Manuals+
Q & A | Deep Search | Upload

Sophos XGS 116

Sophos XGS 116 Zero-Day Protection Manual

Model: XGS 116 | Brand: Sophos

1. Product Overview

The Sophos XGS 116 Zero-Day Protection offers advanced security for your network. This subscription includes a fully cloud-based threat intelligence and threat analysis platform, powered by SophosLabs. It provides deep learning-based file analysis, detailed analysis reporting, and a threat meter to assess the risk of files. The system utilizes multiple layers of analytics to identify known and potential threats, reduce unknowns, and provide verdicts and intelligence reports for common file types.

Key components include Static File Analysis, which uses machine learning models, global reputation, and deep file scanning to identify threats without real-time execution. Dynamic File Analysis executes files in a secure cloud-based sandbox to observe behavior. Threat Intelligence Analysis Reporting delivers comprehensive insights into the nature and capabilities of threats through data science and SophosLabs research.

Figure 1.1: Front view of the Sophos XGS 116 device, showing ports and indicator lights.

2. Key Features

- **Zero-Day Protection License Includes:** Xstream TLS Inspection, Xstream DPI engine, Zero-Day Threat Protection, Powered by SophosLabs Intelix.
- **Xstream TLS Inspection:** Provides TLS 1.3 inspection with prepackaged exceptions for secure communication.
- **Xstream DPI engine:** Features streaming deep-packet inspection for thorough traffic analysis.
- **Zero-Day Threat Protection:** Analyzes all unknown files using AI, Machine Learning (ML), and sandboxing techniques to detect novel threats.
- **Powered by SophosLabs Intelix:** Utilizes cloud-based intelligence and analysis for comprehensive threat detection.

3. Initial Setup

This section outlines the basic steps to set up your Sophos XGS 116 device. For detailed configuration, refer to the official Sophos documentation available on their support portal.

1. **Unpack the Device:** Carefully remove the Sophos XGS 116 from its packaging. Ensure all components are present.
2. **Connect Power:** Connect the power adapter to the device and then to a power outlet. The device will begin to power on.
3. **Connect Network Cables:** Connect your internet service provider's modem or router to the designated WAN port on the XGS 116. Connect your internal network (LAN) devices or a network switch to the LAN ports.
4. **Initial Access:** Access the device's web-based management interface from a connected computer using the default IP address (refer to the quick start guide included with your device for specific details).
5. **Perform Basic Configuration:** Follow the on-screen wizard to set up initial network parameters, administrator credentials, and activate your Zero-Day Protection license.

Figure 3.1: Front panel of the Sophos XGS 116, highlighting connectivity ports and status indicators.

4. Operating Principles

The Sophos XGS 116 Zero-Day Protection operates by integrating multiple security engines to provide comprehensive threat defense. Its core functionality revolves around the Xstream Architecture, which includes:

- **Xstream TLS Inspection:** Decrypts and inspects TLS 1.3 traffic for hidden threats, ensuring secure communication channels are not exploited.
- **Xstream DPI Engine:** Performs deep packet inspection on all network traffic streams, identifying and blocking malicious content and applications.
- **Zero-Day Threat Protection:** Leverages SophosLabs Intelix, a cloud-based platform, to analyze unknown files. This involves:
  - *Static File Analysis:* Uses machine learning and global reputation to quickly identify threats without executing the file.
  - *Dynamic File Analysis:* Executes suspicious files in a secure, isolated sandbox environment to observe their behavior and intent.
  - *Threat Intelligence Analysis Reporting:* Provides detailed reports on identified threats, offering insights beyond simple 'good' or 'bad' verdicts.

This multi-layered approach ensures that both known and emerging threats, including zero-day exploits, are detected and neutralized before they can impact your network.

5. Protection Modules

The Sophos XGS 116 offers a range of protection modules to customize security based on your specific needs. These modules are designed to provide comprehensive defense across various threat vectors.

reporting.

Xstream Architecture
Enables high performance TLS 1.3 inspection, deep-packet inspection, and network flow FastPath to accelerate trusted SaaS, SD-WAN, and cloud application traffic. Note that Network and Web Protection are required to get the full benefits of the Xstream Architecture.

Networking and SD-WAN
Includes networking, routing, and SD-WAN capabilities with zone-based stateful firewall, NAT, VLAN support, multiple WAN link options with SD-WAN routing, fail-over, and fail-back.

Secure Wireless
Built-in wireless controller for Sophos APX wireless access points. Plug-and-play access point discovery makes setup easy. Support for multiple SSIDs, hotspots, guest networks, and the diverse encryption and security standards.

VPN
Provides standards-based site-to-site and remote access VPN (free up to the capacity of the firewall) with support for IPsec and SSL. Sophos Connect remote access VPN client for Windows and Macs offers seamless and easy deployment and configuration options. Sophos unique SD-RED layer 2 site-to-site tunnels offers a light-weight robust VPN alternative.

Reporting
Extensive on-box reporting provides valuable insights into threats, users, applications, web activity, and much more. Note that specific reporting functionality may be dependent on other protection modules to get the full benefits (for example, Web Protection or web and app reports).

The Base Firewall is included with every appliance.

Web Protection

Unmatched visibility and control over all your user's web and application activity.

Powerful user and group web policy
Provides enterprise-level Secure Web Gateway policy controls to easily manage sophisticated user and group web controls. Apply policies based upon uploaded web keywords indicating inappropriate use or behavior.

Application Control and QoS
Enables user-aware visibility and control over thousands of applications with granular policy and traffic-shaping (QoS) options based on application category, risk, and other characteristics. Synchronized Application Control automatically identifies all the unknown, evasive, and custom applications on your network.

Advanced Web Threat Protection
Backed by SophosLabs, our advanced engine provides the ultimate protection from today's polymorphic and obfuscated web threats. Innovative techniques like JavaScript emulation, behavioral analysis, and origin reputation help keep your network safe.

High-performance traffic scanning
Optimized for top performance, our Xstream SSL inspection provides ultra-low latency inspection and HTTPS scanning while maintaining performance.

Web Protection is included in the Xstream and Standard Protection bundles and is also available for separate purchase.

Central Orchestration*

Sophos Central cloud-managed VPN orchestration, firewall reporting, and MTR/XDR integration.

Sophos Central VPN Orchestration
Makes VPN orchestration easy. Wizard-based tunnel configuration helps create full mesh networks, hub-and-spoke models, or complex tunnel setups between multiple firewalls a quick point-and-click exercise. Seamlessly integrates multiple WAN link and SD-WAN functionality and routing optimizations to improve resilience and performance and also integrates with user authentication and Synchronized Security Heartbeat to control access.

Central Firewall Reporting Advanced (30-day)
Cloud-based reporting with several pre-packaged common reports for threats, compliance, and user activity. Includes advanced options for creating custom reports and views with the option to save, schedule or export your custom reports. Includes 30 days of log data retention with the option to add additional storage for additional historical reporting needs.

MTR/XDR Ready
Sophos MTR provides optional 24/7 threat hunting, detection and response delivered by an expert team as a fully-managed service. Sophos XDR offers extended detection and response managed by your own team. Regardless of whether you manage it yourself, or Sophos manages it for you, your Sophos Firewall is ready to share the necessary threat intelligence and data to the cloud.

Central Orchestration is included in the Xstream Protection bundle and is available for separate purchase.

* Expected soon.

access to those you trust.

Next-Gen Intrusion Prevention System
Provides advanced protection from all types of modern attacks. It goes beyond traditional server and network resources to protect users and apps on the network as well.

Security Heartbeat
Creates a link between your Sophos Central protected endpoints and your firewall to identify threats faster, simplify investigation, and minimize impact from attacks. Easily incorporate Heartbeat status into firewall policies to automatically isolate compromised systems.

Advanced Threat Protection
Instant identification and immediate response to today's most sophisticated attacks. Multi-layered protection identifies threats instantly and Security Heartbeat provides an emergency response.

Advanced VPN technologies
Adds unique and simple VPN technologies, including our clientless HTML5 self-service portal that makes remote access incredibly simple or utilize our exclusive light-weight secure SD-RED (Remote Ethernet Device) VPN technology.

Network Protection is included in the Xstream and Standard Protection bundles and is also available for separate purchase.

Zero-Day Protection

AI-driven static and dynamic file analysis techniques combine to bring unprecedented threat intelligence to your firewall and so effectively identify and block ransomware and other known and unknown threats.

Powered by SophosLabs
Powered by the industry-leading SophosLabs, the Zero-Day Protection subscription includes a fully cloud-based threat intelligence and threat analysis platform. This provides deep learning-based file analysis, detailed analysis reporting, and a threat meter to show the risk summary for a file.

We use layers of analytics to identify known and potential threats, reduce unknowns, and derive verdicts and intelligence reports for the most commonly used file types.

Static File Analysis
By harnessing the power of multiple machine learning models, global reputation, deep file scanning, and more, you can quickly identify threats without the need to execute the files in real time.

Dynamic File Analysis
Execute a file in a secure cloud-based sandbox to observe its behavior and intent. Screenshots provide added insight into any key events during the analysis.

Threat Intelligence Analysis Reporting
Rich intelligence reports provide you with much more than just a 'good,' 'bad,' or 'unknown' verdict. Full insight into the nature and capabilities of a threat are delivered through the use of data science and SophosLabs research.

Zero-Day Protection is included in the Xstream Protection bundle and is also available for separate purchase.

Email Protection

Consolidate your email protection with anti-spam, DLP, and encryption. We recommend Sophos Central Email Advanced for the best cloud-based email protection solution. If you require on-box email protection, this module offers essential anti-spam, DLP and encryption.

Integrated Message Transfer Agent
Ensures always-on business continuity for your email, allowing the firewall to automatically queue mail in the event servers become unavailable.

Live Anti-Spam
Provides protection from the latest spam campaigns, phishing attacks, and malicious attachments.

Self-serve Quarantine
Gives employees direct control over their spam quarantine, saving you time and effort.

SPX Email Encryption
Unique to Sophos, SPX makes it easy to send encrypted email to anyone, even those without any kind of trust infrastructure, using our patent-pending password-based encryption technology.

Data Loss Prevention
Policy-based DLP can automatically trigger encryption or block/notify based on the presence of sensitive data in emails leaving the organization.

Email Protection is available for individual purchase only.

Web Server Protection

Harden your web servers and business applications against hacking attempts while providing secure access.

Business Application Policy Templates
Pre-defined policy templates let you protect common applications like Microsoft Exchange Outlook Anywhere or SharePoint quickly and easily.

Protection from the latest hacks and attacks
With a variety of advanced protection technologies

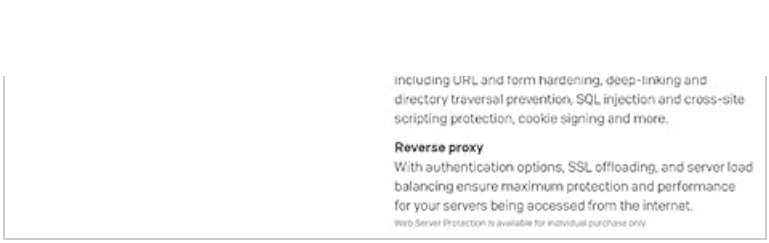


Figure 5.1: Overview of available Protection Modules.

Key Modules Include:

- **Base Firewall:** Includes standard firewall features, routing, NAT, VPN, and reporting.
- **Network Protection:** Offers intrusion prevention, advanced threat protection, and secure wireless capabilities.
- **Web Protection:** Provides web filtering, application control, and web application firewall functionalities.
- **Zero-Day Protection:** Analyzes unknown files using AI, ML, and sandboxing.
- **Central Orchestration:** SD-WAN orchestration, Central Firewall Advanced Reporting, and MTR/XDR ready.
- **Email Protection:** Includes anti-spam, DLP, and email encryption.

6. Sophos Central Management

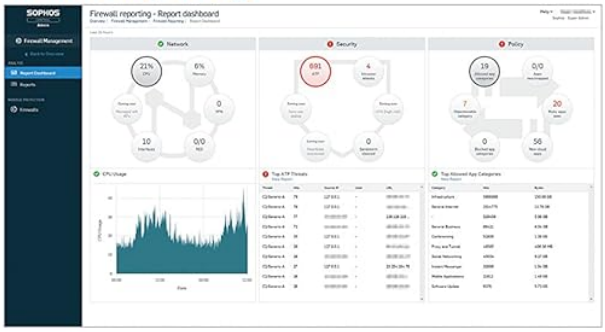
Sophos Central is a unified cloud management platform that allows you to manage your Sophos XGS 116 firewall and other Sophos security solutions from a single console. This simplifies deployment, monitoring, and reporting.

Sophos Central

Sophos Central is at the heart of everything we do. Our cloud management platform provides a single pane of glass to not only manage your firewalls, but also your full portfolio of Sophos security solutions.

Central Management

Central Reporting



Simply manage multiple firewalls

Sophos Central is the ultimate cloud management platform for all your Sophos products. It makes day-to-day setup, monitoring, and management of your Sophos Firewall easy. It also provides helpful features such as alerting, backup management, one-click firmware updates and rapid provisioning of new firewalls.

- Manage all your Sophos Firewalls and other Sophos products from a single console
- Configure changes and apply them to a group of firewalls or manage each firewall individually
- Create a backup schedule and store up to five backups in the cloud
- Schedule firmware updates across your entire network with just a few clicks

Central Management is available at no extra cost.

Firewall Reporting in the cloud

Sophos Central includes powerful reporting tools that enable you to visualize your network, web, application activity, and security over time. You get a flexible reporting experience that combines a variety of built-in reports with powerful tools to create your own custom reports, enabling you to report what you want how you want.

- Increase your visibility into network activity through analytics
- Analyze data to identify security gaps, suspicious user behavior or other events requiring policy changes
- Use the pre-defined modules or customize each report for specific use cases

Central Reporting is available at no extra cost for the storage of up to 7 days of report data. Premium options with longer data retention and additional features are available for optional purchase, either individually or as part of other subscriptions/bundles.

Zero-Touch Deployment

Using Sophos Central, you can create a configuration for a Sophos Firewall which you can then deploy at your convenience – for example, at a remote site. There is no need for technical staff on-site. Simply provide the configuration file, store it on a USB key, and boot the appliance with the USB key connected.

Learn more about the Sophos Central Ecosystem at sophos.com/firewall-central.

Figure 6.1: Sophos Central interface for firewall management and reporting.

Key Capabilities:

- **Simplified Management:** Manage multiple firewalls, configure policies, and apply them to groups of firewalls or individual devices.

- **Cloud Reporting:** Access powerful reporting tools that provide visibility into network activity, security events, and user behavior.
- **Zero-Touch Deployment:** Deploy new appliances remotely by storing configuration files on a USB key and booting the appliance.

For more information, visit sophos.com/firewall-central.

7. Synchronized Security

Sophos Synchronized Security is a unique solution that enables your XGS 116 firewall and endpoint security to communicate and share threat intelligence in real-time. This integration provides enhanced visibility and automated response to threats.

Synchronized Security

Security Heartbeat™: Your firewall and your endpoints are finally talking

Sophos Firewall is the only network security solution that is able to fully identify the user and source of an infection on your network, and automatically limit access to other network resources in response. This is made possible with our unique Sophos Security Heartbeat that shares telemetry and health status between Sophos endpoints and your firewall and integrates endpoint health into firewall rules to control access and isolate compromised systems.

The good news is, this all happens automatically, and is successfully helping numerous businesses and organizations to save time and money in protecting their environments today.

Synchronized Application Control

Using Security Heartbeat, we can do much more than just see the health status of an endpoint. We also have a solution to one of the biggest problems most network administrators face today - lack of visibility into network traffic.

Synchronized Application Control utilizes the Heartbeat connections with Sophos endpoints to automatically identify, classify, and control application traffic. All encrypted, custom, evasive, and generic HTTP or HTTPS applications which are currently going unidentified will be revealed.

You can't control what you can't see. All firewalls today depend on static application signatures to identify apps. But those don't work for most custom, obscure, evasive, or any apps using generic HTTP or HTTPS.

Sophos Firewall utilizes Synchronized Security to automatically identify, classify, and control all unknown applications easily blocking the apps you don't want and prioritizing the ones you do.

Lateral Movement Protection

Lateral Movement Protection automatically isolates compromised systems at every point in the network to stop attacks dead in their tracks. Healthy endpoints assist by ignoring all traffic from unhealthy endpoints, enabling complete isolation, even on the same network segment, to prevent threats and active adversaries from spreading or stealing data.

Synchronized User ID

User authentication is critically important in a next-generation firewall but often challenging to implement in a seamless and transparent way. Synchronized User ID eliminates the need for client or server authentication agents by sharing user identity between the endpoint and the firewall through Security Heartbeat. It's just another great benefit of having your firewall and endpoints integrated and sharing information.

Synchronized SD-WAN: Powerful, reliable application routing

Synchronized SD-WAN harnesses the power of Synchronized Security to optimize WAN path selection for your important business applications.

With Synchronized Application Control, discovered applications, which would otherwise be unknown, can be used for traffic matching criteria in SD-WAN routing policies. This is yet another way that Synchronized Security can improve the efficiency of your network.

Figure 7.1: How Sophos Synchronized Security works.

Key Aspects:

- **Security Heartbeat:** The firewall and endpoints continuously share health status, allowing for immediate identification of compromised systems.

- **Synchronized Application Control:** Automatically identifies, classifies, and controls all unknown applications on the network.
- **Lateral Movement Protection:** Isolates compromised systems to prevent threats from spreading across the network.
- **Synchronized User ID:** Provides transparent user identification for policy enforcement and reporting.
- **Synchronized SD-WAN:** Optimizes application routing based on security and network performance.

8. Maintenance and Best Practices

To ensure optimal performance and security of your Sophos XGS 116, adhere to the following maintenance guidelines:

- **Regular Firmware Updates:** Keep your device's firmware up to date to benefit from the latest security patches, features, and performance improvements.
- **Monitor System Health:** Regularly check the device's status indicators and logs through the Sophos Central management interface for any anomalies.
- **Backup Configurations:** Periodically back up your device's configuration settings. This allows for quick restoration in case of an issue or during migration.
- **Review Security Policies:** Regularly review and update your security policies to adapt to evolving threat landscapes and changes in your network environment.
- **Physical Environment:** Ensure the device is placed in a well-ventilated area, free from dust and extreme temperatures, to prevent overheating.

9. Troubleshooting Common Issues

This section provides general guidance for troubleshooting common issues. For more specific problems, consult the Sophos knowledge base or contact technical support.

- **No Power:** Ensure the power cable is securely connected to both the device and a working power outlet. Check the power indicator light on the device.
- **No Network Connectivity:** Verify that Ethernet cables are properly connected to the correct ports (WAN/LAN) and that link lights are active. Check your modem/router status.
- **Cannot Access Management Interface:** Confirm your computer is on the same network segment as the XGS 116 and that you are using the correct IP address. Try clearing your browser cache or using a different browser.
- **Slow Network Performance:** Check the device's resource utilization (CPU, memory) via the management interface. Review logs for any high-traffic applications or potential security events.
- **License Issues:** Ensure your Zero-Day Protection license is active and not expired. Verify the device is properly registered with Sophos Central.

10. Technical Specifications

Specification	Detail
Model Number	XGS 116
Brand	Sophos

Specification	Detail
ASIN	B095L1R75S
UPC	739420468953
Connectivity Technology	Ethernet
Security Protocol	WPS
Control Method	App
Recommended Uses	Business, Remote Work
Compatible Devices	Laptop
Frequency Band Class	Dual-Band
Special Feature	WPS

11. Warranty and Technical Support

Sophos products are covered by a standard manufacturer's warranty. For specific details regarding your warranty period and coverage, please refer to the documentation included with your purchase or visit the official Sophos website.

For technical assistance, product inquiries, or to report issues, please contact Sophos Technical Support. Support resources, including knowledge bases, forums, and contact information, are available on the official Sophos support portal:

- **Sophos Support Portal:** https://support.sophos.com
- **Sophos Community:** https://community.sophos.com

When contacting support, please have your product model (XGS 116) and license information readily available to expedite the service process.

© 2024 Sophos. All rights reserved.