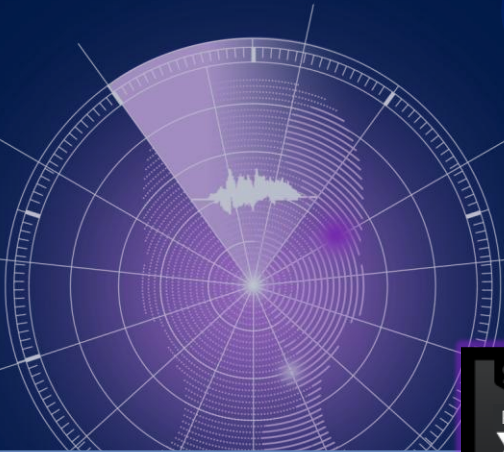
The First MDR/XDR-Optimized Firewall

with purpose-built active threat detection and response capabilities



SOC

MDR
XDR



NEW

SOPHOS NDR
AI Analysis of TLS & DNS

SOPHOS DNS
DNS Protection

SOPHOS X-OPS
APT's
Active C2s

3rd PARTIES
Domains
Bad IPs
IPS



PROGRAMMABLE
Xstream
ARCHITECTURE

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 böartigen 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 Silicon Support
 - [Coming Soon] Entra ID Support
- **Entra ID Conditional Access Support for Sophos Connect VPN**



NDR Active Threat Intelligence

v20

v21

v21.5

v22.1

Sophos X-OPs



SophosLabs Threat Intel Datenbank mit >1 Mio. Bedrohungen

Sophos MDR/XDR




Von Analysten identifizierte Bedrohungen & IOCs

Third-Party



Unabhängige Threat Intelligence Quellen von Drittanbietern


Sophos NDR Essentials



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

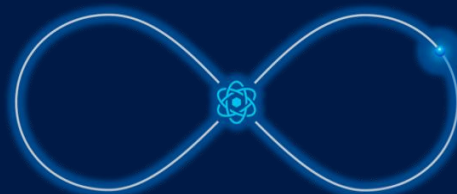
NEW

NDR Active Threat Intelligence

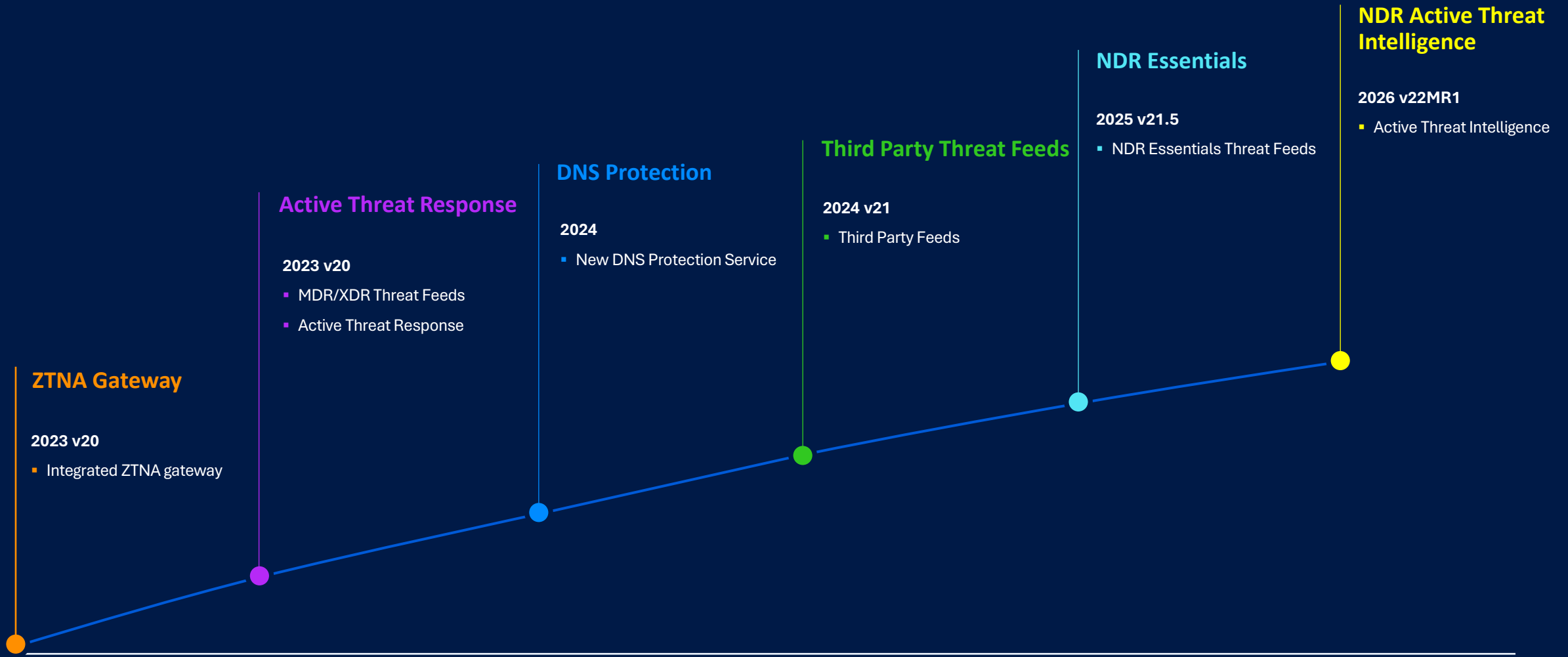


Optimierte iSensor-Muster für die Erkennung von böartigem Traffic & aktiven Angreifern

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

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

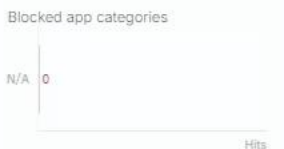
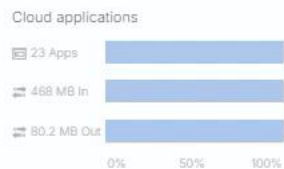
Total 31

Noncompliant policies by policy severity

19 61% Compliant 12 Noncompliant

6/17 High 5/11 Medium 1/3 Low

Traffic insight



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

MDR Status: On Blocked/Monitored: 0

NDR Essentials

NDR Status: On Monitored: 0

Sophos X-Ops

X Status: On Blocked/Monitored: 0

Third-party threat feeds

Threat feeds	Sync status	Blocked/Monitored
AbuseURIhaus	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

Log comp is Central Firewall UI	comp	Status	Username
2026-02-20 07:35:45	Central Firewall UI	Successful	centralsophtest+111@gmail.com
2026-02-20 04:44:05	Central Firewall UI	Successful	centralsophtest+111@gmail.com
2026-02-20 04:43:57	Central Firewall UI	Successful	centralsophtest+111@gmail.com
2026-02-20 04:32:48	Central Firewall UI	Successful	centralsophtest+111@gmail.com
2026-02-20 03:54:49	Central Firewall UI	Successful	centralsophtest+111@gmail.com
2026-02-20 03:54:11	Central Firewall UI	Successful	centralsophtest+111@gmail.com
2026-02-20 03:53:19	Central Firewall UI	Successful	centralsophtest+111@gmail.com

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

The screenshot displays the Sophos Firewall Config Studio v2.0 interface. The main window is titled 'Konfigurationseditor (778 Objekte) EXPERIMENTELL'. It features a search bar, 'Import überprüfen', 'Alle entfernen', 'Importieren', 'Vorschau', and 'Herunterladen' buttons. A progress bar shows four steps: 1. Firewall-Konfiguration hinzufügen, 2. Konfiguration importieren (optional), 3. Vorschau & Export, and 4. Auf Firewall bereitstellen. The main content area is titled 'Firewallregeln (21)' and shows a table of rules. The table has columns for #, Status, Name, Aktion, Quellzonen, Zielzonen, Quellnetzwerke & Hosts, Zielnetzwerke & Hosts, Konfig. Analyse, and Aktionen. A green notification bubble at the bottom right says 'Erfolgreich hinzugefügt'.

#	Status	Name	Aktion	Quellzonen	Zielzonen	Quellnetzwerke & Hosts	Zielnetzwerke & Hosts	Konfig. Analyse	Aktionen
1	ON	ANY	Accept	Any	Any	Any	Any	Verdeckt 17	[Edit] [Delete] [More]
2	ON	Test NAT	Accept	WAN	Any	LUCH Homeoffice IPv4	Any	Verdeckt	[Edit] [Delete] [More]
3	OFF	Auto added firewall policy for MTA	Accept	Any	Any	Any	Any	Verdeckt	[Edit] [Delete] [More]
4	ON	ITSA Access	Accept	VPN	VPN	Any	ITSA Switch Network	Verdeckt	[Edit] [Delete] [More]
5	ON	Temp Blackhole NAT	Drop	WAN	Any	Block List	Any	Verdeckt	[Edit] [Delete] [More]
6	OFF	Test	WAF	Any	Any	Any	Any	Verdeckt	[Edit] [Delete] [More]
7	OFF	Test2	WAF	Any	Any	Any	Any	Verdeckt	[Edit] [Delete] [More]
8	ON	Linux and Factory to Central Email SMTP	Accept	LAN VPN	WAN	Linux Azure Factory +1	Wiesbaden WAN Office IP Relay EU Central 1 +4	Verdeckt	[Edit] [Delete] [More]
9	ON	Linux to WAN SMTP	Drop	LAN	WAN	Linux Azure	Any	Verdeckt	[Edit] [Delete] [More]
10	ON	Linux to WAN	Accept	LAN	WAN	Linux Azure	Any	Verdeckt	[Edit] [Delete] [More]

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

The screenshot displays the Sophos Firewall Config Studio v2.0 interface. The top navigation bar includes the title 'Sophos Firewall Config Studio v2.0', a language dropdown set to 'DE Deutsch', and a home icon. Below the navigation bar, the main content area is titled 'Konfigurationseditor (777 Objekte) EXPERIMENTELL'. It features a search bar for 'Globale Suche...' and several action buttons: 'Import überprüfen', 'Alle entfernen', 'Importieren', 'Vorschau', and 'Herunterladen'. A progress indicator shows four steps: 1. 'Erste Schritte' (Firewall-Konfiguration hinzufügen), 2. 'Konfiguration importieren (optional)', 3. 'Vorschau & Export', and 4. 'Auf Firewall bereitstellen'. The main workspace is divided into a left sidebar and a central table. The sidebar, under 'HOSTS & DIENSTE', lists categories like 'IP-Host' (127), 'FQDN-Host' (420), 'MAC-Host', 'Dienst' (89), 'Dienstgruppe' (1), 'Ländergruppe' (9), 'Cloud-Objekte', 'NETZWERK' (Zone, DHCP-Server, DNS-Hosteintrag), and 'SYSTEM' (Lokale Dienst-ACL). The central table, titled 'IP-Hosts (127)', has a search bar and buttons for 'Auswahl aufheben', 'Ausgewählte löschen (6)', 'Massenhinzufügen', and 'Hinzufügen'. The table columns are '#', 'Name', 'IP-Familie', 'Host-Typ', 'IP-Adresse', 'Konfig. Analyse', and 'Aktionen'. It lists various IP hosts with their respective IP families, types, and addresses, along with status indicators like 'Verwendet in 2' or 'Unbenutzt'.

#	Name	IP-Familie	Host-Typ	IP-Adresse	Konfig. Analyse	Aktionen
11	#PortB	IPv4	System Host	-	Verwendet in 2	
12	BruteForce IP List KBA-000009932	IPv4	IPList	83 IPs	Unbenutzt	
13	Factory	IPv4	IP	172.25.105.19	Verwendet in 1	
14	Luca Green Notebook LAN	IPv4	IP	172.17.170.10	Unbenutzt	
15	Linux Azure 2	IPv4	IP	192.168.1.7	Verwendet in 1	
16	Azure IP	IPv4	IP	52.239.213.228	Unbenutzt	
17	Saleseng.de	IPv4	IP	51.144.76.249	Unbenutzt	
18	SEA-ESX1	IPv4	IP	172.21.110.20	Unbenutzt	
19	UTM RED IP	IPv4	IP	192.168.174.2	Unbenutzt	
20	RED XG Wiesbaden	IPv4	IP	192.168.172.2	Duplikat, Unbenutzt	
21	Test IP	IPv4	IP	10.10.10.15	Unbenutzt	

VPN als Herausforderung

Sophos Annual Threat Report

Akira and Fog

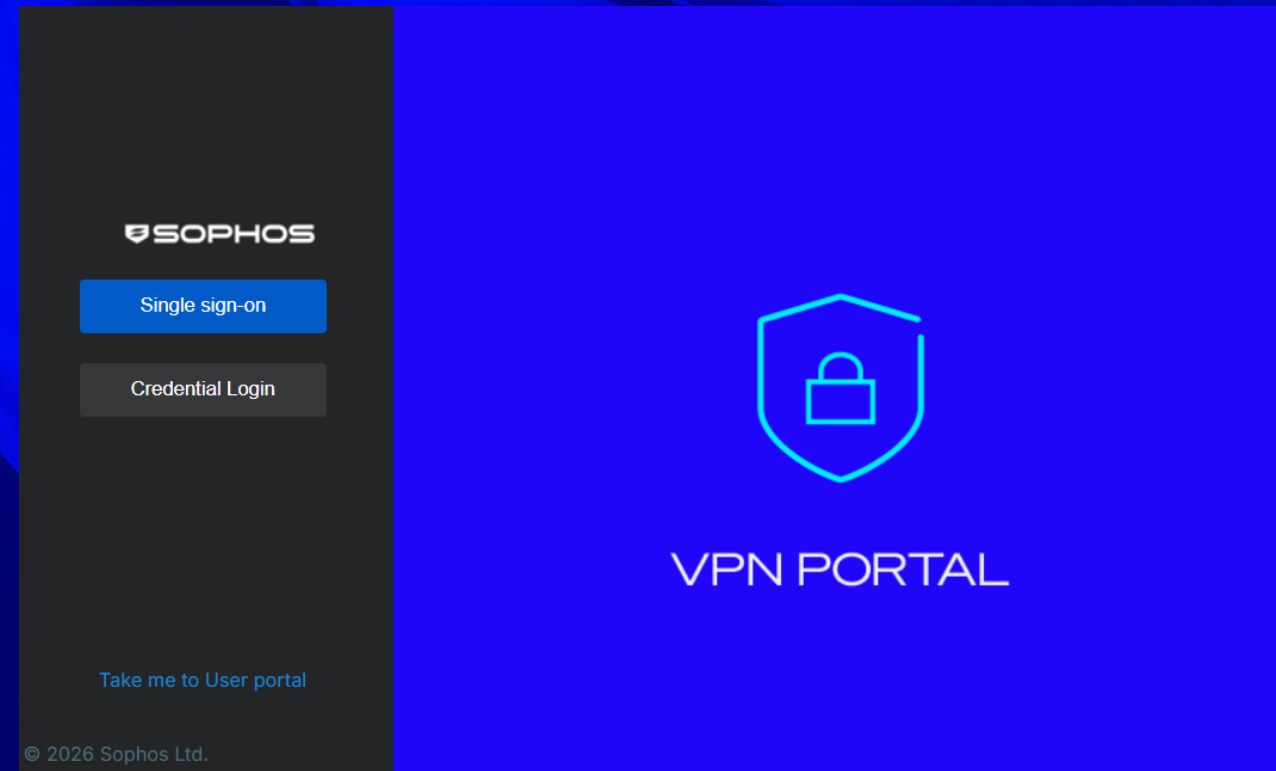
In terms of actual incidents, the Akira ransomware-as-a-service led the pack in 2024, ultimately stepping in to fill the void left by LockBit. Initially seen in 2022, Akira attacks ramped up in late 2023. The group and its affiliates were steadily active throughout 2024, spiking in August when Akira 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.

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 tomils 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)

The image shows a screenshot of the Sophos management interface. The top part displays the 'Firewall health check' dashboard with a 'Policy compliance' summary. It shows 26 compliant policies (84%) and 5 non-compliant policies. The non-compliant policies are broken down by severity: 2 High, 3 Medium, and 0 Low. Below this is a table of non-compliant policies.

#	Policies	Module	Standard	Severity	Status	Action
1	Sophos X-Ops should be turned on. Its Action should be set to Log and drop.	Active threat response	CIS	High	Complies	
2	MDR threat feeds should be turned on. Its Action should be set to Log and drop.	Active threat response	Recommended	High	Complies	
3	Synchronized Application Control should be turned on.	Active threat response	Recommended	Medium	Complies	
4	Security Heartbeat					
5	A firewall rule's Heartbeat setting					
6	Password complexity					
7	Hotfix settings					

Below the table, there is a login overlay for 'saleseng.de'. It offers two authentication methods: 'Benutzername und Kennwort' (Username and Password) and 'Single-Sign-On (SSO)'. The SSO option is highlighted with a blue button. There is also a link for 'VPN-Portal-Port' and a checkbox for 'Benutzername und Kennwort speichern' (Save username and password).

