

# Firewall Competitive: WatchGuard vs Sophos

For Internal and Partner Audiences Only

## Target Market

Sophos is also a good shortlist contender for SMBs, especially for lower-midsize business and distributed-office use cases that value ease of use, security features and firewall/endpoint integration. They cater to organizations with between 100 and 5,000 employees.

## Target Industries:

Education, Healthcare, Retail, Finance & Banking, Government, Public Sector.

## Key Facts and Financials

Headquartered in Abingdon, U.K., Sophos has more than 3,000 employees globally. Sophos, once a leader in the Gartner Magic Quadrant, now is considered a Niche Player for Firewalls.

## Footprint and Flagship Customers

Sophos is a long-time player in the endpoint security and antivirus space, providing solutions to SMBs as well as consumers. Sophos purchased Invincea for its machine-learning malware detection features.

## Flagship Customers:

Konica Minolta, Saint Michael's College, University of San Carlos, Columbia Valley Community Health, North of England Commissioning Support, NHS Trust, PappaRich, Scruton Bland, Peoples Independent Bank, South Oxfordshire District Council.

## Product Offerings

### Sophos UTMs

Sophos firewall product line consists of Sophos XG Series, which includes 19 models, all of which were introduced in 2015 and refreshed in 4Q16; and the legacy Sophos SG Series (sometimes called Sophos UTM).

### InterceptX

Sophos Intercept X is an endpoint solution that employs a comprehensive defense-in-depth approach to endpoint protection rather than simply relying on one primary security technique.

### Synchronized Security

Synchronized Security is a security system that enables defenses to be coordinated from network endpoint, wireless, email, mobile and more to protect against emerging threats.

## Customer Reviews/Ratings – Trust Radius

### WatchGuard Network Security

Score 9.1 out of 10



<https://www.trustradius.com/products/watchguard-network-security/reviews>

### Sophos XG Firewall Reviews

Score 8.5 out of 10



<https://www.trustradius.com/products/sophos-xg-firewall/reviews>

## Cloud Management Feature Comparison

	WatchGuard	Sophos
<b>Multi-Tier, Multi-Tenant Service</b>		
Multi-ten. multi-tenant capabilities	4	1
Simplicity of activation and navigation	4	2
Onboarding of Customers and Operators	3	3
<b>Centralized Deployment &amp; Management</b>		
Zero-touch Deployment	4	3
Deploy secure policies by default	4	3
Easily deploy across many customers	4	3
Offline Configurator	4	1
Configuration Templates	4	3
Management capabilities for security services	3	1
Policy management and configurator	4	1
<b>Flexible Management</b>		
Inventory management experience	4	4
Delegated management capabilities	4	3
<b>Platform Accessibility</b>		
Role-based access control	4	4
Identity-based management	4	4
Audit logs for changes	3	3
<b>Licensing</b>		
Licensing structure and options	4	3
Additional licenses for features or security services	4	3
<b>Reporting &amp; Visibility</b>		
Reporting visuals and functionality	3	4
Custom reporting	4	2
Alerts and notifications	3	3
Custom Branding	4	1
Dark Web Scan	4	0

## Certification Coverage

Certification	WatchGuard	Sophos
CC EAL 4+	✓	✗
FIPS 140-2	✓	✗
NIAP CC	✓	✗
CSfC (Commercial Solutions for Classified Programs)	✓	✗
NetSecOPEN	✓	✗

# Firewall Competitive: WatchGuard vs Sophos

For Internal and Partner Audiences Only

## Strengths

- +** **Single Pane of Glass**  
Sophos Capture Security Center is an all-inclusive security console that unifies management, analytics and control for wired, wireless, cloud and endpoint solutions through a single pane of glass.
- +** **Dedicated Capture Labs Threat Research Team**  
Sophos has a large in-house threat research team.
- +** **Unlimited AV File Scanning Limit**  
Sophos's stream-based approach means they can scan files of any size to detect and block malware.
- +** **Simple Licensing and Low TCO**  
Sophos aggressively prices their Firewall platform and, similar to WatchGuard, offers bundle-based licensing, for an easier customer purchase experience.

## Weaknesses

- ✗** **Performance in Full UTM Mode.** Sophos UTM devices include hardware that offers high performance for simple firewall packet filtering, but **degrades dramatically when full UTM services are enabled**, giving up as much as 95% of throughput when AV protection is active.
- ✗** **UTM as a SD-WAN Solution.** Sophos SD-WAN capabilities lack link monitoring and dynamic path selection. NSS Labs gave Sophos a rating of "Caution" in their SD-WAN test report.
- ✗** **Cloud-based Reporting.** Sophos standard reporting is limited, and occurs on-box. Additional licenses are needed to get close to the functionality of Dimension.
- ✗** **Remote Office Solution.** Sophos RED (Remote Ethernet Device) require remote offices to send all traffic through a VPN connection to the corporate headquarters, and are not UTMs.
- ✗** **Offline Configuration.** Sophos does NOT allow any offline configuration within their management tools.

## Comparative Feeds and Speeds

	XGS 87	T20	XGS 107	XGS 116	T40	XGS 126	T60	XGS 136	M290	XGS 2100	M390	XGS 2300	M590	XGS 3100	XGS 3300	M690	XGS 4300	M4800	XGS 4500	XGS 5500	M5800
Firewall (Mbps)	3700	1780	7000	7700	3400	10500	4700	11500	5800	30000	18000	35000	20000	38000	40000	29700	75000	49600	80000	100000	87000
IPS (Mbps)	2500	271	2900	3500	510	4000	909	4700	1214	5800	2341	7000	3217	9820	13440	4256	25000	33000	35650	40000	36000
UTM (Mbps)	1015	154	1355	2000	294	1800	681	3300	1100	1250	2800	1400	3300	2000	2770	4670	4800	5213	8390	12390	11328
VPN (Mbps)	240	485	330	685	330	900	1400	1000	2400	1250	5280	1400	6840	2000	2770	9920	4800	16400	8390	12390	18800
HTTPS inspection (Mbps)	375	115	420	650	200	800	344	950	696	1100	1,326	1450	2,067	2470	3130	2,941	8000	2558	10600	13500	2845
Connections per second	750	8,761	900	1100	19,456	1800	25000	2500	35,293	1450	97,343	1700	131,291	2750	3200	147,456	4800	254,273	4800	8400	328,143
# of Ports	4x Gb	5x Gb	8x Gb	8x Gb + 1x Module	5x Gb	12x Gb + 1x Module	8x Gb + 1x Module	10x Gb + 1x Module	8x Gb + 1x Module	8x Gb + 1x Module	8x Gb + 1x Module	8x Gb + 1x Module	8x Gb + 1x Module	8x Gb + 1x Module	8x Gb + 1x Module	8x Gb + 1x Module	8x Gb + 2x Modules	8x Gb + 2x Modules	8x Gb + 2x Modules	8x Gb + 3x Modules	8x Gb + 2x Modules
Integrated Wireless	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No
Basic 3-Year	\$ 782	\$ 875	\$ 1,049	\$ 1,499	\$ 1,655	\$ 2,015	\$ 2,815	\$ 2,882	\$ 4,014	\$ 5,423	\$ 5,820	\$ 7,616	\$ 9,815	\$ 10,386	\$ 14,037	\$ 16,648	\$ 21,030	\$ 24,020	\$ 29,132	\$ 41,265	\$ 60,860
Total 3-Year	\$ 892	\$ 1,400	\$ 1,200	\$ 1,740	\$ 2,650	\$ 2,336	\$ 4,505	\$ 3,387	\$ 6,420	\$ 6,664	\$ 9,374	\$ 15,705.00	\$ 15,705.00	\$ 12,658	\$ 17,202	\$ 26,680	\$ 25,794	\$ 46,120	\$ 35,831	\$ 51,592	\$ 107,110

## Landmine Questions to Ask

1. **Do you want to run your UTM will all security features enabled?**  
*Why it works?* Sophos's performance degrades significantly when security services are enabled.
2. **How will you deploy VPNs in remote offices?**  
*Why it works?* Sophos RED devices require all traffic to go through HQ.
3. **Why hasn't Sophos certified for X (CC EAL 4+, FIPS, NetSecOPEN etc.)**  
*Why it works?* Certification help validate that a solution delivers on its promises, avoiding them is suspicious.
4. **Are you interested in SD-WAN?**  
*Why it works?* Sophos does not offer some key SD-WAN features, and NSS Labs has cautioned against using Sophos for SD-WAN deployments.

## Firewall

	WG	Sophos	WatchGuard Advantage
Offline Configuration	Yes	No	Fireboxes can be configured on-site without Internet access.
Device Detection	Yes	No	Network Discovery makes mapping all connected devices easy!
Zero-touch deployment	Yes	No	RapidDeploy for cloud-based, zero-touch deployment.
SD-WAN Coverage	Yes	No	Sophos lacks dynamic path selection and link monitoring
PoE+ Ports	Yes	No	PoE+ ports come standard on many Firebox appliances.
Cloud-ready Visualization Database	Yes	No	Sophos requires iView purchase.
Policy Usage Report	Yes	No	Sophos requires iView purchase.
Usage and Bandwidth Consumption Reports	Yes	No	Sophos requires iView purchase.