ELENCO DELLE FUNZIONALITÀ

Elenco delle funzionalità di Sophos Firewall

Sophos Firewall

Caratteristiche principali

- L'architettura Xstream offre livelli estremi di visibilità, protezione e performance, grazie all'elaborazione dei pacchetti basata su flusso
- La funzionalità Xstream TLS inspection offre alti livelli di performance, supporto di TLS 1.3 senza bisogno di downgrade, policy di classe Enterprise indipendenti dalla porta con eccezioni predefinite, nonché ottima visibilità sulla dashboard e opzioni di risoluzione dei problemi di compatibilità
- Il motore DPI Xstream garantisce protezione mediante scansione del flusso per IPS, antivirus, e controllo del web e delle app, nonché TLS inspection, tutte incluse in un unico motore caratterizzato da alti livelli di performance
- Il Network Flow FastPath di Xstream utilizza le policy per identificare il traffico attendibile e applicare automaticamente un sistema di accelerazione intelligente
- La SD-WAN Xstream offre una selezione dei link basata sulla performance, con reindirizzamento a impatto zero, monitoraggio della SD-WAN, strumenti di orchestrazione SD-WAN multisito e accelerazione FastPath del traffico dei tunnel VPN IPsec
- L'interfaccia utente è appositamente progettata con un Control Center interattivo, e utilizza una segnaletica basata sui colori del semaforo (rosso, giallo, verde) per identificare immediatamente e a colpo d'occhio gli elementi che richiedono attenzione
- Il Control Center fornisce approfondimenti immediati sull'integrità degli endpoint, sulle applicazioni Mac e Windows non identificate, sulle applicazioni cloud e sullo shadow IT, nonché su payload sospetti, utenti a rischio, minacce avanzate, attacchi alla rete, siti web discutibili e molto di più
- Navigazione ottimizzata con tutte le funzionalità a portata di due clic, e ricerca intelligente
- Il widget per le policy nel Control Center monitora l'attività delle policy che riguardano l'azienda, gli utenti e la rete, tenendo traccia di quelle non utilizzate, disattivate, modificate e appena create
- Il modello di policy unificato combina tutte le regole di ispezione per firewall, NAT e TLS in un'unica schermata, offrendo opzioni di raggruppamento, filtro e ricerca
- Gestione semplificata delle regole del firewall per gruppi di regole di grandi dimensioni, con raggruppamento automatico e manuale personalizzato, più una funzionalità di visualizzazione immediata al passaggio del mouse e indicatori di implementazione
- Tutte le regole firewall forniscono un riepilogo immediato delle misure di sicurezza e dei controlli applicati per antivirus, sandboxing, IPS, web, app, shaping del traffico (QoS) e Heartbeat
- Le policy predefinite per IPS, web, app, TLS e shaping del traffico (QoS) offrono configurazione rapida e personalizzazione semplificata per gli scenari di distribuzione più comuni (ad es. policy per CIPA, ambienti di lavoro e altri casi)
- Sophos Security HeartbeatTM collega gli endpoint Sophos al firewall per condividere lo stato di integrità e i dati di telemetria, consentendo così di identificare immediatamente gli endpoint compromessi o a rischio
- La Risposta alle minacce attive identifica, blocca e risponde automaticamente agli active adversary, basandosi sui feed sulle minacce forniti dai SophosLabs, dagli analisti MDR o da terze parti
- Synchronized Application Control identifica tutte le applicazioni Mac/Windows sconosciute presenti sulla rete, classificandole e permettendone automaticamente il controllo
- La Visibilità sulle applicazioni cloud consente di individuare immediatamente lo shadow IT e offre opzioni di shaping del traffico con un solo clic
- Lo strumento di simulazione delle policy permette di simulare e testare le regole firewall e le policy web in base all'utente, all'IP e all'ora del giorno
- I principi di Secure by Design garantiscono la protezione del firewall contro gli attacchi
- API di configurazione per tutte le funzionalità di integrazione RMM/PSA
- L'integrazione NDR basata sul cloud migliora il rilevamento degli active adversary
- Il gateway ZTNA integrato in ogni firewall semplifica l'accesso sicuro alle applicazioni da qualsiasi luogo

SOPHOS

- La gestione e la reportistica basate sul cloud di Sophos Central per più firewall permettono di gestire le policy di gruppo e offrono un'unica console per tutti i prodotti di sicurezza informatica Sophos
- La semplice procedura guidata di installazione permette di distribuire il software in maniera rapida e immediata, poiché richiede solo pochi minuti
- Distribuzione e configurazione zero-touch in Sophos Central per i nuovi firewall
- Perfetta integrazione con Sophos MDR e XDR

Base Firewall

Gestione generale

- Un'interfaccia utente appositamente progettata per semplificare le interazioni, più gestione delle regole firewall per quantità elevate di regole, con opzioni come il raggruppamento (per visualizzare le regole a colpo d'occhio) e indicatori di implementazione
- Supporto dell'autenticazione a due fattori (One-Time Password) per l'accesso amministratore, il portale utenti, IPsec, VPN SSL e WAF
- Strumenti avanzati di registrazione nei log e risoluzione dei problemi nella GUI (ad esempio, l'acquisizione dei pacchetti)
- Supporto della disponibilità elevata (High Availability, HA) con clustering di due dispositivi in modalità attiva-attiva o attiva-passiva e configurazione Quick HA plug-and-play, che supporta più link di sincronizzazione ridondanti
- Interfaccia della riga di comando (CLI) completa, accessibile dalla GUI
- Amministrazione basata sui ruoli con integrazione Azure AD per il Single Sign-On
- Aggiornamenti del firmware tramite SSL con certificate pinning per la massima sicurezza
- Definizioni di oggetti di sistema riutilizzabili e ricercabili in base a rete, servizio, host, periodi di tempo, utenti e gruppi, client e server
- Portale utenti self-service
- Monitoraggio delle modifiche della configurazione
- Controllo flessibile dell'accesso ai dispositivi per i servizi, in base alle aree
- Opzioni di notifica tramite e-mail o trap SNMP
- SNMP v3 (incluso il monitoraggio dell'hardware) e monitoraggio di Netflow/sFlow
- Supporto per la gestione centralizzata tramite Sophos Central (disponibile solo per i clienti con una licenza di supporto in corso di validità)
- Backup e ripristino delle configurazioni: localmente, tramite FTP o e-mail; on-demand, quotidianamente, settimanalmente o mensilmente, con la possibilità di mappare nuovamente le porte durante l'upgrade delle appliance hardware
- Supporto dei certificati Let's Encrypt per WAF, SMTP, configurazione di TLS, accesso tramite hotspot, console di Web Admin, portale utenti, captive portal, portale VPN e portale SPX
- API per integrazioni di terze parti
- Possibilità di rinominare l'interfaccia
- Opzione di accesso remoto per il Supporto tecnico Sophos
- Gestione basata sul cloud delle licenze, tramite MySophos

Firewall, reti e routing

- Firewall con Deep Packet Inspection stateful
- L'architettura di elaborazione dei pacchetti Xstream offre livelli estremi di visibilità, protezione e performance, grazie all'elaborazione dei pacchetti basata sul flusso
- Ispezione TLS Xstream con alti livelli di performance, supporto di TLS 1.3 senza bisogno di downgrade, policy di classe Enterprise indipendenti dalla porta, ottima visibilità sulla dashboard e risoluzione dei problemi di compatibilità
- Il motore DPI Xstream garantisce protezione mediante scansione del flusso per IPS, antivirus, e controllo del web e delle app, nonché TLS inspection, tutte opzioni incluse in un unico motore caratterizzato da alti livelli di performance
- Il Network Flow FastPath di Xstream sfrutta le policy per identificare il traffico attendibile, il traffico VPN IPSec e il traffico TLS crittografato, e applicare automaticamente un sistema di accelerazione intelligente
- Policy basate su utenti, gruppi, ora o rete
- Policy basate sull'ora di accesso per utenti/gruppi
- Applicazione di policy in tutte le aree, le reti o a seconda del tipo di servizio
- Isolamento delle aree e supporto delle policy basate sulle aree
- Aree predefinite per LAN, WAN, DMZ, RETE LOCALE, VPN e Wi-Fi
- Aree personalizzate su LAN o DMZ
- Policy NAT personalizzabili con mascheramento dell'IP e supporto completo degli oggetti per reindirizzare o inoltrare più servizi in un'unica regola, con una comoda procedura guidata per la creazione di regole NAT che consente di creare facilmente e velocemente regole NAT con pochi clic.
- Definizioni di oggetti di rete riutilizzabili per tutte le regole, con ricerca globale intelligente a testo libero

- Protezione antiflood: blocco di DoS, DDoS e portscan
- Blocco per paese tramite IP geo
- Routing: statico, multicast (PIM-SM) e dinamico: RIP, BGP, OSPFv3 (IPv6) BGPv6
- Clonazione di route statiche per attivarle o disattivarle; ridistribuzione di route BGP dinamiche in OSPFv3; utilizzo di opzioni di Blackhole routing ed Equal-Cost Multi-Path (ECMP) per il bilanciamento del carico
- Supporto di proxy upstream
- Routing multicast indipendente dal protocollo con snooping IGMP
- Connessione tramite bridge con supporto di STP e inoltro della trasmissione ARP
- Supporto DHCP per VLAN e tag
- Supporto bridge per VLAN
- Supporto per frame jumbo
- Attivazione/disattivazione di interfacce fisiche
- Supporto di WAN wireless (non disponibile nelle distribuzioni virtuali)
- L'aggregazione dei link per l'interfaccia 802.3ad
- Configurazione completa di DNS, DHCP e NTP
- DNS dinamico (DDNS)
- Certificazione di approvazione del programma per il logo IPv6 Ready
- Delega del prefisso DHCP IPv6
- Supporto del tunneling IPv6, inclusi 6in4, 6to4, 4in6 e distribuzione rapida di IPv6 (6rd) tramite IPsec

SD-WAN Xstream

- I profili SD-WAN di Xstream supportano diverse opzioni per i link WAN, tra cui VDSL, DSL, cavo, LTE/cellulare e MPLS
- Le condizioni SLA basate sulla performance selezionano automaticamente il link WAN migliore in base a jitter, latenza o perdita dei pacchetti
- Bilanciamento del carico SD-WAN su più link SD-WAN, con ponderazione tramite meccanismo round robin o strategie di persistenza della sessione
- Il reindirizzamento a impatto zero mantiene le sessioni delle applicazioni quando la performance del link scende al di sotto delle soglie e si passa a un link WAN con livelli più alti di performance
- I grafici di monitoraggio della SD-WAN forniscono informazioni in tempo reale sulla latenza, sul jitter e sulla perdita dei pacchetti per tutti i link WAN
- Accelerazione FastPath di Xstream per il traffico dei tunnel IPsec SD-WAN
- Synchronized SD-WAN (una funzionalità di Synchronized Security) utilizza la maggiore chiarezza e attendibilità nell'identificazione delle applicazioni, ottenuta grazie alla condivisione di informazioni di Synchronized Application Control tra Sophos Firewall e gli endpoint gestiti da Sophos
- Routing delle applicazioni sui link preferiti, grazie al routing basato sulle regole firewall o sulle policy
- Potente supporto della VPN, che include VPN IPsec e SSL
- Esclusivo tunnel RED Layer 2 con routing

Funzionalità di base di shaping del traffico e quote

- Shaping del traffico flessibile, basato sulla rete o sull'utente (QoS) (opzioni avanzate di shaping del traffico web e delle app incluse con la sottoscrizione Web Protection)
- Impostazione di quote di traffico basate sugli utenti per upload/download o traffico totale, ciclico o non ciclico
- Ottimizzazione del VoIP in tempo reale
- Contrassegno DSCP

Secure Wireless

- Facile distribuzione plug-and-play degli access point wireless Sophos (solo APX Series): vengono visualizzati automaticamente nel Control Center del firewall
- Monitoraggio e gestione centralizzati degli AP e dei client wireless, tramite il controller wireless integrato
- Connessione degli AP tramite bridge a LAN, VLAN o a un'area separata con opzioni di isolamento dei client
- Supporto di più SSID per radio, inclusi gli SSID nascosti
- Supporto di diversi standard di sicurezza e crittografia, tra cui WPA2 Personal ed Enterprise
- Opzione di selezione della larghezza del canale
- Supporto di IEEE 802.1X (autenticazione RADIUS) con supporto per server primario e secondario
- Supporto di 802.11r (transizione rapida)
- Supporto di hotspot per voucher (personalizzati), password del giorno o accettazione dei termini e delle condizioni

- Accesso wireless a Internet per gli utenti guest con opzioni walled garden
- Accesso alla rete wireless basato sull'ora
- Modalità rete mesh con funzionalità di ripetizione e bridge per il wireless con gli AP supportati
- Ottimizzazione della selezione automatica dei canali in background
- Supporto dell'accesso tramite HTTPS

Autenticazione

- L'ID utente sincronizzato utilizza Synchronized Security per condividere l'ID dell'utente di Active Directory attualmente connesso tra gli endpoint Sophos e il firewall, senza alcun bisogno di installare un agente sul server di AD o sul client.
- Autenticazione tramite: Active Directory, eDirectory, RADIUS, LDAP e TACACS+
- Agenti di autenticazione del server per Active Directory SSO, STAS, SATC
- Single Sign-On Active Directory, eDirectory, RADIUS Accounting
- Single Sign-On di Azure AD per l'accesso amministratore alla console di WebAdmin
- Single Sign-On di Azure AD per l'autenticazione degli utenti per l'accesso al web tramite captive portal
- SSO di AD trasparente con implementazione di HSTS, che consente di utilizzare handshake Kerberos e NTLM su HTTP o HTTPS
- Importazione di gruppi di Azure AD e supporto di RBAC
- Agenti di autenticazione del client per Windows, Mac OS X, Linux 32/64
- Autenticazione SSO tramite browser: autenticazione del proxy (NTLM) trasparente e Kerberos
- Captive portal del browser
- Certificati di autenticazione per iOS e Android
- Servizi di autenticazione per IPsec, SSL, L2TP, PPTP
- Supporto dell'autenticazione di Google Chromebook per ambienti con Active Directory e Google G Suite
- Integrazione di Google Workspace tramite client LDAP con SSO di Google Chromebook
- Autenticazione basata su API

Portali self-service per utenti e VPN

- SNMP v3 (incluso il monitoraggio dell'hardware) e monitoraggio di Netflow/sFlow
- Download del Sophos Authentication Client
- Download del client di accesso remoto SSL (Windows) e dei file di configurazione (altri sistemi operativi)
- Informazioni sull'accesso agli hotspot
- Modifica di nome utente e password
- Visualizzazione dell'utilizzo personale di Internet
- Accesso ai messaggi in quarantena e gestione gli elenchi dei mittenti bloccati/autorizzati in base agli utenti (richiede Email Protection)

Opzioni VPN di base

- VPN site-to-site: SSL, IPSec, AES/3DES a 256 bit, PFS, RSA, certificati X.509, chiave precondivisa
- Tunnel VPN site-to-site Sophos RED (affidabile e leggero)
- Accelerazione FastPath di Xstream per il traffico del tunnel IPsec (sia site-to-site, che di accesso remoto)
- Strumenti di importazione, monitoraggio e gestione per i VPC di AWS
- L2TP e PPTP
- VPN basata sulla route con selettori del traffico
- Accesso remoto: supporto di client VPN SSL, IPsec, iPhone/iPad/Cisco/Android
- Supporto di IKEv2
- Failover stateful con disponibilità elevata della connessione IPsec per RBVPN, PBVPN e VPN di accesso remoto, senza perdita degli eventi di sessione in scenari di failover con disponibilità elevata
- Monitoraggio dello stato del tunnel VPN IPsec tramite SNMP
- Supporto avanzato di IPsec per PSK unico e DH-Group 27-30/RFC6954
- Client SSL per Windows e download della configurazione tramite portale utenti

Sophos Connect Client

- Autenticazione: Chiave precondivisa (PSK), PKI (X.509), token e XAUTH
- Supporto del Single Sign-On di Entra ID (Azure AD)

- Abilitazione di Synchronized Security e Security Heartbeat per gli utenti connessi da remoto
- Split tunneling intelligente per il routing ottimale del traffico
- Supporto dell'attraversamento NAT
- Monitoraggio dei client per una panoramica grafica dello stato di connessione
- Supporto di client Mac (IPsec) e Windows (SSL/IPsec)

Network Protection

Intrusion Prevention (IPS)

- Motore Deep Packet Inspection next-gen ad alti livelli di performance, con pattern IPS selettivi che possono essere applicati in base alle regole del firewall per garantire massima performance e protezione.
- Migliaia di firme
- Selezione granulare delle categorie
- Supporto di firme IPS personalizzate
- I filtri intelligenti per le policy IPS consentono di implementare policy dinamiche che si aggiornano automaticamente man mano che vengono aggiunti nuovi pattern

Risposta alle minacce attive e Security Heartbeat™

- La Risposta alle minacce attive monitora/blocca automaticamente le APT e altre minacce identificate dai feed di Sophos X-Ops per garantire protezione avanzata contro minacce provenienti da bot e active adversary che cercano di contattare destinazioni pericolose utilizzando rilevamenti DNS, AFC e firewall su più livelli
- La Risposta alle minacce attive monitora/blocca automaticamente le minacce identificate dai feed di MDR/XDR pubblicati da un analista SOC di Sophos o del cliente/partner quando Sophos Firewall con Xstream Protection viene utilizzato insieme a Sophos MDR/XDR
- La Risposta alle minacce attive monitora/blocca automaticamente i feed sulle minacce di terze parti, generati da origini di dati di intelligence del settore, del mercato verticale o dell'area geografica, grazie a Xstream Protection
- Sophos Synchronized Security Heartbeat segnala immediatamente i dispositivi compromessi con stato di Heartbeat rosso che cercano di contattare qualsiasi indicatore di minacce identificato dalla Risposta alle minacce attive e dai rispettivi feed sulle minacce. Lo stato di Heartbeat è monitorato anche dagli endpoint gestiti da Sophos; viene poi condiviso con il firewall, includendo dettagli quali l'host, l'utente, il processo, il numero di incidenti e l'ora della compromissione
- Le condizioni del Sophos Security Heartbeat possono essere associate a qualsiasi regola firewall, limitando automaticamente l'accesso alle risorse e ai segmenti di rete per un dispositivo che è stato compromesso, fino a quando non torna sicuro
- Sophos Firewall avvia automaticamente anche la protezione contro i movimenti laterali nel caso in cui un endpoint gestito venga compromesso: contatta tutti gli endpoint con stato di integrità integro che sono gestiti da Sophos e li informa che devono rifiutare il traffico proveniente dal dispositivo compromesso, isolando così il dispositivo colpito, anche se si trova sullo stesso segmento LAN.

Gestione dei dispositivi SD-RED

- Gestione centralizzata di tutti i dispositivi SD-RED
- Nessuna configurazione: connessione automatica tramite un servizio di provisioning basato sul cloud
- Tunnel crittografato sicuro, che utilizza certificati digitali X.509 e crittografia AES a 256 bit
- Ethernet virtuale per un trasferimento affidabile di tutto il traffico tra le varie sedi
- Gestione degli indirizzi IP con configurazione definita centralmente per i server DHCP e DNS
- Rimozione remota dell'autorizzazione per i dispositivi RED, dopo un determinato periodo di inattività
- Compressione del traffico nel tunnel
- Opzioni di configurazione per le porte VLAN

VPN indipendente client

- Un esclusivo portale self-service Sophos HTML5 crittografato, con supporto di RDP, SSH, Telnet e VNC

Protezione web

Protezione e controllo web

- Protezione web DPI in streaming o ispezione in modalità proxy esplicita
- La modalità proxy esplicita supporta l'autenticazione in base alla connessione per più utenti sullo stesso IP di origine
- Advanced Threat Protection più potente
- Database di filtri degli URL con milioni di siti suddivisi in 92 categorie, con supporto dei SophosLabs
- Policy basate sull'ora per la quota di navigazione per utente/gruppo

- Policy basate sull'ora di accesso per utenti/gruppi
- Scansione antimalware: blocco di tutte le forme di virus, malware web, trojan e spyware su HTTP/S, FTP, più e-mail basate sul web.
- Protezione avanzata dai malware web con emulazione di JavaScript
- Live Protection in tempo reale, ricerche in tempo reale nel cloud per ottenere i più recenti dati di intelligence sulle minacce
- Secondo motore di rilevamento antimalware indipendente (Avira) per la doppia scansione
- Scansione in tempo reale o in modalità batch
- Protezione antipharming
- Implementazione delle restrizioni per i tenant in O365
- Rilevamento e applicazione del tunneling per il protocollo SSL
- Convalida dei certificati
- Caching dei contenuti web ad alti livelli di performance
- Caching forzato per gli aggiornamenti di Sophos Endpoint
- Filtro dei tipi di file in base al tipo MIME, all'estensione e ai tipi di contenuti attivi (ad es. Activex, applet, cookie ecc.)
- Implementazione di YouTube for Schools in base alla policy (utente/gruppo)
- Applicazione di SafeSearch (basata sul DNS) per i principali motori di ricerca, in base alla policy (utente/gruppo)
- Monitoraggio e applicazione di parole chiave sul web per registrare nei log, segnalare o bloccare i contenuti web corrispondenti a voci negli elenchi di parole chiave, con l'opzione di caricare elenchi personalizzati
- Blocco delle applicazioni potenzialmente indesiderate (PUA)
- Possibilità di sovrascrivere policy web per insegnanti o altri membri del personale, in modo da consentire temporaneamente l'accesso a siti o categorie bloccati; questa opzione è completamente personalizzabile e può essere gestita da utenti selezionati
- Avvisi immediati per tutti gli utenti che navigano su pagine web appartenenti a una categoria soggetta a restrizioni (con frequenza fino a ogni 5 minuti)

Visibilità sulle applicazioni cloud

- Il widget del Control Center mostra la quantità di dati caricati e scaricati su applicazioni cloud classificate come nuove, autorizzate, non autorizzate o tollerate
- Individuazione dello Shadow IT a colpo d'occhio
- Approfondimenti per ottenere dettagli su utenti, traffico e dati
- Accesso con un solo clic a policy di shaping del traffico
- Filtro dell'utilizzo delle applicazioni cloud in base alla categoria o al volume
- Report dettagliato e personalizzabile sull'utilizzo delle applicazioni cloud, per funzionalità complete di reportistica storica

Protezione e controllo delle applicazioni

- Synchronized App Control per identificare, classificare e controllare automaticamente tutte le applicazioni Windows e Mac sconosciute presenti nella rete, attraverso la condivisione di informazioni tra gli endpoint gestiti da Sophos e il firewall
- Controllo delle applicazioni basato sulle firme, con pattern per migliaia di applicazioni
- Visibilità e controllo sulle applicazioni cloud per individuare lo shadow IT
- Filtri intelligenti per il controllo delle app, che permettono di implementare policy dinamiche che si aggiornano automaticamente man mano che vengono aggiunti nuovi pattern
- Individuazione e controllo delle microapp
- Controllo delle applicazioni in base a categoria, caratteristiche (ad es. consumo della larghezza di banda e produttività), tecnologie (ad es. P2P) e livello di rischio.
- Implementazione delle policy di controllo delle applicazioni in base all'utente o alla regola di rete

Shaping del traffico web e delle app

- Opzioni ottimizzate di shaping del traffico (QoS) a seconda della categoria web o dell'applicazione, per limitare o autorizzare upload/download, oppure priorità del traffico totale e velocità di trasmissione in maniera individuale o condivisa

DNS Protection

Servizio DNS basato sul cloud

- Servizio di risoluzione dei nomi di dominio
- Servizio DNS basato sul cloud ad alti livelli di performance
- Con tecnologia dei SophosLabs e IA
- Blocco degli URL dannosi al livello della ricerca DNS
- Controlli di conformità granulari, per bloccare i siti web indesiderati in base alla categoria
- Gestione da Sophos Central

NDR Essentials

Network Detection and Response

- NDR basato sul cloud
- Tecnologie di IA
- Rilevamento delle comunicazioni crittografate delle minacce, senza bisogno della decrittografia TLS
- Rilevamento degli algoritmi di generazione di domini
- Valutazione delle potenziali minacce, con avvisi in caso di minacce che superano la soglia impostata
- Supporto completo della reportistica e della generazione di log

Protezione zero-day

Analisi dinamica nella sandbox

- Integrazione completa nella dashboard della tua soluzione di cybersecurity Sophos
- Ispezione dei file eseguibili e dei documenti che contengono contenuti eseguibili (inclusi i file .exe, .com, .dll, .doc, .docx, docm, .rtf e PDF), nonché degli archivi che contengono uno dei tipi di file elencati sopra (tra cui ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
- Analisi aggressiva dei comportamenti, della rete e della memoria
- Rilevamento dei comportamenti di elusione nella sandbox
- La tecnologia di machine learning con deep learning esegue la scansione di tutti i file eseguibili scartati
- Sono incluse la prevenzione degli exploit e la tecnologia CryptoGuard Protection di Sophos Intercept X
- Report approfonditi sui file dannosi, con screenshot e opzioni di rilascio dei file dalla dashboard
- Selezione facoltativa del data center e opzioni flessibili per le policy di utenti e gruppi relative a tipi di file, esclusioni e azioni sulle analisi
- Supporto di link di download monouso

Analisi statica dei dati di intelligence sulle minacce

- Tutti i file contenenti codice attivo che sono stati scaricati dal web o che vengono inviati al firewall come allegati e-mail, ad es. file eseguibili e documenti con contenuti eseguibili (inclusi file .exe, .com, .dll, .doc, .docx, docm, .rtf e PDF), nonché gli archivi contenenti uno qualsiasi dei tipi di file elencati sopra (tra cui ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) vengono automaticamente inviati per essere sottoposti ad analisi basate sui dati di intelligence sulle minacce
- I file vengono messi a confronto con l'ampio database di dati di intelligence sulle minacce dei SophosLabs e sono analizzati da diversi modelli di machine learning per identificare malware nuovi e sconosciuti
- La reportistica completa include un widget della dashboard per i file analizzati, un elenco dettagliato dei file che sono stati esaminati, e i risultati delle analisi, nonché un report dettagliato che descrive i risultati ottenuti da ciascun modello di machine learning.

Central Orchestration

Orchestrazione SD-WAN

- Orchestrazione SD-WAN e VPN con una procedura guidata che permette di creare tunnel VPN site-to-site tra percorsi di rete in modo semplice e automatizzato, utilizzando un'architettura ottimale (hub-and-spoke, full mesh, o una combinazione delle due)
- Supporto di tunnel VPN IPsec, SSL o RED. Integrazione perfetta con le funzionalità SD-WAN per l'assegnazione di priorità alle applicazioni, l'ottimizzazione del routing e l'utilizzo di più link WAN per garantire resilienza e massimi livelli di performance

Central Firewall Reporting Advanced

- 30 giorni di archiviazione dei dati nel cloud per lo storico della reportistica del firewall, con funzionalità avanzate di salvataggio, pianificazione ed esportazione di report personalizzati

Integrazione con XDR e MDR

- Integrazione con Sophos XDR e MDR per fornire dati di telemetria e intelligence sulle minacce per le attività di threat hunting e analisi delle minacce
- Sophos Active Threat Response utilizza i feed sulle minacce forniti dagli analisti MDR e XDR per identificare, bloccare e isolare automaticamente le minacce attive presenti sulla rete
- La telemetria sugli indicatori di compromissione offerta dalla Synchronized Security raccoglie informazioni importanti su eventuali minacce, utenti, processi e dispositivi compromessi

Protezione delle e-mail

Protezione e controllo delle e-mail

- Scansione delle e-mail con supporto di SMTP, POP3 e IMAP
- Servizio di verifica della reputazione con monitoraggio delle epidemie di spam in base a una tecnologia brevettata di rilevamento dei pattern ricorrenti
- Blocco di spam e malware durante la transazione SMTP
- Protezione antispam DKIM e BATV
- Protezione tramite greylisting dello spam e Sender Policy Framework (SPF)
- Verifica del destinatario in caso di indirizzi e-mail digitati in modo errato
- Secondo motore di rilevamento antimalware indipendente (Avira) per la doppia scansione
- Live Protection in tempo reale, ricerche in tempo reale nel cloud per ottenere i più recenti dati di intelligence sulle minacce
- Aggiornamenti automatici delle firme e dei pattern
- Supporto di smart host per i relay in uscita
- Rilevamento/blocco/scansione dei tipi di file degli allegati
- Accetta, rifiuta o scarta i messaggi di dimensioni troppo elevate
- Rilevamento degli URL di phishing all'interno delle e-mail
- Possibilità di utilizzare regole di scansione dei contenuti predefinite o di creare regole personalizzate basate su una serie di criteri con opzioni granulari ed eccezioni per le policy
- Supporto della crittografia TLS per SMTP, POP e IMAP
- Aggiunta automatica della firma a tutti i messaggi in uscita
- Programma di archiviazione e-mail
- Elenchi individuali di blocco e autorizzazione dei mittenti in base all'utente e gestiti tramite il portale utenti

Gestione della quarantena delle e-mail

- Opzioni di notifica e riepilogo della quarantena dello spam
- Quarantena per malware e spam, con opzioni di ricerca e filtro in base a data, mittente, destinatario, oggetto e motivo, con la possibilità di rilasciare ed eliminare i messaggi
- Portale utenti self-service visualizzare e rilasciare i messaggi in quarantena

Cifratura delle e-mail e DLP

- Crittografia SPX in attesa di brevetto per la crittografia unidirezionale dei messaggi
- Gestione delle password di SPX per la registrazione automatica dei destinatari
- Possibilità di aggiungere allegati alle risposte SPX sicure
- Assoluta trasparenza: non occorrono software o client aggiuntivi
- Motore DLP con scansione automatica delle e-mail e degli allegati per individuare i dati sensibili
- Content Control List (CCL) preconfigurati per dati di natura sensibile quali PII, PCI, HIPAA e altri, gestiti dai SophosLabs

Web Server Protection

Web Application Firewall Protection

- Reverse proxy
- Motore di protezione avanzata (hardening) degli URL, con prevenzione degli attacchi tramite deep linking e directory traversal
- Motore per la protezione avanzata dei moduli (form hardening)
- Protezione contro gli attacchi di SQL injection
- Protezione contro attacchi di cross-site scripting
- Doppio motore antivirus (Sophos e Avira)
- Offload dei dati di crittografia HTTPS (TLS/SSL)
- Cookie contrassegnati con firme digitali
- Routing basato sul percorso
- Implementazione delle policy di IP geo
- Configurazione personalizzata della crittografia e applicazione della corretta versione di TLS
- Implementazione di HSTS e X-Content-Type-Options
- Supporto al protocollo Outlook Anywhere
- Autenticazione inversa (offload) per l'autenticazione basata sui moduli e l'autenticazione di base per l'accesso al server
- Astrazione dei server virtuali e fisici
- Il bilanciatore del carico integrato distribuisce i visitatori su più server

- Salta i singoli controlli in modo granulare, secondo necessità
- Trova corrispondenza per le richieste provenienti dalle reti di origine o dagli URL di destinazione specificati
- Supporto di operatori logici AND/OR
- Offre assistenza per la compatibilità con varie configurazioni e distribuzioni non standard
- Opzioni di modifica dei parametri per la performance dell'application firewall
- Possibilità di impostare un limite per le dimensioni delle scansioni
- Autorizzazione/blocco di intervalli IP
- Supporto di caratteri jolly per i percorsi dei server e i domini
- Aggiunta automatica di un prefisso/suffisso per l'autenticazione

Report e Log

Central Firewall Reporting

- Report predefiniti con opzioni di personalizzazione flessibili
- Reportistica per i Sophos Firewall: hardware, software, virtuali e cloud
- L'interfaccia utente intuitiva fornisce una rappresentazione grafica dei dati
- La dashboard dei report offre una panoramica a visualizzazione immediata degli eventi delle ultime 24 ore
- Facile identificazione delle attività di rete, delle tendenze e dei potenziali attacchi
- Backup facile dei log, con opzioni di recupero rapido per qualsiasi esigenza di controllo
- Distribuzione semplificata, senza bisogno di competenze tecniche specializzate

Central Firewall Reporting Advanced

- Reportistica aggregata per più firewall
- Possibilità di salvare modelli di report personalizzati
- Reportistica pianificata
- Esportazione di report in formato PDF, CFV o HTML
- Fino a un anno di archiviazione dei dati per ogni firewall
- Connettore per il Data Lake di MDR/XDR per il threat hunting

Reportistica integrata nell'appliance

- NOTA: La reportistica di Sophos Firewall è inclusa senza costi aggiuntivi, ma la disponibilità di singoli log, report e widget può dipendere dalle licenze dei rispettivi moduli di protezione.
- Centinaia di report integrati nell'appliance, con opzioni personalizzate di reportistica: Dashboard (traffico, sicurezza e quoziente di minaccia dell'utente), Applicazioni (rischio app, app bloccate, app sincronizzate, motori di ricerca, server web, corrispondenza delle parole chiave sul web, FTP), Rete e minacce (risposta alle minacce attive e feed sulle minacce, Security Heartbeat, IPS, wireless, protezione zero-day), VPN, E-mail, Conformità (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
- Monitoraggio delle attività attuali: integrità del sistema, utenti live, connessioni IPsec, utenti remoti, connessioni attive, client wireless, quarantena e attacchi DoS
- Monitoraggio della performance del link SD-WAN in base a jitter, latenza e perdita dei pacchetti
- Report Anonimi
- Pianificazione dei report per più destinatari in base al gruppo di report, con opzioni di frequenza flessibili
- Esportazione dei report in formato HTML, PDF, Excel (XLS)
- Segnalibri per i report
- Personalizzazione della conservazione dei log in base alla categoria
- Un visualizzatore di log completo con vista a colonne e vista dettagliata, più potenti opzioni di filtro e ricerca, ID regola con link ipertestuale e personalizzazione della visualizzazione dei dati

Gestione con Central

Sophos Central

- Le opzioni di gestione e reportistica per più firewall basate sul cloud di Sophos Central aiutano ad amministrare le policy e offrono un'unica console per tutti i prodotti di cybersecurity Sophos
- La gestione delle policy di gruppo consente di modificare oggetti, impostazioni e policy una sola volta, per poi sincronizzarli automaticamente su tutti i firewall del gruppo
- Task Manager fornisce un audit trail storico completo, più il monitoraggio dello stato delle modifiche delle policy di gruppo
- La gestione dei backup del firmware in Sophos Central archivia gli ultimi cinque file di backup della configurazione per ciascun firewall, uno dei quali può essere contrassegnato per l'archiviazione permanente e accesso semplificato
- La pianificazione degli aggiornamenti del firmware da Sophos Central consente di applicare facilmente aggiornamenti automatici in qualsiasi momento
- Una volta completata la configurazione iniziale in Sophos Central, la distribuzione zero-touch permette di esportarla e caricarla sul dispositivo all'avvio, da un'unità flash, per connettere automaticamente il dispositivo a Sophos Central

Zero Trust Network Access

- Gateway Sophos ZTNA integrato, per un accesso sicuro alle applicazioni ospitate dietro il firewall
- Gestione da Sophos Central

Secure by Design

- Il Controllo integrità di Sophos Firewall svolge un'analisi comparativa di decine di impostazioni di configurazione, paragonandole alle best practice di settore al fine di identificare potenziali rischi, con facili opzioni di approfondimento che permettono di risolvere i problemi
- Capacità di applicare automaticamente hotfix over-the-air in modalità zero-touch, per correggere le vulnerabilità senza dover programmare tempi di inattività
- Kernel con protezione avanzata per una maggiore sicurezza, performance superiori e un'ottima scalabilità, grazie all'isolamento rigoroso dei processi e alla mitigazione degli attacchi tramite canali laterali
- Monitoraggio remoto dell'integrità a cura di Sophos, per mezzo di un sensore XDR integrato che consente di monitorare in tempo reale l'integrità del sistema offrendo la possibilità di individuare le configurazioni non autorizzate, l'esecuzione di codice pericoloso, la manomissione di file e altro ancora, al fine di intercettare gli attacchi e avviare rapidamente un'azione di risposta
- Architettura Xstream next-gen, con nuovo piano di controllo per garantire massima sicurezza e scalabilità
- Containerizzazione dei principali limiti di attendibilità e dei portali utente/VPN
- Gestione centralizzata crittografata e sicura tramite Sophos Central, che elimina qualsiasi necessità di accesso da remoto da parte degli amministratori
- L'autenticazione multifattoriale su tutti i sistemi protegge da rischi quali il furto di credenziali e gli attacchi brute force
- Gateway ZTNA integrato per un accesso remoto più sicuro e una maggiore protezione delle applicazioni
- Le distribuzioni sicure e subito pronte all'uso garantiscono l'adozione delle best practice in materia di sicurezza, con rigorosi controlli di accesso

Riepilogo delle caratteristiche di Sophos Firewall in base alla sottoscrizione

	Bundle di protezione Xstream							Disponibile separatamente		
	Bundle di protezione Standard					Disponibile separatamente				
	Base Firewall	Network Protection	Web Protection	DNS Protection	Disponibile solo nei bundle	Protezione zero-day	Central Orchestration	Central Firewall Reporting Adv.	Protezione delle e-mail	Web Server Protection
Gestione generale (incl. disponibilità elevata)	✓									
Architettura Xstream	✓									
Firewall, reti e routing	✓									
SD-WAN Xstream	✓									
Funzionalità di base di shaping del traffico e quote	✓									
Secure Wireless	✓									
Autenticazione	✓									
Portale self-service per gli utenti	✓									
VPN (IPsec, SSL ecc.)	✓									
VPN site-to-site RED	✓									
Client VPN Sophos Connect	✓									
Intrusion Prevention (IPS)		✓								
Risposta alle Minacce Attive										
Feed Sophos X-Ops sulle minacce		✓								
Feed MDR/XDR sulle minacce					✓					
Feed di terze parti sulle minacce					✓					
Synchronized Security Heartbeat		✓								
Gestione dei dispositivi SD-RED		✓								
VPN indipendente client		✓								
Synchronized Application Control			✓							
Protezione e controllo web			✓							
Protezione e controllo delle applicazioni			✓							
Visibilità sulle applicazioni cloud			✓							
Shaping del traffico web e delle app			✓							
Sicurezza e conformità DNS				✓						
NDR Essentials					✓					
Analisi dinamica nella sandbox						✓				
Analisi Threat Intelligence						✓				
Orchestrazione SD-WAN							✓			
Dati di Central Firewall Reporting*		7 giorni	7 giorni	7 giorni	7 giorni	7 giorni	30 giorni	Fino a 1 anno	7 giorni	7 giorni
Funzionalità di CFR Advanced							✓	✓		
Protezione e controllo delle e-mail									✓	
Gestione della quarantena delle e-mail									✓	
Cifratura delle e-mail e DLP									✓	
Web Application Firewall Protection										✓
Log/report nell'appliance	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Gestione con Sophos Central**		✓	✓	✓	✓	✓	✓	✓	✓	✓
Gateway ZTNA**		✓	✓	✓	✓	✓	✓	✓	✓	✓
Progettato per garantire una sicurezza di altissimo livello	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Nota: Alcune funzionalità non sono supportate sui modelli XGS 87 e XGS 88: reportistica integrata nell'appliance, doppia scansione AV, scansione AV del WAF e agente di trasferimento messaggi e-mail (MTA)

Le opzioni di licenza MSP sono leggermente diverse da quelle indicate sopra

* Il tempo di conservazione dei dati è una stima basata su un utilizzo medio della rete, e varia a seconda del volume effettivo dei dati di log. Strumento per il calcolo dello spazio di archiviazione.

** Funzionalità inclusa in tutti i bundle, pacchetti di supporto o sottoscrizioni di protezione. I clienti che hanno solo una licenza di base devono aggiungere il supporto per poter usufruire di queste funzionalità.

Elenco delle funzionalità di Sophos Firewall

SOPHOS

Riepilogo delle caratteristiche di Sophos Firewall in base alla sottoscrizione

	Supporto Enhanced (Incluso nei bundle Standard e Xstream Protection)	Supporto Enhanced Plus (disponibile come upgrade per il Supporto Enhanced)
Supporto multi-channel 24/7 (tramite telefono, portale web, chat), compresa l'assistenza remota e l'accesso self-service alla knowledge base e ai forum di supporto	✓	✓
Download, aggiornamenti e rilasci di manutenzione del firmware **	✓	✓
Sophos Central Management, reportistica e gateway ZTNA	✓	✓
Sostituzione avanzata dell'hardware per i dispositivi attivi	✓	✓
Sostituzione avanzata dell'hardware per un dispositivo di disponibilità elevata passivo*		✓
Sostituzione dell'hardware avanzata per dispositivi SD-RED/APX		✓
Accesso VIP (chiamate inoltrate a tecnici senior)		✓
Consulenza da remoto (2-8 ore all'anno)		✓

* Per abilitare la copertura con autorizzazione al reso (RMA) avanzata per un dispositivo HA passivo, il dispositivo attivo deve avere una licenza di supporto Enhanced Plus
Per i dettagli completi, consulta la Guida al servizio di supporto tecnico Sophos.

** Nota: per ricevere gli aggiornamenti del firmware, occorre aggiungere il Supporto ai moduli individuali acquistati

Vendite per Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

2025-12-15 IT (DD)