FEATURE-LISTE

Sophos Firewall Feature-Liste

Sophos Firewall

Vorteile auf einen Blick

- Die Xstream-Architektur bietet durch die Stream-basierte Paketverarbeitung eine extrem hohe Transparenz, Sicherheit und Performance
- Xstream TLS Inspection bietet eine hohe Leistung, Unterstützung von TLS 1.3 ohne Downgrading, Port-Unabhängigkeit, Richtlinien der Enterprise-Klasse mit vorkonfigurierten Ausnahmen, einzigartige Dashboard-Transparenz und Kompatibilitäts-Troubleshooting
- Die Xstream DPI Engine bietet Stream-Scanning-Schutz für IPS, Antivirus, Web, Application Control und TLS Inspection in einer einzigen Hochleistungs-Engine
- Der Xstream Network Flow FastPath ermöglicht automatisch eine richtliniengesteuerte und intelligente Beschleunigung des vertrauenswürdigen Datenverkehrs
- Xstream SD-WAN bietet eine Performance-basierte Verbindungsauswahl mit Zero-Impact-Umleitungen, SD-WAN-Überwachung, SD-WAN-Orchestrierungstools für mehrere Standorte und FastPath-Beschleunigung von IPsec-VPN-Tunnelverkehr
- In der speziell entwickelten Benutzeroberfläche mit interaktivem Control Center werden Anzeigen in Ampelfarben (rot, gelb, grün) verwendet, damit Sie sofort erkennen, wo Maßnahmen erforderlich sind
- Das Control Center bietet sofortigen Einblick in den Integritäts-Status von Endpoints, nicht identifizierte Mac- und Windows-Anwendungen, Cloud-Anwendungen und Schatten-IT, verdächtige Payloads, riskante Benutzer, komplexe Bedrohungen, Netzwerk-Angriffe, bedenkliche Websites u.v.m.
- Optimierte Navigation „mit zwei Mausklicks zum Ziel“ und intelligenter Suche
- Das Policy Control Center Widget überwacht die Richtlinienaktivität für Geschäfts-, Benutzer- und Netzwerkrichtlinien und verfolgt ungenutzte, deaktivierte, geänderte und neue Richtlinien
- Dank des zentralen Richtlinienmodells werden alle Firewall-, NAT- und TLS-Inspection-Regeln in einer Ansicht kombiniert – mit Gruppierungs-, Filter- und Suchoptionen
- Effiziente Verwaltung von Firewall-Regeln für große Regelsätze mit benutzerdefinierter automatischer und manueller Gruppierung sowie übersichtlichen Mouseover-Anzeigen von Regelfunktionen und Durchsetzungsparametern
- Für alle Firewall-Regeln gibt es eine übersichtliche Zusammenfassung aller angewandten Sicherheits- und Kontrollmaßnahmen für Anti-Virus, Sandboxing, IPS, Web, App, Traffic Shapping (QoS) und Heartbeat
- Vordefinierte Richtlinien für IPS, Web, App, TLS und Traffic Shaping (QoS) ermöglichen eine schnelle Einrichtung und einfache Anpassung für gängige Bereitstellungsszenarien (u. a. Richtlinien zum Kinder- und Jugendschutz sowie typische Arbeitsplatzrichtlinien)
- Sophos Security HeartbeatTM verbindet Sophos-Endpoints mit der Firewall. So können der Integritäts-Status und Telemetrie-Daten übermittelt und unsichere oder kompromittierte Endpoints sofort erkannt werden
- Active Threat Response erkennt, blockiert und reagiert automatisch auf aktive Angreifer – anhand von Bedrohungsfeeds, die von den SophosLabs, MDR-Analysten oder Drittanbietern bereitgestellt werden
- Synchronized Application Control erkennt, klassifiziert und kontrolliert automatisch alle unbekannten Mac-/Windows-Anwendungen im Netzwerk
- Transparenz über Cloud-Anwendungen ermöglicht die sofortige Erkennung von Schatten-IT und ermöglicht Traffic Shaping mit einem Klick
- Mit dem Richtlinien-Testsimulator können Firewall-Regeln und Web-Richtlinien einfach simuliert und für bestimmte Benutzer, IPs und Tageszeiten getestet werden
- Die Prinzipien von „Secure by Design“ gewährleisten, dass die Firewall gegen Angriffe gehärtet ist
- Konfigurations-API für alle Funktionen zur RMM/PSA-Integration

SOPHOS

- Cloudbasierte NDR-Integration verbessert die Erkennung aktiver Angreifer
- Das in jede Firewall integrierte ZTNA-Gateway ermöglicht sicheren Zugriff auf Anwendungen von überall aus
- Die cloudbasierte Verwaltung und Report-Erstellung von Sophos Central für mehrere Firewalls bietet effiziente Management-Funktionen für Gruppenrichtlinien und eine zentrale Konsole für alle Ihre Sophos-IT-Security-Produkte
- Ein einfacher, effizienter Setup-Assistent ermöglicht innerhalb von wenigen Minuten eine schnelle Bereitstellung ohne manuelle Konfigurationen
- Zero-Touch-Bereitstellung und -Konfiguration in Sophos Central für neue Firewalls
- Nahtlose Integration mit Sophos MDR und XDR

Basis-Firewall

Allgemeine Verwaltung

- Speziell entwickelte, optimierte Benutzeroberfläche und Verwaltung von Firewall-Regeln für große Regelsätze mit Gruppierung und übersichtlichen Anzeigen von Regelfunktionen und Durchsetzungsparametern
- Unterstützung von Zwei-Faktor-Authentifizierung (Einmalpasswort) für Administratorzugriff, Benutzerportal, IPsec, SSL-VPN und WAF
- Erweiterte Protokollierungs- und Troubleshooting-Tools in der GUI (z. B. Packet Capture)
- Hochverfügbarkeit (HA) unterstützt Clustering von zwei Geräten im Aktiv-Aktiv- oder Aktiv-Passiv-Modus mit Plug-and-Play Quick HA-Einrichtung, wodurch mehrere redundante Synchronisierungsverbindungen ermöglicht werden
- Vollständige Befehlszeilen-Schnittstelle (CLI), auf die über die GUI zugegriffen werden kann
- Rollenbasierte Administration mit Azure-AD-Integration für Single Sign-On
- Firmware-Updates über SSL mit Zertifikats-Pinning für maximale Sicherheit
- Wiederverwendbare und durchsuchbare Systemobjektdefinitionen für Netzwerke, Dienste, Hosts, Zeiträume, Benutzer und Gruppen, Clients und Server
- Self-Service-Portal für Benutzer
- Verfolgung von Konfigurationsänderungen
- Flexible Gerätezugriffssteuerung für Dienste nach Zonen
- Benachrichtigungsoptionen für E-Mails und SNMP-Traps
- SNMP v3 (einschließlich Hardware Monitoring) und Netflow/sFlow Monitoring
- Zentrale Verwaltung über Sophos Central (nur für Kunden mit gültigem Support-Vertrag)
- Wiederherstellungs-Konfigurationen: lokal, über FTP oder E-Mail; nach Bedarf, täglich, wöchentlich oder monatlich – mit der Option, Ports beim Upgrade von Hardware-Appliances neu zuzuweisen
- Unterstützung von Let's Encrypt-Zertifikaten für WAF-, SMTP-, TLS-Konfigurationen, Hotspot-Anmeldung, die Web-Admin-Oberfläche, das Benutzerportal, Captive Portal sowie das VPN-Portal und SPX-Portal
- API für Fremdanbieter-Integrationen
- Schnittstellen-Umbenennung
- Remote-Zugriffsoption für Sophos Support
- Cloudbasierte Lizenzverwaltung über MySophos

Firewall, Networking und Routing

- Stateful Deep Packet Inspection Firewall
- Die Xstream-Paketverarbeitungs-Architektur bietet durch die Stream-basierte Paketverarbeitung eine extrem hohe Transparenz, Sicherheit und Performance
- Xstream TLS Inspection mit hoher Leistung, Unterstützung von TLS 1.3 ohne Downgrading, Port-Unabhängigkeit, Richtlinien der Enterprise-Klasse, einzigartiger Dashboard-Transparenz und Kompatibilitäts-Troubleshooting
- Die Xstream DPI Engine bietet Stream-Scanning-Schutz für IPS, Antivirus, Web, Application Control und TLS Inspection in einer einzigen Hochleistungs-Engine
- Xstream Network Flow FastPath ermöglicht automatisch eine richtliniengesteuerte und intelligente Beschleunigung von vertrauenswürdigem Anwendungsverkehr, IPSec VPN-Datenverkehr und TLS-verschlüsseltem Datenverkehr
- Benutzer-, Gruppen-, Zeit- oder netzwerkbasierte Richtlinien
- Zugriffszeitrichtlinien pro Benutzer/Gruppe
- Durchsetzung von Richtlinien über Zonen, Netzwerke oder Service-Typen hinweg
- Zonenisolierung und zonenbasierte Richtlinienunterstützung
- Standardzonen für LAN, WAN, DMZ, LOKAL, VPN und WLAN

- Benutzerdefinierte Zonen auf LAN oder DMZ
- Anpassbare NAT-Richtlinien mit IP-Maskierung und vollständiger Objektunterstützung zur Umleitung oder Weiterleitung mehrerer Services in einer einzigen Regel – mit einem praktischen NAT-Regel-Assistenten, der mit nur wenigen Klicks schnell und einfach komplexe NAT-Regeln erstellt
- Wiederverwendbare Netzwerkobjekt-Definitionen für alle Regeln mit globaler intelligenter Freitextsuche
- Flood Protection: DoS-, DDoS- und Portscan-Blockierung
- Länderblockierung nach geografischem IP-Standort
- Routing: statisch, Multicast (PIM-SM) und dynamisch: RIP, BGP, OSPFv3 (IPv6) BGPv6
- Klonen sowie Ein- und Ausschalten statischer Routen, Umverteilung von BGP-Routen in OSPFv3, Blackhole-Routen-Option und Equal-Cost Multi-Path (ECMP) für Load Balancing
- Unterstützung von Upstream-Proxys
- Protokollunabhängiges Multicast Routing mit IGMP Snooping
- Bridging mit STP-Unterstützung und ARP-Broadcast-Weiterleitung
- VLAN-DHCP-Unterstützung und -Tagging
- Unterstützung von VLAN Bridge
- Jumbo-Frame-Unterstützung
- Aktivieren/Deaktivieren physischer Schnittstellen
- Wireless-WAN-Unterstützung (gilt nicht für virtuelle Bereitstellungen)
- 802.3ad Interface Link Aggregation
- Vollständige Konfiguration von DNS, DHCP und NTP
- Dynamisches DNS (DDNS)
- Im Rahmen des IPv6 Ready Logo Program als Ipv6-fähig zertifiziert
- IPv6 -DHCP-Präfixdelegation
- IPv6-Tunnel-Unterstützung einschließlich 6in4, 6to4, 4in6 und schneller IPv6-Einführung (6rd) über IPsec

Xstream SD-WAN

- Xstream-SD-WAN-Profile unterstützen mehrere WAN-Link-Optionen, einschließlich VDSL, DSL, Kabel, LTE/Mobilfunk und MPLS
- Performance-basierte SLAs wählen basierend auf Störungen, Latenz oder Paketverlust automatisch die beste WAN-Verbindung aus
- SD-WAN Load Balancing über mehrere SD-WAN-Links mit Round-Robin-Gewichtungen und Strategien zur Sitzungs-Persistenz
- Wenn die Verbindungsleistung unter bestimmte Schwellenwerte fällt, wird auf eine bessere Verbindung umgestellt. Bei diesen Zero-Impact-Umleitungen werden Anwendungssitzungen aufrechterhalten
- SD-WAN-Überwachungsdiagramme bieten Echtzeiteinblick in Latenz, Störungen und Paketverlust für alle WAN-Verbindungen
- Xstream FastPath-Beschleunigung des SD-WAN-IPsec-Tunnelverkehrs
- Die Synchronized-Security-Funktion Synchronized SD-WAN macht sich den Umstand zunutze, dass Anwendungen durch den Austausch synchronisierter Application-Control-Daten zwischen mit Sophos verwalteten Endpoints und der Sophos Firewall eindeutig und zuverlässig bestimmt werden können.
- Routing von Anwendungen über Vorzugsverbindungen mittels Firewallregeln oder Richtlinien
- Robuste VPN-Unterstützung einschließlich IPsec und SSL VPN
- Einzigartiger RED-Layer-2-Tunnel mit Routing

Basisfunktionen für Traffic Shaping und Kontingente

- Flexibles netzwerk- oder benutzerbasiertes Traffic Shaping (QoS) (erweiterte Web- und App-Traffic-Shaping-Optionen sind in der Web Protection Subscription enthalten)
- Einrichtung benutzerbasierter Datenverkehrskontingente für Upload/Download oder Gesamtverkehr sowie auf zyklischer oder nicht-zyklischer Basis
- VoIP-Optimierung in Echtzeit
- DSCP-Markierung

Secure Wireless

- Einfache Plug-and-Play-Bereitstellung von Sophos Wireless Access Points (nur APX-Serie) – wird automatisch im Firewall Control Center angezeigt
- Zentrale Überwachung und Verwaltung von APs und Wireless Clients über den integrierten Wireless Controller
- Bridging von APs zu LAN, VLAN oder einer separaten Zone mit Optionen zur Client-Isolierung

- Unterstützung mehrerer SSID pro Sender, einschließlich verborgener SSIDs
- Unterstützung diverser Sicherheits- und Verschlüsselungsstandards, einschließlich WPA2 Personal und Enterprise
- Option zur Auswahl der Kanalbreite
- Unterstützung von IEEE 802.1X (RADIUS-Authentifizierung) mit Unterstützung primärer und sekundärer Server
- Unterstützung von 802.11r (Fast Transition)
- Hotspot-Unterstützung für (benutzerdefinierte) Voucher, Tagespasswort oder Annahme der Nutzungsbedingungen
- WLAN-Zugang für Gäste mit Möglichkeiten zur Beschränkung („kontrollierte Umgebung“)
- Zeitbasierter WLAN-Zugriff
- WLAN Repeating und Bridging Mesh-Netzwerk-Modus mit unterstützten APs
- Automatische Hintergrundoptimierung der Kanalauswahl
- Unterstützung von HTTPS-Anmeldung

Authentifizierung

- Die Synchronized User ID tauscht mittels Synchronized Security die aktuell bei Active Directory angemeldete Benutzer-ID zwischen Sophos Endpoints und der Firewall aus – ohne Agent auf dem AD-Server oder Client
- Authentifizierung über: Active Directory, eDirectory, RADIUS, LDAP und TACACS+
- Server-Authentifizierungs-Agenten für Active Directory SSO, STAS, SATC
- Single-Sign-On: Active Directory, eDirectory, RADIUS Accounting
- Azure AD Single Sign-On für Administratorzugriff auf die WebAdmin-Konsole
- Azure AD Single Sign-On für Benutzer zum Authentifizieren für Webzugriff über das Captive Portal
- Transparentes AD SSO mit HSTS-Durchsetzung, die Kerberos- und NTLM-Handshakes über HTTP oder HTTPS ermöglicht
- Import von Azure-AD-Gruppen und RBAC-Unterstützung
- Client-Authentifizierungs-Agenten für Windows, Mac OS X, Linux 32/64
- Browser-SSO-Authentifizierung: Transparente Proxy-Authentifizierung (NTLM) und Kerberos
- Browser Captive Portal
- Authentifizierungszertifikate für iOS und Android
- Authentifizierungsdienste für IPsec, SSL, L2TP, PPTP
- Unterstützung von Google-Chromebook-Authentifizierung für Umgebungen mit Active Directory und Google G Suite
- Integration von Google Workspace über LDAP Client mit Google Chromebook SSO
- API-basierte Authentifizierung

Self-Service- und VPN-Portale für Benutzer

- SNMP v3 (einschließlich Hardware Monitoring) und Netflow/sFlow Monitoring
- Sophos Authentication Client herunterladen
- SSL Remote Access Client (Windows) und Konfigurationsdateien (andere Betriebssysteme) herunterladen
- Hotspot-Zugriffsinformationen
- Änderung von Benutzernamen und Passwort
- Anzeige der eigenen Internetnutzung
- Zugriff auf isolierte Nachrichten und Verwaltung benutzerbasierter Listen zum Erlauben und Blockieren von Absendern (erfordert Email Protection)

Basis-VPN-Optionen

- Site-to-Site VPN: SSL, IPsec, 256-Bit AES/3DES, PFS, RSA, X.509-Zertifikate, vorinstallierter Schlüssel
- Sophos RED Site-to-Site VPN-Tunnel (robust und leichtgewichtig)
- Xstream-FastPath-Beschleunigung von IPsec-Tunnelverkehr (Site-to-Site und Remote-Zugriff)
- Tools für Import, Überwachung und Verwaltung von AWS VPC
- L2TP und PPTP
- Routenbasiertes VPN mit Verkehrskennzeichnern
- Remote-Zugriff: SSL, IPsec, iPhone/iPad/Cisco/Android VPN-Client-Unterstützung
- IKEv2-Unterstützung
- IPsec Connection Stateful HA Failover für RBVPN, PBVPN und Remote Access VPN ohne Verlust von Sitzungsereignissen in HA Failover-Szenarien

- IPsec-VPN-Tunnelstatus-Überwachung über SNMP
- Erweiterte IPsec-Unterstützung für eindeutiges PSK und DH-Gruppe 27-30/RFC6954
- SSL Client für Windows und Konfigurationsdownload über Benutzerportal

Sophos Connect Client

- Authentifizierung: Vorinstallierter Schlüssel (PSK), PKI (X.509), Token und XAUTH
- Unterstützt Entra ID (Azure AD) Single Sign-On
- Aktiviert Synchronized Security und Security Heartbeat für remote angebundene Benutzer
- Intelligentes Split-Tunneling für optimales Traffic-Routing
- NAT-Traversal-Unterstützung
- Client-Monitor für eine grafische Übersicht über den Verbindungsstatus
- Unterstützung von Mac- (IPsec) und Windows-Clients (SSL/IPsec)

Network Protection

Intrusion Prevention (IPS)

- Leistungsstarke Next-Gen IPS Deep Packet Inspection Engine mit selektiven IPS-Mustern, die für maximale Performance und Sicherheit auf Basis von Firewall-Regeln angewendet werden können
- Tausende von Signaturen
- Detaillierte Kategorie-Auswahl
- Unterstützung benutzerdefinierter IPS-Signaturen
- IPS-Richtlinien-Smartfilter ermöglichen dynamische Richtlinien, die beim Hinzufügen neuer Muster automatisch aktualisiert werden

Active Threat Response und Security Heartbeat™

- Active Threat Response überwacht/blockiert automatisch APT und andere Bedrohungen, die über Sophos-X Ops Threat Feeds erkannt werden. So wird modernster Bedrohungsschutz vor Bots und aktiven Angreifern gewährleistet, die versuchen, über mehrschichtige DNS-, AFC- und Firewall-Erkennungen mit schädlichen Zielen in Kontakt zu treten
- Active Threat Response überwacht/blockiert automatisch Bedrohungen, die durch die von einem Sophos- oder SOC-Analysten eines Kunden/Partners veröffentlichte MDR/XDR-Bedrohungsfeeds erkannt wurden, wenn eine Sophos Firewall mit Xstream Protection mit Sophos MDR/XDR kombiniert wird
- Active Threat Response überwacht/blockiert automatisch Bedrohungsfeeds von Drittanbietern aus branchenspezifischen, vertikalen oder regionalen Quellen mit Xstream Protection
- Sophos Synchronized Security Heartbeat kennzeichnet kompromittierte Geräte sofort mit einem roten Heartbeat-Status, die versuchen, Bedrohungsindikatoren zu erreichen, die von Active Threat Response und den zugehörigen Bedrohungsfeeds erkannt wurden. Der Heartbeat-Status wird auch von Sophos-verwalteten Endpoints überwacht und mit der Firewall geteilt. Er enthält Details wie Host, Benutzer, Prozess, Anzahl von Vorfällen und Zeitpunkt der Kompromittierung
- Sophos Security Heartbeat-Bedingungen können an jede Firewall-Regel angehängt werden, wodurch der Zugriff auf Netzwerkressourcen und -segmente für ein kompromittiertes Gerät bis zu dessen Bereinigung automatisch eingeschränkt wird.
- Die Sophos Firewall aktiviert bei Kompromittierung eines verwalteten Endpoints zudem automatisch Lateral Movement Protection. Alle sicheren, von Sophos verwalteten Endpoints werden informiert, Datenverkehr vom kompromittierten Gerät abzulehnen und das Gerät zu blockieren (sogenanntes „Stonewalling“) – sogar im selben LAN-Segment

Verwaltung von SD-RED-Geräten

- Zentrale Verwaltung aller SD-RED-Geräte
- Keine Konfiguration: Stellt automatisch eine Verbindung über einen cloudbasierten Einrichtungsservice her
- Sicherer verschlüsselter Tunnel mit digitalen X.509-Zertifikaten und AES-256-Bit-Verschlüsselung
- Virtuelles Ethernet für eine zuverlässige Übertragung des gesamten Datenverkehrs zwischen Standorten
- IP-Adressverwaltung mit zentral definierter DHCP- und DNS-Serverkonfiguration
- Remote-Aufhebung der Authorisierung von SD-RED-Geräten nach einem bestimmten Inaktivitäts-Zeitraum
- Komprimierung von Tunnelverkehr
- Konfigurationsoptionen für VLAN-Ports

VPN ohne Client

- Einzigartiges verschlüsseltes HTML5-Self-Service-Portal von Sophos mit Unterstützung von RDP, SSH, Telnet und VNC

Web Protection

Web Protection and Control

- Streaming-DPI-Webschutz oder Überprüfung des expliziten Proxymodus
- Expliziter Proxymodus unterstützt eine Authentifizierung pro Verbindung für mehrere Benutzer auf derselben Quell-IP
- Verbesserte Advanced Threat Protection
- URL-Filter-Datenbank mit Millionen von Websites in 92 Kategorien, unterstützt durch die SophosLabs
- Richtlinien mit Surf-Zeitbeschränkungen nach Benutzer/Gruppe
- Zugriffszeitrichtlinien pro Benutzer/Gruppe
- Malware-Scans: Blockieren alle Formen von Viren, Web-Malware, Trojanern und Spyware auf HTTP/S, FTP und in webbasierten E-Mails
- Erweiterter Schutz vor Web-Malware mit JavaScript-Emulation
- Live-Schutz, der verdächtige Dateien in Echtzeit über die Cloud mit neuesten Bedrohungsdaten abgleicht
- Zweite unabhängige Malware-Erkennungs-Engine (Avira) für Dual-Scanning
- Echtzeit- oder Batch-Modus-Scans
- Pharming-Schutz
- Durchsetzung von Mandantenbeschränkungen für O365
- Erkennung und Durchsetzung von SSL-Protokoll-Tunneling
- Zertifikat-Validierung
- Hochleistungs-Caching von Webinhalten
- Erzwungenes Caching für Sophos-Endpoint-Updates
- Dateitypfilter nach MIME-Typ, Erweiterung und aktiven Inhaltstypen (z. B. ActiveX, Applets, Cookies usw.)
- Durchsetzung von YouTube für Schulen pro Richtlinie (Benutzer/Gruppe)
- Durchsetzung von SafeSearch (DNS-basiert) für die führenden Suchmaschinen pro Richtlinie (Benutzer/Gruppe)
- Web Keyword Monitoring und Durchsetzung zum Protokollieren, Melden oder Blockieren von Web-Inhalten, die mit Keyword-Listen übereinstimmen, mit der Option zum Hochladen benutzerdefinierter Listen
- Blockierung potenziell unerwünschter Anwendungen (PUAs)
- Die Option zum Umgehen von Internetrichtlinien für Lehrer und andere Mitarbeiter ermöglicht einen vorübergehenden Zugriff auf gesperrte Websites oder Kategorien, die von ausgewählten Benutzern vollständig angepasst und verwaltet werden können
- Sofortige Alerts für jeden Benutzer, der eine eingeschränkte Webkategorie aufruft (bis zu alle 5 Minuten).

Transparenz über Cloud-Anwendungen

- Das Control Center Widget zeigt die Menge der Daten an, die in Cloud-Anwendungen hochgeladen und aus diesen heruntergeladen wurden, kategorisiert als neu, sanktioniert, nicht sanktioniert oder toleriert
- Erkennen von Schatten-IT auf einen Blick
- Drilldown zum Abruf von Daten zu Benutzern, Traffic und Daten
- Zugriff auf Traffic-Shaping-Richtlinien mit einem Klick
- Filtern der Nutzung von Cloud-Anwendungen nach Kategorie oder Volumen
- Detaillierter, anpassbarer Report zur Nutzung von Cloud-Anwendungen für vollständige Verlaufsreports

Schutz und Kontrolle von Anwendungen

- Synchronized App Control zum automatischen Erkennen, Klassifizieren und Kontrollieren aller unbekannten Windows- und Mac-Anwendungen im Netzwerk durch den Austausch von Informationen zwischen von Sophos verwalteten Endpoints und der Firewall
- Signaturbasierte Application Control mit Mustern für Tausende von Anwendungen
- Transparenz und Kontrolle von Cloud-Anwendungen zur Erkennung von Schatten-IT
- App-Control-Smartfilter, die dynamische Richtlinien ermöglichen, die beim Hinzufügen neuer Muster automatisch aktualisiert werden
- Erfassung und Kontrolle von Micro-Apps
- Application Control basierend auf Kategorie, Merkmalen (z. B. Bandbreite und Produktivitäts-Beeinträchtigung), Technologie (z. B. P2P) und Risikostufe
- Durchsetzung von Application-Control-Richtlinien pro Benutzer oder Netzwerk-Regel

Traffic Shaping für Web und Anwendungen

- Erweiterte Traffic Shaping (QoS)-Optionen nach Web-Kategorie oder Anwendung zur Beschränkung oder Garantie von Upload/Download oder komplette Datenverkehrspriorität und individuelle oder geteilte Bitrate

DNS Protection

Cloudbasierter DNS-Service

- Domain Name Resolution Service
- Cloudbasierter Hochleistungs-DNS-Service
- Mit dem Know-how der SophosLabs und KI
- Blockiert schädliche URLs bei der DNS-Suche
- Granulare Compliance-Kontrollen zum Blockieren unerwünschter Websites nach Kategorie
- Verwaltung über Sophos Central

NDR Essentials

Network Detection and Response

- Cloudbasierte NDR
- Mit der Power von KI
- Erkennt verschlüsselte Bedrohungskommunikation ohne TLS-Entschlüsselung
- Erkennt Algorithmen zur Domänen-Generierung
- Bewertet potenzielle Bedrohungen und warnt bei Bedrohungen, die den festgelegten Schwellenwert überschreiten
- Umfassende Unterstützung für Reporting und Protokollierung

Zero-Day Protection

Dynamische Sandbox-Analyse

- Vollständige Integration in das Dashboard Ihrer Sophos-Sicherheitslösung
- Prüft ausführbare Dateien und Dokumente mit ausführbarem Inhalt (einschließlich .exe, .com, .dll, .doc, .docx, docm und .rtf und PDF) und Archive, die jegliche der oben genannten Dateitypen enthalten (einschließlich ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
- Extensive Verhaltens-, Netzwerk- und Speicheranalyse
- Erkennt Sandbox-Evasionsverhalten
- Machine-Learning-Technologie mit Deep Learning scannt alle verworfenen ausführbaren Dateien
- Umfasst Exploit Prevention und CryptoGuard-Protection-Technologie von Sophos Intercept X
- Detaillierte Reports zu Schad-Dateien mit Screenshots und Möglichkeit zur Dashboard-Dateifreigabe
- Optionale Rechenzentrums-Auswahl und flexible Benutzer- und Gruppenrichtlinien-Optionen für Dateityp, Ausnahmen und Maßnahmen bei der Analyse
- Unterstützt Einmal-Download-Links

Statische Threat-Intelligence-Analyse

- Alle Dateien mit aktivem Code, die über das Internet heruntergeladen werden oder als E-Mail-Anhänge in die Firewall gelangen, z. B. ausführbare Dateien und Dokumente mit ausführbarem Inhalt (einschließlich .exe, .com, .dll, .doc, .docx, docm und .rtf und PDF) und Archive, die jegliche der oben genannten Dateitypen enthalten (einschließlich ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) werden automatisch zur Threat-Intelligence-Analyse gesendet
- Die Dateien werden in der umfangreichen Threat-Intelligence-Datenbank der SophosLabs überprüft und mehreren Machine-Learning-Modellen unterzogen. So wird neue und unbekannte Malware zuverlässig erkannt
- Das umfangreiche Reporting umfasst ein Dashboard Widget für analysierte Dateien, eine detaillierte Liste der analysierten Dateien und die Analyse-Ergebnisse sowie einen detaillierten Report, in dem die Ergebnisse der einzelnen Machine-Learning-Modelle aufgeführt werden

Central Orchestration

SD-WAN-Orchestrierung

- SD-WAN- und VPN-Orchestrierung mit einfacher und automatisierter assistentenbasierter Erstellung von Site-to-Site-VPN-Tunneln zwischen Netzwerk-Standorten unter Verwendung einer optimalen Architektur (Hub-and-Spoke, Full Mesh oder eine Kombination)
- Unterstützt IPsec-, SSL- und RED-VPN-Tunnel. Nahtlose Integration in SD-WAN-Funktionen zur Priorisierung von Anwendungen, Routing-Optimierung und Nutzung mehrerer WAN-Links für Ausfallsicherheit und Performance

Central Firewall Reporting Advanced

- 30 Tage Cloud-Datenspeicherung für Firewall-Verlaufsreports mit erweiterten Funktionen zum Speichern, Planen und Exportieren benutzerdefinierter Reports

Verknüpfung mit XDR und MDR

- Integration mit Sophos XDR und MDR zur Bereitstellung von Telemetriedaten und Bedrohungsinformationen für Threat Hunting und Bedrohungsanalyse
- Sophos Active Threat Response nutzt Bedrohungsfeeds von MDR- und XDR-Analysten, um aktive Bedrohungen im Netzwerk automatisch zu erkennen, zu blockieren und zu isolieren
- Synchronisierte Sicherheit IoC-Telemetrie erhebt wichtige Informationen über kompromittierte Bedrohungen, Benutzer, Prozesse und Geräte

Email Protection

Email Protection and Control

- E-Mail-Scans mit SMTP-, POP3- und IMAP-Unterstützung
- Reputationsdienste mit Spam-Ausbruchsüberwachung auf Basis patentierter Recurrent-Pattern-Detection-Technologie
- Blockieren von Spam und Malware während der SMTP-Transaktion
- DKIM- und BATV-Spam-Schutz
- Spam Greylisting und Sender Policy Framework (SPF)-Schutz
- Empfängerüberprüfung für falsch eingegebene E-Mail-Adressen
- Zweite unabhängige Malware-Erkennungs-Engine (Avira) für Dual-Scans
- Live-Schutz, der verdächtige Dateien in Echtzeit über die Cloud mit neuesten Bedrohungsdaten abgleicht
- Automatische Signatur- und Muster-Updates
- Smart-Host-Unterstützung für ausgehende Relays
- Dateityperkennung/-blockierung/Scans von Anhängen
- Annehmen, Ablehnen oder Verwerfen von übergroßen Nachrichten
- Erkennt Phishing-URLs in E-Mails
- Vordefinierte Regeln zum Scannen von Inhalten und alternativ Möglichkeit zum Erstellen eigener benutzerdefinierter Regeln auf Grundlage einer Vielzahl von Kriterien mit detaillierten Richtlinien-Optionen und -Ausnahmen
- Unterstützung von TLS-Verschlüsselung für SMTP, POP und IMAP
- Automatisches Anfügen von Signaturen zu allen ausgehenden Nachrichten
- E-Mail-Archivdatei
- Individuelle benutzerbasierte Listen zum Blockieren und Erlauben von Absendern über das Benutzerportal

E-Mail-Quarantäneverwaltung

- Optionen für Spam-Quarantäne-Digest und Benachrichtigungen
- Malware- und Spam-Quarantäne mit Such- und Filteroptionen nach Datum, Absender, Empfänger, Betreff und Grund mit der Option zum Freigeben und Löschen von Nachrichten
- Self-Service-Benutzerportal zur Anzeige und Freigabe und von Quarantäne-Nachrichten

E-Mail-Verschlüsselung und DLP

- Zum Patent angemeldete SPX-Verschlüsselung zur unidirektionalen Nachrichtenverschlüsselung
- Selbstregistrierung des Empfängers mit SPX-Passwortverwaltung
- Anfügen von Anhängen zu sicheren SPX-Antworten
- Völlig transparent, keine zusätzliche Software oder weiterer Client erforderlich
- DLP Engine mit automatischem Scannen von E-Mails und Anhängen für vertrauliche Daten
- Vorkonfigurierte, von den SophosLabs gepflegte CCLs (Content Control Lists) für vertrauliche Datentypen (z. B. personenbezogene Daten, Bezahldaten, Gesundheitsdaten)

Webserver Protection

Web Application Firewall (WAF)

- Reverseproxy
- URL Hardening Engine mit Deep-Linking und Directory Traversal Prevention
- Form Hardening Engine
- SQL-Injection-Schutz

- Cross-site-Scripting-Schutz
- Zwei Antivirus-Engines (Sophos und Avira)
- Offloading der HTTPS(TLS/SSL)-Verschlüsselung
- Cookie-Signierung mit digitalen Signaturen
- Pfadbasiertes Routing
- Geo-IP-Richtliniendurchsetzung
- Benutzerdefinierte Verschlüsselungskonfiguration und TLS-Versionsdurchsetzung
- HSTS- und X-Content-Type-Options-Durchsetzung
- Unterstützung des „Outlook Anywhere“-Protokolls
- Reverse Authentication (Offloading) für formularbasierte und Basisauthentifizierung zum Serverzugriff
- Abstraktion von virtuellen und physischen Servern
- Integrierter Load Balancer verteilt Besucher auf mehrere Server
- Möglichkeit, einzelne Prüfungen bei Bedarf gezielt zu überspringen
- Abgleich von Anfragen von Quellnetzwerken oder angegebenen Ziel-URLs
- Unterstützung logischer „and/or“-Operatoren
- Unterstützt die Kompatibilität mit verschiedenen Konfigurationen und nicht standardmäßigen Bereitstellungen
- Optionen zum Ändern von Performance-Parametern der Web Application Firewall
- Option zur Begrenzung der Scangröße
- Erlauben/Blockieren von IP-Bereichen
- Unterstützung von Platzhaltern für Serverpfade und Domänen
- Automatisches Anfügen von Präfix/Suffix für die Authentifizierung

Reporting und Protokollierung

Central Firewall Reporting

- Vorkonfigurierte Reports mit flexiblen Anpassungsmöglichkeiten
- Reporting für die Sophos Firewalls: Hardware, Software, virtuell und Cloud
- Intuitive Benutzeroberfläche mit grafischer Datenaufbereitung
- Im Report Dashboard übersichtliche Anzeige aller Ereignisse der letzten 24 Stunden
- Einfache Identifizierung von Netzwerkaktivitäten, Trends und potenziellen Angriffen
- Einfaches Back-up von Protokollen mit schnellem Abrufen für Audit-Zwecke
- Einfache Bereitstellung – kein technisches Fachwissen notwendig

Central Firewall Reporting Advanced

- Aggregierte Reports für mehrere Firewalls
- Speichern benutzerdefinierter Report-Vorlagen
- Geplante Reports
- Exportieren von Reports ins PDF-, CFV- oder HTML-Format
- Bis zu ein Jahr Datenspeicher pro Firewall
- MDR/XDR Data Lake Connector für Threat Hunting

On-Box Reporting

- HINWEIS: Das Reporting der Sophos Firewall ist kostenlos inbegriffen. Die Verfügbarkeit einzelner Protokolle, Reports und Widgets kann jedoch von den jeweils lizenzierten Schutzmodulen abhängen.
- Hunderte von On-Box-Reports mit benutzerdefinierten Report-Optionen: Dashboards (Datenverkehr, Sicherheit und User Threat Quotient), Anwendungen (Anwendungsrisiko, blockierte Anwendungen, synchronisierte Anwendungen, Suchmaschinen, Webserver, Web Keyword Match, FTP), Netzwerk und Bedrohungen (Active Threat Response und Bedrohungsfeeds, Security Heartbeat, IPS, Wireless, Zero-Day-Bedrohungsschutz), VPN, E-Mail, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP V3, CIPA)
- Überwachung der aktuellen Aktivität: Systemstatus, Live-Benutzer, IPsec-Verbindungen, Remote-Benutzer, Live-Verbindungen, Wireless Clients, Quarantäne und DoS-Angriffe
- Überwachung der SD-WAN-Link-Performance auf Störungen, Latenz und Paketverlust
- Anonymisierungs-Funktion für Reports
- Report-Planung für mehrere Empfänger nach Report-Gruppe mit flexiblen Frequenzoptionen

- Exportieren von Reports ins HTML-, PDF- oder Excel(XLS)-Format
- Report-Lesezeichen
- Anpassung der Protokollspeicherung nach Kategorie
- Log Viewer mit vollem Funktionsumfang, Spalten- und Detailansicht sowie leistungsstarken Filter- und Suchoptionen, verlinkter Regel-ID und anpassbarer Datenansicht

Central Management

Sophos Central

- Mit der cloudbasierten Verwaltung und Report-Erstellung von Sophos Central für mehrere Firewalls erhalten Sie effiziente Management-Funktionen für Gruppenrichtlinien und eine zentrale Konsole für alle Ihre Sophos-IT-Security-Produkte
- Mithilfe der Verwaltung von Gruppenrichtlinien können Objekte, Einstellungen und Richtlinien einmal geändert und automatisch mit allen Firewalls in der Gruppe synchronisiert werden
- Der Task-Manager bietet einen vollständigen Audit-Verlauf und Statusüberwachung von Änderungen der Gruppenrichtlinien
- Über die Verwaltung der Backup-Firmware in Sophos Central werden die letzten fünf Back-up-Dateien für jede Firewall gespeichert. Eine dieser Dateien kann für eine permanente Speicherung und einfachen Zugriff angeheftet werden
- Die Planung von Firmware-Updates über Sophos Central ermöglicht jederzeit eine einfache automatisierte Installation von Updates
- Die Erstkonfiguration kann per Zero-Touch-Bereitstellung in Sophos Central erfolgen. Diese Konfiguration kann anschließend exportiert und per Flash-Laufwerk auf das Gerät geladen werden, wodurch das Gerät automatisch wieder mit Sophos Central verbunden wird

Zero Trust Network Access

- Integriertes Sophos ZTNA-Gateway für sicheren Zugriff auf Anwendungen, die hinter der Firewall gehostet werden
- Verwaltung über Sophos Central

Secure by Design

- Der Sophos Firewall Health Check gleicht eine Vielzahl von Konfigurationseinstellungen mit Best Practices ab, um potenzielle Risiken zu identifizieren und Probleme durch einfachen Drilldown zu beheben.
- Automatisierte, drahtlose Over-the-Air-Hotfix-Funktion zur Behebung von Schwachstellen ohne Ausfallzeiten
- Gehärteter Kernel für verbesserte Sicherheit, Performance und Skalierbarkeit mit strenger Isolierung und Schutz vor Seitenkanalangriffen
- Sophos bietet Remote Integrity Monitoring der Systemintegrität mithilfe eines integrierten XDR-Sensors, um die Systemintegrität in Echtzeit zu überwachen. Dies umfasst die Erkennung nicht autorisierter Konfigurationen, die Ausführung von Schadcode, Dateimanipulationen und mehr, um Angriffe schnell zu erkennen und darauf zu reagieren.
- Next-Gen-Xstream-Architektur mit neuer Steuerebene für maximale Sicherheit und Skalierbarkeit
- Containerisierung wichtiger Trust Boundaries und Benutzer/VPN-Portale
- Verschlüsselte und sichere zentrale Verwaltung über Sophos Central, wodurch Remote-Zugriff für Administratoren überflüssig wird
- Die systemweite Multi-Faktor-Authentifizierung schützt vor Harvesting von Zugangsdaten und Brute-Force-Angriffen
- Integriertes ZTNA-Gateway für sichereren Remote-Zugriff und Anwendungsschutz
- Sichere, sofort einsatzbereite Bereitstellungen gewährleisten die Implementierung von Security Best Practices mit strengen Zugriffskontrollen.

Übersicht der Funktionen der Sophos Firewall nach Subscription

	Xstream Protection Bundle							Separat erhältlich		
	Standard Protection Bundle					Separat erhältlich				
	Basis-Firewall	Network Protection	Web Protection	DNS Protection	Bundle-spezifische Funktionen	Zero-Day Protection	Central Orchestration	Central Firewall Reporting Adv.	Email Protection	Webserver Protection
Allgemeine Verwaltung (inkl. HA)	✔									
Xstream-Architektur	✔									
Firewall, Networking und Routing	✔									
Xstream SD-WAN	✔									
Basisfunktionen für Traffic Shaping und Kontingente	✔									
Secure Wireless	✔									
Authentifizierung	✔									
Self-Service-Portal für Benutzer	✔									
VPN (IPsec, SSL usw.)	✔									
RED Site-to-Site VPN	✔									
Sophos Connect VPN Client	✔									
Intrusion Prevention (IPS)		✔								
Active Threat Response										
Sophos X-Ops-Bedrohungsfeeds		✔								
MDR/XDR-Bedrohungs-Feed					✔					
Bedrohungsfeeds von Drittanbietern					✔					
Synchronized Security Heartbeat		✔								
Verwaltung von SD-RED-Geräten		✔								
VPN ohne Client		✔								
Synchronized Application Control			✔							
Web Protection and Control			✔							
Schutz und Kontrolle von Anwendungen			✔							
Transparenz über Cloud-Anwendungen			✔							
Traffic Shaping für Web und Anwendungen			✔							
DNS Security und Compliance				✔						
NDR Essentials					✔					
Dynamische Sandbox-Analyse						✔				
Threat Intelligence Analysis						✔				
SD-WAN-Orchestrierung							✔			
Central Firewall Reporting-Daten*		7 Tage	7 Tage	7 Tage	7 Tage	7 Tage	30 Tage	Bis zu 1 Jahr	7 Tage	7 Tage
CFR-Advanced-Funktionen							✔	✔		
Email Protection and Control									✔	
E-Mail-Quarantäneverwaltung									✔	
E-Mail-Verschlüsselung und DLP									✔	
Web Application Firewall (WAF)										✔
On-Box-Protokollierung/Reporting	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Sophos Central Management**		✔	✔	✔	✔	✔	✔	✔	✔	✔
ZTNA Gateway**		✔	✔	✔	✔	✔	✔	✔	✔	✔
Secure by Design	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Hinweis: Einige Funktionen werden auf den Modellen XGS 87 und XGS 88 nicht unterstützt (On-Box-Reporting, Antivirus-Scans mit zwei Engines, WAF-AV-Scans und Message-Transfer-Agent[MTA]-Funktionalität)

Die angebotenen MSP-Lizenzen weichen geringfügig von den oben genannten ab

* Die Länge der Datenspeicherung ist eine Schätzung basierend auf der durchschnittlichen Netzwerknutzung und variiert je nach tatsächlichem Protokolldatenvolumen. Tool zur Schätzung des Speicherbedarfs.

** In jedem Bundle, Support-Vertrag und jeder Protection Subscription enthalten. Kunden mit einer Basislizenz müssen nur Support hinzufügen, um diese Funktionen nutzen zu können.

Sophos Firewall Feature-Liste

SOPHOS

Übersicht der Funktionen der Sophos Firewall nach Subscription

	Enhanced Support (In Standard und Xstream Protection Bundles enthalten)	Enhanced Plus Support (verfügbar als Upgrade von Enhanced Support)
Rund um die Uhr erreichbarer Multi-Channel-Support (Telefon, Webportal, Chat), einschließlich Remote-Unterstützung und Selbsthilfe-Zugriff auf KB und Support-Foren	✔	✔
Firmware-Downloads, Updates und Maintenance Releases **	✔	✔
Sophos Central Management, Reporting und ZTNA-Gateway	✔	✔
Vorabaustausch-Service für aktive Geräte	✔	✔
Vorabaustausch-Service für ein passives HA-Gerät*		✔
Vorabaustausch-Service für SD-RED/APX-Geräte		✔
VIP-Zugriff (Anrufe werden an Senior Engineers weitergeleitet)		✔
Remote-Consulting (2-8 Stunden pro Jahr)		✔

* Um den Vorabaustausch-Service für ein passives HA-Gerät in Anspruch nehmen zu können, muss das aktive Gerät über eine Enhanced Plus Support-Lizenz verfügen

Weitere Informationen finden Sie im Sophos Support Service Guide.

** Hinweis: Für den Erhalt von Firmware-Updates muss beim Kauf von jedem einzelnen Modul Support hinzugefügt werden

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.:+49 611 5858 0
E-Mail: sales@sophos.com

2025-12-15 DE (DD)