Sophos Buyers Guide

2018

Presented by

Firewalls.com
Get Secure. Stay Secure. ™

T: 317-225-4117 | E: sales@firewalls.com

Table of Contents

Why Buy Sophos?

14th Annual Info Security Products Guide Global Excellence Awards – Info Security PG's Global Excellence Awards honor achievements in several facets of security and information technology and last year, Sophos laid claim to a slew of awards for both hardware and software excellence.

At the Red Carpet Awards Gala, Sophos was named:

Gold Winner in Endpoint Security for Sophos Intercept X

Gold Winner for Innovation in Next-Generation Security

Gold Winner for Firewalls with XG Firewall

Bronze Winner for Network Security & Management

XG Firewalls

Why Buy Sophos?

2018 SC Media Awards – SC Media is a network security & information tech organization that provides detailed, unbiased information for cybersecurity professionals. Each year, they issue awards for the great innovations, technology, and vision in a number of security categories.

In 2018, Sophos was named:

Best Mobile Security Solution for Sophos Mobile

Best UTM Security Solution for XG Firewalls

Computing's Security Excellence Awards – Praise for Intercept X and its next-generation protections against ransomware, exploits, and advanced threats was abundant in 2018. Computing announced **Intercept X as 2018's Security Innovation of the Year** at the Enterprise Security & Risk Management Summit.

Intercept X

Sophos Models by Recommended Number of Users

Recommended User Counts - Network security best practices dictate that organizations should deploy a firewall that is able to comfortably house twice the number of users expected to operate on a network. By leaving additional room in security infrastructure, businesses can anticipate large influxes of users, accommodate future growth without purchasing new hardware, & provide a high ceiling of throughput and other performance potential.

Throughput Requirements – Generally speaking, your firewall throughput should at least equal your available Internet bandwidth to make the most of performance. Some networks may have higher performance needs due to data-heavy job functions.

Security Service Subscriptions – The age of set-it-and-forget-it network security has long passed. Today's advanced threats require networks that proactively monitor, detect, prevent, & mitigate threat actors from a multitude of attack angles. However, enabling these services impacts the overall performance integrity of your network. Administrators who intend to deploy security services should consider a firewall option with greater throughput potential than their network may otherwise require.

Sophos XG Models by Recommended Number of Users			
1 to 10 Users	XG 85	200 to 300 Users	XG 230
10 to 25 Users	XG 105	300 to 500 Users	XG 310
25 to 35 Users	XG 115	500 to 750 Users	XG 430
35 to 50 Users	XG 125	750 to 1000 Users	XG 450
50 to 100 Users	XG 135	1000 to 2500 Users	XG 550
100 to 200 Users	XG 210	Over 2500 Users	XG 650 / XG 750

Note: A "User" is defined as any Internet-connected device that will be operating on your network. This includes not only PCs, but laptops, mobile devices, printers, IoT devices, & more.

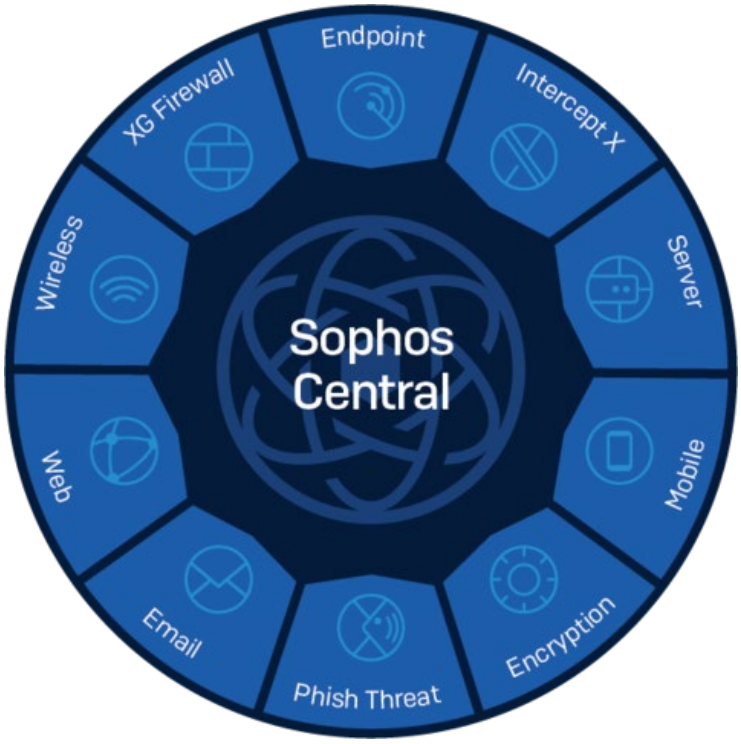
Sophos Security Service Bundles

FullGuard Bundles – FullGuard bundles consist of Network Protection, Web Protection, Email Protection, Web Server Protection, & Enhanced Support. This is ideal for SMB businesses and enterprises that maintain their own online web servers or cloud-based servers. The inclusion of Web Server Protection secures your website and signals to customers that you're serious about securing their data. The FullGuard Plus bundle includes Sandstorm Cloud-Sandbox Protection.

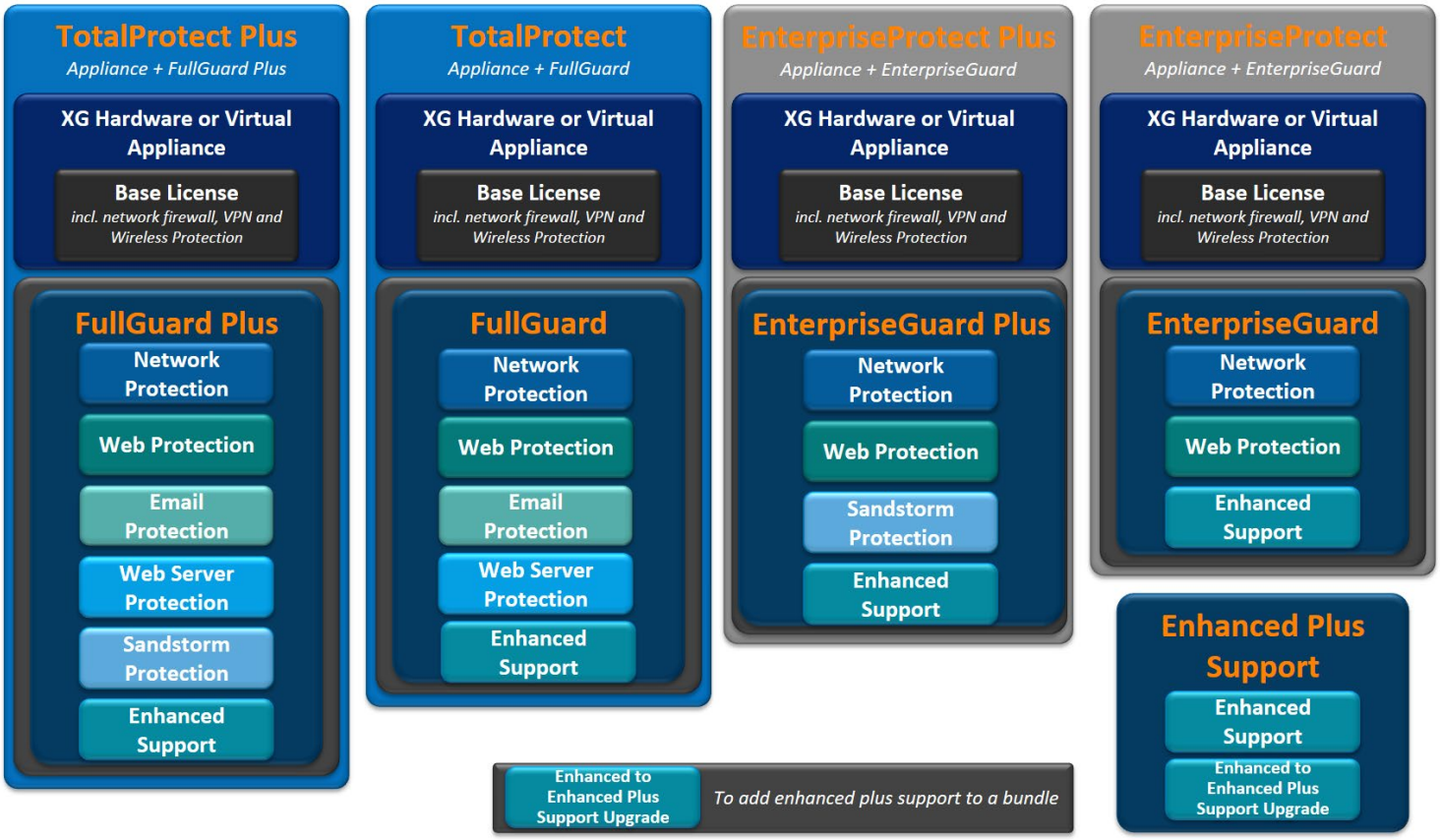
TotalProtect Bundles – TotalProtect bundles are the most convenient way for organizations of all sizes to deploy a new firewall and comprehensive services while saving both time & money by bundling. TotalProtect bundles include an XG Firewall or Virtual Appliance and all of the services outlined above in the FullGuard Bundles.

EnterpriseGuard Bundles – Includes Network Protection, Web Protection, & Enhanced Support. These bundles are designed for mid-sized to enterprise-sized organizations looking to add XG Firewall capabilities or minimal asset protection to their network. The EnterpriseGuard Plus version of this bundle includes Sandstorm Cloud-Sandbox Protection.

EnterpriseProtect Bundles – The EnterpriseProtect and EnterpriseProtect Plus bundles include everything detailed above in the EnterpriseGuard bundles, with the addition of an XG Firewall appliance or Virtual Appliance. Protect bundles package together both services & hardware.



The below infographic breaks down the hardware, subscriptions, & services included in the different bundles outlined above.



What is the Sophos Security Heartbeat?

When a Sophos XG Firewall is registered with Sophos Central, your endpoints can send automatic reports about their security status and network health to your firewall. These small, frequent reports are known as Sophos Security Heartbeats. Each Security Heartbeat transmits real-time health data about a given device so that any potentially compromised or breached devices can be restricted from accessing the rest of the network. Sophos Central administrators will receive alerts about any threats targeting your machine and receive recommendations on how to remediate the issue.

Security Heartbeat reports are given a simple traffic light-style visualized status that makes managing multiple devices a breeze for administrators.

Green Status – A Green status means that your security software is active and functioning properly. No active or inactive malware are present on your network and no Potentially Unwanted Applications (PUA) have been detected. No further action is required by administrators.

Yellow Status – A Yellow status indicates that a potential threat may have been located on your network. While not strictly necessary to remediate, administrators may want to act to prevent any further issues. A Yellow status usually indicated the detection of inactive malware or a PUA.

Red Status – Red status occurs when a threat has successfully impacted a device and further action is required by administrators to prevent damage to the network. Red status usually indicates that active malware has been detected, malicious traffic has been identified, or Sophos security software is not working correctly. Red status alerts will include recommended actions to remediate the threat and restore network health.

Enabling Sophos Security Heartbeat monitoring requires:

Sophos XG Next-Gen Firewall or Virtual Appliance

&

Sophos Central Endpoint Advanced or Sophos Central Server Advanced

Glossary of Sophos Terms

While this is by no means an exhaustive list of cyber security or Sophos-specific terminology, this glossary outlines some of the more common acronyms and vocabulary you will encounter when shopping for XG Firewall appliances & services.

XG Firewalls – XG Firewalls are the next generation of firewall protection offered by Sophos, taking advantage of the latest breakthroughs in network security innovation. XG Firewalls use Intel multi-core technology, solid-state drives, and accelerated in-memory content scanning. Sophos packet optimization technology ensures maximum throughput even under heavy security demands.

SG Firewalls – The previous generation of Sophos Firewalls, SG appliances are designed to provide the optimal balance between performance and protection. Firewalls.com does not recommend purchasing SG Firewalls as these older models are outclassed by their XG Firewall counterparts.

PUA - Potentially Unwanted Applications are unwanted or potentially dangerous applications that may pose a threat to the network. While not always malicious, PUAs may sometimes contain implementations that compromise security, privacy, or performance. This can include Adware or Spyware.

Sandstorm – Sophos' cloud-based security sandbox detonates potentially dangerous payloads in a safe, quarantined environment where damage cannot affect your network security. Sandstorm provides an additional layer of protection against ransomware and targeted attacks. No additional hardware is required. Sandstorm is included with all of the "Plus" bundles pictured on Page 7.

Sophos Central – A unified console that allows administrators to manage all active Sophos products and services through one convenient, visualized dashboard.

Synchronized Security – Synchronized Security enables your defenses to work together as a single system by integrating all of your Sophos products and services into a coordinated, real-time security platform. Sophos products communicate to share critical information, creating a holistic approach to network security.

Sophos RED – Sophos Remote Ethernet Devices extend your security network beyond your main facility, making a convenient and affordable method to build secure distributed networks. Perfect for branch offices, outposts, or retail locations.

Sophos Free 30-Day Trials

Sophos offers a wide range of 30-day trials that allow you to test out their products and services at absolutely no cost. Below, you will find direct links to a number of helpful trials to get you started.

Intercept X Trial – Anti-Malware. Anti-Exploit. Root Cause Analysis. Next-Gen Protection against Ransomware and Malware.

XG Firewall Trial – Block unknown threats with a comprehensive suite of advanced protection including IPS, ATP, Sandboxing, Dual AV, Web & App Control, Anti-Phishing, and more.

Endpoint Protection Trial – Proven endpoint protection for laptops, desktops, and virtual environments.

Sophos Central Trial – One unified console for all your Sophos products. Monitor network traffic and deploy policies for all users.

Email Gateway Trial – Block spam and phishing attacks at the gateway, and get unobtrusive, automatic encryption for all email.

Phish Threat Trial – Simulate phishing attacks and train your end users through automated attack simulations, quality security awareness training, and actionable reporting.

What Next?

Ultimately, the best decision you can make when shopping for a network firewall is to consult an expert that you trust. Manufacturer-certified resellers can answer any questions specific to your needs to ensure you're getting the most out of your security investment without leaving performance on the table. Whether you have to meet regulatory compliance standards, tackle complex deployments, or are looking to roll out your first secure business network, cyber security experts possess specialized knowledge to help keep your data safe.

Firewalls.com stocks our Indianapolis-based Security Operations Center with engineers qualified at the highest-possible certification tiers for all of the manufacturers and brands we represent. Our team has assisted thousands of customers with finding the right appliances, services, & solutions to secure their networks.

Visit our Sophos Products Page for pricing, technical specifications, datasheets, & more.

Speak with one of our network security gurus by phone at 317-225-4117 or message us at sales@firewalls.com.

Request a call on our Contact Us page to have a firewall expert reach out to you.

Firewalls.com also offers advanced configurations, managed security services, Security-as-a-Service, premium support, & professional services. Get Secure & Stay Secure with Firewalls.com.