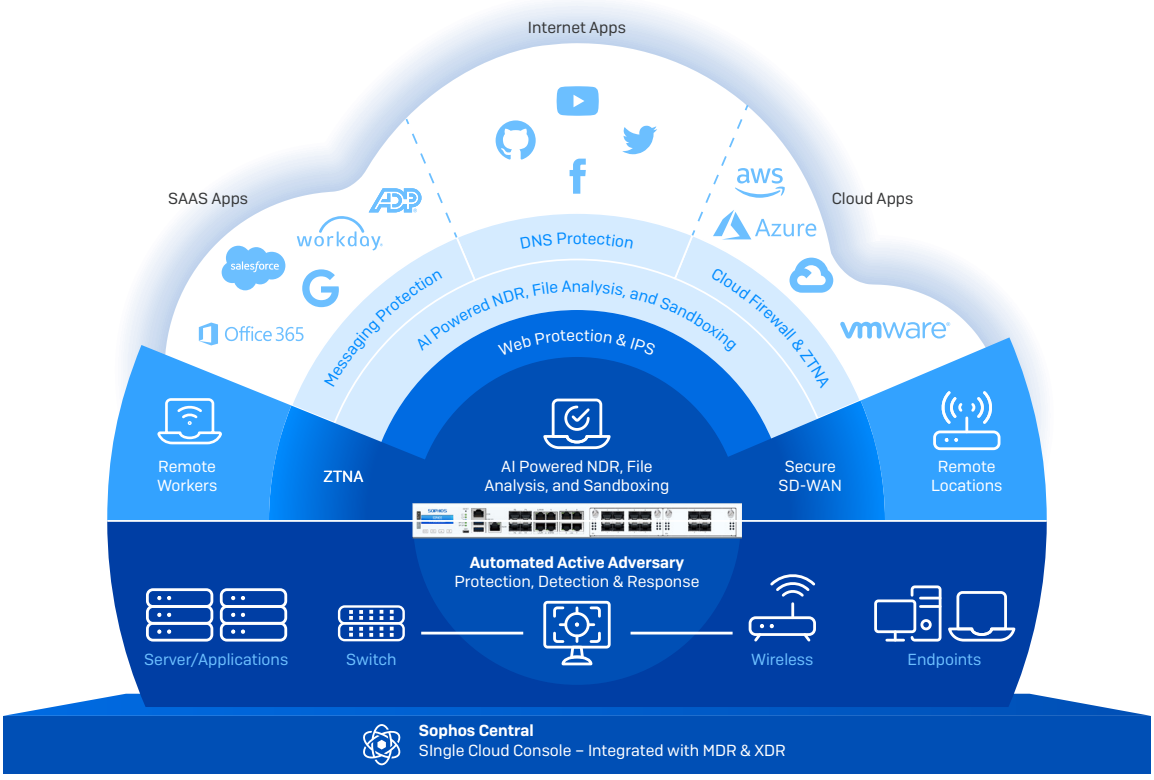
SOPHOS

Sophos Firewall

Much More Than a Firewall

Sophos Firewall and XGS Series appliances are at the heart of the world's best network security platform. Consolidate your network protection with our integrated and extensible platform to secure your hybrid networked world.



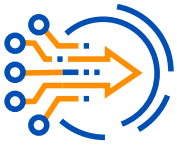
Powerful Protection and Performance

Sophos Firewall includes the latest advanced protection technologies and threat intelligence, including:

- Streaming DPI engine with web protection and IPS
- Accelerated TLS 1.3 encrypted traffic inspection
- Zero-day AI and machine learning analysis
- Real-time cloud sandboxing
- DNS Protection
- Network Detection and Response

The best part is, you don' t need to compromise on performance. This is thanks to our programmable Xstream architecture. It offloads benign traffic flows and crypto operations as well as VPN and select application routing to accelerate these network traffic flows and create performance headroom for traffic that actually needs deep packet inspection.

Sophos Firewall leverages the Sophos Cloud to ensure that your organization is protected from the latest threats and further maximize your performance. You get the latest AI and machine learning technology from SophosLabs working to identify previously unseen threats and malicious URLs. Using a common cloud, any new threat attacking a single Sophos customer is instantly shared across all our customers, blocking it everywhere. In addition, offloading this analysis from your firewall to the cloud boosts your performance even further.



Active Threat Response

Sophos Firewall uniquely integrates with many Sophos products to automatically coordinate a response to an active adversary or attack:

- Sophos Endpoint and XDR
- Sophos Managed Detection and Response services
- Sophos switches and wireless access points
- Sophos ZTNA remote access
- Sophos messaging protection
- Sophos NDR
- And third-party threat intelligence solutions

Regardless of how the threat is first identified, whether at the firewall, by another product, or by a security analyst, Sophos Firewall coordinates a Synchronized Security response across Sophos products. It will identify and isolate the compromised host and prevent lateral movement and external communications until the threat can be investigated and cleaned up.

Sophos Synchronized Security integration between products also provides additional capabilities you can't get anywhere else that adds tremendous value to your network:

- Synchronized Application Control takes advantage of telemetry gathered by the endpoint about active, networked applications and shares that with the firewall enabling control of applications that might otherwise go unidentified.
- Synchronized User ID works similarly to share user identity between the endpoint agent and the firewall to enforce user-based policies without the need for a separate client or server identity solution.
- Synchronized SD-WAN leverages Synchronized Application Control for traffic matching operations to effectively route custom or otherwise unknown application traffic across your network.

Work From Anywhere

Sophos Firewall offers the ultimate in flexible connectivity and secure access for even the most demanding networks. You get a fully integrated SD-WAN solution, along with a full suite of secure access products for Zero Trust Network Access, SD-RED edge devices, VPN, switching, and wireless — all managed from Sophos Central.

Securing and managing remote workers with ZTNA ensures users only have access to the applications they need, and not the whole network. ZTNA also integrates with Sophos Firewall and Sophos Endpoint to ensure a compromised device can't access the network at all. ZTNA also protects your applications from hacks and attacks by making them invisible to the outside world. The best part is, Sophos Firewall integrates a Sophos ZTNA gateway directly into your firewall to make deployment easy.

Sophos Firewall also includes one of the best integrated SD-WAN solutions available in any firewall. Xstream SD-WAN provides a powerful integrated SD-WAN solution with:

- Performance-based link selection and routing
- Load balancing with configurable weightings across multiple links
- Zero-impact transitions between links in the event of a disruption
- Central cloud-managed orchestration
- Xstream FastPath acceleration of VPN tunnel traffic

Sophos Firewall makes interconnecting your hybrid distributed enterprise easy and makes it extremely robust, ensuring maximum reliability and uptime.

Single Console Management

With Sophos Central, you get a single cloud management platform for all your Sophos products, including rich and powerful tools for group firewall management, SD-WAN overlay network orchestration, ZTNA and user management, and infrastructure management for your switches and wireless access points. You also get full in-depth dashboards and reports, cross-product integration and automation with other Sophos products, and much more. Sophos Firewall is so much more than just a firewall – consolidate and streamline your network security management starting with your firewall.

- Manage all of your Sophos Firewalls and other Sophos products from a single console
- Configure changes and apply them to a group of firewalls or manage each firewall individually
- Create a backup schedule and store up to five backups in the cloud
- Schedule firmware updates across your entire network with just a few clicks
- Use zero-touch deployment for new firewalls from Sophos Central: just drop ship the device to any location and set it up remotely. A USB drive is no longer required (but can still be used if you prefer).

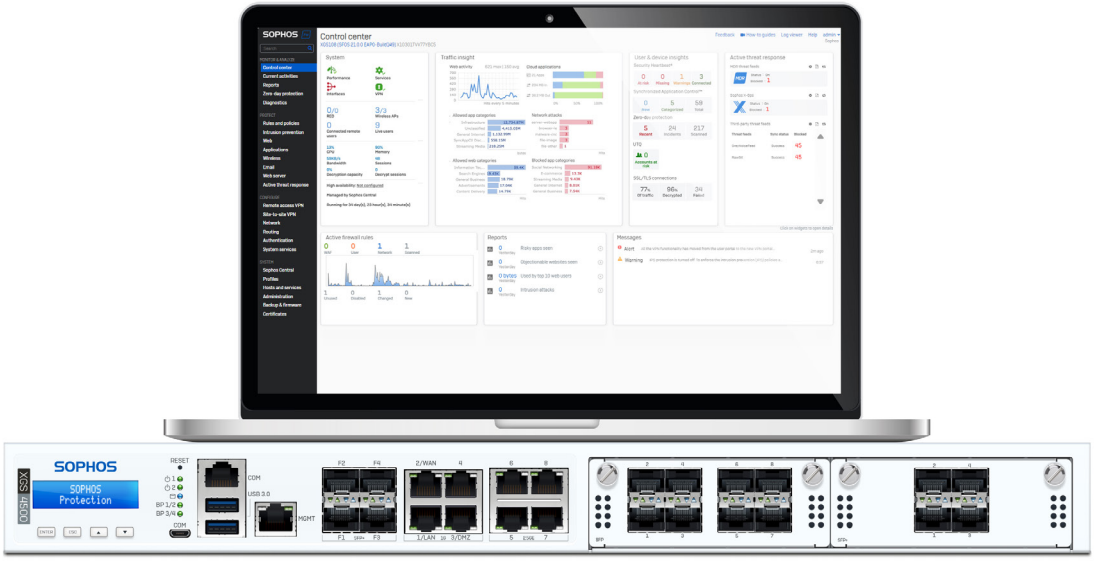
Central Management is included with all protection bundles, support or any individual subscriptions (excludes the Base License). Customers with a Base License only must add support (or any other subscription) for access to Sophos Central management and the 7-day allocation of Central Firewall Reporting. Support is also required to receive firmware updates and full access to customer support.

Sophos Central also includes powerful reporting and orchestration tools that enable you to visualize your network, web, application activity, and security over time:

- Flexible reporting combines a variety of built-in reports with powerful tools that you can use to create your own custom reports
- Analyze data to identify security gaps, suspicious user behavior, or other events requiring policy changes
- Data is shared across Sophos products through the Sophos Central data lake for threat hunting, forensics, and automated response to active threats
- Utilize point-and-click SD-WAN orchestration to easily setup a fully redundant VPN overlay network for your hybrid distributed network
- Central reporting is available at no extra cost with storage of up to seven days of reporting data for all customers with a protection bundle, individual subscription (except the Base License), or support.

Central Orchestration and Central Reporting with up to 30 days* of data retention are included at no extra charge in the Xstream Protection bundle. Premium reporting options with longer data retention are available for optional purchase.

* Calculated based on average traffic volumes per appliance size. In high-traffic environments, the retention period can be lower.



Learn more about the Sophos Central ecosystem at sophos.com/firewall-central