LÖSUNGSBROSCHÜRE

Sophos Workspace Protection

Einfacher und kostengünstiger Schutz für Remote- und Hybrid-Mitarbeitende

Mit Sophos Workspace Protection erhalten Sie die Kontrolle über Ihre Geschäftsumgebung zurück: Gewähren Sie Mitarbeitenden und Gästen sicheren Zugriff auf Ihre Anwendungen und Daten – überall, einfach und kostengünstig.

Die Arbeitswelt hat sich verändert

Traditionelle Netzwerkgrenzen sind längst Geschichte. Mitarbeitende, Anwendungen und Daten befinden sich heute an vielen verschiedenen Orten. Unternehmen hosten und betreiben eigene, private Anwendungen oder nutzen SaaS-Anwendungen – und jeder verlässt sich täglich auf Anwendungen, Services und Websites im Internet. Zudem haben die meisten Unternehmen eine hybride Belegschaft aus Mitarbeitenden, die vor Ort sowie remote oder mobil arbeiten – im Büro, zu Hause, unterwegs oder auch in öffentlichen Umgebungen. Dies stellt Unternehmen vor die große Herausforderung, alles zuverlässig im Blick zu haben, zu kontrollieren und abzusichern.

Traditionelle cloudbasierte SASE- oder SSE-Lösungen haben sich als teuer im Betrieb erwiesen und sind daher oft keine sinnvolle Investition. Sie erfordern ein Backhauling des Datenverkehrs an cloudbasierte Zugangspunkte zur Überprüfung und Durchführung einer Man-in-the-Middle Entschlüsselung, was zu unerwünschter Latenz und Usability-Problemen führt. Hier bietet Sophos Workspace Protection eine bessere Lösung.

Effektiver Schutz für Anwendungen, Daten und Gäste

Sophos Workspace Protection bietet eine einfache und kostengünstige Lösung zum Schutz Ihrer Anwendungen, Daten, Mitarbeitenden und Gäste – überall. Der erforderliche Schutz wird komplett in eine einzige Anwendung – nämlich den Browser – integriert, sodass kein Backhauling von Datenverkehr, keine Cloud-Verarbeitung und keine zusätzliche Entschlüsselung mehr erforderlich sind.

Alle Komponenten auf einen Blick

Sophos Protected Browser

Bietet eine einzige Anwendung zum Schutz aller übrigen Anwendungen. ZTNA, DNS Protection, SaaS-Anwendungssteuerung, ein sicheres Web-Gateway und lokale Datenkontrollen sind in einen gehärteten Chromium-Browser integriert, der sich intuitiv bedienen lässt und vollkommen transparent arbeitet.

Sophos ZTNA

Ermöglicht einen sicheren Zugriff auf ausschließlich die Anwendungen, die Benutzer tatsächlich benötigen, und sorgt dafür, dass sie für andere Personen nicht sichtbar sind – auch nicht öffentlich. So bleiben die Anwendungen vor Angriffen geschützt.

Sophos DNS Protection für Endpoints

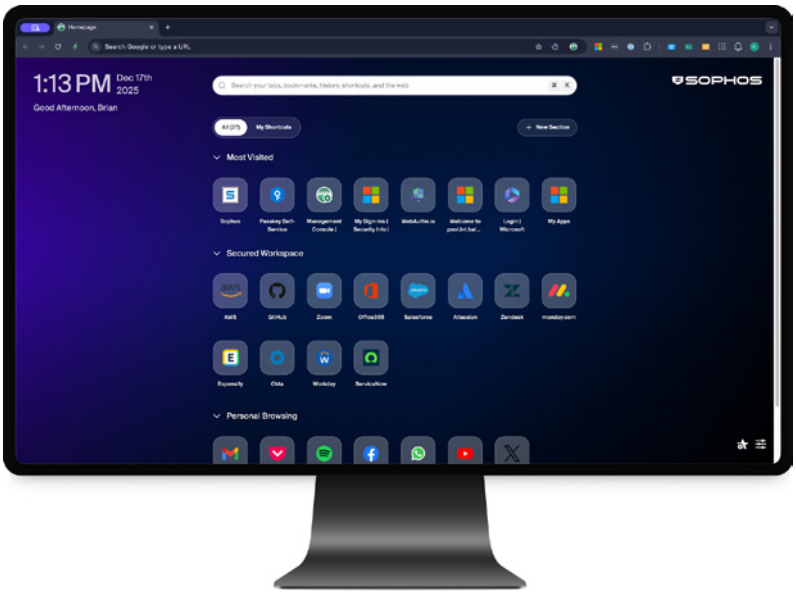
Bietet eine zusätzliche Schutzschicht gegen schädliche und unerwünschte Webinhalte, sowohl im Browser als auch für webfähige Anwendungen – egal, wo sich die Mitarbeitenden aufhalten.

Das Sophos Email Monitoring System

Ist mit Ihrer bestehenden E-Mail-Lösung kompatibel und optimiert die Sicherheit, Transparenz und Report-Erstellung für E-Mail-Bedrohungen, die andere Lösungen übersehen.

VORTEILE

- Schutz für Anwendungen, Daten, Mitarbeitende und Gäste
- Sicherer Anwendungszugriff und Schutz der Anwendungen vor Angriffen
- Beseitigen von Schatten-IT und sichere Nutzung neuer Technologien wie generative KI
- Schutz von Mitarbeitenden im Internet und Durchsetzen von Richtlinien für sicheres Surfen
- Sicherer temporärer Zugriff für Gäste sowie neues Personal im Rahmen von Fusionen/Übernahmen
- Ausweiten von Synchronized Security auf Remote- und Hybrid-Mitarbeitende
- Schutz vor Angriffen und Sicherheitslücken



Das bietet Sophos Workspace Protection

Beseitigen von Schatten-IT:
Überwachen und kontrollieren Sie die nicht genehmigte Nutzung von Web- und SaaS-Anwendungen.

Einfache Einführung generativer KI:
Fördern und überwachen Sie die Nutzung genehmigter KI-Lösungen, kontrollieren Sie den Zugriff und beschränken Sie den Datenfluss.

Online-Schutz für Mitarbeitende:
Ermöglichen Sie eine einheitliche Richtliniendurchsetzung für Webanwendungen und Zugriff von überall.

Vermeiden kostspieliger Datenfehler:
Blockieren Sie das Kopieren und Einfügen sowie den Austausch sensibler Daten mit Websites und Anwendungen, um Datenverluste zu verhindern.

Schutz für Anwendungen:
Gewähren Sie sicheren ZTNA-Zugriff auf Ihre eigenen gehosteten Anwendungen und verbergen Sie die Anwendungen vor der Außenwelt.

Sicherer Gastzugang:
Aktivieren Sie ganz einfach den sicheren Zugriff auf Ihre Anwendungen und Systeme für Gäste, externe Dienstleister oder Mitarbeitende nach einer Übernahme.

Synchronized Security:
Nutzen Sie Sophos Synchronized Security , um kompromittierte Geräte vorübergehend vom Zugriff auf wichtige Anwendungen und Systeme auszuschließen.

Schutz vor Kompromittierungen:
Schützen Sie Ihr Netzwerk vor potenziellen Kompromittierungen, die dadurch entstehen können, dass Systeme, Anwendungen und Mitarbeitende dem Internet ausgesetzt sind.

Bessere E-Mail Sicherheit:
Verbessern Sie Ihren E-Mail Sicherheitsstatus mit einer zusätzlichen Schutzschicht, die Ihre bestehenden Abwehrmechanismen ergänzt.

Einfach, kostengünstig, sicher

Sophos Workspace Protection ist einfacher und kostengünstiger als cloudbasierte SASE- oder SSE-Lösungen, erfordert weder Backhauling noch Man-in-the-Middle-Entschlüsselung und lässt sich einfach implementieren und skalieren. Sie erhalten eine einfache Anwendung, die Sie ohnehin benötigen – einen Browser –, der alle Ihre anderen Anwendungen schützt und über die zentrale Cloud-Konsole Sophos Central verwaltet wird. Sophos Protected Browser verwandelt einen bisherigen Sicherheitsschwachpunkt in einen wertvollen Sicherheitsvorteil.

Das Bindeglied für stärkeren und konsistenteren Firewall- und Endpoint-Schutz

Firewalls schützen Ihr Netzwerk, Endpoints schützen Ihre Geräte und Sophos Workspace Protection schützt alles andere: Ihre Anwendungen, Ihre Daten, Ihre Mitarbeitenden und Ihre Gäste. Sophos Workspace Protection vereinheitlicht und erweitert Ihren Netzwerk- und Endpoint-Schutz und optimiert so die Sicherheit Ihrer gesamten Arbeitsumgebung. Beim kombinierten Einsatz mit der Sophos Firewall und Sophos Endpoint weiten Sie den Synchronized Security Heartbeat zudem auf Ihre Remote- und Hybrid-Mitarbeitenden aus. Wenn ein Gerät kompromittiert ist, können Heartbeat-Richtlinien bis zu dessen Bereinigung verhindern, dass es sich mit wichtigen Anwendungen und Daten verbindet.

Einfache Lizenzierung – hervorragendes Preis-Leistungs-Verhältnis

Der Kauf von Sophos Workspace Protection könnte dank einfacher nutzerbasierter Lizenzierung und lukrativer Preisgestaltung nicht einfacher sein:

- **Standalone:** Kaufen Sie Sophos Workspace Protection als Standalone-Lösung und erhalten Sie alles inklusive: Sophos Protected Browser, Sophos ZTNA, Sophos DNS Protection für Endpoints und Sophos EMS, das mit jeder Firewall- und Endpoint-Lösung kompatibel ist.
- **Kauf mit Sophos Endpoint**: Erwerben Sie beide Produkte in einem praktischen Bundle und nutzen Sie alle Vorteile von Synchronized Security – bei gemeinsamer Verwaltung in Sophos Central.
- **Kauf mit der Sophos Firewall:** Weiten Sie Ihre Netzwerksicherheit auf Remote- und Hybrid-Mitarbeitende sowie Gäste aus, schützen Sie Ihre Anwendungen mit ZTNA und vieles mehr – komplett verwaltet über Sophos Central.

Sophos Workspace Protection ist die perfekte Ergänzung für jede bestehende oder neue Sophos-Installation.

Technische Spezifikationen

Die Produkte von Sophos Workspace Protection sind so konzipiert, dass sie sich nahtlos in Ihre bestehenden Umgebungen einfügen und mit gängigen Identitätsanbietern und Plattformen kompatibel sind.

Identitätsanbieter:

ZTNA- und Endpoint-DNS-Schutz:
Microsoft Active Directory (lokal), Microsoft Entra ID (Azure Active Directory), Okta

Protected Browser:
Microsoft Entra ID (Azure Active Directory), Okta

Betriebssysteme und Plattformen:

ZTNA Gateway:
VMware ESXi 7+, Hyper-V 2016+ und Sophos Firewall

ZTNA-Agent:
Windows 10, Windows 11 (Intel- und ARM-Prozessoren); macOS Sonoma, Sequoia, Tahoe (Intel- und Apple-Prozessoren)

Endpoint DNS Protection:
Windows 10, Windows 11 (Intel- und ARM-Prozessoren)

Protected Browser:
Windows 10, Windows 11, Windows Server 2022, Windows Server 2025 (nur Intel-Prozessoren – ARM folgt in Kürze); macOS Sonoma, Sequoia, Tahoe (Intel- und Apple-Prozessoren)

Gerätestatus:

ZTNA-Agent:
Sophos Security Heartbeat (Sophos Endpoint)

Protected Browser:
Status von Betriebssystem, Endpoint Protection (Sophos und andere Anbieter) und Festplattenverschlüsselung

ZTNA-Gateway – Spezifikationen

Empfohlene VM:
2 Core/4 GB

Multi-Knoten-Clustering:
VMs können mit bis zu 9 Knoten geclustert werden und die Sophos Firewall kann im HA-Modus bereitgestellt werden, um die Gateway-Performance, Kapazität und Geschäftskontinuität zu verbessern.

Knoten-Kapazität und -Skalierung:
10.000 Agent-Verbindungen für einen einzelnen Knoten, bis zu 90.000 Agent-Verbindungen in einem Cluster (max. 9 Knoten)

Mehr erfahren und kostenlos testen unter sophos.de/workspace-protection

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.:+49 611 5858 0
E-Mail: sales@sophos.com

2026-01-07 BR-DE (DD)