

SOPHOS

Sophos Firewall Features



Sophos Firewall

Highlights

- › Xstream Architecture provides extreme levels of visibility, protection, and performance through stream-based packet processing
- › Xstream TLS inspection offers high performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade policies with pre-packaged exceptions, unique dashboard visibility, and compatibility troubleshooting
- › Xstream DPI Engine provides stream scanning protection for IPS, AV, web, app control, and TLS inspection in a single-high performance engine
- › Xstream Network Flow FastPath delivers policy-driven and intelligent acceleration of trusted traffic automatically
- › Xstream SD-WAN provides performance-based link selection with zero-impact re-routing, SD-WAN monitoring, multi-site SD-WAN orchestration tools, and FastPath acceleration of IPsec VPN tunnel traffic
- › Purpose-built user interface with interactive control center utilizes traffic-light indicators (red, yellow, green) to instantly identify what needs attention at a glance
- › Control Center offers instant insights into endpoint health, unidentified Mac and Windows applications, cloud applications and shadow IT, suspicious payloads, risky users, advanced threats, network attacks, objectionable websites, and much more
- › Optimized two-clicks-to-anywhere navigation with intelligent search
- › Policy Control Center widget monitors policy activity for business, user, and network policies and tracks unused, disabled, changed, and new policies
- › Unified policy model combines all firewall, NAT, and TLS inspection rules onto a single screen with grouping, filtering, and search options
- › Streamlined firewall rule management for large rule sets with custom auto and manual grouping plus at-a-glance mouse-over feature and enforcement indicators
- › All firewall rules provide an at-a-glance summary of the applied security and control for AV, sandboxing, IPS, web, app, traffic shaping (QoS), and Heartbeat
- › Pre-defined IPS, web, app, TLS, and traffic shaping (QoS) policies enable quick setup and easy customization for common deployment scenarios (e.g. CIPA, typical workplace policies, and more)
- › Sophos Security Heartbeat™ connects Sophos endpoints with the firewall to share health status and telemetry, enabling instant identification of unhealthy or compromised endpoints
- › Active Threat Response identifies, blocks and automatically responds to active adversaries from threat feeds provided by SophosLabs, MDR analysts, or third-parties
- › Synchronized Application Control automatically identifies, classifies, and enables control of all unknown Mac/Windows applications on the network
- › Cloud Application Visibility enables shadow IT discovery instantly and offers one-click traffic shaping
- › Policy test simulator tool enables firewall rule and web policy simulation and testing by user, IP, and time of day
- › User Threat Quotient identifies risky users based on recent browsing behavior and ATP triggers
- › Configuration API for all features for RMM/PSA integration
- › Cloud-based NDR integration enhances active adversary detection
- › Integrated ZTNA Gateway in every firewall makes secure access to applications easy from anywhere
- › Sophos Central cloud-based management and reporting for multiple firewalls provides group policy management and one console for all your Sophos IT security products
- › Easy streamlined setup wizard enables fast out-of-the box deployment in just a few minutes
- › Zero-touch deployment and configuration in Sophos Central for new firewalls
- › Seamless integration with Sophos MDR and XDR

Base Firewall

General Management

- Purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators
- Two-factor authentication (one-time-password) support for administrator access, user portal, IPsec and SSL VPN
- Advanced logging and troubleshooting tools in GUI (e.g., packet capture)
- High Availability (HA) support clustering two devices in active-active or active-passive mode with plug-and-play Quick HA setup supporting multiple redundant synchronization links
- Full command line interface (CLI) accessible from GUI
- Role-based administration with Azure AD integration for single sign-on
- Automated firmware update notification with easy automated update process and roll-back features (available to customers with valid support only)
- Reusable and searchable system object definitions for networks, services, hosts, time periods, users and groups, clients, and servers
- Self-service user portal
- Configuration change tracking
- Flexible device access control for services by zones
- Email or SNMP trap notification options
- SNMP v3 and Netflow support
- Central management support via Sophos Central (available to customers with valid support only)
- Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly, or monthly - with the option to remap ports when upgrading hardware appliances
- Let's Encrypt certificate support for WAF, SMTP, TLS configuration, hotspot sign-in, the Web Admin console, user portal, captive portal, VPN portal, and SPX portal
- API for third-party integration
- Interface renaming
- Remote access option for Sophos Support
- Cloud-based license management via MySophos

Firewall, Networking, and Routing

- Stateful deep packet inspection firewall
- Xstream packet processing architecture provides extreme levels of visibility, protection, and performance through stream-based packet processing
- Xstream TLS inspection with high performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade policies, unique dashboard visibility, and compatibility troubleshooting
- Xstream DPI Engine provides stream scanning protection for IPS, AV, web, app control, and TLS inspection in a single high-performance engine
- Xstream Network Flow FastPath delivers policy-driven and intelligent acceleration of trusted application traffic, IPsec VPN traffic, and TLS encrypted traffic automatically
- User, group, time, or network-based policies
- Access time policies per user/group
- Enforce policy across zones, networks, or by service type
- Zone isolation and zone-based policy support
- Default zones for LAN, WAN, DMZ, LOCAL, VPN, and Wi-Fi
- Custom zones on LAN or DMZ
- Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule with a convenient NAT rule wizard to quickly and easily create complex NAT rules in just a few clicks
- Re-usable network object definitions for all rules with global intelligent free-text search
- Flood protection: DoS, DDoS, and portscan blocking
- Country blocking by geo-IP
- Routing: static, multicast (PIM-SM), and dynamic: RIP, BGP, OSPFv3 (IPv6) BGPv6
- Clone static routes and turn them on or off, Redistribute dynamic BGP routes into OSPFv3, utilize Blackhole route options, and utilize Equal-Cost Multi-Path (ECMP) for load balancing
- Upstream proxy support
- Protocol-independent multicast routing with IGMP snooping
- Bridging with STP support and ARP broadcast forwarding
- VLAN DHCP support and tagging
- VLAN bridge support

- › Jumbo frame support
- › Enable/disable physical interfaces
- › Wireless WAN support (n/a in virtual deployments)
- › 802.3ad interface link aggregation
- › Full configuration of DNS, DHCP, and NTP
- › Dynamic DNS (DDNS)
- › IPv6 Ready Logo Program Approval Certification
- › IPv6 DHCP Prefix Delegation
- › IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPsec

Xstream SD-WAN

- › Xstream SD-WAN profiles support multiple WAN link options including VDSL, DSL, cable, LTE/cellular, and MPLS
- › Performance-based SLAs automatically select the best WAN link based on jitter, latency, or packet loss
- › SD-WAN load balancing across multiple SD-WAN links with round robin weighting or session persistence strategies
- › Zero-impact re-routing maintains application sessions when link performance falls below thresholds and a transition is made to a better performing WAN link
- › SD-WAN monitoring graphs provide real-time insights into latency, jitter and packet loss for all WAN links
- › Xstream FastPath acceleration of SD-WAN IPsec tunnel traffic
- › Synchronized SD-WAN, a Synchronized Security feature, leverages the added clarity and reliability of application identification that comes with the sharing of Synchronized Application Control information between Sophos-managed endpoints and Sophos Firewall
- › Application routing over preferred links via firewall rules or policy-based routing
- › Robust VPN support including IPsec and SSL VPN
- › Unique RED Layer 2 tunnel with routing

Base Traffic Shaping and Quotas

- › Flexible network- or user-based traffic shaping (QoS) (enhanced web and app traffic shaping options included with the Web Protection subscription)
- › Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical
- › Real-time VoIP optimization
- › DSCP marking

Secure Wireless

- › Simple plug-and-play deployment of Sophos wireless access points (APX Series only) – automatically appear on the firewall control center
- › Central monitoring and management of APs and wireless clients through the built-in wireless controller
- › Bridge APs to LAN, VLAN, or a separate zone with client isolation options
- › Multiple SSID support per radio including hidden SSIDs
- › Support for diverse security and encryption standards including WPA2 Personal and Enterprise
- › Channel width selection option
- › Support for IEEE 802.1X (RADIUS authentication) with primary and secondary server support
- › Support for 802.11r (fast transition)
- › Hotspot support for (custom) vouchers, password of the day, or T&C acceptance
- › Wireless guest internet access with walled garden options
- › Time-based wireless network access
- › Wireless repeating and bridging meshed network mode with supported APs
- › Automatic channel selection background optimization
- › Support for HTTPS login

Authentication

- › Synchronized User ID utilizes Synchronized Security to share currently logged in Active Directory user ID between Sophos endpoints and the firewall without an agent on the AD server or client
- › Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
- › Server authentication agents for Active Directory SSO, STAS, SATC
- › Single sign-on: Active directory, eDirectory, RADIUS Accounting
- › Azure AD single sign-on for administrator access to the Webadmin console
- › Azure AD single sign-on for users to authenticate for web access via the captive portal
- › Transparent AD SSO with HSTS enforced, enabling Kerberos and NTLM handshakes over HTTP or HTTPS
- › Azure AD Group Import and RBAC support
- › Client authentication agents for Windows, Mac OS X, Linux 32/64

- › Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos
- › Browser Captive Portal
- › Authentication certificates for iOS and Android
- › Authentication services for IPsec, SSL, L2TP, PPTP
- › Google Chromebook authentication support for environments with Active Directory and Google G Suite
- › Google Workspace integration via LDAP client with Google Chromebook SSO
- › API-based authentication

User Self-Service & VPN Portals

- › Supports Entra ID (Azure AD) single sign-on for VPN portal
- › Download the Sophos Authentication Client
- › Download SSL remote access client (Windows) and configuration files (other OS)
- › Hotspot access information
- › Change user name and password
- › View personal internet usage
- › Access quarantined messages and manage user-based block/allow sender lists (requires Email Protection)

Base VPN Options

- › Site-to-site VPN: SSL, IPsec, 256-bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
- › Sophos RED site-to-site VPN tunnel (robust and lightweight)
- › Xstream FastPath acceleration of IPsec tunnel traffic (both site-to-site and remote-access)
- › AWS VPC import, monitoring and management tools
- › L2TP and PPTP
- › Route-based VPN with traffic selectors
- › Remote access: SSL, IPsec, iPhone/iPad/Cisco/Android VPN client support
- › IKEv2 Support
- › IPsec Connection Stateful HA Failover for RBVPN, PBVPN, and remote access VPN without losing session event in HA failover scenarios
- › IPsec VPN tunnel status monitoring via SNMP
- › Advanced IPsec support for unique PSK and DH-Group 27-30 / RFC6954
- › SSL client for Windows and configuration download via user portal

Sophos Connect Client

- › Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH
- › Supports Entra ID (Azure AD) single sign-on
- › Enables Synchronized Security and Security Heartbeat for remote connected users
- › Intelligent split-tunneling for optimum traffic routing
- › NAT-traversal support
- › Client-monitor for graphical overview of connection status
- › Mac (IPsec) and Windows (SSL/IPsec) client support

Network Protection

Intrusion Prevention (IPS)

- › High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection
- › Thousands of signatures
- › Granular category selection
- › Support for custom IPS signatures
- › IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added

Active Threat Response and Security Heartbeat™

- › Active Threat Response automatically monitors/blocks APT and other threats identified via Sophos-X Ops Threat Feeds for advanced threat protection from bots and active adversaries attempting to contact malicious destinations using multi-layered DNS, AFC, and firewall detections
- › Active Threat Response automatically monitors/blocks threats identified by MDR/XDR threat feeds published by a Sophos or customer/partner SOC analyst when Sophos Firewall with Xstream Protection is combined with Sophos MDR/XDR
- › Active Threat Response automatically monitors/blocks third-party threat feeds from industry, vertical, or regional threat intel sources with Xstream Protection
- › Sophos Synchronized Security Heartbeat instantly flags compromised devices with a red Heartbeat status that are attempting to contact any threat indicator identified by Active Threat Response and its related threat feeds. Heartbeat status is also monitored by Sophos-managed endpoints and shared with the firewall and will include details such as host, user, process, incident count, and time of compromise

- › Sophos Security Heartbeat conditions can be attached to any firewall rule, automatically limiting access to network resources and segments for a device that has been compromised until it is cleaned up
- › Sophos Firewall also automatically initiates lateral movement protection in the event a managed endpoint is compromised by informing all healthy Sophos-managed endpoints to reject traffic from the compromised device effectively stonewalling the device - even on the same LAN segment

SD-RED Device Management

- › Central management of all SD-RED devices
- › No configuration: Automatically connects through a cloud-based provisioning service
- › Secure encrypted tunnel using digital X.509 certificates and AES 256-bit encryption
- › Virtual Ethernet for reliable transfer of all traffic between locations
- › IP address management with centrally defined DHCP and DNS server configuration
- › Remotely de-authorize SD-RED devices after a select period of inactivity
- › Compression of tunnel traffic
- › VLAN port configuration options

Clientless VPN

- › Sophos unique encrypted HTML5 self-service portal with support for RDP, SSH, Telnet, and VNC

Web Protection

Web Protection and Control

- › Streaming DPI web protection or explicit proxy mode inspection
- › Explicit proxy mode supports per-connection authentication for multiple users on the same source IP
- › Enhanced Advanced Threat Protection
- › URL Filter database with millions of sites across 92 categories, backed by SophosLabs
- › Surfing quota time policies per user/group
- › Access time policies per user/group
- › Malware scanning: block all forms of viruses, web malware, trojans, and spyware on HTTP/S, FTP and web-based email
- › Advanced web malware protection with JavaScript emulation
- › Live Protection real-time, in-the-cloud

lookups for the latest threat intelligence

- › Second independent malware detection engine [Avira] for dual-scanning
- › Real-time or batch mode scanning
- › Pharming protection
- › Enforce tenant restrictions for O365
- › SSL protocol tunnelling detection and enforcement
- › Certificate validation
- › High performance web content caching
- › Forced caching for Sophos Endpoint updates
- › File type filtering by mime-type, extension, and active content types (e.g. ActiveX, applets, cookies, etc.)
- › YouTube for Schools enforcement per policy (user/group)
- › SafeSearch enforcement [DNS-based] for major search engines per policy (user/group)
- › Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload custom lists
- › Block potentially unwanted applications (PUAs)
- › Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users
- › User/group policy enforcement on Google Chromebooks

Cloud Application Visibility

- › Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
- › Discover Shadow IT at a glance
- › Drill down to obtain details on users, traffic, and data
- › One-click access to traffic shaping policies
- › Filter cloud application usage by category or volume
- › Detailed customizable cloud application usage report for full historical reporting

Application Protection and Control

- › Synchronized App Control to automatically, identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between Sophos-managed endpoints and the firewall
- › Signature-based application control with patterns for thousands of applications
- › Cloud Application Visibility and Control to discover shadow IT

- › App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added
- › Micro app discovery and control
- › Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g. P2P), and risk level
- › Per-user or network rule application control policy enforcement

Web and App Traffic Shaping

- › Enhanced traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared

DNS Protection

Cloud-Based DNS Service

- › Domain Name Resolution Service
- › High-performance cloud-based DNS service
- › Powered by SophosLabs and AI
- › Blocks malicious URLs at DNS lookup
- › Granular compliance controls to block unwanted websites by category
- › Managed from Sophos Central

NDR Essentials

Network Detection and Response

- › Cloud-based NDR
- › Powered by AI
- › Detects encrypted threat communications without TLS decryption
- › Detects domain generation algorithms
- › Scores potential threats and alerts on any threat exceeding your set threshold
- › Full reporting and logging support

Zero-Day Protection

Dynamic Sandbox Analysis

- › Full integration into your Sophos security solution dashboard
- › Inspects executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)

- › Aggressive behavioral, network, and memory analysis
- › Detects sandbox evasion behavior
- › Machine learning technology with deep learning scans all dropped executable files
- › Includes exploit prevention and CryptoGuard Protection technology from Sophos Intercept X
- › In-depth malicious file reports with screen shots and dashboard file release capability
- › Optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis
- › Supports one-time download links

Static Threat Intelligence Analysis

- › All files containing active code downloaded via the web or coming into the firewall as email attachments such as executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) are automatically sent for threat intelligence analysis
- › Files are checked against SophosLabs' massive threat intelligence database and subjected to multiple machine learning models to identify new and unknown malware
- › Extensive reporting includes a dashboard widget for analyzed files, a detailed list of the files that have been analyzed and the analysis results, and a detailed report outlining the outcome of each machine learning model

Central Orchestration

SD-WAN Orchestration

- › SD-WAN and VPN orchestration with easy and automated wizard-based creation of site-to-site VPN tunnels between network locations using an optimal architecture (hub-and-spoke, full mesh, or some combination)
- › Supports IPsec, SSL or RED VPN tunnels. Integrates seamlessly with SD-WAN features for application prioritization, routing optimization, and leveraging multiple WAN links for resiliency and performance

Central Firewall Reporting Advanced

- › 30-days of cloud data storage for historical firewall reporting with advanced features to save, schedule, and export custom reports

XDR and MDR Integration

- › Integration with Sophos XDR and MDR to feed telemetry and threat intelligence for threat hunting and analysis
- › Sophos Active Threat Response utilizes threat feeds from MDR and XDR analysts to automatically identify, block, and isolate active threats on the network
- › Synchronized Security IoC telemetry gathers important information about any threat, users, process and device that has been compromised

Email Protection

Email Protection and Control

- › Email scanning with SMTP, POP3, and IMAP support
- › Reputation service with spam outbreak monitoring based on patented recurrent-pattern detection technology
- › Block spam and malware during the SMTP transaction
- › DKIM and BATV anti-spam protection
- › Spam greylisting and Sender Policy Framework (SPF) protection
- › Recipient verification for mistyped email addresses
- › Second independent malware detection engine (Avira) for dual scanning
- › Live Protection real-time, in-the-cloud lookups for the latest threat intelligence
- › Automatic signature and pattern updates
- › Smart host support for outbound relays
- › File type detection/blocking/scanning of attachments
- › Accept, reject, or drop over-sized messages
- › Detects phishing URLs within e-mails
- › Use pre-defined content scanning rules or create your own custom policy rules based on a variety of criteria with granular policy options and exceptions
- › TLS encryption support for SMTP, POP, and IMAP
- › Append signature automatically to all outbound messages
- › Email archiver
- › Individual user-based block and allow sender lists maintained through the user portal

Email Quarantine Management

- › Spam quarantine digest and notifications options
- › Malware and spam quarantines with search and filter options by date, sender, recipient, subject, and reason with option to release and delete messages
- › Self-serve user portal for viewing and releasing quarantined messages

Email Encryption and DLP

- › Patent-pending SPX encryption for one-way message encryption
- › Recipient self-registration SPX password management
- › Add attachments to SPX secure replies
- › Completely transparent - no additional software or client required
- › DLP engine with automatic scanning of emails and attachments for sensitive data
- › Pre-packaged sensitive data type content control lists (CCLs) for PII, PCI, HIPAA, and more, maintained by SophosLabs

Web Server Protection

Web Application Firewall Protection

- › Reverse proxy
- › URL hardening engine with deep-linking and directory traversal prevention
- › Form hardening engine
- › SQL injection protection
- › Cross-site scripting protection
- › Dual-antivirus engines (Sophos and Avira)
- › HTTPS (TLS/SSL) encryption offloading
- › Cookie signing with digital signatures
- › Path-based routing
- › Geo IP policy enforcement
- › Custom cipher configuration and TLS version enforcement
- › HSTS and X-Content-Type-Options enforcement
- › Outlook anywhere protocol support
- › Reverse authentication (offloading) for form-based and basic authentication for server access
- › Virtual server and physical server abstraction
- › Integrated load balancer spreads visitors across multiple servers
- › Skip individual checks in a granular fashion as required
- › Match requests from source networks or specified target URLs
- › Support for logical and/or operators
- › Assists compatibility with various configurations and non-standard deployments
- › Options to change web application firewall performance parameters
- › Scan size limit option

- › Allow/block IP ranges
- › Wildcard support for server paths and domains
- › Automatically append a prefix/suffix for authentication

Reporting and Logging

Central Firewall Reporting

- › Pre-defined reports with flexible customization options
- › Reporting for Sophos Firewalls: hardware, software, virtual, and cloud
- › Intuitive user interface provides graphical representation of data
- › Report dashboard provides an at-a-glance view of events over the past 24 hours
- › Easily identify network activities, trends, and potential attacks
- › Easy backup of logs with quick retrieval for audit needs
- › Simplified deployment without the need for technical expertise

Central Firewall Reporting Advanced

- › Multi-firewall aggregate reporting
- › Save custom report templates
- › Scheduled reporting
- › Export reports in PDF, CFV, or HTML format
- › Up to one year data storage per firewall
- › MDR/XDR data lake connector for threat hunting

On-box Reporting

NOTE: Sophos Firewall reporting is included at no extra charge, but individual log, report, and widget availability may be dependent on their respective protection module licenses.

- › Hundreds of on-box reports with custom report options: Dashboards [Traffic, Security, and User Threat Quotient], Applications [App Risk, Blocked Apps, Synchronized Apps, Search Engines, Web Servers, Web Keyword Match, FTP], Network and Threats [Active Threat Response and threat feeds, Security Heartbeat, IPS, wireless, zero-day threat protection], VPN, Email, Compliance [HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA]
- › Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks

- › SD-WAN link performance monitoring for jitter, latency, and packet loss
- › Report anonymization
- › Report scheduling to multiple recipients by report group with flexible frequency options
- › Export reports as HTML, PDF, Excel [XLS]
- › Report bookmarks
- › Log retention customization by category
- › Full-featured log viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization

Central Management

Sophos Central

- › Sophos Central cloud-based management and reporting for multiple firewalls provides group policy management and a single console for all your Sophos IT security products
- › Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group
- › Task Manager provides a full historical audit trail and status monitoring of group policy changes
- › Backup firmware management in Sophos Central stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access
- › Firmware update scheduling from Sophos Central enables easy automated updates to be applied at any time
- › Zero-touch deployment enables the initial configuration to be performed in Sophos Central and then exported for loading onto the device from a flash drive at startup, automatically connecting the device back to Sophos Central

Zero Trust Network Access

- › Integrated Sophos ZTNA gateway for secure access to applications hosted behind the firewall
- › Managed from Sophos Central

Sophos Firewall Features by Subscription Summary

	Xstream Protection Bundle					Available Separately				
	Standard Protection Bundle					Available Separately				
	Base Firewall	Network Protection	Web Protection	DNS Protection	Bundle Only Features	Zero-Day Protection	Central Orchestration	Central Firewall Reporting Adv.	Email Protection	Web Server Protection
General Management (incl. HA)	●									
Xstream Architecture	●									
Firewall, Networking and Routing	●									
Xstream SD-WAN	●									
Base Traffic Shaping and Quotas	●									
Secure Wireless	●									
Authentication	●									
Self-Serve User Portal	●									
VPN (IPsec, SSL, etc)	●									
RED Site-to-Site VPN	●									
Sophos Connect VPN Client	●									
Intrusion Prevention (IPS)		●								
Active Threat Response										
Sophos X-Ops Threat Feeds		●								
MDR/XDR Threat Feeds					●					
Third Party Threat Feeds					●					
Synchronized Security Heartbeat		●								
SD-RED Device Management		●								
Clientless VPN		●								
Synchronized Application Control			●							
Web Protection and Control			●							
Application Protection and Control			●							
Cloud Application Visibility			●							
Web and App Traffic Shaping			●							
DNS Security and Compliance				●						
NDR Essentials					●					
Dynamic Sandbox Analysis						●				
Threat Intelligence Analysis						●				
SD-WAN Orchestration							●			
Central Firewall Reporting Data*		7 Days	7 Days	7 Days	7 Days	7 Days	30 Days	Up to 1 Year	7 Days	7 Days
CFR Advanced Features							●	●		
Email Protection and Control									●	
Email Quarantine Management									●	
Email Encryption and DLP									●	
Web Application Firewall Protection										●
On-box Logging/Reporting	●	●	●	●	●	●	●	●	●	●
Sophos Central Management**		●	●	●	●	●	●	●	●	●
ZTNA Gateway**		●	●	●	●	●	●	●	●	●

Please note: Some features are not supported on XGS 87 and XGS 88 models
(on-box reporting, dual AV scanning, WAF AV scanning and email message transfer agent (MTA) functionality)

MSP licensing options differ slightly to the above

* Data storage retention time is an estimate based on average network usage and will vary depending on actual log data volume. [Storage Estimation Tool](#).

** Included with any bundle, support, or protection subscription. Customers with a Base License only must add support to be eligible for these features.

Support Plans

	ENHANCED SUPPORT (Included in Standard and Xstream Protection bundles)	ENHANCED PLUS SUPPORT (available as an upgrade from Enhanced Support)
24/7 multi-channel support (phone, web portal, chat) including remote assistance and self-help access to KB and support forums	•	•
Firmware downloads, updates, and maintenance releases **	•	•
Sophos Central Management, Reporting, and ZTNA Gateway	•	•
Advanced hardware replacement for active devices	•	•
Advanced hardware replacement for a passive HA device*		•
Advanced hardware replacement for SD-RED/APX devices		•
VIP Access (calls routed to senior engineers)		•
Remote consulting (2-8 hours per year)		•

* To enable advanced RMA coverage for a passive HA device, the active device must have an Enhanced Plus support license. Refer to the [Sophos Support Service Guide](#) for full details.

** Note: Support must be added to any individual module purchase to receive firmware updates

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