

# Solution Brief



## XG Firewall

v18

**SOPHOS**  
Cybersecurity evolved.

# Contents

<b>Sophos XG Firewall</b>	<b>2</b>
<b>Exposing Hidden Risks</b>	<b>3</b>
Xstream SSL Inspection	3
Control Center	3
Synchronized Application Control	6
Top Risk Users	7
Flexible Reporting Options	8
<b>Blocking Unknown Threats</b>	<b>9</b>
Xstream Protection and Performance	9
Zero-Day Threat Protection	10
Static Machine Learning Analysis	11
Dynamic Run-Time Sandboxing Analysis	12
Threat Protection Reporting	13
Unified Rule Management	14
Managing Your Security Posture at a Glance	15
Enterprise-Grade Secure Web Gateway	16
Education Features	17
Simplified NAT Configuration	18
<b>Automatic Response to Incidents</b>	<b>19</b>
Security Heartbeat	20
It's a Zero Trust World	21
<b>Add XG Firewall to Any Network – Simply</b>	<b>22</b>

# Sophos XG Firewall

Sophos XG Firewalls are developed right from the start to address today's top problems that plague existing firewalls while also providing a platform designed specifically to tackle the evolving threat and network landscape. XG Firewall brings a fresh approach to the way you identify hidden risks, protect against threats, and respond to incidents without taking a performance hit. Our Xstream Architecture for XG Firewall utilizes a packet processing architecture that delivers extreme levels of visibility, protection, and performance.

XG Firewall provides unrivaled visibility into risky users, unwanted applications, suspicious payloads, and persistent threats. It tightly integrates a full suite of modern threat protection technologies that are easy to set up and maintain. And unlike legacy firewalls, XG Firewall communicates with other security systems on the network, enabling it to become your trusted enforcement point to contain threats and block malware from spreading or exfiltrating data out of the network – automatically – in real time.

Sophos XG Firewall has three key advantages over other network firewalls:

- 1. Exposes hidden risks** XG Firewall does a far better job exposing hidden risks than other solutions through a visual dashboard, rich on-box and cloud reporting, and unique risk insights.
- 2. Blocks unknown threats** XG Firewall makes blocking unknown threats faster, easier and more effective than other firewalls with a full suite of advanced protection capabilities that are very easy to set up and manage.
- 3. Automatically responds to incidents** XG Firewall with Synchronized Security automatically responds to incidents on the network thanks to Sophos Security Heartbeat™ which shares real-time intelligence between your endpoints and your firewall.

# Exposing Hidden Risks

It's critically important for a modern firewall to parse through the mountain of information it collects, correlate data where possible, and highlight only the most important information requiring action – ideally before it's too late.

## Xstream SSL Inspection

There's a perfect storm brewing around encrypted traffic. According to Google, the volume of encrypted traffic on networks has grown to over 80%. This increase represents an opportunity for cybercriminals to launch attacks that are hidden and therefore difficult to detect. After all, you can't stop what you can't see. Unfortunately, most organizations are powerless to do anything about it because their current firewall lacks the performance necessary to utilize TLS/SSL inspection without slowing down dramatically.

XG Firewall, with its new Xstream SSL inspection engine, has a much higher capacity for concurrent connections and offers flexible policy tools to make intelligent decisions about what should and can be scanned, offloading where appropriate. Using the SSL policy tools, organizations can create enterprise-grade TLS/SSL policies related to un-decryptable traffic, certificates, protocols, cipher enforcement options, and more. XG Firewall supports TLS 1.3 and all modern crypto suites across every port and application in the system.

Additional tools available right on the dashboard enable administrators to see exactly how much network traffic is encrypted, and how it's being handled. XG Firewall does a much better job at surfacing this information than other solutions, particularly with how it highlights errors that are encountered due to certificate validation or websites that don't support the latest encryption standards.

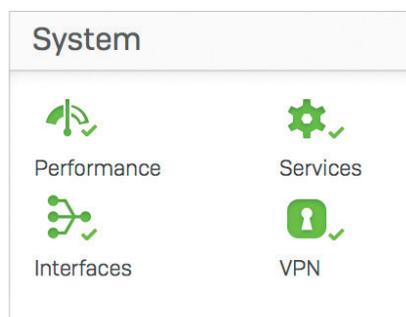
Administrators can also pop up a detailed window to see exactly which sites are problematic, and why, as well as users experiencing issues. From there, they can take action directly to exclude the application or site from decryption to prevent further issues. No other SSL inspection solution offers the same accessibility to this information.

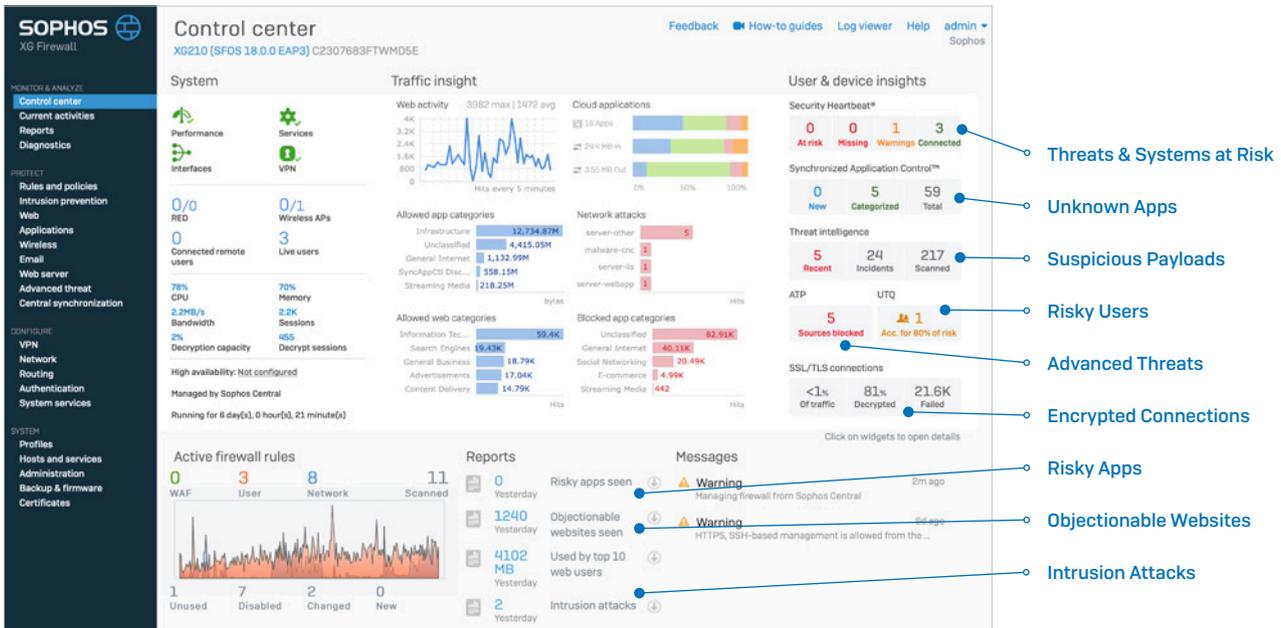
## Control Center

XG Firewall's Control Center provides an unprecedented level of visibility into activity, risks, and threats on your network.

It uses "traffic light" style indicators to focus your attention on what's most important to you.

If something's red, it requires immediate attention. Yellow indicates a potential problem. And if everything is green, no further action is required.





Every widget on the Control Center offers additional information that is easily revealed simply by clicking that widget. For example, the status of interfaces on the device can be obtained by clicking the “Interfaces” widget on the Control Center.

INTERFACE	TYPE	STATUS	RECEIVED KBITS/S	TRANSMITTED KBITS/S
IoT_Bridge	Bridge-pair	Connected	1.98	0.62
Port1	Physical	Connected, 1000 Mbps - Full Duplex	183.91	864.02
Port2	Physical	Connected, 1000 Mbps - Full Duplex	925.65	176.26
Port7	Physical	Unplugged	0.00	0.00
Port8	Physical	Disabled	0.00	0.00

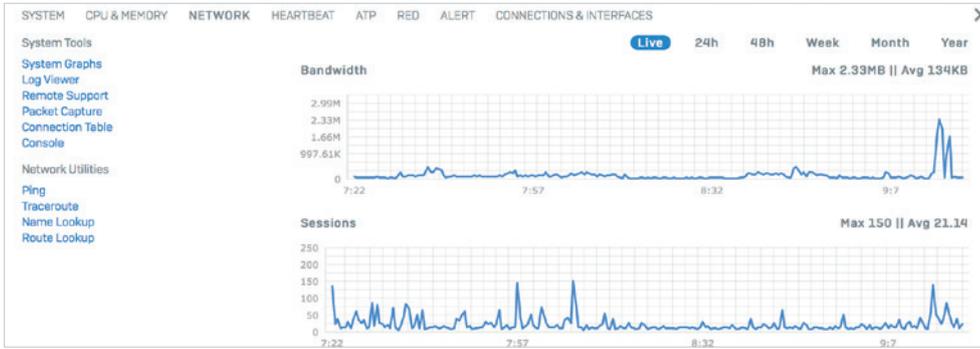
  

GATEWAY NAME	GATEWAY IP	INTERFACE	TYPE	WEIGHT	STATUS
BACKUP_WAN	128.0.0.1	Port7	Active	1	●
DHCP_Port2_GW	50.68.180.1	Port2	Active	1	●

The host, user, and source of an advanced threat are also easily determined simply by clicking the ATP (advanced threat protection) widget in the dashboard.

HOSTNAME, IP	THREAT	COUNT
● Mac Server 100.1.10	C2/Generic-A /Users/Chris/Desktop/MacBadActor.app/Contents/MacOS/MacBadActor	2

System graphs also show performance over time with selectable timeframes, whether you want to look at the last two hours to the last month or year. And they provide quick access to commonly used troubleshooting tools to resolve potential issues.



The live log viewer is available from every screen with just a single click. You can open it in a new window to keep one eye on the relevant log while working on the console. It provides two views, a simpler column-based format by firewall module, as well as a more detailed unified view with powerful filter and sort options that aggregates logs from across the system into a single real-time view.

Time	Log Comp	Action	Username	Firewall Rule	In Interface	Out Interface	Source IP	Destination IP	Rule Type	Message ID	Live PCAP	Message
2017-11-29 09:48:16	Invalid Traffic	Denied		0	Port2		23.45.114.117	50.68.180.222	0	01001	Open PCAP	Could not associate packet to any connection.
2017-11-29 09:48:14	Firewall Rule	Allowed	mindy	4	Port1	Port2	10.0.1.52	64.58.194.92	2	00001	Open PCAP	
2017-11-29 09:48:13	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	34.200.434.40	2	00001	Open PCAP	
2017-11-29 09:48:13	Firewall Rule	Allowed		10	Port3	Port2	192.168.1.10	54.87.89.218	1	00001	Open PCAP	
2017-11-29 09:48:12	Firewall Rule	Allowed		10	Port6	Port2	192.168.1.11	12.149.218.73	1	00001	Open PCAP	
2017-11-29 09:48:06	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	54.186.179.15	2	00001	Open PCAP	
2017-11-29 09:48:03	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	23.45.114.117	2	00001	Open PCAP	
2017-11-29 09:48:03	Firewall Rule	Allowed		4	Port1		10.0.1.15	23.45.114.117	2	00001	Open PCAP	
2017-11-29 09:48:02	Firewall Rule	Allowed		10	Port3	Port2	192.168.1.10	54.87.89.218	1	00001	Open PCAP	
2017-11-29 09:48:02	Firewall Rule	Allowed	chris	4	Port1	Port2	10.0.1.15	64.58.194.92	2	00001	Open PCAP	

If you're like most network administrators, you've probably wondered whether you have too many firewall rules, and which ones are really necessary versus ones that are not actually being used. With Sophos XG Firewall, you don't need to wonder anymore.

Time	Log Comp	Action	Username	Firewall Rule	In Interface	Out Interface	Source IP	Destination IP	Rule Type	Message ID	Live PCAP	Message
2017-11-29 09:44:30	Invalid Traffic	Denied		0	Port2		23.45.114.117	50.68.180.222	0	01001	Open PCAP	Could not associate packet to any connection.
2017-11-29 09:44:27	Invalid Traffic	Denied		0	Port2		23.45.114.117	50.68.180.222	0	01001	Open PCAP	Could not associate packet to any connection.
2017-11-29 09:44:25	Invalid Traffic	Denied		0	Port2		23.45.114.117	50.68.180.222	0	01001	Open PCAP	Could not associate packet to any connection.
2017-11-29 09:44:22	Invalid Traffic	Denied		0	Port2		23.45.114.117	50.68.180.222	0	01001	Open PCAP	Could not associate packet to any connection.
2017-11-29 09:44:19	Invalid Traffic	Denied		0	Port2		23.45.114.117	50.68.180.222	0	01001	Open PCAP	Could not associate packet to any connection.

The Active Firewall Rules widget shows a real-time graph of traffic processed by the firewall by rule type: Business Application, User, and Network Rules. It also shows an active count of rules by status, including unused rules, providing you with an opportunity to do some housekeeping. As with other areas of the Control Center, clicking any of these will drill down, in this case, to the firewall rules table sorted by the type or status of rule.



## Synchronized Application Control

The problem with application control in today's next-generation firewalls is that most application traffic goes unidentified: it's either unclassified or labelled as unknown, generic HTTP, or generic HTTPS.

There's a simple reason for this: all firewall app control engines rely on signatures and patterns to identify applications. And as you might expect, custom vertical market applications such as medical and financial apps will never have signatures.

### Synchronized Application Control™



Other evasive apps like BitTorrent clients and VoIP as well as messaging apps are constantly changing their behavior and signature to evade detection and control. Many of them now use encryption to escape detection, while others have simply resorted to using generic web browser-like connections to communicate out through the firewall because port 80 and 443 are generally unblocked on most firewalls.

The result is a complete lack of visibility into apps on the network, and you can't control what you can't see. The solution to this is very elegant yet effective: Sophos Synchronized Application Control, which uses our unique Synchronized Security connection with Sophos managed endpoints.

Here's how it works. When the XG Firewall sees application traffic it can't identify with signatures, it asks the endpoint which application is generating that traffic.

Here's how it works. When the XG Firewall sees application traffic it can't identify with signatures, it asks the endpoint which application is generating that traffic.

Application	Category	Endpoints	Occurrences	Last occurrence	Manage
Apple Maps Applications/~/MacOS/Maps	General Internet	Found on 1 Endpoints	11	2018-04-06 14:30	ⓘ ⚙
BitTorrent <UserProfile\...\bittorrent.exe <UserProfile\...\bittorrents.exe	P2P	Found on 1 Endpoints	212	2018-11-20 15:37	ⓘ ⚙
Messages Applications/~/MacOS/Messages	Instant Messenger	Found on 1 Endpoints	6	2018-11-28 15:23	ⓘ ⚙
VirtualBox Applications/~/MacOS/VirtualBox	Infrastructure	Found on 2 Endpoints	26	2018-11-27 12:31	ⓘ ⚙
VMware Fusion Applications/~/VMware Fusion	Infrastructure	Found on 1 Endpoints	1	2018-07-17 23:37	ⓘ ⚙

The endpoint can then share the executable, the path, and often its category, and pass that information back to the firewall. The firewall can then use this information to classify and control the application automatically in most situations.

If XG Firewall can't determine the appropriate application category automatically, the administrator can set the desired category or assign the app to an existing policy.

**Customize Application** [X]

Here you can modify attributes of the automatically categorized application, such as name, category and filter.

Application Name:

Application Path \*:

Application Category:

[Save] [Cancel]

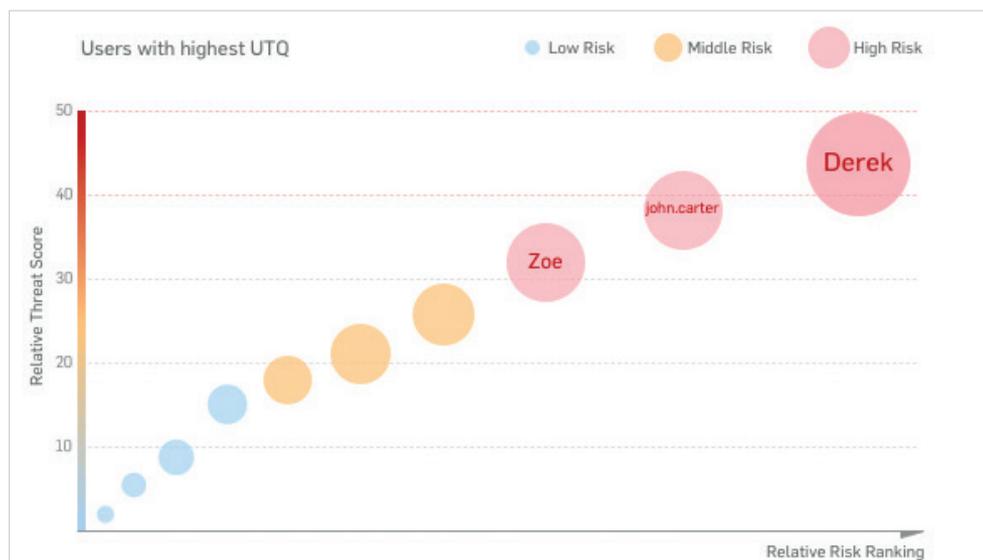
Once an application is classified – either automatically or by the network administrator – the application is subject to the same policy controls as all other applications in that category, making it very easy to block all the unidentified apps you don't want, and prioritize the apps you do want.

Synchronized Application Control is a breakthrough in application visibility and control, providing absolute clarity over every application in use on the network including those that were previously unidentified or uncontrolled.

## Top Risk Users

Studies have proven that users are the weakest link in the security chain. The good news is patterns of human behavior can be analyzed and used to predict and prevent attacks. Also, usage patterns can help illustrate how efficiently corporate resources are utilized and whether user policies need to be fine-tuned.

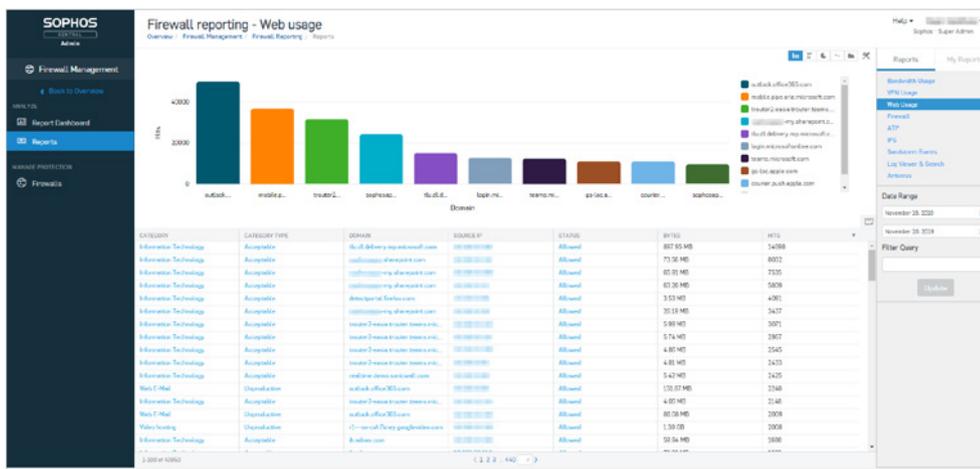
Sophos User Threat Quotient (UTQ) helps security administrators spot users who pose a risk based on suspicious web behavior and threat and infection history. A user's high UTQ risk score may indicate unintended actions due to a lack of security awareness, a malware infection, or intentional rogue actions.



Knowing the user and the activities that caused a risk helps network security administrators take required actions and either educate top risk users or enforce stricter or more appropriate policies to get user behavior under control.

## Flexible Reporting Options

XG Firewall is unique among NGFW and UTM products, providing flexible cloud-based and on-box reporting options with a high degree of customization at no extra charge. Sophos Central Firewall Reporting (CFR) enables organizations to gain deeper insight into network activity through analytics. With its comprehensive set of built-in reports and the tools to create hundreds of variations, CFR offers actionable intelligence on user behavior, application usage, security events, and more. Interactive reports and an at-a-glance report dashboard enable administrators to drill down into the syslog data stored in your Sophos Central account for a granular view that is presented in a visual format for easy understanding. The data can then be analyzed for trends that could identify gaps in the security posture and highlight the need for potential policy change.



XG Firewall also provides on-box reporting. Choose from a comprehensive set of reports, conveniently organized by type, with several built-in dashboards. There are hundreds of reports with customizable parameters across all areas of the firewall, including traffic activity, security, users, applications, web, networking, threats, VPN, email, and compliance. You can easily schedule periodic reports to be emailed to you or your designated recipients, and save reports as HTML, PDF, or CSV.

# Blocking Unknown Threats

Protection from the latest network threats requires a symphony of technologies all working together, and orchestrated by a master conductor – the network administrator. Unfortunately, most firewalls operate more like a one-man-band who plays while juggling throwing knives, with firewall rules set up in one area, web policies in another, TLS/SSL inspection somewhere else, and App Control in a completely different part of the product.

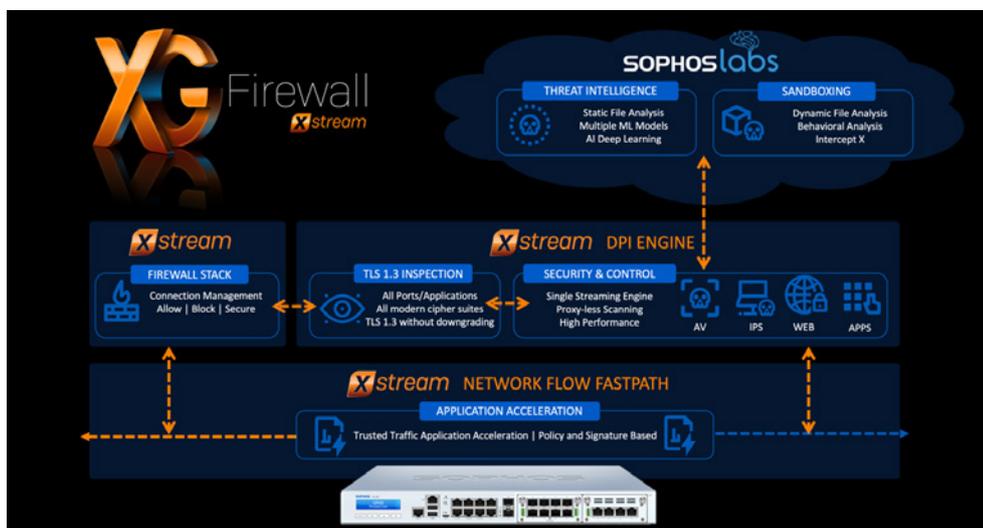
At Sophos, not only do we believe you need the most advanced protection technology available, we also understand it needs to be simple to configure, deploy, and manage day-to-day because misconfigured protection is often worse than having no protection at all.

A commitment to simplicity has always been a key part of the Sophos DNA. But perhaps more importantly, Sophos has a rare willingness to embrace change and take the necessary steps to do things differently in the interest of providing both better protection and ultimately a better user experience.

XG Firewall does things differently that make a big difference.

## Xstream Protection and Performance

Firewall performance shouldn't slow down when you turn on the security you need to keep your network safe from threats. One of the core components of XG Firewall's Xstream packet processing architecture is a high-speed Deep Packet Inspection (DPI) engine. The DPI engine provides proxy-less, single-pass security scanning for IPS, Web, AV, and App Control as well as our Xstream SSL inspection.



When a new connection is established, it is processed by the firewall stack which makes decisions about whether to allow, block, or scan the traffic for threats. If the traffic requires security scanning, it forwards the packets on to the proxy-less high-performance streaming DPI engine which scans the packets, even if they're encrypted. This is only used for the initial few packets. After that, the firewall stack steps out of the way and offloads the processing completely to the DPI engine. This significantly improves latency, and performance.

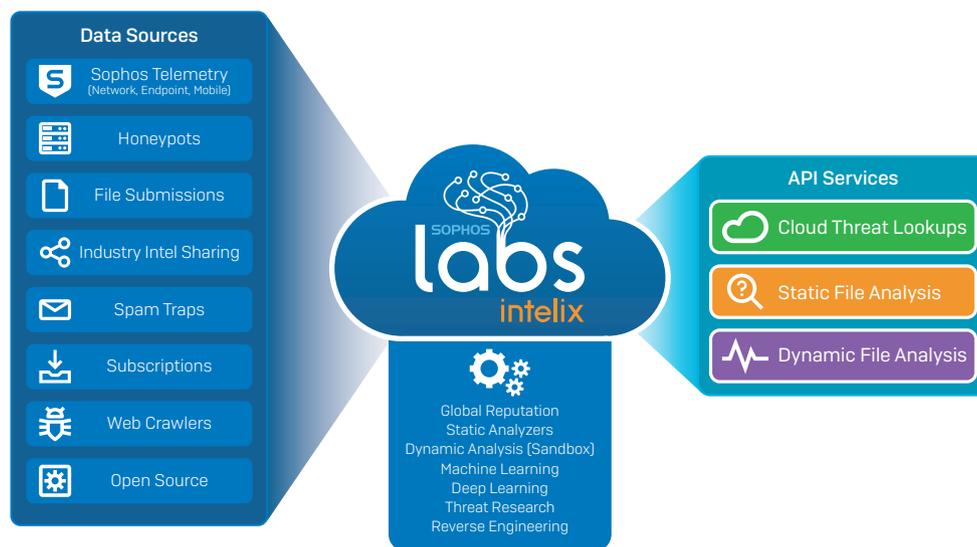
Then, if the stream is considered secure and no longer requires further inspection, the DPI engine can completely offload the flow to the Sophos Network Flow FastPath which provides an accelerated path for trusted traffic. This boosts performance dramatically by freeing up other resources from inspecting traffic that doesn't need it.

## Zero-Day Threat Protection

With advanced threats like ransomware becoming more targeted and evasive, there's a critical need for predictive zero-day threat identification and protection. The ultimate solution to this is two-fold:

1. **Static Machine Learning Analysis** – This provides predictive analysis and detection through multiple artificial neural network machine learning models, combined with global reputation and deep file scanning, all without needing to execute the file in real time.
2. **Dynamic Run-time Sandbox Analysis** – This detonates malware real-time in a cloud sandbox environment for unmatched insights into file activity to reveal the true nature and capabilities of an unknown threat.

XG Firewall includes both of these important protection technologies, powered by SophosLabs Intelix. SophosLabs, our critically acclaimed Tier-1 Cybersecurity threat research lab has developed the ultimate threat analysis and intelligence platform in SophosLabs Intelix. It utilizes the latest machine learning technology, decades of threat research, and petabytes of intelligence, providing unmatched protection against the latest previously unseen threats.



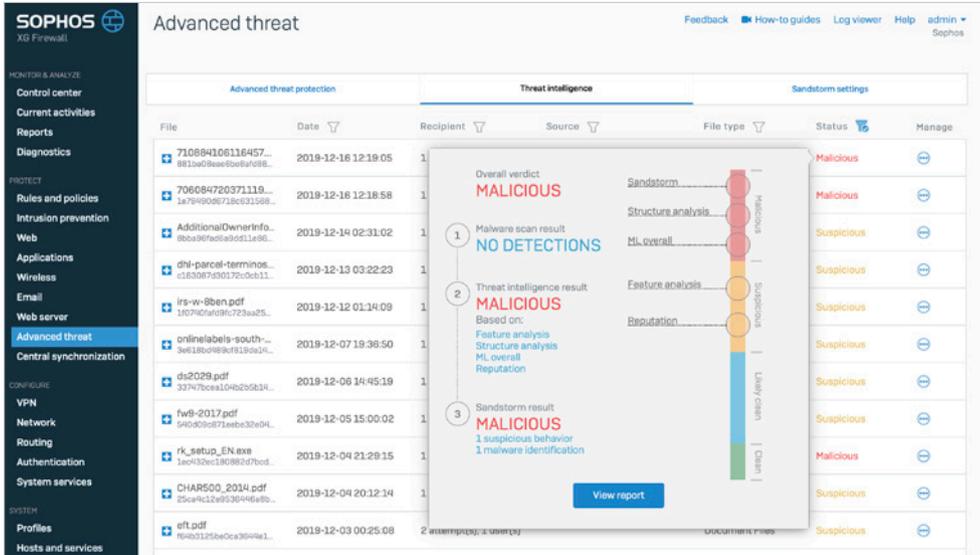
When the XG Firewall Xstream DPI engine performs AV analysis on a file entering the network and determines there is active code, it holds the file temporarily and sends the file to SophosLabs Intelix service in the cloud for both static and dynamic file analysis. It then provides a summary of the results on the XG Firewall Control Center via the Threat Intelligence widget and this click-through report (below) and only releases

### Threat intelligence

5 Recent	24 Incidents	217 Scanned
-------------	-----------------	----------------

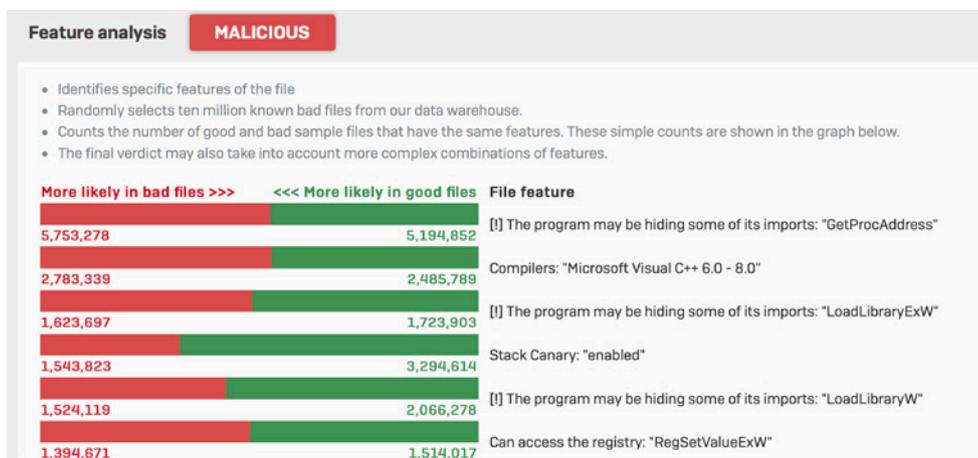
the file to the downloader or email recipient if the file is clean.

This last step is important, as many firewall advanced malware solutions often release the file to the end-user before the analysis is complete, possibly resulting in a messy and costly cleanup if the file was ultimately convicted as a threat.



## Static Machine Learning Analysis

Static file analysis utilizes multiple machine learning models to analyze various characteristics, features, genetics and reputation elements of the file, comparing it with millions of known good and bad files in SophosLabs database to render a verdict in seconds on any new and previously unseen file. It's remarkably fast and effective at identifying new threats and new variants of existing threats, particularly threats that are not easily sandboxed, such as password protected documents containing malware.

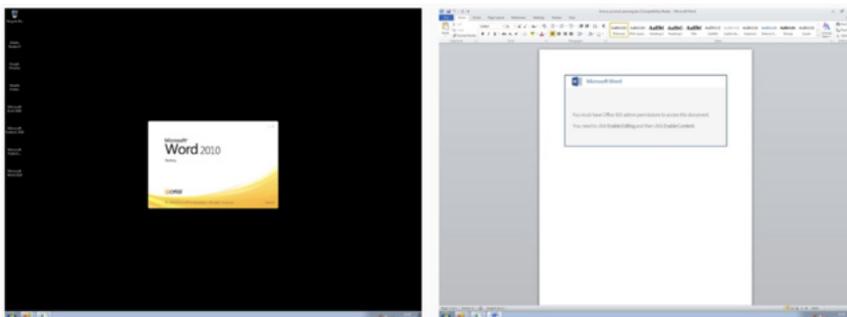


## Dynamic Run-Time Sandboxing Analysis

When sandboxing technology first emerged, it was only affordable for the largest enterprises. But now, thanks to cloud-based sandboxing solutions like Sophos Sandstorm, it's incredibly affordable for even the smallest businesses. For the first time, small and mid-size organizations have access to sandboxing with deep learning technology that goes well beyond the capabilities of dedicated on-premises sandboxing solutions that enterprises were deploying for millions of dollars only a few years ago.

Because it's cloud-based there's no additional software or hardware required, and no impact on firewall performance. Any file determined by the Xstream DPI Engine to contain active code, such as an email attachment or web download is automatically uploaded and detonated in SophosLabs Intelix cloud sandbox in parallel with the Static analysis (above) to determine its run-time behavior before being allowed onto your network.

To identify threats, SophosLabs have integrated the latest protection technologies from our industry-leading Intercept X next-gen endpoint product into Sophos Sandstorm, including deep learning, exploit detection, and CryptoGuard (to detect active Ransomware encrypting files in real time). It also monitors all file, memory, registry and network activity for characteristics of malicious intent to render a verdict. No other firewall offers this kind of run-time analysis with the world's best threat protection – Intercept X. And no other firewall offers the level of insights and reporting that XG Firewall provides – including a full set of screen shots of what transpired as the file was run.



Sandboxing is particularly effective at detecting threats that lurk in normally benign files that may not have any obvious malicious characteristics. Office files with macros, or benign executables or application updates that have been subverted.

# Threat Protection Reporting

Every file analyzed by XG Firewall has an accompanying report that provides full details on the results of the various analysis and the verdicts. There are 6 different elements of the report including the various machine learning analysis, file reputation, sandboxing, and even 3rd party VirusTotal data.

### Investigation and actions

[drive]\[redacted]\file.exe

**Blocked 5 times for 3 users.** [Source details](#)

**Time of analysis**  
 Static: 2019-07-26 21:09:08  
 Sandstorm: 2019-04-16 17:40:58

**Overall verdict**

MALICIOUS



### Analysis summary

MALICIOUS	MALICIOUS	MALICIOUS	SUSPICIOUS	NOT DETECTED	9/71	None
Machine learning Overall analysis	Machine learning File features	Machine learning File structure	File reputation	Sandstorm	VirusTotal detections	XG malware scan

#### Information about your file

File name [drive]\[redacted]\file.exe  
 File type application/x-dosexec  
 SHA1 41b88b777b6fd365e72f1344ae29fcdaf2f2e9af  
 SHA256 6f14a34560d2076523e95ae66b126d363d5552730459399a9cb3d9a4f2172086  
 File size 10,096,640 bytes  
[All details](#)

### Machine learning

MALICIOUS

Overall verdict based on the Sophos deep learning model

Our model identifies many attributes of the file and compares their occurrence, individually and in different combinations, with millions of known good and known malware samples. The reports below show probabilities based on key components of the overall score. Each component isn't a strong indicator on its own but, in combination, they provide a critical insight. This model identifies many different characteristics of your file and compares the occurrence of those characteristics, individually and in combinations, across millions of known good and known malware samples.

#### Feature analysis

- Identifies specific features of the file.
- Randomly selects one million (out of **2,906,531**) known good and one million (out of **20,045,125**) known bad files.
- Counts the number of good and bad sample files that have the same features. These simple counts are shown in the graph below.
- The verdict may also take into account more complex combinations of features
- This test rates **file.exe** as **MALICIOUS**.

More likely in bad files	<<< More likely in good files	File feature
6,747	5,292	Can access the registry: "RegDeleteKeyW"
30,962	31,332	[!] The program may be hiding some of its imports: "GetProcAddress"
23,868	22,093	[!] The program may be hiding some of its imports: "LoadLibraryA"
48,199	49,165	Stack Canary: "disabled"
122	30	Packer: "Unusual section name found: .vmp0"
108	24	Packer: "Unusual section name found: .vmp1"

#### Feature combinations

## Unified Rule Management

Managing a firewall can be incredibly challenging. With multiple rules, policies, and security settings spread across a variety of functional areas and often with several different rules required to provide the necessary protection, there's a lot to do.

With XG Firewall, we took the opportunity to completely re-think the way firewall rules are organized and how your security posture is managed. Instead of having to hunt around the management console looking for the right policies, we collected all firewall rule and enforcement management into a single unified screen. You can now view, filter, search, edit, add, modify, and organize all your firewall rules in one place.

The screenshot displays the 'Rules and policies' management interface in the Sophos XG Firewall console. The interface is organized into several sections:

- Header:** Includes the Sophos logo, 'Rules and policies' title, and navigation links like 'Feedback', 'How-to guides', 'Log viewer', 'Help', and 'admin'.
- Navigation:** A sidebar on the left contains various management categories such as 'MONITOR & ANALYZE', 'CONTROL CENTER', 'PROTECT', 'CONFIGURE', and 'SYSTEM'.
- Filtering:** At the top, there are tabs for 'Firewall rules', 'NAT rules', and 'SSL/TLS inspection rules'. Below these are filters for 'IPv4', 'IPv6', and 'Disable filter', along with 'Add firewall rule', 'Disable', and 'Delete' buttons.
- Table:** A main table lists individual rules with columns for:
  - Rule type:** A dropdown menu.
  - Name:** The rule's name, often with a status icon (e.g., green for active, red for disabled).
  - Source zone:** The source of traffic.
  - Destination zone:** The destination of traffic.
  - What:** The service or application being managed.
  - Status:** The current state of the rule.
  - ID:** A unique identifier for the rule.
  - Action:** The action taken by the rule (e.g., 'Accept').
  - Feature and service:** A list of associated features and services.
- Summary:** A summary row for a group of rules, such as 'Server Access and ...' with a total size of 'in: 4.30 KB, out: 1.58 KB'.

Rules for users, business applications, NAT, TLS/SSL inspection, and networking make it easy to view only the policies you need while providing a single convenient screen for management.

Indicator icons provide important information about policies such as their type, status, and enforcement, plus much more.

## Managing Your Security Posture at a Glance

Whether through your Sophos Central account in the cloud or the XG Firewall user interface, Sophos makes it incredibly easy to configure and manage everything needed for modern protection and do it all from a single screen.

The screenshot shows the 'Security features' configuration page. Callouts on the right side point to various features:

- Dual AV**: Points to the 'Malware and content scanning' section.
- Sandboxing**: Points to the 'Detect zero-day threats with Sandstorm' checkbox.
- SSL Inspection**: Points to the 'Filtering common web ports' section.
- Heartbeat**: Points to the 'Configure Synchronized Security Heartbeat' section.
- App Control**: Points to the 'Identify and control applications (App control)' section.
- QoS**: Points to the 'Shape traffic' section.
- Prioritization**: Points to the 'DSCP marking' section.
- IPS**: Points to the 'Detect and prevent exploits (IPS)' section.

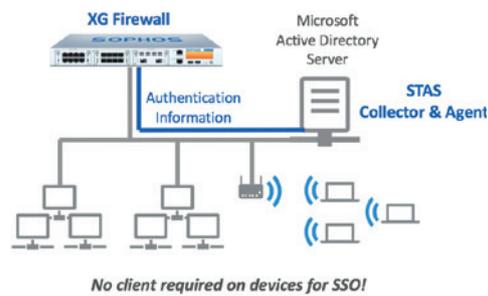
You can set up and snap in security and control for antivirus, TLS/SSL inspection, sandboxing, IPS, traffic shaping, web and app control, Security Heartbeat, NAT, routing, and prioritization all in one place — and all on a rule by rule, user by user, or group by group basis.

And if you want to see exactly what any of your snap-in policies are doing, or even make changes, you can edit them in place without having to leave the firewall rule and visit another part of the product.

The screenshot shows the 'Edit web policy' configuration page. It includes a table with the following columns: Users, Activities, Action, Constraints, Manage, and Status.

Users	Activities	Action	Constraints	Manage	Status
chris joe	All web traffic and with content Ethnicity terms [Canada] Objectionable Terms			+ (c) (i) (t)	ON
Anybody	Anonymizers			+ (c) (i) (t)	ON
Anybody	Weapons			+ (c) (i) (t)	ON
Anybody	Extreme			+ (c) (i) (t)	ON
Anybody	Phishing & Fraud			+ (c) (i) (t)	ON

Flexible authentication options enable you to easily know who's who, and include directory services such as Active Directory, eDirectory, and LDAP, as well as NTLM, Kerberos, RADIUS, TACACS+, RSA, client agents, or a captive portal. And Sophos Transparent Authentication Suite (STAS) provides integration with directory services such as Microsoft Active Directory for easy, reliable, and transparent single sign-on authentication.



## Enterprise-Grade Secure Web Gateway

Web protection and control is a staple of any firewall, but unfortunately, it feels like an afterthought in most firewall implementations. Our experience building enterprise-grade web protection solutions has provided us with the background and knowhow to deploy the kind of web policy control you would normally only find in enterprise secure web gateway (SWG) solutions costing 10 times as much. We've implemented a top-down inheritance policy model, which makes building sophisticated policies easy and intuitive. Pre-defined policy templates, available right out of the box, are included for most common deployments such as typical workplace environments, CIPA compliance for education, and much more. It means you can be up and compliant immediately with easy fine-tuning and customization options at your fingertips.

Users	Activities	Action	Constraints	Manage	Status
Anybody	Uncategorized and with content Ethnicity terms [USA] Objectionable Terms	Block		+ @ -	On
job	Social Networking	Allow		+ @ -	Off
Anybody	Not Suitable for the Office	Block		+ @ -	On
	Default Action	Allow			

Policy Name	Description	Count	Manage	Status
Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments	0	+ @ -	On
No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites	0	+ @ -	On
No Explicit Content	Deny access to sexually explicit sites	0	+ @ -	On
No Games Ads or Explicit Content	Deny access to games, advertisements, and sexually explicit sites	0	+ @ -	On
No Online Chat	Deny access to online chat sites	0	+ @ -	On
No Web Mail	Deny access to web mail sites	0	+ @ -	On

In fact, we know that web policy is one of the most frequently changed elements on a day-to-day basis in your firewall, which is why we've invested heavily in making it easy for you to manage and tweak policies based on your user and business needs. You can easily customize users and groups, activities (comprised of URLs, categories, content filters, and file types), actions (to block, allow, or warn), and add or adjust time-of-day and day-of-week constraints.

## Education Features

XG Firewall offers several features ideally suited for education environments where web policy and compliance are critical requirements. Education specific features include:

- Pre-packaged web policies for CIPA compliance
- Content filtering and reporting on keywords
- SafeSearch and YouTube Restriction settings on a user/group policy basis
- Blockpage overrides that can be managed by teachers
- Comprehensive built-in reporting to identify potential issues early

Web policies now include the option to log, monitor, and even enforce policy related to dynamic content based on keyword lists. This feature is particularly important in education environments to ensure online child safety and provide insights into students using keywords related to self-harm, bullying, radicalization, or otherwise inappropriate content. Keyword libraries can be uploaded to the firewall and applied to any web filtering policy as added criteria with actions to log, monitor, or block search results or websites containing the keywords of interest.

Comprehensive reporting is provided to identify keyword matches and users that are searching or consuming keyword content of interest, enabling proactive intervention before an at-risk user becomes a real problem.

XG Firewall helps with CIPA policy compliance right out of the box, enabling quick compliance. It also offers flexible and powerful controls over SafeSearch and YouTube restrictions on a user/group policy basis. And teachers can be granted the option to set up and manage their own policy overrides to enable their classrooms to access websites that would normally be blocked as part of the curriculum.

It's powerful web policy made simple.

## Simplified NAT Configuration

Anyone who's tried to configure NAT (Network Address Translation) rules knows how challenging this can be. However, it doesn't have to be. XG Firewall includes full enterprise NAT capabilities for powerful and flexible NAT configurations including Source NAT (SNAT) and Destination NAT (DNAT) in a single rule with granular selection criteria. To make complex DNAT simpler, an easy-to-use wizard walks you through the process of creating a full NAT configuration in just a few clicks.

Administrators can also take advantage of the convenient Linked NAT option when creating a firewall rule. Linked NAT will automatically create a corresponding NAT configuration rule, further reducing time spent creating and configuring NAT rules.

**Server access assistant (DNAT)**

Review your selection

Select **Save** to add NAT rules and firewall rules with the following configuration:

Internal server to access from the internet  
IP host: **10.0.1.10**  
Hostname: **Mac Server**

Public IP address through which users access the internal server  
IP host: **50.68.180.222**  
Hostname: **#Port2**

Services that users can access:  
**Server Port Forwarding**

Sources from which users can access the server:  
**Any**

Creates three NAT rules:  
Inbound NAT (DNAT): Traffic destined to the public IP address **50.68.180.222** is translated to the internal server address **10.0.1.10**.  
Outbound NAT (SNAT): Masquerades outbound traffic from the internal server **10.0.1.10** with the public IP address **50.68.180.222**.  
Loopback NAT: Internal network uses the same public IP address **50.68.180.222** to access the internal server **10.0.1.10**.

Creates one firewall rule:  
Allows access to the internal server for **Server Port Forwarding** services from the sources **Any**.

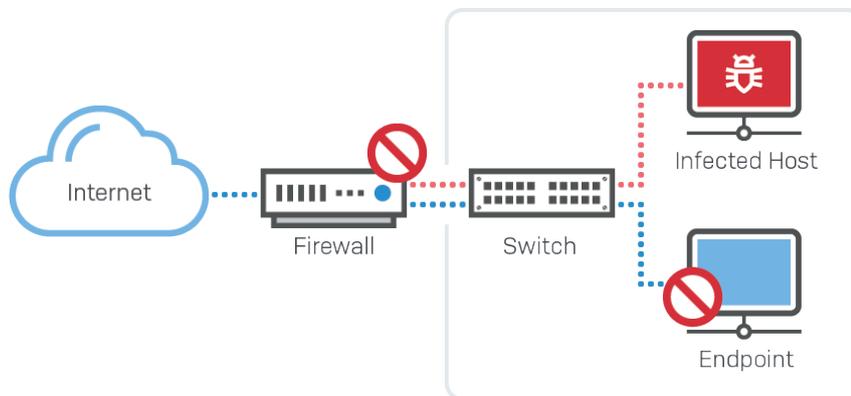
The rules are added at the top of the table and are turned on by default.

[Cancel](#) 5 of 5 [Back](#) [Save and finish](#)

# Automatic Response to Incidents

One of the most requested firewall features from network administrators is the ability to automatically respond to security incidents on the network.

Sophos XG Firewall is the only network security solution that fully identifies the source of an infection on your network and automatically limits the infected device's access to other network resources in response. This is made possible with our unique Sophos Security Heartbeat, which shares telemetry and health status between Sophos-managed endpoints and your firewall.



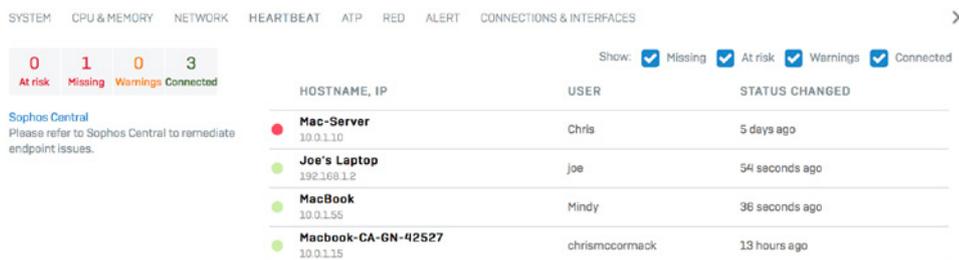
XG Firewall uniquely integrates the health of connected hosts into your firewall rules, enabling you to automatically limit access to sensitive network resources from any compromised system until it's decontaminated.

Not only can XG Firewall isolate endpoints from accessing other parts of the network at the firewall, it can also enlist the aid of all the healthy endpoints on the network to further isolate a compromised host at the endpoint level.

This Lateral Movement Protection, as we call it, isolates and prevents threats or attackers from moving laterally across the network to other systems, even if they are on the same network segment or broadcast domain where the firewall normally can't intervene. It's an extremely simple and effective solution to the challenge of active adversaries operating on your network. And it's only possible if your endpoint and firewall are working together on a coordinated or synchronized defense.

## Security Heartbeat

Sophos Security Heartbeat shares intelligence in real time using a secure link between your Sophos-managed endpoints and XG Firewall. This simple step of synchronizing security products that previously operated independently creates more effective protection against advanced malware and targeted attacks.



Security Heartbeat not only identifies the presence of advanced threats instantly, it can also be used to communicate important information



about the nature of the threat, the host system, and the user. And perhaps most importantly, Security Heartbeat can also automatically act to isolate or limit access to compromised systems until they are free of malware. It's exciting technology that has revolutionized the way IT security solutions identify and respond to advanced threats.

Security Heartbeat for managed endpoints behind your firewall can be in one of three states:

**Green Heartbeat** status indicates the endpoint device is healthy and allowed to access all appropriate network resources.

**Yellow Heartbeat** status indicates a warning that a device may have a potentially unwanted application (PUA), is out of compliance, or is experiencing other issues. You can choose which network resources a yellow heartbeat can access until the issue is resolved.

**Red Heartbeat** status indicates a device that is at risk of being infected with an advanced threat and may be attempting to call home to a botnet or command and control server. Using the Security Heartbeat policy settings in your firewall, you can easily isolate systems with a red heartbeat status until they can be cleaned to reduce the risk of data loss or stop the infection from spreading.

**Synchronized Security**

Minimum Source HB Permitted:

GREEN   
  YELLOW   
  No Restriction

Block clients with no heartbeat

Minimum Destination HB Permitted:

GREEN   
  YELLOW   
  No Restriction

Block request to destination with no heartbeat

Only Sophos can provide a solution like the Security Heartbeat, because only Sophos is a leader in both endpoint and network security solutions. While other vendors are starting to realize this is the future of IT security and are scrambling to implement something similar, they are all at a distinct disadvantage: they don't own both an industry-leading endpoint solution and an industry-leading firewall solution that integrate together.

## It's a Zero Trust World

Trust has become a dangerous word in IT, especially when that trust is implicit. Creating a large, sealed-off corporate perimeter and trusting everything inside has proven to be a flawed design.

Zero Trust is a holistic approach to security that addresses these changes and how organizations work and respond to threats. It's a model and a philosophy for how to think about and do security.

No one and no thing should be automatically trusted, whether inside or outside of the corporate network. Eventually, however, something needs to be trusted. With Zero Trust, this trust is temporary and established from multiple sources of data, and it's constantly re-evaluated.

Zero Trust enables us to control our entire estate, from inside the office out to the cloud platforms we use. No more lack of control outside the corporate perimeter, or struggles with remote users.

How do we move towards Zero Trust and take advantage of all the benefits it offers? While no one can provide Zero Trust as a singular solution, Sophos has a wide portfolio of security technologies and controls that accelerates and simplifies your journey to Zero Trust.

**Sophos Central** Our cloud-based cybersecurity platform puts these disparate and complementary technologies into a single hub to help you orchestrate and monitor your Zero Trust network.

**Synchronized Security** Cybersecurity that continuously shares information between systems, providing insight and visibility to one another.

**XG Firewall** Create segments or micro-perimeters around users, devices, apps, networks, and more.

**Server Protection and Intercept X** Assign a Device Health status for every device so that, in the event one is compromised, the devices can be automatically isolated and blocked from connecting with other devices.

**Managed Threat Response (MTR) service** Monitors all user activity across the network and identifies potentially compromised user credentials.

# Add XG Firewall to Any Network – Simply

## XG Firewall and Intercept X



## Inline Deployment



## Discover Mode



XG Series hardware appliances offer flexible deployment options with fail-open bypass ports standard on all 1U models and available in Flexi Port Modules to enable this feature on our 2U appliances as well. The bypass ports enable XG Firewall to be installed in bridge mode in line with existing firewalls. If the XG Firewall needs to be shut down or rebooted to update the firmware, the bypass ports provide business continuity by allowing traffic to continue to flow ensuring no disruptions to the network. This feature enables new deployment options that are completely risk free without replacing any existing network infrastructure. And what's more, our next-gen endpoint protection, Intercept X, runs alongside any existing desktop antivirus product, enabling a complete Sophos Synchronized Security solution to be deployed in any network without replacing anything.

Sophos XG Firewall: It's cybersecurity made simple.

## Request Pricing

Request a no-obligation quote customized to your needs at [sophos.com/firewall-quote](https://sophos.com/firewall-quote)

United Kingdom and Worldwide Sales  
Tel: +44 (0)8447 671131  
Email: [sales@sophos.com](mailto:sales@sophos.com)

North America Sales  
Toll Free: 1-866-866-2802  
Email: [nasales@sophos.com](mailto:nasales@sophos.com)

Australia and New Zealand Sales  
Tel: +61 2 9409 9100  
Email: [sales@sophos.com.au](mailto:sales@sophos.com.au)

Asia Sales  
Tel: +65 62244168  
Email: [salesasia@sophos.com](mailto:salesasia@sophos.com)