Sophos XGS 128 (Gen2)

Sophos XGS 128 (Gen2) Network Security Appliance Instruction Manual

Model: XGS 128 (Gen2)

Brand: Sophos

1. Introduction

This manual provides essential information for the installation, operation, and maintenance of your Sophos XGS 128 (Gen2) Network Security Appliance. The Sophos XGS 128 is designed for larger networks, offering robust security and high performance.

Key features include:

- Next-generation firewall appliance with Xstream Protection for zero-day defense, cloud sandboxing, email filtering, intrusion prevention, and advanced reporting.
- 9 x 2.5 GE copper ports and 1 SFP fiber port, providing up to 19.1 Gbps firewall throughput.
- TLS inspection and next-generation intrusion prevention to block hidden threats in encrypted traffic.
- Managed through Sophos Central for unified policies and reporting.

2. Product Overview

The Sophos XGS 128 (Gen2) is a compact yet powerful network security appliance. Familiarize yourself with its physical components.

Figure 2.1: Front view of the Sophos XGS 128 (Gen2) Network Security Appliance.

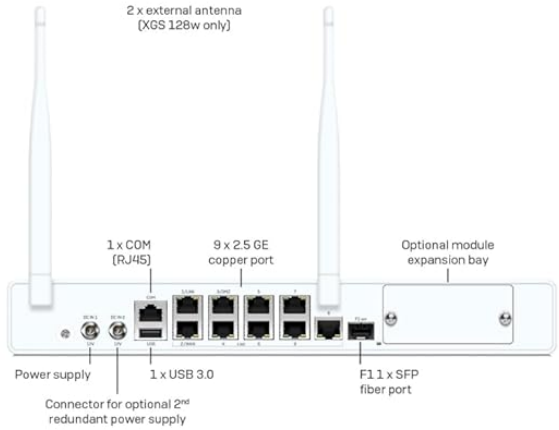
Figure 2.2: Detailed front panel showing LED indicators and ports.

Sophos XGS Series Desktop: SMB and Branch Office Gen.2: XGS 128, XGS 128w

Technical specifications

Front View

Back View



Physical Specifications	
Mounting	Rackmount kit available (to be ordered separately)
Dimensions: Width X height X depth	320 x 44 x 212 mm
Weight	2.4 kg/5.29 lbs (unpacked) 3.9 kg/8.60 lbs (packed) (w-model minimally more)

Environment	
Power supply	External auto-ranging AC-DC 100-240VAC, 2A@50-60 Hz 12VDC, 5.42A, 65W Optional second redundant power supply
Power consumption	26.5 W/90.42 BTU/hr (128 idle) 30 W/102.36 BTU/hr (128w idle) 30 W/102.36 BTU/hr (128 max.) 35 W/119.42 BTU/hr (128w max.)
Noise level (avg.) Typical/Max. operation	XGS 128 - 17.3/26.9 dBA XGS 128(w) - 19.5/31 dBA
Operating temperature	0°C to 40°C (operating) -20°C to +70°C (storage)
Humidity	10% to 90%, non-condensing

Product Certifications	
Certifications	CB, CE, UKCA, UL, FCC, ISED, VCCI, KC*, BSMI, RCM, NOM, Anatel*, TEC

* XGS 128 only

Performance	XGS 128(w)
Firewall throughput	19,100 Mbps
Firewall IMIX	14,500 Mbps
IPS throughput	4,650 Mbps
Threat Protection throughput	4,000 Mbps
NGFW	4,350 Mbps
Concurrent connections	6,000,000
New connections/sec	72,250
IPsec VPN throughput	15,050 Mbps
IPsec VPN concurrent tunnels	2,500
SSL VPN concurrent tunnels	1,500
Xstream SSL/TLS Inspection	1,450 Mbps
Xstream SSL/TLS concurrent connections	18,432

Note: For performance testing methodology, see page 10

Wireless Specification (XGS 128w only)	
No. of antennas	2 external
MIMO capabilities	2 x 2:2
Wireless interface	Wi-Fi 6 (802.11ax) 2.4 GHz/5 GHz concurrent

Physical Interfaces	
Storage (local quarantine/logs)	64 GB UFS 2.1
Ethernet interfaces (fixed)	9 x 2.5 GE copper 1 x SFP fiber
Power-over-Ethernet (fixed)	0
Management ports	1 x COM RJ45 1 x Micro-USB (cable incl.)
Other I/O ports	1 x USB 2.0 (front) 1 x USB 3.0 (rear)
Number of expansion slots	1
Optional add-on connectivity	5G module (Gen.2)

Figure 2.3: Rear panel illustrating the 9 x 2.5 GE copper ports, 1 SFP fiber port, and other connectors.

Your browser does not support the video tag.

Video 2.1: An overview of the Sophos XGS Series 2nd Gen Desktop Appliances, highlighting key features and design.

3. Setup Instructions

3.1 Unpacking and Placement

- Carefully unpack the appliance and all accessories.
- Place the appliance on a stable, flat surface in a well-ventilated area. Ensure adequate space around the device for airflow.
- Avoid placing the appliance near heat sources or in direct sunlight.

3.2 Connecting the Appliance

1. **Connect Power:** Plug the power adapter into the DC IN 1 or DC IN 2 port on the rear of the appliance, then connect it to a power outlet.
2. **Connect Network Cables:**
    - Connect your internet service provider's modem or router to the designated WAN port (e.g., Port 2/WAN) using an Ethernet cable.
    - Connect your internal network switch or a computer directly to a LAN port (e.g., Port 1/LAN) using an Ethernet cable.
    - For SFP fiber connectivity, insert the appropriate SFP module into the SFP port (F1 SFP) and connect the fiber optic cable.
3. **Initial Access:** Connect a computer to a LAN port. The appliance will typically assign an IP address via DHCP. Access the web administration interface by navigating to the default IP address (refer to the quick start guide or Sophos documentation for the specific default IP).

4. Operating Instructions

The Sophos XGS 128 (Gen2) is managed primarily through its web-based administration interface or Sophos Central.

4.1 Initial Configuration

- Follow the on-screen wizard for initial setup, including setting up network zones, basic firewall rules, and administrative passwords.
- Register your appliance with Sophos Central for centralized management and licensing.

4.2 Core Security Features

- **Firewall:** Configure rules to control network traffic based on source, destination, service, and user.
- **Intrusion Prevention System (IPS):** Enable IPS to detect and block known exploits and attacks.
- **TLS Inspection:** Decrypt and inspect encrypted traffic (HTTPS, SMTPS) for hidden threats.
- **Xstream Protection:** Leverage advanced threat protection features like cloud sandboxing and zero-day defense.
- **SD-WAN:** Optimize network performance and reliability for branch office connectivity.

For detailed configuration of specific features, refer to the comprehensive Sophos Firewall documentation available on the Sophos support portal.

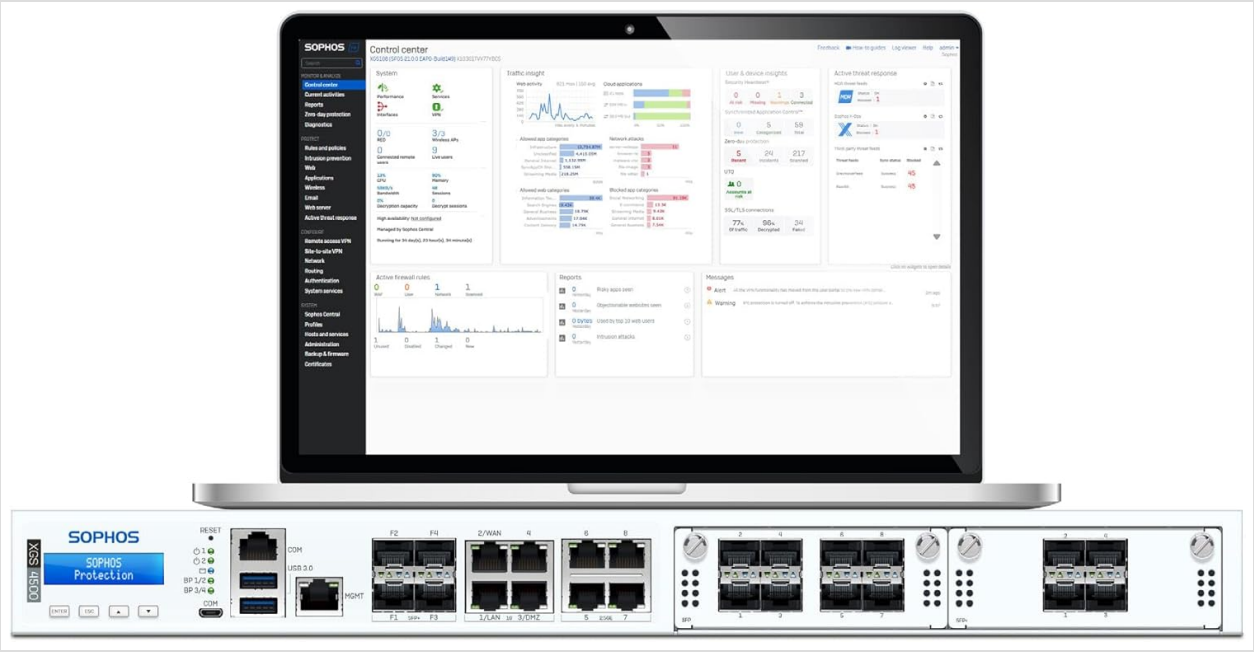


Figure 4.1: Example of the Sophos Central dashboard, providing centralized management and visibility.

5. Maintenance

Regular maintenance ensures optimal performance and security of your Sophos XGS 128 appliance.

- **Firmware Updates:** Regularly check for and apply the latest firmware updates to benefit from new features, performance improvements, and security patches.
- **Configuration Backups:** Periodically back up your appliance configuration. This is crucial for quick recovery in case of unforeseen issues.
- **System Monitoring:** Monitor system logs, resource utilization, and security alerts through the web interface or Sophos Central.
- **Physical Inspection:** Ensure the appliance is free from dust and that ventilation openings are not obstructed.

6. Troubleshooting

This section covers common issues and basic troubleshooting steps.

6.1 LED Indicators

Refer to the front panel LEDs for quick status checks:

- **Power LED:** Indicates power status.
- **Status LEDs:** Provide information on system health and activity. Consult the Sophos documentation for specific LED patterns and their meanings.
- **Port LEDs:** Indicate link status and activity for each network port.

6.2 Common Issues

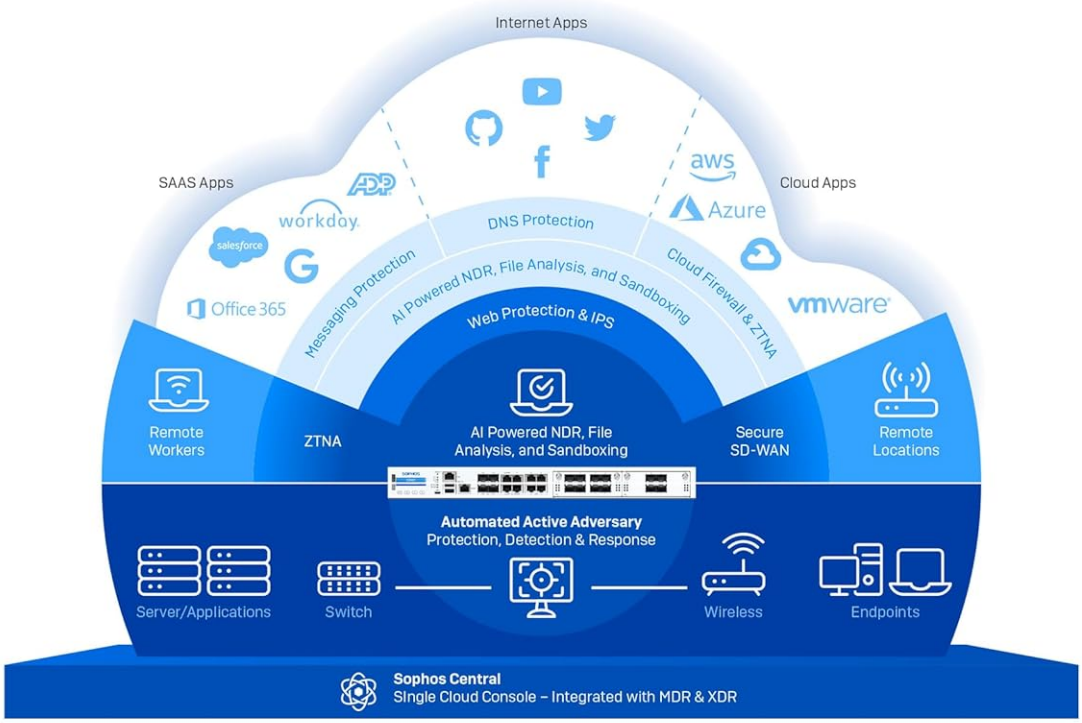
- **No Network Connectivity:**
    - Check all network cable connections.
    - Verify power status of the appliance and connected devices.
    - Ensure correct IP configuration on connected devices.

- **Slow Performance:**
    - Check CPU and memory utilization via the administration interface.
    - Review firewall rules and security policies for potential bottlenecks.
    - Ensure the appliance firmware is up to date.

If issues persist, consult the Sophos support resources or contact Sophos technical support.

7. Specifications

Detailed technical specifications for the Sophos XGS 128 (Gen2) Network Security Appliance.



Powerful Protection and Performance

Sophos Firewall includes the latest advanced protection technologies and threat intelligence, including:

- Streaming DPI engine with web protection and IPS
- Accelerated TLS 1.3 encrypted traffic inspection
- Zero-day AI and machine learning analysis
- Real-time cloud sandboxing
- DNS Protection
- Network Detection and Response

The best part is, you don' t need to compromise on performance. This is thanks to our programmable Xstream architecture. It offloads benign traffic flows and crypto operations as well as VPN and select application routing to accelerate these network traffic flows and create performance headroom for traffic that actually needs deep packet inspection.

Sophos Firewall leverages the Sophos Cloud to ensure that your organization is protected from the latest threats and further maximize your performance. You get the latest AI and machine learning technology from SophosLabs working to identify previously unseen threats and malicious URLs. Using a common cloud, any new threat attacking a single Sophos customer is instantly shared across all our customers, blocking it everywhere. In addition, offloading this analysis from your firewall to the cloud boosts your performance even further.

Figure 7.1: Technical specifications table for the Sophos XGS 128 (Gen2) and related models.

Sophos XGS 128 (Gen2) Key Specifications

Feature	Detail
Brand	Sophos
Model Name	XGS 128
Connectivity Technology	Ethernet, Optical Fiber Port
Operating System	Sophos OS
Number of Ports	10 (9 x 2.5 GE copper, 1 x SFP fiber)
Firewall Throughput	Up to 19.1 Gbps
IPS Throughput	Up to 4.5 Gbps
TLS Inspection Throughput	Up to 1.45 Gbps
Dimensions (H x W x D)	320 x 44 x 212 mm
Weight	2.4 kg (5.29 lbs) unpacked

Sophos XGS Series Appliances

The XGS Series models offer excellent performance and connectivity at every price point to power the protection you need for today's diverse, distributed, and encrypted networks.

Product Matrix

Model		Tech Specs			Throughput			
Model	Form Factor	Ports/Slots (Max Ports)	w-model	Swappable Components	Firewall (Gbps)	IPsec VPN (Gbps)	Threat Protection (Gbps)	Xstream SSL/TLS (Gbps)
XGS 88(w)	Gen.2 Desktop**	4/- (4)	Wi-Fi 6	n/a	9.9	6.0	2.0	600 Mbps
XGS 108(w)		7/-(7)		Optional: 2nd power supply	12.5	8.2	2.5	800 Mbps
XGS 118(w)		10/1(10)		Optional: 2nd power supply, 5G module*	15.5	13.0	3.2	1.1
XGS 128(w)		10/1(10)			19.1	15.0	4.0	1.4
XGS 138		8/1(8)	n/a		19.1	6.6	4.7	1.7
XGS 2100	1U Short	10/1 (18)	n/a	Optional: external power supply	30.0	17.0	5.0	1.1
XGS 2300			n/a		39.0	20.5	5.5	1.4
XGS 3100		12/1 (20)	n/a		47.0	25.5	7.4	2.4
XGS 3300			n/a		58.0	31.1	10.0	3.1
XGS 4300	1U Long	12/2 (28)	n/a		75.0	62.5	25.2	8.0
XGS 4500			n/a	Optional: internal power supply	80.0	75.5	31.8	10.6
XGS 5500	2U	16/3 (48)	n/a	Built in: redundant power, SSDs, fans	100.0	92.5	46.0	13.5
XGS 6500		20/4 (68)	n/a		120.0	109.8	53.5	16.0
XGS 7500		22/4 (70)	n/a		160.0	117.0	70.0	19.5
XGS 8500			n/a		190.0	141.0	92.5	24.0

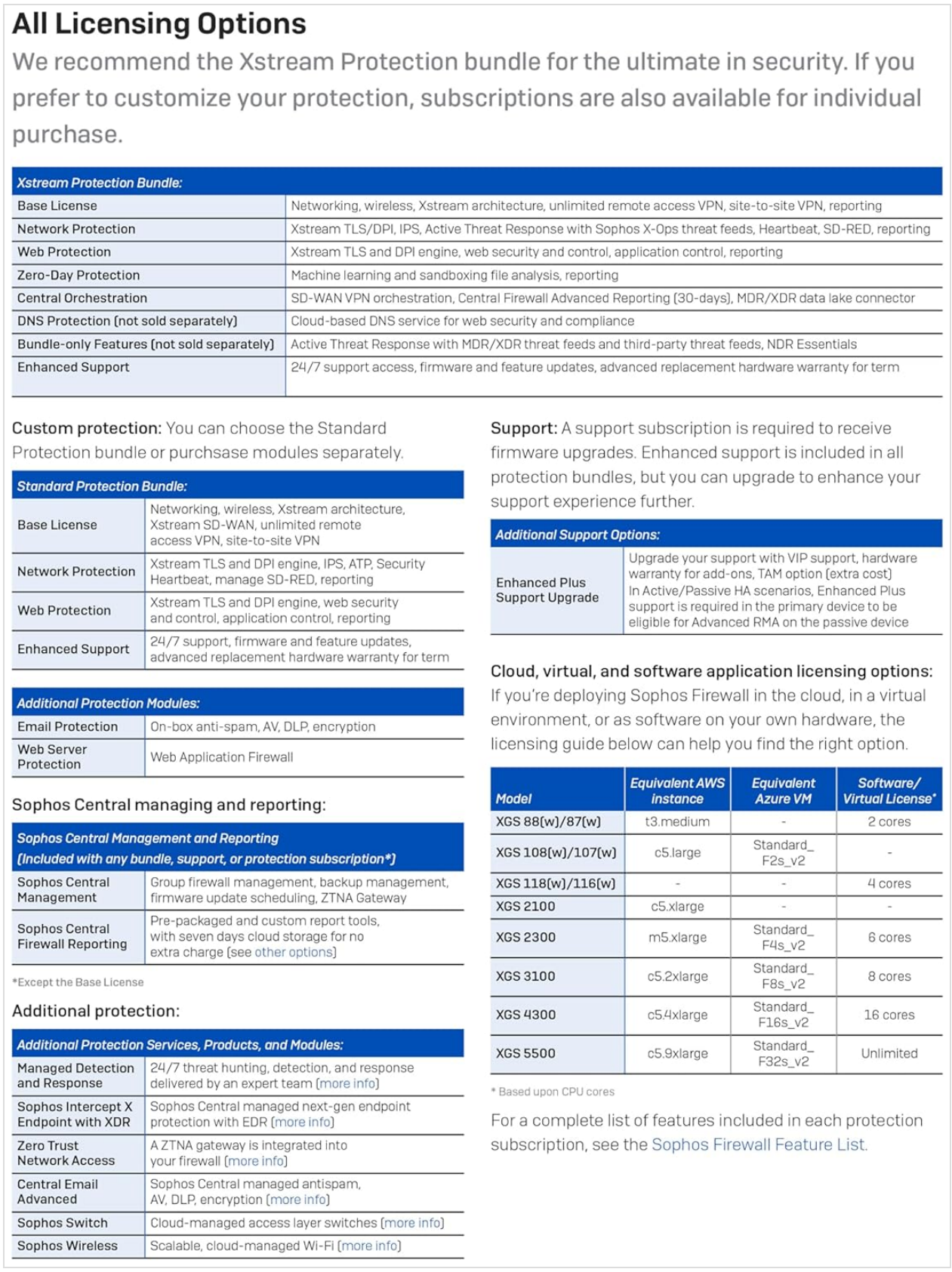
* Not available in Japan

** All Gen.2 desktop models include two or more 2.5G ports

Figure 7.2: Product matrix comparing various Sophos XGS Series models and their technical specifications.

8. Licensing and Protection

The Sophos XGS 128 (Gen2) leverages various licensing options to provide comprehensive security. This appliance includes a 3-year Xstream Protection subscription.



All Licensing Options

We recommend the Xstream Protection bundle for the ultimate in security. If you prefer to customize your protection, subscriptions are also available for individual purchase.

Xstream Protection Bundle:	
Base License	Networking, wireless, Xstream architecture, unlimited remote access VPN, site-to-site VPN, reporting
Network Protection	Xstream TLS/DPI, IPS, Active Threat Response with Sophos X-Ops threat feeds, Heartbeat, SD-RED, reporting
Web Protection	Xstream TLS and DPI engine, web security and control, application control, reporting
Zero-Day Protection	Machine learning and sandboxing file analysis, reporting
Central Orchestration	SD-WAN VPN orchestration, Central Firewall Advanced Reporting (30-days), MDR/XDR data lake connector
DNS Protection (not sold separately)	Cloud-based DNS service for web security and compliance
Bundle-only Features (not sold separately)	Active Threat Response with MDR/XDR threat feeds and third-party threat feeds, NDR Essentials
Enhanced Support	24/7 support access, firmware and feature updates, advanced replacement hardware warranty for term

Custom protection: You can choose the Standard Protection bundle or purchsase modules separately.

Standard Protection Bundle:	
Base License	Networking, wireless, Xstream architecture, Xstream SD-WAN, unlimited remote access VPN, site-to-site VPN
Network Protection	Xstream TLS and DPI engine, IPS, ATP, Security Heartbeat, manage SD-RED, reporting
Web Protection	Xstream TLS and DPI engine, web security and control, application control, reporting
Enhanced Support	24/7 support, firmware and feature updates, advanced replacement hardware warranty for term

Additional Protection Modules:	
Email Protection	On-box anti-spam, AV, DLP, encryption
Web Server Protection	Web Application Firewall

Sophos Central managing and reporting:

Sophos Central Management and Reporting (Included with any bundle, support, or protection subscription)*	
Sophos Central Management	Group firewall management, backup management, firmware update scheduling, ZTNA Gateway
Sophos Central Firewall Reporting	Pre-packaged and custom report tools, with seven days cloud storage for no extra charge (see other options)

*Except the Base License

Additional protection:

Additional Protection Services, Products, and Modules:	
Managed Detection and Response	24/7 threat hunting, detection, and response delivered by an expert team (more info)
Sophos Intercept X Endpoint with XDR	Sophos Central managed next-gen endpoint protection with EDR (more info)
Zero Trust Network Access	A ZTNA gateway is integrated into your firewall (more info)
Central Email Advanced	Sophos Central managed antispam, AV, DLP, encryption (more info)
Sophos Switch	Cloud-managed access layer switches (more info)
Sophos Wireless	Scalable, cloud-managed Wi-Fi (more info)

Support: A support subscription is required to receive firmware upgrades. Enhanced support is included in all protection bundles, but you can upgrade to enhance your support experience further.

Additional Support Options:	
Enhanced Plus Support Upgrade	Upgrade your support with VIP support, hardware warranty for add-ons, TAM option (extra cost) In Active/Passive HA scenarios, Enhanced Plus support is required in the primary device to be eligible for Advanced RMA on the passive device

Cloud, virtual, and software application licensing options: If you're deploying Sophos Firewall in the cloud, in a virtual environment, or as software on your own hardware, the licensing guide below can help you find the right option.

Model	*Equivalent AWS instance*	*Equivalent Azure VM*	*Software/ Virtual License**
XGS 88(w)/87(w)	t3.medium	-	2 cores
XGS 108(w)/107(w)	c5.large	Standard_ F2s_v2	-
XGS 118(w)/116(w)	-	-	4 cores
XGS 2100	c5.xlarge	-	-
XGS 2300	m5.xlarge	Standard_ F4s_v2	6 cores
XGS 3100	c5.2xlarge	Standard_ F8s_v2	8 cores
XGS 4300	c5.4xlarge	Standard_ F16s_v2	16 cores
XGS 5500	c5.9xlarge	Standard_ F32s_v2	Unlimited

* Based upon CPU cores

For a complete list of features included in each protection subscription, see the Sophos Firewall Feature List.

Figure 8.1: Overview of all available licensing options for Sophos XGS appliances, including Xstream Protection and Standard Protection bundles.

8.1 Xstream Protection

Xstream Protection is an advanced security bundle designed to provide comprehensive defense against sophisticated cyberattacks. It includes:

- Zero-day protection with cloud sandboxing.
- Email filtering.

- Automated threat response.
- Advanced reporting.

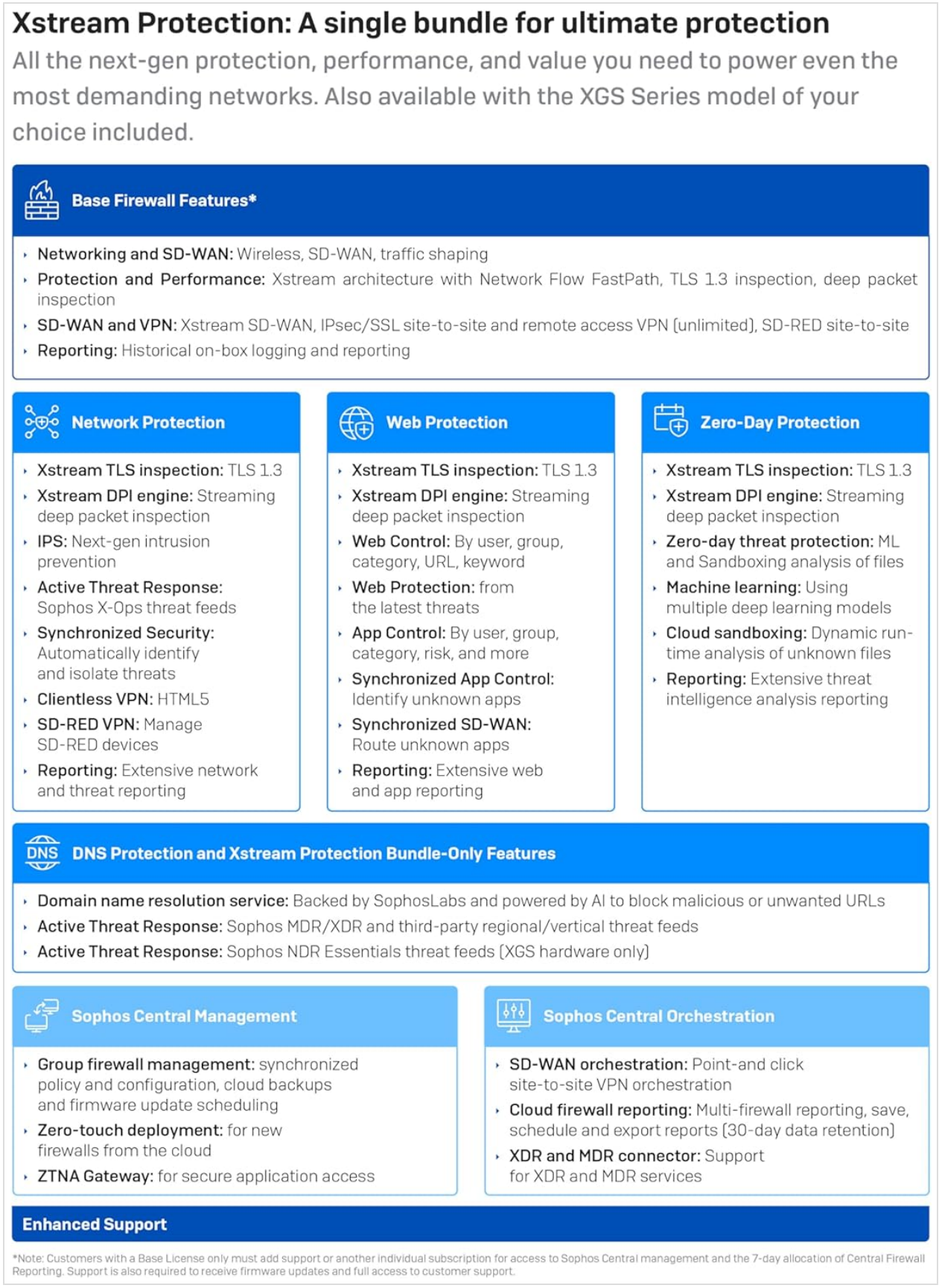


Figure 8.2: Detailed breakdown of features included in the Xstream Protection bundle, covering network, web, and zero-day protection.

9. Warranty and Support

Your Sophos XGS 128 (Gen2) Network Security Appliance comes with a manufacturer's warranty. The specific

duration and terms of the warranty are dependent on your purchase agreement and region. This particular model includes 3 years of Xstream Protection, which typically includes support services.

For technical assistance, warranty claims, or to access additional resources, please visit the official Sophos support website:

- Sophos Support Portal

It is recommended to register your product with Sophos to ensure you receive timely updates and support notifications.