SOLUTION BROCHURE

Sophos Workspace Protection

Easy, affordable protection for remote and hybrid workers

Sophos Workspace Protection enables you to take back control of your business workspace. Secure access to your apps, your data, your workers, and your guests – everywhere, easily, and affordably.

How people work has changed

The network perimeter has disappeared. Workers, apps, and data are everywhere. You have private applications you own and host or SaaS applications you rent, and everyone has applications, services and sites on the Internet they depend on daily. Most organizations also have a hybrid workforce of on-premise and remote or mobile workers who may be in the office, at home, on the road, even working in public spaces. This all adds up to an incredible challenge for any organization to properly monitor, control, and secure.

Traditional cloud-delivered SASE or SSE solutions have proven to be expensive to operate and therefore expensive to buy. They require backhauling traffic to cloud-based points of presence for inspection, and doing man-in-the-middle decryption which adds unwanted latency and creates usability issues. There has to be a better way. Fortunately there is — Sophos Workspace Protection.

Protect your apps, data, works, and guests

Sophos Workspace Protection provides an easy and affordable solution for protecting your apps, data, workers, and guests — everywhere. It utilizes a single app, the browser, to integrate all the protection you need so there's no backhauling of traffic, no cloud processing, no added decryption — just a transparent and secure experience.

What you get

Sophos Protected Browser

Provides a single app to protect all your other apps. It integrates ZTNA, DNS protection, SaaS app controls, a secure web gateway, and local data controls into a hardened Chromium browser that feels familiar and is fully transparent.

Sophos ZTNA

Provides secure access to only the applications that users need, while making them invisible to everyone else—including the outside world—protecting them from attack.

Sophos DNS Protection for Endpoints

Adds an extra layer of security to protect against malicious and unwanted web content both in the browser and for web-enabled applications wherever workers go.

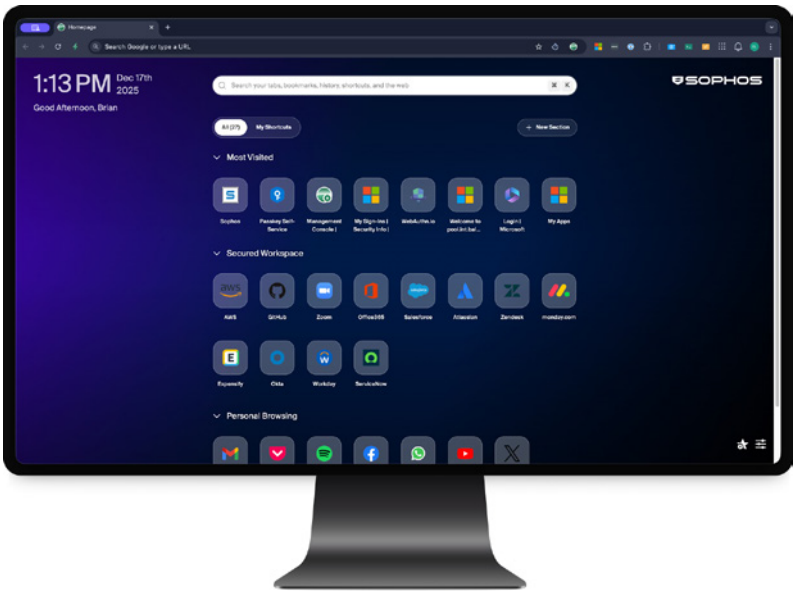
The Sophos Email Monitoring System

Works with your existing email solution to enhance security, visibility, and reporting into advanced email threats that other solutions miss.

BENEFITS

- Protect your apps, data, workers, and guests.
- Enable secure access to your apps while securing them from attacks.
- Eliminate shadow IT and safely embrace new technologies like Generative AI.
- Protect workers on the web and enforce safe browsing policies.
- Easily secure guests, M&A staff, or anyone else who needs temporary access.
- Extend Synchronized Security to remote and hybrid workers.
- Protect against attacks and breaches

SOPHOS



What Sophos Workspace Protection delivers

Eliminate shadow IT:
Monitor and control unsanctioned web and SaaS application usage.

Enable generative AI adoption:
Promote and monitor your sanctioned AI solution, control access, and restrict data movement.

Protect workers on the web:
Enable consistent policy enforcement for web apps and access everywhere.

Prevent costly data mistakes:
Block copy and paste or the exchange of sensitive data with websites and apps to prevent data leakage mistakes.

Protect your apps:
Provide secure access to your own hosted applications while making them invisible to the outside world

Secure guest access:
Easily enable access to your apps and systems for guests, contractors, or acquisition staff

Extend Synchronized Security:
Utilize Sophos Synchronized Security to temporarily block compromised devices from accessing important apps and systems

Protect against breaches:
Protect your network from potential breaches that can arise from systems, apps, and workers being exposed to the Internet

Enhance your email security:
Enhance your email security posture with an extra layer of security that complements your existing defenses

Easy, Affordable, Secure

Sophos Workspace Protection is easier and more affordable than cloud-delivered SASE or SSE solutions, doesn't require back-hauling or man-in-the-middle decryption, and is easy to deploy and scale. You get a simple app you already need — a browser — that protects all your other apps, all managed from a single cloud console: Sophos Central. Sophos Protected Browser turns what has been a security liability into a hardened security asset.

Unify and extend your firewall and endpoint protection

Firewalls protect your network, endpoints protect your devices, and Sophos Workspace Protection protects everything else: your apps, your data, your workers, and your guests. It unifies and extends your network and endpoint protection to secure the workspace. It also works better together with Sophos Firewall and Sophos Endpoint by extending Synchronized Security Heartbeat to your remote and hybrid workers. If a device is compromised Heartbeat policies can prevent it from connecting to important applications and data until it's cleaned up.

Simple licensing — great value

Buying Sophos Workspace Protection couldn't be easier with simple user-based licensing and attractive pricing:

- **Stand-alone:** Buy Sophos Workspace Protection stand-alone and get everything including Sophos Protected Browser, Sophos ZTNA, Sophos DNS Protection for Endpoints, and Sophos EMS that works with any firewall or endpoint solution.
- **Buy together with Sophos Endpoint**: with a convenient bundle for simpler purchasing of both products that work better together with Synchronized Security – both managed from Sophos Central.
- **Buy together with Sophos Firewall:** extend your network security to remote and hybrid workers and guests, protect your apps with ZTNA, and more – all managed from Sophos Central.

Sophos Workspace Protection is the perfect enhancement to any existing or new Sophos installation.

Technical specifications

Sophos Workspace Protection products are designed to fit seamlessly into your existing environments, integrating with the most popular identity providers and platforms.

Identity providers:

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

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

Operating systems and platforms:

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

ZTNA Agent:
Windows 10, Windows 11 (Intel and ARM processors); macOS Sonoma, Sequoia, Tahoe (Intel and Apple processors)

Endpoint DNS Protection:
Windows 10, Windows 11(Intel and ARM processors)

Protected browser:
Windows 10, Windows 11, Windows Server 2022, Windows Server 2025, (Intel processors only — ARM coming soon); macOS Sonoma, Sequoia, Tahoe (Intel and Apple processors)

Device posture:

ZTNA Agent:
Sophos Security Heartbeat (Sophos Endpoint)

Protected browser:
OS, Endpoint Protection (Sophos and other vendors), and Disk Encryption status

ZTNA gateway specifications

Recommended VM:
2 Core/4GB

Multi-node clustering:
VMs can be clustered with up to 9 nodes and Sophos Firewall can be deployed in HA for added gateway performance, capacity, and business continuity

Node capacity and scaling:
10,000 agent connections for a single node, up to 90,000 agent connections in a cluster (max. 9 nodes)

Learn more and start your free trial at sophos.com/workspace-protection

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

© Copyright 2026. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2026-01-07 BR-EN (DD)