BROCHURE DELLA SOLUZIONE

Sophos Workspace Protection

Protezione semplice e conveniente per i dipendenti remoti e ibridi

Sophos Workspace Protection ti aiuta a riprendere il controllo dello spazio di lavoro della tua azienda. Offre accesso sicuro ad app, dati, dipendenti e utenti guest da qualsiasi luogo e con la massima praticità e convenienza.

L'evoluzione delle dinamiche lavorative

Il perimetro di rete non esiste più. Dipendenti, app e dati sono ovunque. Utilizzi applicazioni private di tua proprietà e ospitate nella tua rete interna, oppure applicazioni SaaS su abbonamento e tutti gli utenti si servono di applicazioni, servizi e siti su Internet di cui non possono fare a meno per svolgere il loro lavoro ogni giorno. Inoltre, la maggior parte delle organizzazioni è composta da una forza lavoro ibrida, con dipendenti che lavorano on-premise e in smart working, nonché team che operano in mobilità e che possono trovarsi in ufficio, a casa, in viaggio o persino in spazi pubblici. Tutto ciò rappresenta un'enorme sfida per qualsiasi azienda che desideri monitorare, controllare e proteggere adeguatamente i propri dati.

Le tradizionali soluzioni SASE o SSE fornite tramite cloud hanno dimostrato di essere onerose, che si traducono in un prezzo d'acquisto elevato. Richiedono il backhaul verso Point of Presence nel cloud per eseguire l'ispezione del traffico, nonché la decrittografia man-in-the-middle, che aggiunge latenza indesiderata e compromette la praticità d'uso. Deve esserci un'alternativa migliore. Fortunatamente esiste, e si chiama Sophos Workspace Protection.

Proteggi app, dati, processi e utenti guest

Sophos Workspace Protection offre una soluzione semplice e conveniente per proteggere app, dati, dipendenti e utenti guest, ovunque si trovino. Utilizza un'unica app, ovvero il browser, per integrare tutta la protezione di cui hai bisogno. Di conseguenza, non si rende necessario alcun backhaul del traffico, alcuna elaborazione nel cloud e alcuna decrittografia aggiuntiva: solo un'esperienza trasparente e sicura.

Cosa è incluso

Sophos Protected Browser

Offre un'unica app per garantire la sicurezza di tutte le altre Include ZTNA, DNS Protection, controlli delle app SaaS, un gateway web sicuro e controlli dei dati locali integrati in un browser Chromium dotato di protezione avanzata, per un'esperienza utente familiare e massima trasparenza.

Sophos ZTNA

Garantisce accesso sicuro solo alle applicazioni essenziali per gli utenti, rendendole invisibili a chiunque altro (incluso il mondo esterno) e proteggendole dagli attacchi.

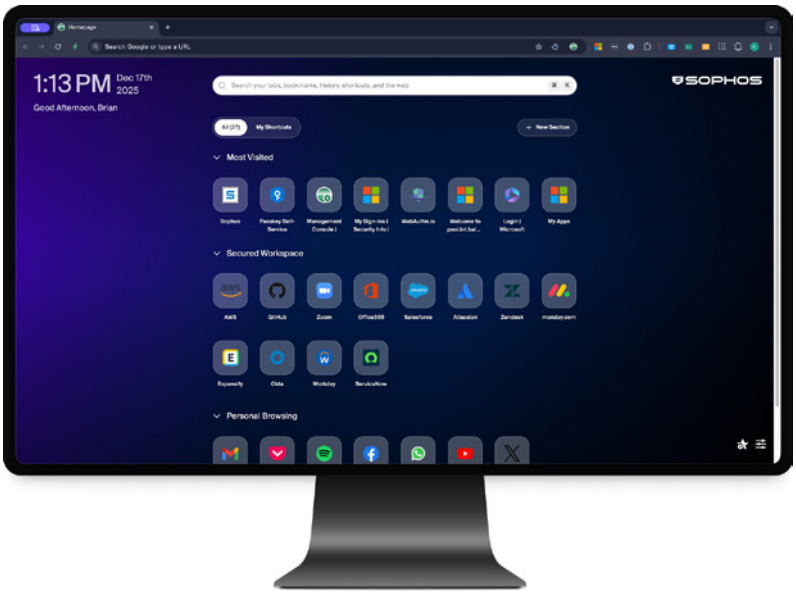
Sophos DNS Protection for Endpoints

Aggiunge un ulteriore livello di sicurezza contro contenuti web dannosi e indesiderati, sia nel browser che nelle applicazioni abilitate al web, proteggendo i tuoi dipendenti ovunque si trovino.

VANTAGGI

- Proteggi app, dati, dipendenti e utenti guest.
- Concedi accesso sicuro alle tue app, difendendole dagli attacchi.
- Elimina lo shadow IT e adotta in tutta sicurezza nuove tecnologie come l'IA generativa.
- Tutela i lavoratori sul web e implementa policy di navigazione sicura.
- Proteggi facilmente utenti guest, team coinvolti in fusioni e acquisizioni o chiunque richieda accesso provvisorio.
- Estendi la Synchronized Security per includere anche i dipendenti remoti e ibridi.
- Proteggi i sistemi contro attacchi e violazioni

SOPHOS



Sophos Email Monitoring System

Viene utilizzato in combinazione con la tua soluzione di posta elettronica già esistente per potenziare la sicurezza, la visibilità e la reportistica sulle minacce e-mail più avanzate, che riescono a sfuggire alle altre soluzioni.

Cosa offre Sophos Workspace Protection

Elimina lo shadow IT:
Monitora e controlla l'uso non autorizzato del web e delle applicazioni SaaS.

Abilita l'adozione dell'IA generativa:
Permette di promuovere e monitorare la tua soluzione di IA autorizzata, nonché di controllare gli accessi e limitare il trasferimento di dati.

Tutela i tuoi dipendenti sul web:
Applica criteri coerenti per le app web e l'accesso, indipendentemente dalla piattaforma o dalla località.

Evita i costi esosi associati alla perdita dei dati:
Blocca la funzionalità di copia e incolla o lo scambio di dati di natura sensibile con siti web e app, per prevenire la fuga accidentale di dati.

Protegge le tue app:
Offre accesso sicuro alle tue applicazioni in hosting, rendendole invisibili agli utenti esterni.

Abilita l'accesso protetto per gli utenti guest:
Semplifica l'accesso alle tue app e ai tuoi sistemi per utenti guest, collaboratori esterni o personale coinvolto nelle acquisizioni.

Estende la Synchronized Security:
Utilizza Sophos Synchronized Security per bloccare temporaneamente i dispositivi compromessi e impedire che accedano ad app e sistemi critici.

Difende dalle violazioni:
Protegge la tua rete da potenziali tentativi di violazione che potrebbero derivare da sistemi, app e dipendenti connessi a Internet.

Migliora la sicurezza delle tue e-mail:
Ottimizza il profilo di sicurezza della tua posta elettronica con un livello aggiuntivo di protezione che estende l'efficacia dei sistemi di difesa che già usi.

Una soluzione facile, conveniente e sicura

Sophos Workspace Protection è più semplice e conveniente rispetto alle soluzioni SASE o SSE fornite tramite cloud. Inoltre, non richiede backhaul o decrittografia man-in-the-middle, è facile da distribuire e offre un'ottima scalabilità. Quello che ottieni è un'app pratica e trasparente che useresti comunque (un browser) e che protegge inoltre tutte le altre tue app, con un sistema gestito interamente da un'unica console basata sul cloud: Sophos Central. Sophos Protected Browser trasforma un punto debole in una risorsa di sicurezza avanzata.

Unifica ed estendi la portata del firewall e della protezione endpoint

I firewall difendono la tua rete, gli endpoint garantiscono la sicurezza dei tuoi dispositivi e Sophos Workspace Protection protegge tutto il resto: app, dati, dipendenti e utenti guest. Unifica ed estendi la portata della tua protezione della rete e degli endpoint per mettere in sicurezza l'area di lavoro. Puoi sfruttarne la massima efficacia utilizzandola insieme a Sophos Firewall e Sophos Endpoint, per rendere disponibile il Synchronized Security Heartbeat anche ai dipendenti remoti e ibridi. In caso di compromissione, le policy di Heartbeat possono impedire a un dispositivo di connettersi ad applicazioni e dati importanti, fino a quando non torna a uno stato sicuro.

Licenze semplici, ottimo rapporto qualità-prezzo

Acquistare Sophos Workspace Protection non potrebbe essere più semplice, grazie alla semplicissima struttura di licensing basata sul numero di utenti e ai prezzi estremamente vantaggiosi:

- **Soluzione autonoma:** acquista la versionestand-alone di Sophos Workspace Protection e ottieni tutte le funzionalità, inclusi Sophos Protected Browser, Sophos ZTNA, Sophos DNS Protection for Endpoints e Sophos EMS, con perfetta compatibilità con qualsiasi soluzione firewall o endpoint.
- **Acquistala insieme a Sophos Endpoint**: con un comodo bundle per semplificare l'accesso a entrambi i prodotti e sfruttarne appieno il potenziale insieme a Synchronized Security, gestendo tutti i componenti da Sophos Central.
- **Acquistala insieme a Sophos Firewall:** estendi la sicurezza della tua rete per includere anche dipendenti remoti, ibridi e utenti guest; puoi anche proteggere le tue app con ZTNA e molto di più, in un ecosistema interamente gestito da Sophos Central.

Sophos Workspace Protection è la scelta ideale per ottimizzare qualsiasi installazione Sophos nuova o già esistente.

Specifiche tecniche

I prodotti Sophos Workspace Protection sono progettati per integrarsi perfettamente nei tuoi ambienti attuali, in quanto si integrano perfettamente con i principali provider di identità e le piattaforme più diffuse.

Provider di identità:

ZTNA e DNS Protection per Endpoint:
Microsoft Active Directory (on-premise), Microsoft Entra ID (Azure Active Directory), Okta

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

Sistemi operativi e piattaforme:

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

Agente ZTNA:
Windows 10, Windows 11 (processori Intel e ARM); macOS Sonoma, Sequoia, Tahoe (processori Intel e Apple)

DNS Protection per Endpoint:
Windows 10, Windows 11 (processori Intel e ARM)

Browser protetto:
Windows 10, Windows 11, Windows Server 2022, Windows Server 2025 (solo processori Intel; ARM presto disponibile); macOS Sonoma, Sequoia, Tahoe (processori Intel e Apple)

Profilo di sicurezza del dispositivo:

Agente ZTNA:
Sophos Security Heartbeat (Sophos Endpoint)

Browser protetto:
Sistema operativo, protezione endpoint (Sophos e altri produttori) e stato di crittografia del disco

Specifiche per il gateway ZTNA

VM consigliata:
2 core/4 GB

Cluster a più nodi:
Le VM possono essere raggruppate in cluster con un massimo di 9 nodi e Sophos Firewall può essere distribuito in disponibilità elevata per migliorare la capacità, la continuità operativa e la performance del gateway

Capacità e scalabilità dei nodi:
10.000 connessioni agent per un singolo nodo, fino a 90.000 connessioni agent in un cluster (max 9 nodi)

Per saperne di più e per iniziare una prova gratuita, visita: sophos.com/workspace-protection

Vendite per Italia:
Tel: (+39) 02 94 75 98 00
Email: sales@sophos.it

2026-01-07 BR-IT (DD)