SOPHOS

Digitale Schule sicher gestalten:

Cybersecurity-Förderung im Rahmen des Digitalpakt 2.0



Martin Weiß
Senior Sales Engineer Public



Euer Sprecher



Martin Weiß
Senior Sales Engineer Public

- Senior Sales Engineer Public bei Sophos Deutschland mit über 20 Jahren Erfahrung in IT-Security, Netzwerken, Automatisierung, Cloud und Rechenzentrumsbetrieb.
- Verantwortete früher den 24/7-Betrieb sowie die ISO27001-Zertifizierung eines Münchener Internetproviders.
- Fokus im Sophos Sales Engineering: Beratung und technische Unterstützung für Auftraggeber des öffentlichen Sektors in Deutschland.
- Zertifizierte Fachkraft für Datenschutz



SOPHOS

Digitalpakt 2.0: Was gefördert wird

SOPHOS

Digitalpakt 2.0: Was gefördert wird

FÖRDERVOLUMEN

5 Mrd. €

bis 2030

Bund-Länder-Förderung für die digitale Weiterentwicklung der Schulen

WER FÖRDERT



Bund und Länder

Gemeinsames Förderprogramm für Schulen

WAS DAZUGEHÖRT



IT-Sicherheit ist förderfähig

Schutz der Infrastruktur gehört dazu

SOPHOS

IT-Sicherheit ist förderfähig, aber vielen unbekannt

Verwaltungsvereinbarung Digitalpakt Schule 2.0

§ 2 Abs. 4 Nr. 3 lit. a)

Förderfähig sind auch **befristete Ausgaben** in unmittelbarer Verbindung mit Investitionsmaßnahmen für den Auf- und Ausbau von Strukturen für die **professionelle Administration** der digitalen Infrastrukturen und den **professionellen Support**.

Fußnote 1: Dazu zählen auch Sachmittel für die Beauftragung externer Dienstleister in direkter Verbindung mit Investitionsmaßnahmen.

Details regeln die Förderprogramme der Länder: je nach Programm auch Softwarelizenzen, Administration und Leistungen für den laufenden Betrieb.

12,5 %

der Befragten wissen nicht, ob IT-Sicherheit überhaupt förderfähig ist

28 %

haben IT-Sicherheit bereits fest in ihre Investitionsplanung aufgenommen

50 %

denken darüber nach, entsprechende Maßnahmen einzuplanen

SOPHOS

Aktuelle Bedrohungen für Schulen

SOPHOS

Positive Selbsteinschätzung trifft auf viele reale Vorfälle

SOPHOS-UMFRAGE JULI 2026 | 200 VERANTWORTLICHE AUS SCHULEN, SCHULTRÄGERN UND VERWALTUNGEN

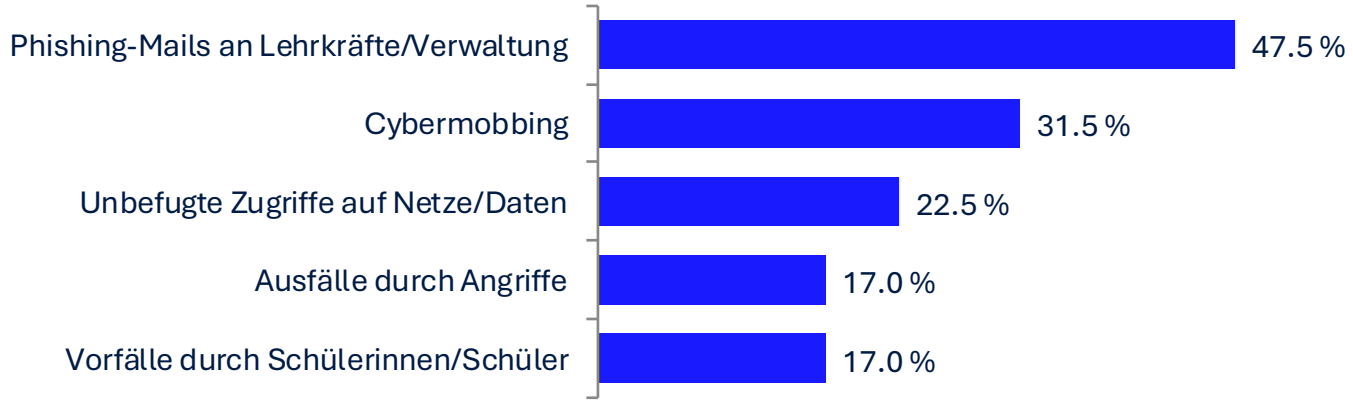
67,5 %

bewerten ihren Sicherheitsstand als gut oder sehr gut. Nur 28,5 % sehen deutliche Lücken.

78 %

berichten von mindestens einer konkreten Bedrohung oder einem Sicherheitsvorfall in den letzten zwölf Monaten.

Beobachtete Bedrohungen in den vergangenen zwölf Monaten



Wer Lücken sieht, erlebt mehr

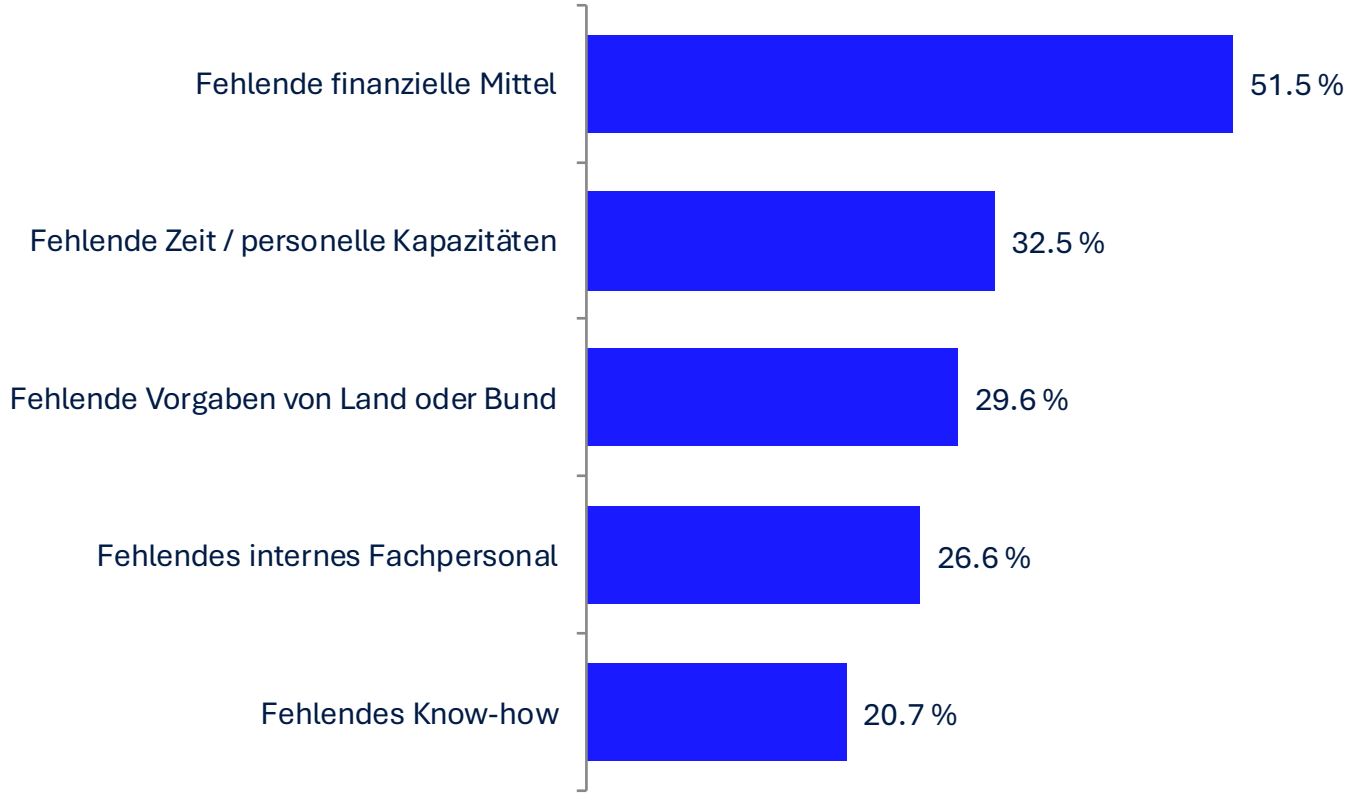
33,3 % der Befragten mit lückenhaftem Sicherheitsstand berichten von unbefugten Zugriffen. Bei gutem Sicherheitsstand sind es 18,3 %. Nur 19,5 % kennen gar keine Vorfälle.

SOPHOS

IT-Sicherheit bleibt oft eine Zusatzaufgabe

Größte Engpässe auf dem Weg zu besserer IT-Sicherheit

169 Befragte, die ihren Sicherheitsstand noch nicht als sehr gut einstufen



~ 25 %

verfügen über eine interne Fachkraft, die ausschließlich für IT-Sicherheit zuständig ist

> 50 %

der nebenamtlich zuständigen Lehrkräfte nennen fehlende Zeit und Kapazitäten als Belastung

Die Verantwortung liegt meist bei der allgemeinen IT, der Schulleitung, einem externen Dienstleister oder IT-affinen Lehrkräften, zusätzlich zum Tagesgeschäft.

SOPHOS

Phishing mit KI: Wenn Angriffe täuschend echt wirken

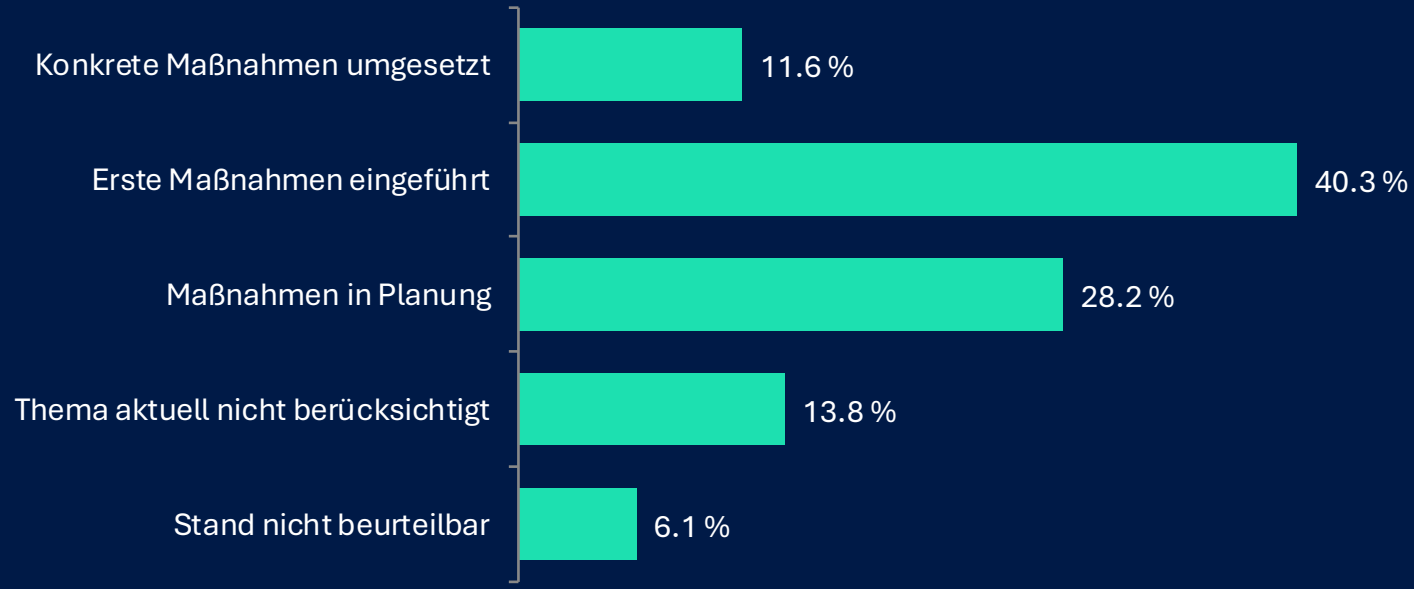
90,5 %

haben KI-gestützte Angriffe und KI-Risiken im Blick; 66,5 % erwarten spürbaren Einfluss in zwei Jahren

11,6 %

haben bereits konkrete Schutzmaßnahmen gegen KI-Risiken umgesetzt

Stand der Maßnahmen gegen KI-Risiken (181 Befragte)



Woran eine KI-generierte Phishing-Mail erkennbar bleibt

Abweichende Internetadresse
Vertrauter Name, fremde Domain

Ungewöhnlicher Zeitdruck
Frist und angedrohte Sperrung

Zugangsdaten erneut abfragen
Link führt zu einem fremden Login

SOPHOS

Wenn das Risiko außerhalb der Schule liegt

87 %

nutzen Lernplattformen, Schulverwaltungssysteme oder Cloud-Dienste

38 %

haben deren Sicherheitsstandards geprüft

34 %

setzen Plattformen ohne formale Prüfung ein

15 %

haben kein Personal und keine Ressourcen für eine Prüfung

Drei Risikofelder außerhalb des eigenen Netzwerks

Externe Plattformen

Lernmanagement, Schulverwaltung, Schulfoto-Dienste: Konten und Daten liegen bei Dritten, die Prüfpflicht bleibt beim Träger.

Schatten-IT

Ungeprüfte Hard- und Software läuft unverwaltet im Schulnetz und vergrößert die Angriffsfläche.

KI-Anwendungen

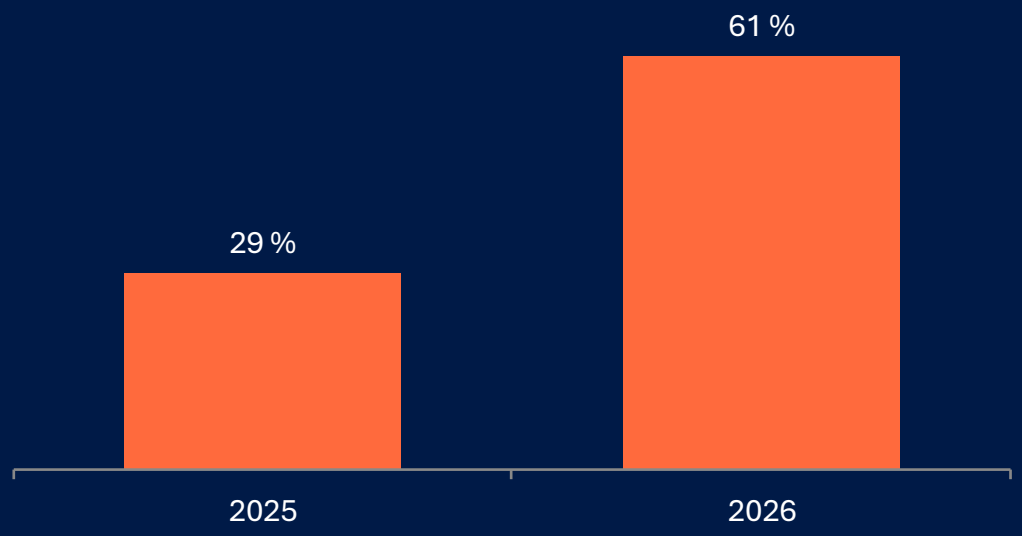
Unkontrollierte KI-Nutzung durch Lehrkräfte und Schüler: Datenabfluss und fehlende Richtlinien.

SOPHOS

Ransomware im Bildungssektor: Identitäten als Einfallstor

SOPHOS STATE OF RANSOMWARE REPORT 2026, BILDUNGSSEKTOR

Verschlüsselungsrate in der allgemeinen Bildung



mehr als verdoppelt innerhalb eines Jahres

85 %

der Angriffe im Bildungssektor identitätsbasiert ausgelöst

31 %

der Angriffe mit bösartigen E-Mails als häufigste technische Ursache

31 %

brauchten einen Monat oder länger zur Wiederherstellung, mehr als jeder andere Sektor

39 %

der Sicherheitsteams melden Ausfälle durch Stress oder psychische Belastung

Häufigste betriebliche Ursachen: menschliches Versagen (52 %), mangelnder Schutz (47 %), unbekannte Sicherheitslücken (42 %), Personal- oder Kapazitätsmangel (41 %).

Fallbeispiel: LockBit-Angriff auf ein Schulnetzwerk in der Vorderpfalz, Januar 2025. 45 Schulen betroffen, 2,5 TB Daten im Darknet, darunter Zeugnisse und Gesundheitsinformationen.

SOPHOS

IT-Sicherheit strategisch in die Investitionsplanung integrieren

SOPHOS

Vom Förderantrag zum sicheren Betrieb: vier Schritte

Bestandsaufnahme

Netzwerke, Server, Endgeräte, Cloud-Dienste, Identitäten und Drittanbieter erfassen, inklusive Schatten-IT.

Zuständigkeiten klären

Wer verantwortet Betrieb, Überwachung und Reaktion? Schule, Träger, Dienstleister, Managed Service.

Sicherheitskonzept

Technische und organisatorische Maßnahmen ableiten: Netzwerksicherheit, Schulungen, MFA, Cloud-Sicherheit, KI-Richtlinien.

Förderfähige Vorhaben

Maßnahmen gegen Länderprogramm prüfen und als Investition inklusive Administration und Support beantragen.

Was Schulträger bereits priorisieren (Sophos-Umfrage 2026)

1 Netzwerksicherheit

2 Schulungen

3 Multi-Faktor-Authentifizierung

4 Cloud-Sicherheit

5 Richtlinien für sicheren KI-Einsatz

SOPHOS

Wie kann Sophos helfen?

KI heute verändert alles.

TEMPO

Angriffe erfolgen in Maschinengeschwindigkeit

MENGE

KI ermöglicht einen exponentiellen Anstieg des Angriffsvolumens

UMFANG

KI vergrößert die Angriffsfläche und die Komplexität der Ausführung

SOPHOS

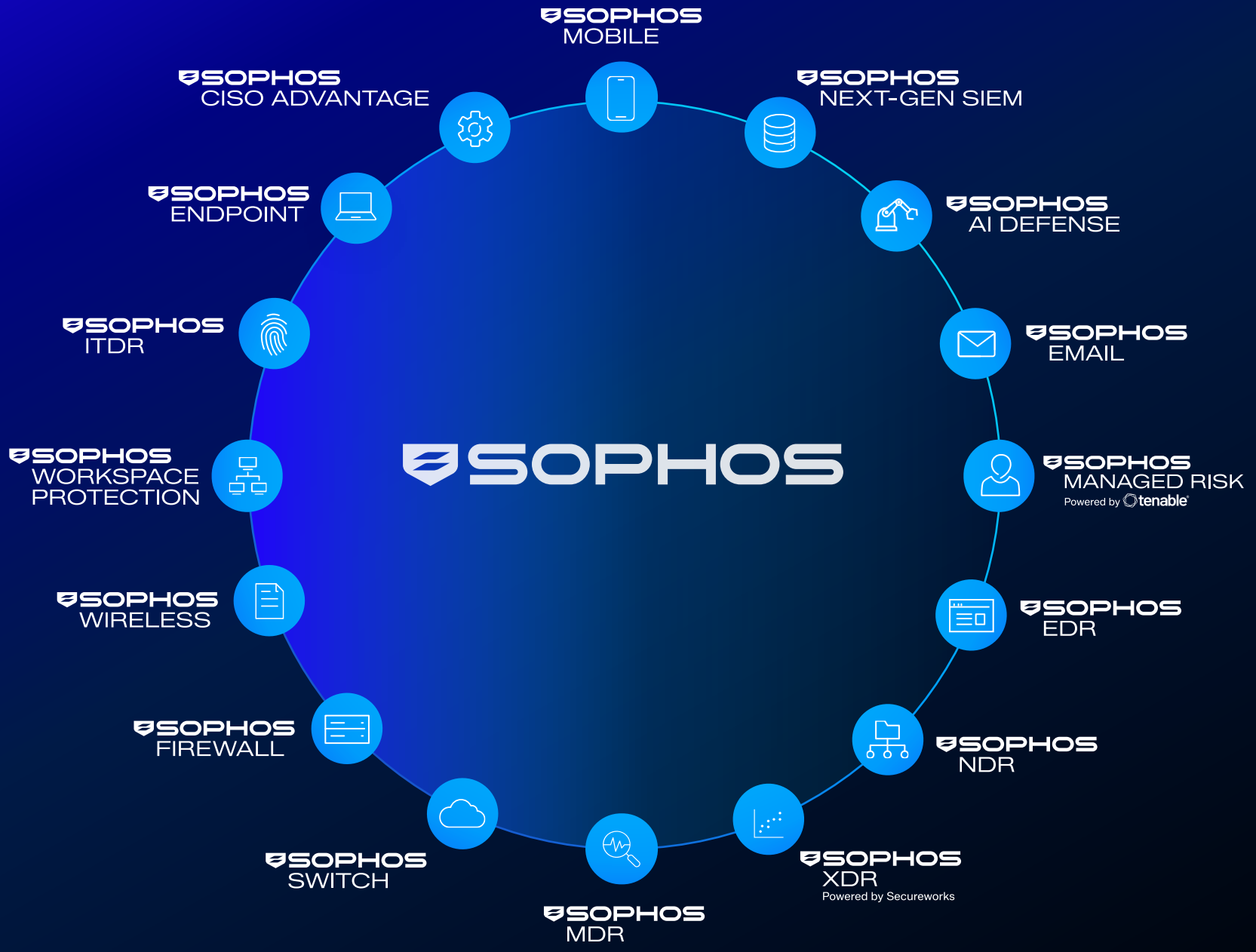
Der Lösungsweg

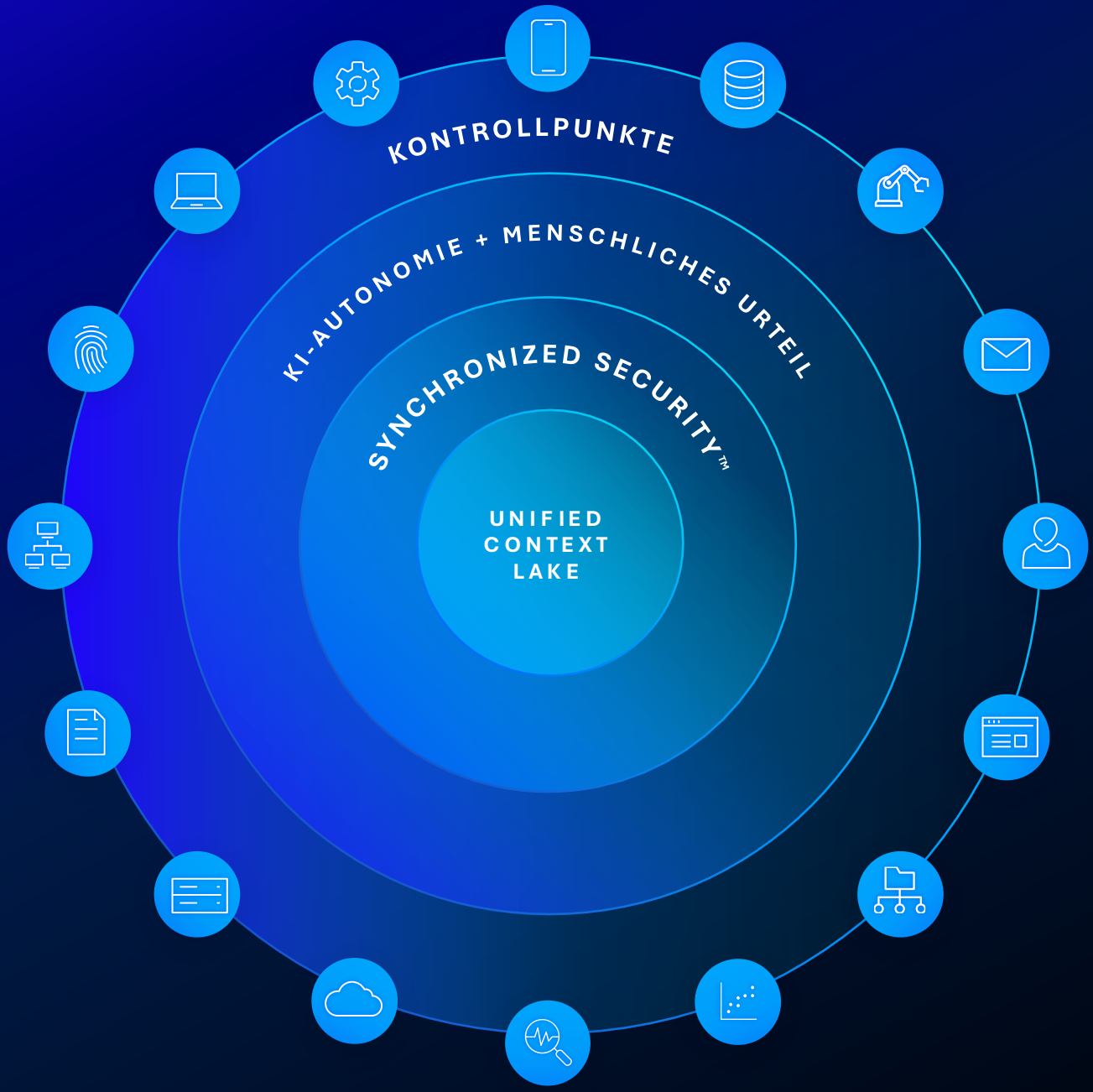
Drei Hebel machen Cybersecurity für Schulen beherrschbar.

Hebel 1: Ein System statt Tool-Wildwuchs

- Sophos Fusion agiert als System
- Über 500 Drittanbieter-Integrationen liefern Telemetrie – bestehende Lösungen bleiben nutzbar, ohne die Komplexität zu erhöhen.
- Schulträger verwalten die Sicherheit aller Schulen zentral in Sophos Fusion statt in vielen Einzelkonsolen.
- Ergebnis: weniger Administrationsaufwand, ein gemeinsames Lagebild und spürbare Entlastung für die IT.




SOPHOS
SOPHOS MOBILE
SOPHOS NEXT-GEN SIEM
SOPHOS AI DEFENSE
SOPHOS EMAIL
SOPHOS MANAGED RISK
Powered by tenable
SOPHOS EDR
SOPHOS NDR
SOPHOS XDR
Powered by Secureworks
SOPHOS MDR
SOPHOS SWITCH
SOPHOS FIREWALL
SOPHOS WIRELESS
SOPHOS WORKSPACE PROTECTION
SOPHOS ITDR
SOPHOS ENDPOINT
SOPHOS CISO ADVANTAGE



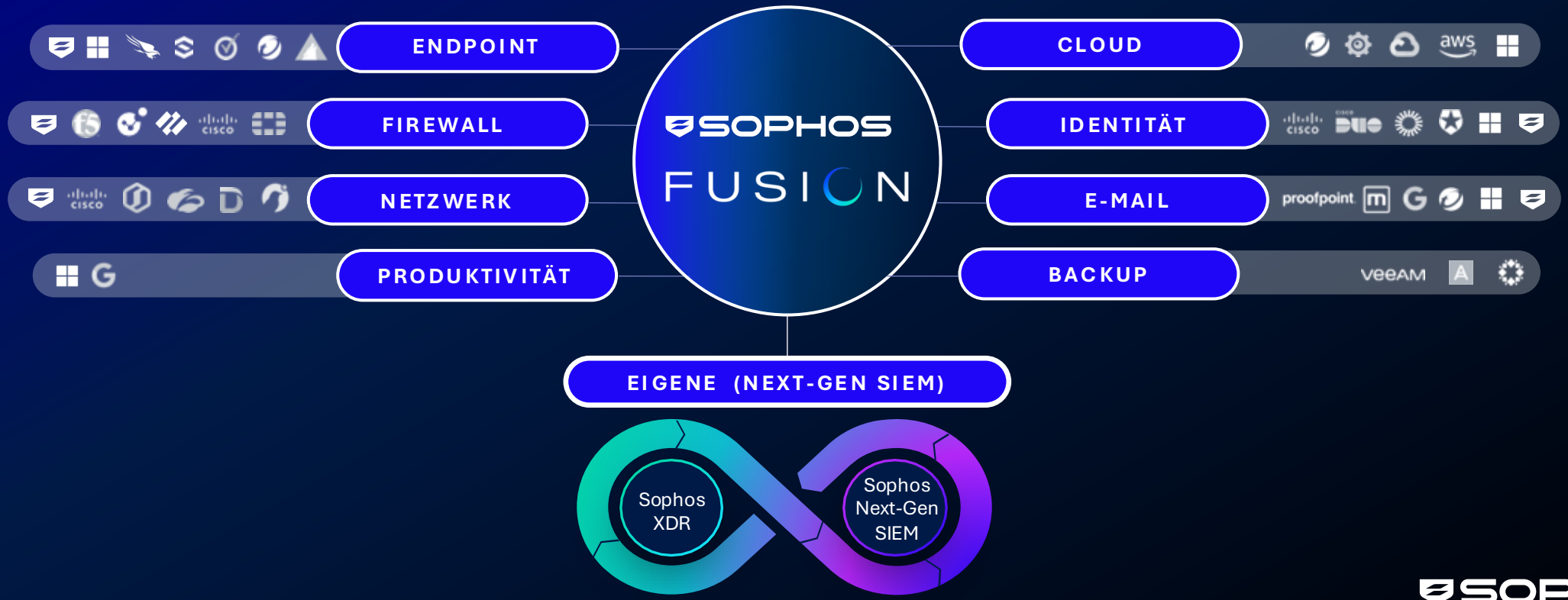
FUSION

AI-Native Cybersecurity Defense System

SOPHOS

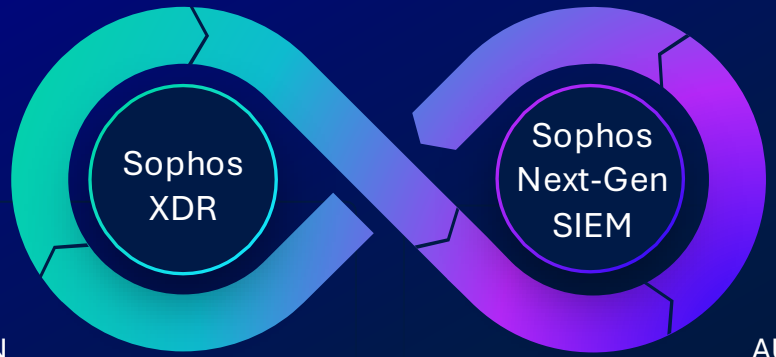
Offen konzipiert.

500+ Sicherheits- und IT-Integrationen



SOPHOS

Sophos XDR mit Next-Gen SIEM



SECURITY OPERATIONS

ERKENNUNG | UNTERSUCHUNG | REAKTION

- **Offenes, hersteller-unabhängiges System**
- **Überlegener integrierter Schutz**
- **Leistungsstarke Bedrohungserkennung und Reaktion**
- **KI-natives SOC**
- **Automatisierung (SOAR)**
- **Integrierte Threat Intelligence**

COMPLIANCE

AUFBEWAHRUNG | BERICHTE | NACHWEIS

- **Flexible Datenintegrationen**
- **Langzeitaufbewahrung bis 10 Jahre**
- **Planbare Kosten**
- **Security- und Compliance-Daten**

UNIFIED CONTEXT LAKE

SOPHOS

Sophos Fusion: alle Kontrollpunkte, eine Architektur

Endgeräte und Mobilgeräte	• Sophos Endpoint mit CryptoGuard stoppt Malware, Exploits und Verschlüsselung. Sophos Mobile verwaltet Tablets und Notebooks nach einheitlichen Richtlinien.
Netzwerk und WLAN	• Sophos Firewall segmentiert Netze, setzt Jugendschutzfilter um und bindet Standorte per RED Device an. Sophos Wireless sichert das Schul-WLAN.
E-Mail und Identitäten	• Sophos Email blockiert Phishing und schädliche Links. Sophos ITDR erkennt riskante Anmeldungen und den Missbrauch von Konten.
KI-Nutzung im Schulalltag	• Sophos AI Defense macht den Einsatz von KI sichtbar, steuert ihn über klare Regeln und unterbindet gefährliche KI-Aktivitäten.

SOPHOS

Hebel 2: Erkennung und Reaktion rund um die Uhr

- Sophos XDR führt Signale aus Endpoints, Netzwerk, Identitäten und Cloud zusammen und macht Angriffsmuster sichtbar.
- Sophos MDR übernimmt Monitoring, Untersuchung und Reaktion 24/7 – geliefert vom weltweit größten agentischen SOC.
- Agentische KI untersucht in Sekunden, erfahrene Analysten verantworten die Entscheidung und stoppen aktive Angriffe.
- Das kleine IT-Team wird entlastet: keine Nachtschichten, keine unbeachteten Alarme, klare Handlungsempfehlungen.



Wenn es ernst wird: die passende Eskalationsstufe

Sophos MDR

- 24/7 Überwachung durch erfahrene Security-Analysten
- Bedrohungen werden aktiv bekämpft, nicht nur gemeldet
- Nutzt bestehende Security-Tools oder Sophos-Technologie

Sophos MDR Plus

- Unbegrenzte Critical Incident Response durch das Sophos Incident-Response-Team bei schwerwiegenden Sicherheitsvorfällen.
- Dedizierte Unterstützung im Krisenfall, inklusive Incident-Response-Lead, Root-Cause-Analyse sowie Wiederherstellungs- und Remediation-Empfehlungen.
- Breach Protection Warranty mit finanzieller Absicherung für qualifizierte Kunden im Fall eines erfolgreichen Angriffs.

Sophos Digital Forensics and Incident Response (DFIR)

- Im Falle eines Cyber-Notfalls stellt Sophos DFIR funktionsübergreifende Experten zur Verfügung, die die aktive Bedrohung umgehend einstufen und stoppen, inkl. Empfehlungen wie das verhindert werden kann
- Ermittlung wie der Angreifer eingedrungen ist, und Empfehlung von Maßnahmen, um eine Wiederholung zu verhindern.

SOPHOS

Sophos MDR

625,000+
Sophos Kunden weltweit

50.000+
MDR Kunden

1.000+
Untersuchungen täglich abgeschlossen

200+
echte Angriffe täglich gestoppt
-> pro MDR Kunde Ø 1,8 pro Jahr

9 SOCs weltweit



Geprüft. Bewährt. Vertrauenswürdig.

- Gartner Peer Insights Customers' Choice 2024 — **Customers' Choice**
- MITRE ATT&CK® — **Top Performer**
- FROST & SULLIVAN — **Leader**
- Gartner Peer Insights™ — **Highest-Rated**
- Bundesamt für Sicherheit in der Informationstechnik — **qualifizierter APT-Responder**

Sophos MDR: Entlastung für Schulträger mit kleinen IT-Teams

24/7 Überwachung

Überwachung, Untersuchung und Reaktion rund um die Uhr, auch am Wochenende und in den Ferien.

Experten statt Zusatzaufgabe

Das weltweit größte agentenbasierte SOC übernimmt, was IT-affine Lehrkräfte nebenbei nicht leisten können.

Angriffskette früh unterbrechen

Identitäts-, Endpoint- und Netzwerksignale werden korreliert; Bedrohungen werden neutralisiert, bevor verschlüsselt wird.

Compliance im Blick

Next-Gen SIEM als Add-on: langfristige Datenaufbewahrung, Compliance-Berichte, eigene Integrationen.

Warum das zum Digitalpakt passt

Die Verwaltungsvereinbarung nennt Strukturen für professionelle Administration und Support sowie die Beauftragung externer Dienstleister ausdrücklich als förderfähig. Ein Managed Service adressiert genau die drei größten Engpässe der Umfrage: Geld, Zeit und Fachpersonal.

SOPHOS



Hebel 3: Schritt für Schritt statt alles auf einmal

- Nicht alle Maßnahmen gleichzeitig: klare Prioritäten verhindern Überforderung und halten das Projekt steuerbar.
- Starten Sie dort, wo die meisten Angriffe beginnen – bei Identitäten und E-Mail.
- Jede Stufe liefert einen sichtbaren Sicherheitsgewinn und lässt sich im Digitalpakt 2.0 als Vorhaben abbilden.
- Was das Team nicht selbst leisten kann, wird als Service eingekauft statt liegen gelassen.

SOPHOS

Die Roadmap für Schulen und Schulträger

Bestand aufnehmen	• Geräte, Netze, Cloud-Dienste und Zuständigkeiten erfassen. Schatten-IT sichtbar machen und Risiken dokumentiert bewerten.
Basis absichern	• Multi-Faktor-Authentifizierung, Endpoint-Schutz, E-Mail-Sicherheit und Netzsegmentierung zuerst – das deckt die häufigsten Einfallstore ab.
Überwachung übergeben	• MDR und XDR aktivieren, damit Erkennung und Reaktion rund um die Uhr laufen, ohne eigenes Schichtmodell.
Dauerhaft verankern	• Awareness mit Phish Threat, geprüfte Backups, ein eingeübter Notfallplan und eine jährliche Überprüfung der Wirksamkeit.

SOPHOS

Praxisbeispiele und Sophos-Lösungen für Schulen

Lösungsmatrix: Herausforderungen und Sophos-Bausteine

Herausforderung	Sophos-Lösung	Nutzen für Schulen und Schulträger
Zentrale Verwaltung der gesamten Sicherheitsinfrastruktur	**Sophos Fusion**	Alle Kontrollpunkte in einer Architektur, Abwehr als Einheit, weniger Aufwand für kleine Teams
Sichere Anbindung verteilter Schulstandorte	**Sophos Firewall + RED Devices**	Standorte ohne zusätzliche Administration sicher anbinden; Jugendschutzfilter per Benutzerrichtlinie
Netzwerk absichern und segmentieren	**Sophos Firewall, Sophos Endpoint**	Zero-Day Protection, Erkennung versteckter Malware, Segmentierung begrenzt laterale Bewegung
WLAN bereitstellen und absichern	**Sophos Wireless**	Flächendeckendes WLAN mit zentral gesteuerten Sicherheitsvorgaben aus Firewall und Sophos Central
Endgeräte und Tablets schützen	**Sophos Endpoint, Sophos Mobile**	EDR, CryptoGuard gegen Ransomware, einheitliche Richtlinien unabhängig von Gerätetyp und Besitzer
Phishing-Mails an Lehrkräfte und Verwaltung	**Sophos Email, ITDR, Phish Threat**	Phishing und Impersonation blocken, Identitätsrisiken erkennen, Lehrkräfte mit Simulationen sensibilisieren
Identitätsbezogene Risiken, 24/7-Reaktion	**Sophos ITDR, XDR, MDR**	Kompromittierte Konten erkennen, Signale korrelieren, Experten reagieren rund um die Uhr
Sichere Nutzung von KI-Tools im Schulalltag	**Sophos AI Defense**	KI-Nutzung erkennen, anhand eigener Vorgaben steuern, gefährliche KI-Aktivitäten unterbinden

Je nach Ausgestaltung des jeweiligen Länderprogramms können diese Maßnahmen im Rahmen des Digitalpakts 2.0 förderfähig sein.

SOPHOS

Die nächsten Schritte:

Sophos Fusion

Sicherheit im Zeitalter der KI

Verbindet Sicherheitslösungen, Daten und KI zu einem intelligenten Verteidigungssystem.

- Erkennt und stoppt Bedrohungen schneller
- Verknüpft Sophos- und Drittanbieter-Lösungen
- KI-gestützte Reaktion mit menschlicher Kontrolle

sophos.de/fusion

Sophos MDR

Managed Detection and Response rund um die Uhr

Das Sophos- Expertenteam überwacht Ihre Umgebung und stoppt Angriffe.

- 24/7 Überwachung durch erfahrene Security-Analysten
- Bedrohungen werden aktiv bekämpft, nicht nur gemeldet
- Nutzt bestehende Security-Tools oder Sophos-Technologie

sophos.de/mdr

AI Defense

Sichere Nutzung von KI im Unternehmen

Überblicken und kontrollieren Sie die KI-Nutzung in Ihrer gesamten Umgebung.

- KI-Aktivitäten überblicken
- KI-Nutzung kontrollieren
- KI-Risiko reduzieren
- KI-Bedrohungen stoppen

sophos.de/ai-defense

Kontakt

Wir sind für Sie da

Sie möchten eines der Themen vertiefen oder eine Demo sehen? Ihr Sophos-Ansprechpartner hilft Ihnen gerne weiter.

sophos.de/kontakt

SOPHOS


SOPHOS