DATASHEET

Sophos ZTNA

Sophos ZTNA is being integrated into Sophos Workspace Protection, with standalone availability ending in late April/early May 2026. For more information, visit sophos.com/workspace-protection.

Securely connect anyone, anywhere, to any application. Sophos ZTNA transparently connects users to important business applications and data, providing enhanced segmentation, security, and visibility over traditional remote access VPN.

Regain trust in a world of zero trust

Sophos ZTNA delivers on the principles of zero trust: trust nothing, verify everything. Individual users and devices become their own micro-segmented perimeter that are constantly validated and verified. They are no longer "on the network" with all the implied trust and access that usually comes with it. Trust is now earned – not given.

Enable remote workers

Sophos ZTNA enables your remote workers to securely and seamlessly access the applications and data they need while making deployment, enrollment, and management much easier than traditional VPN.

Micro-segment your applications

Sophos ZTNA provides the ultimate micro-segmentation so you can deliver secure application access whether your applications are hosted on premises, in a data center, or in your public cloud infrastructure. You also get real-time visibility into application activity for status, security posture, and usage. Control access to many SaaS applications with Sophos ZTNA using IP address restrictions to only allow connections from your ZTNA gateways.

Stop ransomware and threats

The possibility for ransomware and other threats to propagate across the network from a compromised user device is no longer a concern with ZTNA. Users and devices only have explicit policy-based access to specific applications. This eliminates the implied trust and broad network access that is one of the key challenges with VPN.

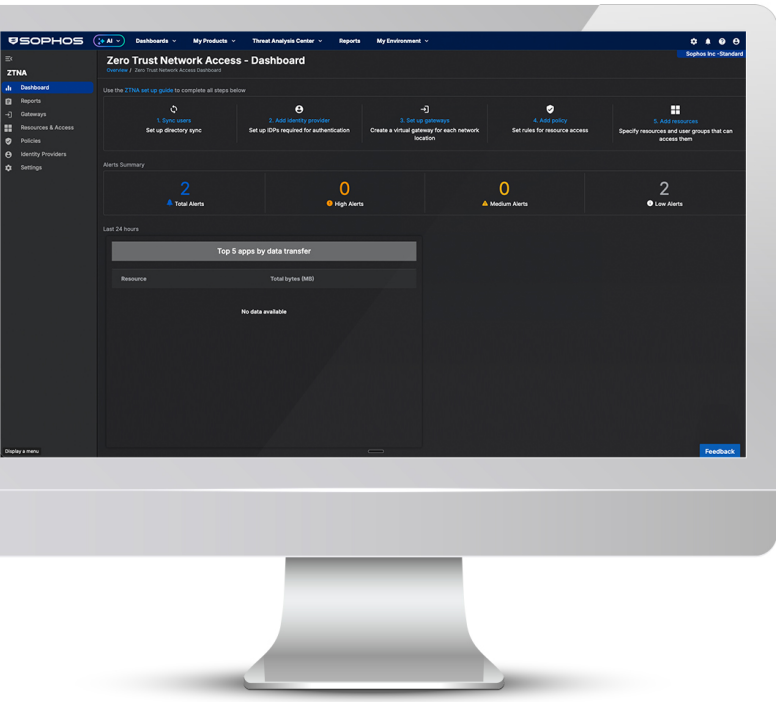
Deploy, adapt, and scale quickly

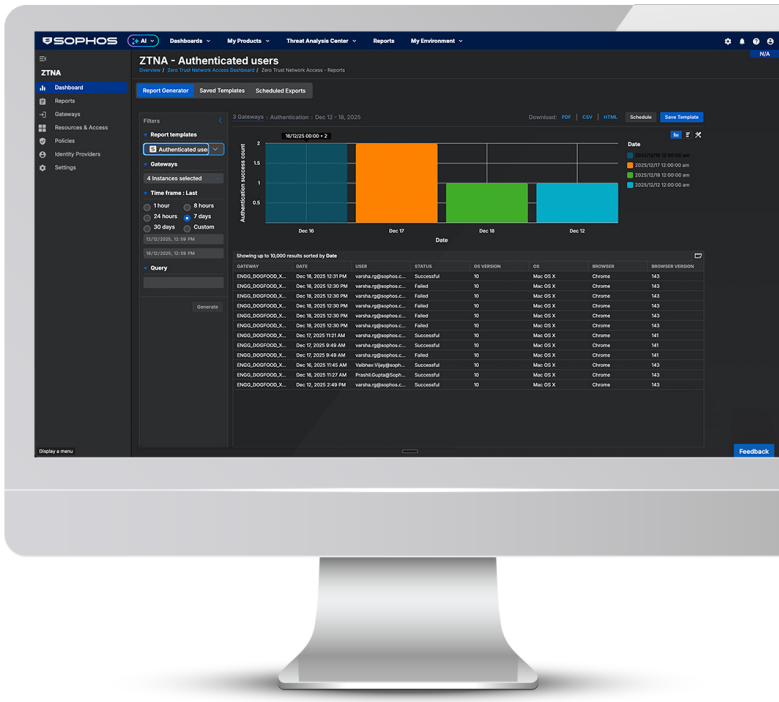
Sophos ZTNA is built for the modern network that is dynamically changing, rapidly growing, and moving quickly to the cloud. It is a lean, clean solution that makes it quick and easy to stand up new applications securely, enroll or decommission users and devices, and get important insights into application status and usage.

Highlights

- Zero trust: trust nothing, verify everything.
- Integrated across Sophos Firewall, Endpoint, and Sophos Workspace Protection.
- Gateway built into Sophos Firewall.
- The ultimate remote-access VPN replacement.
- Micro-segment and secure your network applications.
- Works anywhere, on the network or off.
- Rich RDP and SSH client in Sophos Protected Browser.
- Transparent for end users.
- Superior visibility and insights into your applications.
- Integrates Synchronized Security device health into access policies.

SOPHOS





Sophos Central Management

Sophos ZTNA has been designed from the start to make zero trust network access easy, integrated, and secure. Sophos ZTNA is cloud-delivered and cloud-managed, and integrated into Sophos Central, the world's most trusted cybersecurity cloud management and reporting platform.

Sophos Central provides a single convenient and easy to use console for all your day-to-day cybersecurity management. Manage your entire Workspace Protection suite including ZTNA, Protected Browser, DNS, and more — alongside your Sophos Firewalls and Endpoints - anywhere, anytime, from any device.

Part of Sophos Workspace Protection

Sophos ZTNA is a key part of Sophos Workspace Protection that also includes Sophos Protected Browser, DNS Protection for Endpoints, and our Email Monitoring System. Together, Sophos Workspace Protection provides an affordable and easy solution for protecting your apps, data, workers, and guests.

Uniquely integrated with Sophos Workspace, Firewall, and Endpoint

Sophos ZTNA is built-in and tightly integrated with the rest of the Sophos Platform to make deployment and management as easy as possible.

- Sophos Protected Browser: A rich RDP and SSH ZTNA client is built into the Sophos Protected Browser for easy and secure access to remote systems.
- Sophos Endpoint: ZTNA is tightly integrated with Sophos Endpoint to obtain device posture and health status including Synchronized Security Heartbeat status for controlling access if a device becomes compromised.
- Sophos Firewall: A ZTNA gateway is built in to every Sophos Firewall greatly simplifying deployment and enabling secure access to your on-premise applications by remote or hybrid workers.

Scalable application gateways

A Sophos ZTNA gateway is built-in to every Sophos Firewall making deployment easy. If you need additional gateways on-premise or in the cloud, they are free and easy to deploy as a virtual appliance. You can also deploy high-availability gateways if needed, and scale them as your organization grows.

Synchronized device health

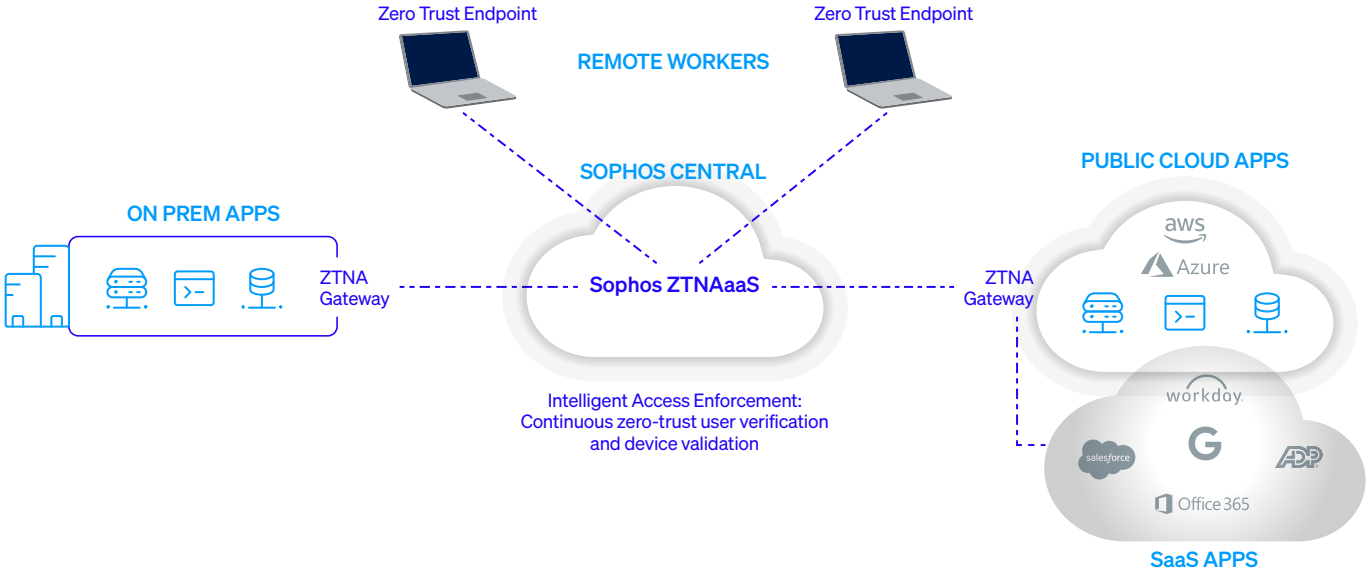
Sophos ZTNA takes full advantage of Sophos Synchronized Security, utilizing the Security Heartbeat™ status shared between Sophos Endpoints, Sophos Firewall, and Sophos Central. It is continuously assessing device health to identify active threats and signs of compromise. The result is an instant response to limit access to important corporate applications and data, both on the network and off, for compromised or non-compliant devices.

Integrated identity

With zero trust, identity is everything. Sophos ZTNA continuously verifies user identity with support for the most popular IDP solutions, including Microsoft AD, Entra ID, and Okta. Of course, you can also leverage your preferred multi-factor authentication (MFA) solution that integrates with these IDPs to guard against credential theft or compromised devices.

Sophos Zero Trust Endpoint

Run agentless, use the lightweight ZTNA agent for thick apps, or use our unique Sophos Protected Browser which provides a hardened chromium browser and integrated RDP and SSH ZTNA client support. Everything is included with Sophos Workspace Protection and you can deploy just what you need. Sophos ZTNA also works better together with Sophos Endpoint for device health, but can work alongside any third-party endpoint protection solution.



Sophos Central

Makes ZTNA easy with quick deployment, granular policy controls, and insightful visibility and reporting from the cloud. It integrates with popular identity providers to enable intelligent access enforcement for your applications through continuous user verification and device validation.

Sophos ZTNA Gateway

Integrated into all Sophos Firewalls including hardware, virtual, and cloud (AWS and Azure) and also available as a stand-alone virtual appliance on Hyper-V and VMware. Sophos ZTNA gateways are free and easy to deploy. It makes your applications invisible to the public internet while providing a secure connection for verified users and their validated devices to the applications they need to do their job.

Sophos ZTNA feature summary

- Secure access: for business applications hosted on premises or in your public cloud infrastructure.
- Applications: all browser-based web apps in clientless mode; thick apps like SSH, VNC, RDP, and others via the Sophos ZTNA client or Sophos Protected Browser.
- Access policies: user group-based policies, Synchronized Security health-based access policies.
- Reporting, monitoring, logging, and auditing of application status, access, and usage through Sophos Central.
- User portal for end users to access bookmarked applications.

Technical Specifications

Supported Platforms	
Identity Providers	Microsoft Active Directory (on-premise), Microsoft Entra ID (Azure Active Directory), Okta
ZTNA Gateway Platforms	VMware ESXi 7+, Hyper-V 2016+, and Sophos Firewall
ZTNA Client Platforms	Windows 10, Windows 11(Intel and ARM processors); macOS Sonoma, Sequoia, Tahoe (Intel and Apple processors)
ZTNA Device Health	Sophos Security Heartbeat (Sophos Endpoint)

Gateway Specifications	
Recommended VM	2 Core / 4 GB
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)

How to buy

Sophos ZTNA is part of Sophos Workspace Protection and is licensed on a per-user basis. ZTNA gateways are free to deploy as needed (and included with Sophos Firewall running any active license subscription).

Full product and licensing details are available at sophos.com/ztna

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

2026-01-09 DS-EN (NP)