



MSP-WEBINAR

Sophos Firewall Hardware-as-a-Service (HWaaS)

22. Juli 2026

Ihre Referenten



Barbara Hudson

Global Product Marketing
Director, Sophos



Sascha Pfeiffer

Senior Director, Sales
Engineering, EMEA Central,
Sophos

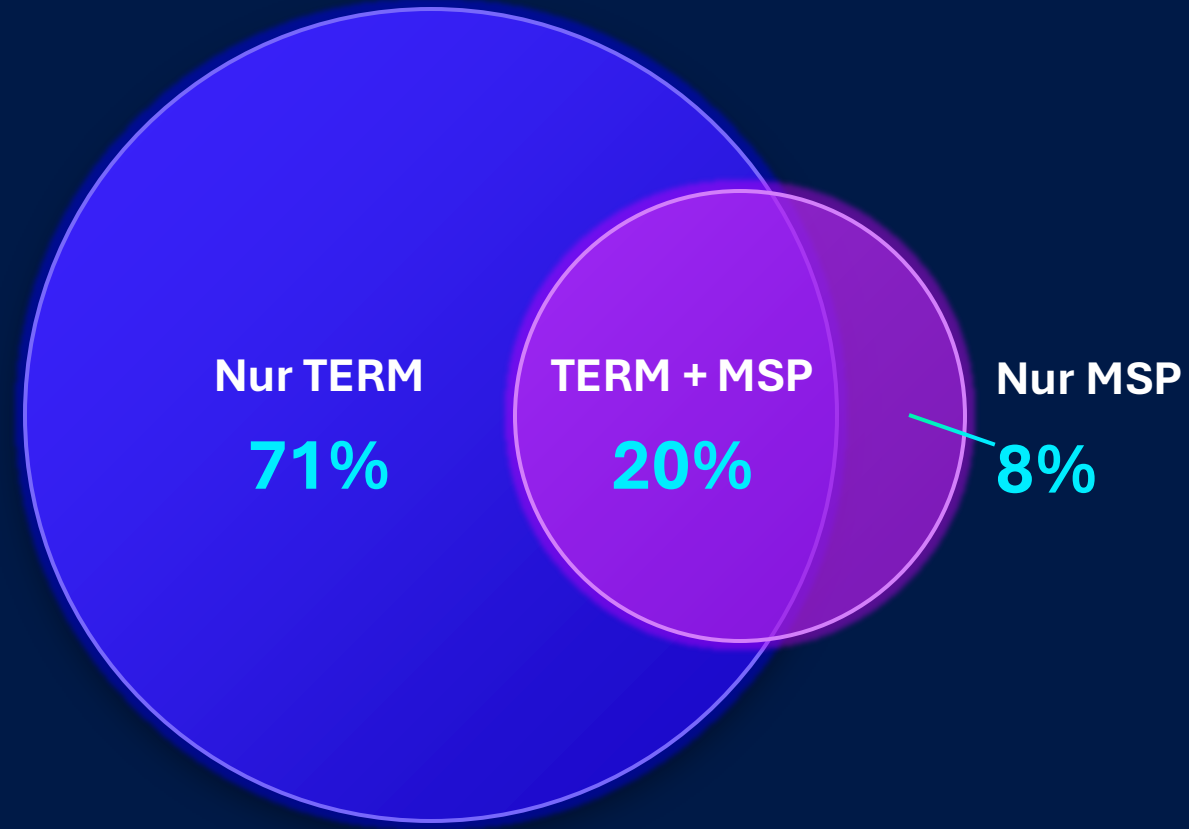
Am Ende dieser Session...

...werden Sie verstehen

- Warum Firewalls für die aktuelle Bedrohungslandschaft entwickelt sein müssen.
- Warum wir HWaaS einführen.
- Wie HWaaS Ihnen hilft, Ihr Geschäft auszubauen.
- Welche Kampagnen-Assets verfügbar sind, um Sie zu unterstützen.
- Was Ihre nächsten Schritte sein sollten.

Die Markt- und Partner-Landschaft

Die EMEA Partner-Landschaft (Alle Produkte)



Die ungenutzte Chance

DER BEWEIS IN UNSEREN DATEN

Vorabkosten lassen Umsatz liegen und begrenzen den Überblick für Ihre Kunden ein

3.800

MSP-Flex-Partner, die Sophos Firewall noch nicht nutzen

~200.000

Der von ihnen betreuten Endkunden nutzen keine Sophos Firewall

Nr. 1

Vorab-Hardwarekosten sind der häufigste Grund, warum Firewall-Deals ins Stocken geraten

Quelle: Interne Sophos-Daten

Sichtbarkeit muss alle Ebenen abdecken – diese Anforderung hilft Ihnen, diese Chance in Pipeline zu verwandeln ... mit HWaaS.

Die Bedrohungslandschaft

WARUM SICHERHEIT NICHT WARTEN KANN

18 % der Ransomware-Angriffe im Jahr 2025 begannen mit einer ausgenutzten Schwachstelle in der Firewall.

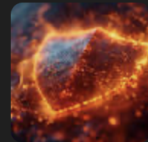
Quelle: Anbieterunabhängige Studie im Auftrag von Sophos

 SecurityWeek

Hundreds of FortiGate Firewalls Hacked in AI-Powered Attacks: AWS

Threat actors have been hacking FortiGate firewalls via exposed ports and weak credentials with the help of AI.

1 week ago



 GBHackers News

Hackers Launch Massive SonicWall Firewall Attack Using 4,000+ IP Addresses

Hackers are actively mapping SonicWall firewalls worldwide, launching more than 84000 SonicOS scanning sessions from over 4000 unique IP...

9 hours ago



 Cybersecurity Insiders

Ransomware attack makes customer file lawsuit against SonicWall Firewall Vulnerability

Explore how a ransomware attack led to a customer lawsuit over a SonicWall firewall vulnerability, what it means for security and steps to...

5 days ago



 CISO Series

Cybersecurity News: Australia BadCandy warning, Cisco firewall attack, Aardvark eats bugs

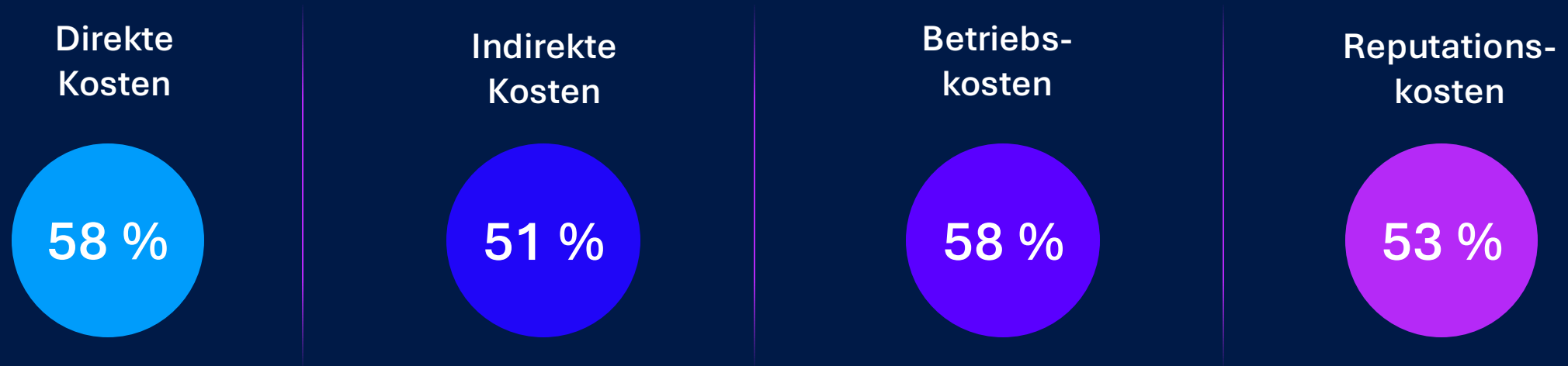
Australia warns of BADCANDY Attacks Exploiting Cisco IOS XE. The Australian Signals Directorate (ASD) is warning of cyber attacks targeting...

Nov 3, 2025



Medianzeit zwischen der Patch- oder Advisory-Veröffentlichung eines Anbieters und der Ausnutzung der Schwachstelle durch Angreifer: 322 Tage.

99 % der MSPs hatten Kosten aufgrund von Firewall-Schwachstellen



Quelle: Anbieterunabhängige Umfrage unter 700 MSPs in 7 Ländern, beauftragt von Sophos, durchgeführt im 1. Quartal 2026

HWaaS: Warum jetzt?

MARKTKONTEXT

Wie Kunden Firewalls kaufen, wird von drei Sachen beeinflusst



CAPEX bremst den Abschluss

Bestehende MSP-Kunden erwarten monatliche Preise. Vorab-Hardwarekosten verzögern Abschlüsse und erzeugen Cashflow-Risiken



Refresh-Zyklen entscheiden über den Erfolg

Hardware-Refresh-Zyklen und Wettbewerbsverlängerungen sind die Momente, in denen man gewinnt oder verliert



Nachfrage übersteigt Budgets

Vielen Kunden fehlt noch eine Next-Gen-Firewall, doch sie scheuen Investitionsausgaben

Für Kunden, die für andere Produkte und Lösungen bereits monatlich zahlen, können die Vorabkosten für eine Firewall-Appliance ein Dealbreaker sein.

Der Firewall-Markt heute

- Der Firewall-Markt ist derzeit sehr volatil.
- Die Preise steigen, entsprechend hoch ist der Preisdruck.
- Einige Wettbewerber verkürzen Preiszusagen; andere berechnen eine Gebühr für individuelle Preisangebote.
- Immer mehr Anbieter zielen auf SMB- und Mid-Market-Kunden.

Vertrauensvolle Partnerbeziehungen waren noch nie so wichtig.



Über HWaaS

Was ändert sich mit HWaaS?

DAS HWAAS-ERGEBNIS

Hardware-as-a-Service verwandelt die bisherigen Herausforderungen in Ihren Vorteil



Monatlich abrechnen. Verkaufen Sie so, wie Sie bereits abrechnen – über MSP Flex



Schneller abschließen. Keine CAPEX-Hürde für den Kunden



Frei skalieren. Firewalls bereitstellen, ohne Kapital zu binden



Wechsel-Business gewinnen. Wettbewerber schlagen, wenn der Preis das Hindernis ist

Das Ergebnis: Bekannter Vertriebsansatz, schnellere Abschlüsse und mehr Erfolg – aber ohne die CAPEX-Hürde





Sophos Firewall Hardware as a Service

Sophos Firewall (XGS)
über Sophos MSP Flex
erwerben

XGS 88 bis XGS 3300



Neues monatliches Hardware-Abrechnungsmodell
Sophos Firewall HWaaS bietet MSPs Zugang zu Firewalls ausschließlich über die monatliche MSP-Flex-Abrechnung



Für die Arbeitsweise von MSPs gemacht

Beseitigt Hürden bei Vorab-Capex, Cashflow-Belastung und Hardware-Risiko und erleichtert so Einführung und Skalierung



Voraussetzungen

Firewall HWaaS erfordert eine Mindestlaufzeit von 12 Monaten, bevor ein Wechsel auf eine monatliche Laufzeit möglich ist, und ist ausschließlich auf das HWaaS-Xstream-Protection-Bundle beschränkt



Was HWaaS NICHT ist

- Ein einmaliger Hardware-Investitionskauf
- Ein Leasing- oder Finanzierungsvertrag mit Dritten/Sophos
- Eine Änderung an Lizenzbezug/-verwaltung

Firewall-HWaaS – Umsetzungsüberblick

Vertraute Bestellabwicklung



- Bestellen Sie über Ihren Standard-Distributor mit demselben Prozess, den MSPs heute nutzen
- Marketplace-Bestellungen folgen dem Distributor-Workflow per E-Mail oder API
- HWaaS-SKUs sind ausschließlich für Flex
 - Nicht verfügbar für Term-Lizenzierung oder Angebotstools
 - Nicht berechtigt für aktuelle Promo-Codes oder Rabatte

Funktioniert wie heute, nur mit weniger Aufwand



- Die Aktivierung funktioniert wie gewohnt, mit automatischer Registrierung
- Nicht aktivierte Geräte werden nach 30 Tagen automatisch registriert
- HWaaS-Geräte sind nicht für Testversionen berechtigt
- Der Standard-RMA-Prozess gilt
- Nur das HWaaS-Xstream-Protection-Bundle wird unterstützt (keine anderen MSP Flex Optionen)
- Vollständig über Sophos Central verwaltbar

Verfügbarkeit



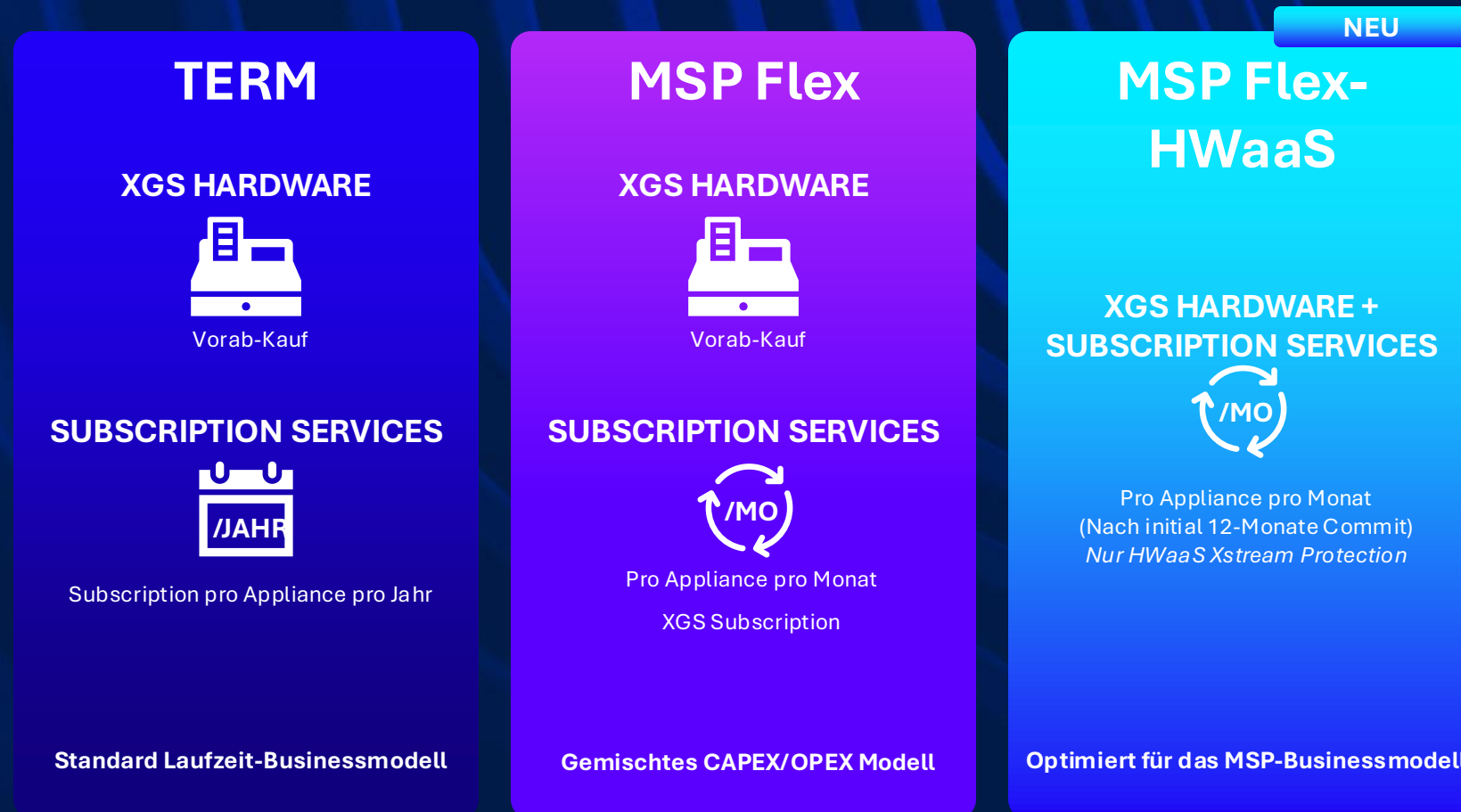
- Einführung in freigegebenen Ländern (siehe nächste Folie)
- Teilnehmende Distributoren ab 1. Juli 2026

Freigegebene Länder – Globale Abdeckung

- Länder, die Drop-Shipping ohne USt.-Anforderungen unterstützen

Amerika	EMEA				APJ
USA Kanada	West-EU	UKI	DACH	Ost-EU	Australien Indien Japan
	Belgien Zypern Frankreich Griechenland Italien Luxemburg Malta Niederlande Portugal Spanien	Vereinigtes Königreich Irland Isle of Man	Deutschland Österreich Schweiz	Bulgarien Kroatien Tschechien Estland Ungarn Lettland Litauen Polen Rumänien Slowenien	
		Nordeuropa			
		Dänemark Finnland Schweden			

SOPHOS FIREWALL Hardware Kauf- Optionen



Diskussion: Ihre Fragen bisher



Sophos Firewall: Entwickelt für den MSP-Betrieb im KI-Zeitalter

Sophos Firewall ist auf die Arbeitsweise von MSPs ausgelegt – nicht nur auf Firewall-Funktionen.

Firewall-Betrieb vereinfachen

- Eine Cloud-Konsole zur Verwaltung der Firewalls über alle Kunden hinweg
- Integriertes Reporting, Health-Checks und Logging auf jeder Appliance
- Keine Add-ons, keine Zusatztools, kein Wildwuchs an Konsolen

Notfalleinsätze vermeiden

- Over-the-Air-Hotfixes ohne Neustart
- Keine Wartungsfenster für kritische Sicherheitsprobleme
- Probleme werden in Maschinengeschwindigkeit gelöst, nicht im Technikertempo

Standardisieren in großem Maßstab

- Zero-Touch- und USB-Bereitstellung inklusive
- Hardware per Drop-Shipping, automatische Bereitstellung, schnelles Go-Live
- Konsistente Konfigurationen über Kunden und Standorte hinweg

Secure by Design ist das Fundament, das Vereinfachung, Effizienz und Standardisierung für MSPs möglich macht – damit Sie besser skalieren können.

Zusammenfassung

HWaaS-Zusammenfassung: So hilft es Ihnen



Firewall-Wechsel

BESTEHENDE FIREWALLS DER
KUNDEN DURCH SOPHOS ERSETZEN



Cross-Sell erhöhen

FIREWALLS BEI KUNDEN MIT SOPHOS
ENDPOINT ODER SOPHOS MDR
INSTALLIEREN



Neukundengewinnung

NEUE KUNDEN GEWINNEN, DIE
ÜBERLEGENE ABWEHR IM KI-
ZEITALTER BENÖTIGEN

**HWaaS hilft Ihnen, neue Kunden zu gewinnen sowie das Geschäft mit Bestandskunden auszubauen.
Sophos Firewall ist Secure by Design und schützt Ihre Kunden im KI-Zeitalter.**

Nächste Schritte: Sophos Firewall Kampagnen-Ressourcen

Vielfältige Ressourcen inklusive:

- Sophos Academy Learning
- Desk aids
- Battlecards
- Sizing Guide
- Config Studio (inkl. Migrations-Tools)
- Migrations-Guide
- Wettbewerbs-Webseiten
- MSP Transition Playbook
 - On-demand Webinar

