

Dlaczego klienci wybierają Sophos Firewall zamiast produktów konkurencji:

Lepsze zarządzanie chmurą dzięki Sophos Central –

Sophos Central to bardziej kompletna i dobrze zintegrowana platforma do zarządzania chmurą niż jakakolwiek oferta firmy Fortinet:

- › Jedna konsola do zarządzania chmurą dla wszystkich produktów związanych z cyberbezpieczeństwem
- › Łatwiejsze zarządzanie zarówno dla przeciętnego informatyka, jak i doświadczonego analityka bezpieczeństwa
- › Łatwy wgląd dzięki bogatym pulpitom nawigacyjnym i raportom
- › Nie pobieramy dodatkowych opłat za centralne zarządzanie i bezpłatnie udostępniamy dane raportowe z 7 dni

Lepsza automatyzacja między produktami dzięki zsynchronizowanemu zabezpieczeniu i aktywnej reakcji na zagrożenia —

Umożliwia wymianę informacji między produktami i automatyczną reakcję na aktywne zagrożenia:

- › Każde zagrożenie wykryte przez zaporę ogniową, punkt końcowy lub analityka XDR/MDR jest natychmiast udostępniane wszystkim produktom.
- › Wszystkie produkty współpracują ze sobą, aby automatycznie izolować zagrożone urządzenie.
- › Wymiana informacji między produktami zapobiega również ruchom bocznym i identyfikuje aplikacje oraz użytkowników.
- › Do uruchomienia nie są wymagane żadne dodatkowe produkty ani licencje

Bezpieczeństwo od samego początku –

Atakujący biorą na cel zapory sieciowe i inną infrastrukturę sieciową wystawioną na działanie Internetu:

- › Firma Sophos zainwestowała znaczne środki w zasady bezpieczeństwa od samego początku, aby zmniejszyć powierzchnię ataku
- › Jesteśmy jedyną firmą oferującą bezprzewodowe aktualizacje poprawek, które pozwalają rozwiązać pilne problemy bez konieczności aktualizacji oprogramowania układowego
- › Wyróżniamy się tym, że aktywnie monitorujemy całą bazę klientów pod kątem wszelkich oznak ataku i podejmujemy natychmiastowe działania w przypadku wykrycia jakichkolwiek nieprawidłowości.

Inne zalety –

Ułatwiamy wdrażanie, zarządzanie i aktualizowanie zapory sieciowej:

- › Wdrożenie bezobsługowe jest łatwe i bezpłatne dzięki Sophos Firewall – nie są wymagane żadne dodatkowe produkty ani licencje
- › Wysoka dostępność to funkcja typu „plug-and-play”, z której można korzystać w dowolnym momencie, bez żadnych problemów
- › Nasza programowalna architektura Xstream oznacza, że otrzymujesz bezpłatne aktualizacje wydajności i ochrony bez konieczności modernizacji sprzętu

Lepsza wartość –

Najważniejsze jest to, że dzięki rozwiązaniu Sophos Network Security Solution zyskujesz wyjątkową wartość:

- › W naszym pakiecie Xstream Protection oferujemy więcej niż jakikolwiek inny dostawca – w tym funkcje niedostępne u innych, takie jak zsynchronizowane zabezpieczenia, aktywna reakcja na zagrożenia czy integracja z NDR

Pytania odkrywające

Ogólne: Jakiego rodzaju zapory sieciowej obecnie używasz? Co Ci się w niej podoba? Czy chciałbyś, żeby działała lepiej?

Ogólne pytania otwierające:

- ▶ Jakiego rozwiązania firewallowego używasz obecnie? Co Ci się w nim podoba? Czego mu brakuje?
- ▶ Kiedy należy odnowić obecny produkt?

Ochrona:

- ▶ Czy doświadczyli Państwo ataków, naruszeń lub exploitów? Jak je wykryli Państwo? Czy zapora sieciowa okazała się pomocna?
- ▶ Czy masz jakieś zabezpieczenia, które zapobiegają przemieszczaniu się zagrożeń w sieci?
- ▶ Czy Twoja zapora sieciowa miała jakieś luki w zabezpieczeniach? Jak zostały one załatwane?

Wydajność:

- ▶ Jaka jest wydajność Twojej zapory sieciowej?
- ▶ Czy jesteś w stanie włączyć wszystkie potrzebne zabezpieczenia i nadal mieć zapas wydajności?
- ▶ Czy Twój dostawca zapewnia lepszą wydajność dzięki aktualizacjom oprogramowania układowego, czy też wydajność spada?

Zarządzanie:

- ▶ Ile produktów związanych z cyberbezpieczeństwem zarządzasz? Ile konsol? Ilu dostawców?
- ▶ Czy któreś z Twoich produktów współpracują ze sobą w celu wymiany informacji i reagowania na ataki?
- ▶ W jaki sposób zarządzasz obecnie zaporą ogniową i inną infrastrukturą, taką jak przełączniki i punkty dostępowe?
- ▶ Jak łatwo jest wdrożyć zapory sieciowe w nowych lokalizacjach?
- ▶ Czy potrafisz odpowiedzieć na podstawowe pytania dotyczące użytkowników o najwyższym ryzyku, aktywnych zagrożeń, niechcianych aplikacji, shadow IT, zaszyfrowanej zawartości ruchu sieciowego, podejrzanych plików do pobrania?

Sieć:

- ▶ Jak zarządzasz dostępem zdalnym? Czy korzystasz obecnie z rozwiązania ZTNA?
- ▶ Ile lokalizacji posiadacie? Jak nimi zarządzacie?

Wyobraź sobie, że mógłbyś...

Konsolidować:

- ▶ znacząco ograniczyć liczbę dostawców oraz konsol, którymi musisz zarządzać,
- ▶ otrzymać od Sophos wszystko, czego potrzebujesz, w ramach współpracy z jednym dostawcą,
- ▶ korzystać z pełnego portfolio: firewalli, przełączników, sieci Wi-Fi, ZTNA, ochrony endpointów, ochrony poczty i komunikacji, usług MDR i wielu innych.

Upraszczać:

- ▶ podnosić poziom bezpieczeństwa, poświęcając mniej czasu na jego obsługę,
- ▶ zarządzać wszystkimi produktami z poziomu jednej konsoli w chmurze – Sophos Central,
- ▶ korzystać z rozwiązań, które wymieniają się informacjami i współdziałają, aby automatycznie reagować na zagrożenia,
- ▶ wybierać produkty wysoko oceniane przez klientów,
- ▶ mieć jeden punkt kontaktu w zakresie wsparcia technicznego – jednego dostawcę.

Oszczędzać:

- ▶ na licencjach, wsparciu oraz czasie poświęcanym na zarządzanie bezpieczeństwem,
- ▶ na kosztach administracyjnych dzięki łatwym w obsłudze produktom i Sophos Central,
- ▶ na kosztach sieci dzięki wiodącej w branży relacji ceny do chronionego Mbps,
- ▶ na kosztach potencjalnych naruszeń i ataków, eliminując je, zanim staną się realnym problemem,
- ▶ dzięki atrakcyjnemu pakietowi o wysokiej wartości, takim jak Xstream Protection,
- ▶ zyskując przyszłe usprawnienia wydajności i ochrony bez konieczności modernizacji sprzętu.






Seria Sophos Firewall XGS z procesorami Xstream Flow

Zapoznaj się z narzędziem doboru rozmiaru, aby uzyskać zalecenia dotyczące konkretnych modeli





Małe i średnie przedsiębiorstwa oraz oddziały: komputery stacjonarne serii XGS ^{drugiej} generacji

				
XGS 88(w)	XGS 108(w)	XGS 118(w)	XGS 128(w)	XGS 138
SOHO, ograniczone, bez wentylatora	Małe biuro, bez wentylatora	Oddział	Oddział	MŚP, oddział

Małe i średnie przedsiębiorstwa oraz oddziały: Komputery stacjonarne serii XGS ^{pierwszej} generacji





				
XGS 87(w)	XGS 107(w)	XGS 116(w)	XGS 126(w)	XGS 136(w)
SOHO, ograniczone	Małe biuro	Oddział	Oddział	MŚP, oddział

Rozproszona krawędź: seria XGS 1U do montażu w szafie rack

			
XGS 2100/2300	XGS 3100/3300	XGS 4300	XGS 4500
Średniej wielkości biuro	Średniej wielkości, rozproszona organizacja	Średnie i duże przedsiębiorstwo rozproszone	

Duże przedsiębiorstwo rozproszone

Kampus i duże przedsiębiorstwo rozproszone

			
XGS 5500	XGS 6500	XGS 7500	XGS 8500
Duże, rozproszone przedsiębiorstwo		Przedsiębiorstwa i kampusy	

Komputer stacjonarny	Łączność			Przepustowość		
	Porty/ gniazda rozszerzeń	Maksymalna liczba portów (w tym moduły)	Model w	Zapora sieciowa (Mbps)	Ochrona przed zagrożeniami (Mbps)	Xstream SSL/TLS (Mbps)
2 generacji						
XGS 88(w)	4/-	4	Wi-Fi 6	9900	2000	600
XGS 108(w)	7/-	7	Wi-Fi 6	12 500	2500	800
XGS 118(w)	10/1	10	Wi-Fi 6	15 500	3250	1100
XGS 128(w)	10/1	10	Wi-Fi 6	19 100	4000	1450
XGS 138*	8/1	8	n/d	19 100	4750	1700

Komputer stacjonarny	Łączność			Przepustowość		
	Porty/ gniazda rozszerzeń	Maksymalna liczba portów (w tym moduły)	Model w	Zapora sieciowa (Mbps)	Ochrona przed zagrożeniami (Mbps)	Xstream SSL/TLS (Mbps)
1 generacji						
XGS 87(w)	5/-	5	Wi-Fi 5	3850	850	375
XGS 107(w)	9/-	9	Wi-Fi 5	7000	1110	420
XGS 116(w)	9	9	Wi-Fi 5	7700	2160	650
XGS 126(w)	14/1	14	Wi-Fi 5	10 500	2700	800
XGS 136(w)	14/1	14	Wi-Fi 5	11 500	3000	950

Modele 1U	Specyfikacja techniczna		Przepustowość		
	Porty/gniazda rozszerzeń	Maksymalna liczba portów (w tym modułów)	Zapora sieciowa (Mbps)	Ochrona przed zagrożeniami (Mbps)	Xstream SSL/TLS (Mbps)
XGS 2100	10/1	18	30 000	5000	1100
XGS 2300	10/1	18	39 000	5550	1450
XGS 3100	12/1	20	47 000	7400	2470
XGS 3300	12/1	20	58 000	10 000	3130
XGS 4300	12	28	75 000	25 200	8
XGS 4500	12/2	28	80 000	31 850	10 600

Modele 2U	Specyfikacja techniczna		Przepustowość		
	Porty/gniazda rozszerzeń	Maksymalna liczba portów (w tym modułów)	Zapora sieciowa (Mbps)	Ochrona przed zagrożeniami (Mbps)	Xstream SSL/TLS (Mbps)
XGS 5500	16/3	48	100 000	46 000	13 500
XGS 6500	20/4	68	120 000	53 500	16 000
XGS 7500	22/4	70	160 000	70 000	19 500
XGS 8500	22/4	70	190 000	92 500	24 000

Opcje licencjonowania zapory Sophos

Aby zapewnić najwyższy poziom bezpieczeństwa, zalecamy pakiet Xstream Protection. Wszystkie subskrypcje są również dostępne do indywidualnego zakupu.

Pakiet Xstream Protection	
Licencja podstawowa	Sieć, bezprzewodowa, architektura Xstream, nieograniczony zdalny dostęp VPN, VPN typu site-to-site, raportowanie
Ochrona sieci	Xstream TLS/DPI, IPS, aktywna reakcja na zagrożenia z wykorzystaniem informacji o zagrożeniach Sophos X-Ops, Heartbeat, SD-RED, raportowanie
Ochrona sieci	Silnik Xstream TLS i DPI, bezpieczeństwo i kontrola sieci, kontrola aplikacji, raportowanie
Ochrona przed atakami typu zero-day	Uczenie maszynowe i analiza plików w środowisku sandbox, raportowanie
Centralna koordynacja	Koordynacja SD-WAN VPN, centralna zapora sieciowa Zaawansowane raportowanie (30 dni), łącznik MDR/XDR data lake
Ochrona DNS (nie sprzedawane oddzielnie)	Usługa DNS w chmurze zapewniająca bezpieczeństwo sieci i zgodność z przepisami
Funkcje dostępne wyłącznie w pakiecie (nie sprzedawane oddzielnie)	Aktywna reakcja na zagrożenia dzięki kanałom zagrożeń MDR/XDR i kanałom zagrożeń stron trzecich, NDR Essentials
Rozszerzona pomoc techniczna	Całodobowy dostęp do pomocy technicznej, aktualizacje oprogramowania układowego i funkcji, rozszerzona gwarancja na wymianę sprzętu w okresie obowiązywania umowy
Dodatkowe moduły ochrony	
Ochrona poczty elektronicznej	Wbudowane oprogramowanie antyspamowe, antywirusowe, DLP, szyfrowanie
Ochrona serwera WWW	Zapora sieciowa aplikacji internetowych

Zarządzanie i raportowanie Sophos Central:

Zarządzanie i raportowanie Sophos Central (bezpłatne):	
Zarządzanie Sophos Central	Zarządzanie zaporą sieciową grupy, zarządzanie kopiami zapasowymi, planowanie aktualizacji oprogramowania układowego
Raportowanie zapory Sophos Central	Gotowe i niestandardowe narzędzia do tworzenia raportów, z siedmiodniowym przechowywaniem w chmurze bez dodatkowych opłat (zobacz inne opcje)

Wsparcie techniczne: Aby otrzymywać aktualizacje oprogramowania sprzętowego, wymagana jest subskrypcja wsparcia technicznego. Wszystkie pakiety ochronne obejmują rozszerzone wsparcie techniczne, ale można je uaktualnić, aby jeszcze bardziej zwiększyć komfort korzystania z pomocy technicznej.

Dodatkowe opcje wsparcia:	
Rozszerzone wsparcie techniczne Plus	Rozszerz wsparcie techniczne o wsparcie VIP, gwarancję sprzętową na dodatki, opcję TAM (dodatkowa opłata) W scenariuszach aktywnej/pasywnej wysokiej dostępności (HA) rozszerzone wsparcie Plus jest wymagane w urządzeniu głównym, aby kwalifikować się do zaawansowanej usługi RMA w urządzeniu pasywnym

Elastyczne wdrażanie

Zapora Sophos Firewall obsługuje różne platformy chmurowe, wirtualne i programowe, aby sprostać różnorodnym potrzebom.



Lista kontrolna cytatów

Sophos Firewall

- Urządzenie serii XGS
 - Moduły łączności/zestaw do montażu w szafie rack
 - 2 redundantny zasilacz
 - Zestaw do montażu w szafie
 - Urządzenie HA (aktywne-aktywne lub aktywne-pasywne)
- Urządzenie wirtualne lub programowe

Pakiet Network-in-a-Box:

- Zawiera zaporę ogniową, przełącznik(i) i punkt(y) dostępowy(e) AP6

Dodatkowe opcje dostępu do sieci:

- Przełączniki Sophos
- Bezprzewodowe punkty dostępowe AP6
- Urządzenia SD-RED
- ZTNA (Zero Trust Network Access)

Subskrypcje ochrony i raportowania:

- Pakiet ochrony Xstream
- Central Email Advanced (poczta e-mail w chmurze)
- Ochrona poczty e-mail w urządzeniu
- Ochrona serwera WWW
- Subskrypcje HA dla trybu aktywny-aktywny
- Zaawansowane raportowanie centralnej zapory sieciowej
- 1-5 CFR Advanced na każdy firewall (minimum 1 firewall)

Wsparcie i usługi związane z zaporą ogniową:

- Rozszerzone wsparcie Plus Upgrade
- Czas usług profesjonalnych