Sophos ZTNA

Zero Trust Network Access

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. It works as a standalone product and as a fully integrated Synchronized Security solution with Sophos Firewall and Intercept X.

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. You can also 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.

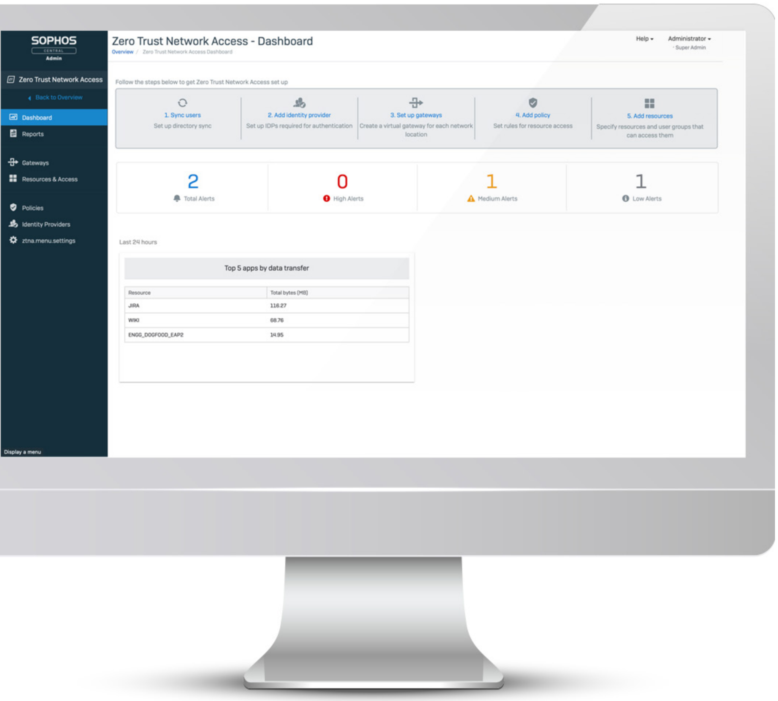
Deploy, Adapt, and Scale Quickly

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
- Agent integrated with Sophos Intercept X
- Gateway built-into Sophos Firewall
- Single agent, single gateway, single console solution
- The ultimate remote-access VPN replacement
- Micro-segment and secure your network applications
- Works anywhere, on the network or off
- Cloud-managed, cloud-delivered
- Transparent for end users
- Superior visibility and insights into your applications
- Integrates device health into access policies
- Simpler per-user annual subscription licensing with free gateways

SOPHOS



Zero Trust Network Access - Dashboard

Overview / Zero Trust Network Access Dashboard

Follow the steps below to get Zero Trust Network Access set up

1. Sync users
Set up directory sync

2. Add identity provider
Set up IDPs required for authentication

3. Set up gateways
Create a virtual gateway for each network location

4. Add policy
Set rules for resource access

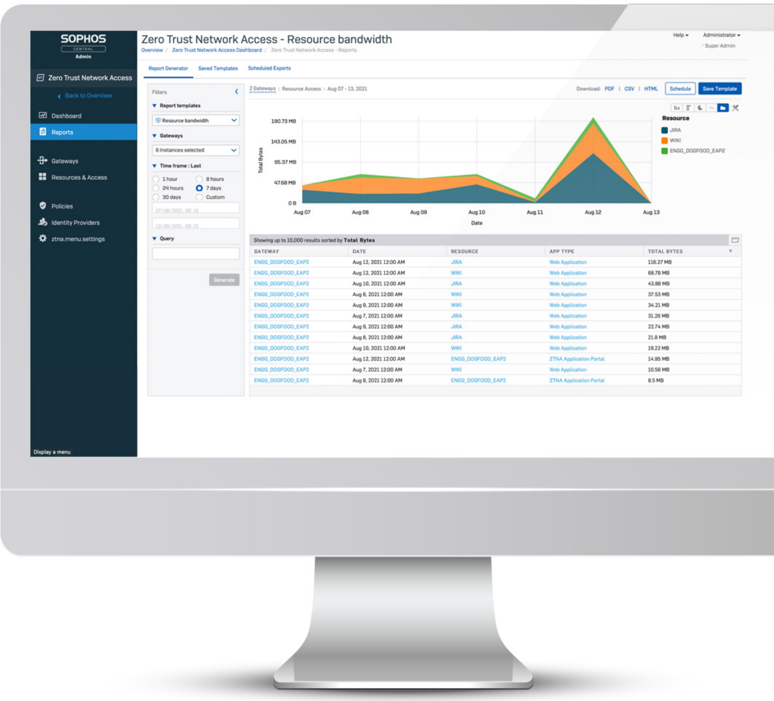
5. Add resources
Specify resources and user groups that can access them

2	0	1	1
Total Alerts	High Alerts	Medium Alerts	Low Alerts

Last 24 hours

Top 5 apps by data transfer

Resource	Total bytes (MB)
JIRA	116.27
WIKI	68.76
ENGG_DOGFOOD_EAP2	14.95



Zero Trust Network Access - Resource bandwidth

Overview / Zero Trust Network Access Dashboard / Zero Trust Network Access - Reports

Filters

Report templates: Resource bandwidth

Gateways: 6 Instances selected

Time frame : Last

○ 1 hour ○ 8 hours
○ 24 hours ● 7 days
○ 30 days ○ Custom

07/08/2021, 00:15

13/08/2021, 00:15

Query

2 Gateways : Resource Access : Aug 07 - 13, 2021

Showing up to 10,000 results sorted by **Total Bytes**

GATEWAY	DATE	RESOURCE	APP TYPE	TOTAL BYTES
ENGG_DOGFOOD_EAP2	Aug 12, 2021 12:00 AM	JIRA	Web Application	116.27 MB
ENGG_DOGFOOD_EAP2	Aug 12, 2021 12:00 AM	WIKI	Web Application	68.76 MB
ENGG_DOGFOOD_EAP2	Aug 10, 2021 12:00 AM	JIRA	Web Application	43.88 MB
ENGG_DOGFOOD_EAP2	Aug 8, 2021 12:00 AM	WIKI	Web Application	37.53 MB
ENGG_DOGFOOD_EAP2	Aug 9, 2021 12:00 AM	WIKI	Web Application	34.21 MB
ENGG_DOGFOOD_EAP2	Aug 7, 2021 12:00 AM	JIRA	Web Application	31.26 MB
ENGG_DOGFOOD_EAP2	Aug 9, 2021 12:00 AM	JIRA	Web Application	22.74 MB
ENGG_DOGFOOD_EAP2	Aug 8, 2021 12:00 AM	JIRA	Web Application	21.8 MB
ENGG_DOGFOOD_EAP2	Aug 10, 2021 12:00 AM	WIKI	Web Application	19.22 MB
ENGG_DOGFOOD_EAP2	Aug 12, 2021 12:00 AM	ENGG_DOGFOOD_EAP2	ZTNA Application Portal	14.95 MB
ENGG_DOGFOOD_EAP2	Aug 7, 2021 12:00 AM	WIKI	Web Application	10.56 MB
ENGG_DOGFOOD_EAP2	Aug 8, 2021 12:00 AM	ENGG_DOGFOOD_EAP2	ZTNA Application Portal	8.5 MB

Cloud-Delivered, Cloud-Managed

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.

From Sophos Central, you can not only manage ZTNA, but also your Sophos firewalls, endpoints, server protection, mobile devices, cloud security, email protection, and so much more. You can log in and manage your IT security from anywhere, anytime, on any device.

Single Agent, Single Gateway, Single Console, Single Vendor

Sophos ZTNA uniquely integrates with the full Sophos cybersecurity ecosystem to make your job a lot easier. You get a single agent solution for both ZTNA and your next-gen endpoint protection. You get a ZTNA gateway integrated into your Sophos Firewall and you also get a single-pane-of-glass management console in Sophos Central for unprecedented insights across all your IT security products. All from a single vendor.

Uniquely Integrated: ZTNA and Next-Gen Endpoint Protection

Sophos ZTNA is the only ZTNA solution that is tightly integrated with a next-gen endpoint product – Sophos Intercept X. This provides significant benefits in protection, deployment, and management.

- End-to-end protection: Secure your application access and protect your endpoints and networks from breaches and threats like ransomware with the most powerful machine learning and next-gen endpoint technology available.
- Synchronized Security: With your ZTNA and endpoint integrated, they are constantly sharing status and health information to automatically isolate compromised systems to prevent threats from moving or stealing data.
- Single agent, single console, single vendor convenience.

It's a winning combination that you won't find anywhere else.

Single Agent Deployment

Sophos ZTNA is tightly integrated with Sophos Intercept X next-gen endpoint protection, enabling a single client deployment option.

You can have the world's best endpoint and ransomware protection along with the ultimate in application security and segmentation, all with a single client deployment.

Clientless access for browser-based applications is also an option.

Scalable Application Gateways

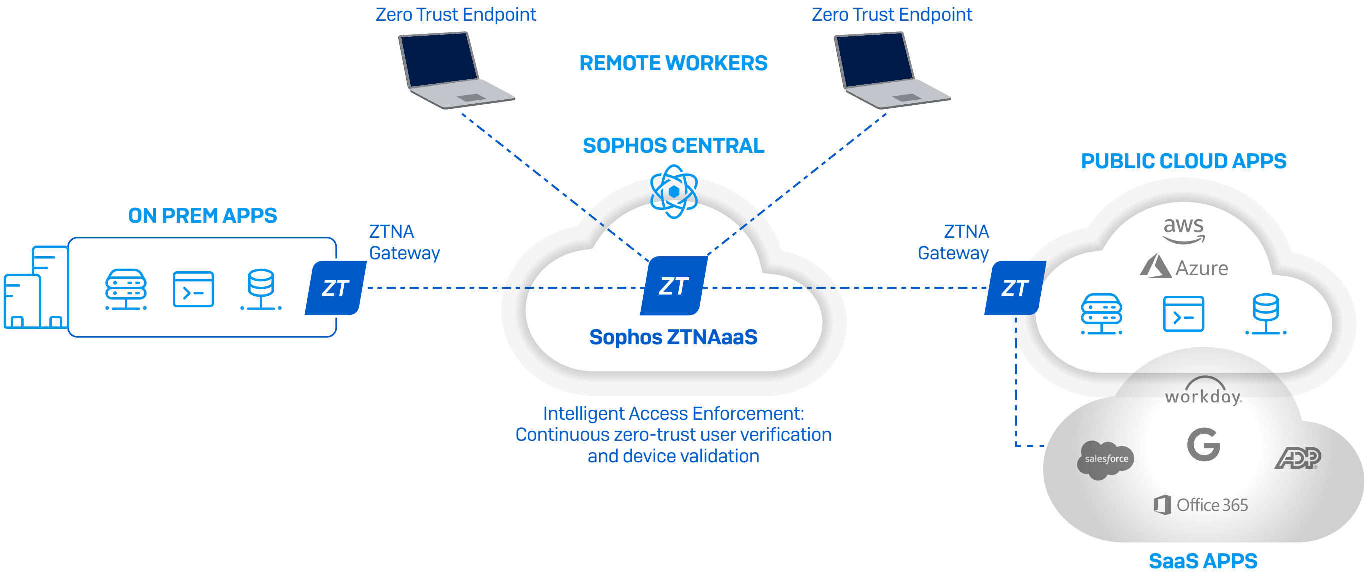
Sophos ZTNA gateways are free and easy to deploy where you need them. Available as a virtual appliance, you can easily deploy high-availability gateways and scale them as your organization grows.

Synchronized Device Health

Sophos ZTNA takes full advantage of Sophos Synchronized Security, utilizing the Security Heartbeat™ between Sophos Intercept X endpoints and Sophos Central and ZTNA to assess device health and identify active threats and signs of compromise. The result is an instant response to limit access, 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 or use our unique lightweight Sophos ZTNA agent that integrates with Sophos Intercept X to provide the ultimate zero trust endpoint solution with Synchronized Security. Sophos ZTNA also works with your existing endpoint protection product if you prefer.

Sophos Central

Makes ZTNA as a Service 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 v20 and later 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 ZTNA client
- 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 6.5+, Hyper-V 2016+, and Sophos Firewall v20+ (all hardware, virtual, and cloud platforms including AWS and Azure)
ZTNA Client Platforms	Windows 10 1803 or later, macOS 11 (Big Sur) or later; All platforms support agentless web application access
ZTNA Device Health	Sophos Security Heartbeat (Intercept X)

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 licensed on a per-user annual subscription basis. ZTNA Gateways are free to deploy as many as required.

To learn more, visit:
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

© Copyright 2024. 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.

SOPHOS