SOPHOS

Security Audit Report

March 16 - March 22, 2025

Prepared for:
Ladol Integrated - HQ

Appliance:
XGS2300

Appliance Key:
X23021YXR2JJV68

Firmware Version:
SFOS 21.0.0 GA-Build169

Server Time : Sun Mar 23 04:08:19 WAT 2025

Security Audit Report

This report aims to provide visibility into the risks averted by Sophos Firewall for Ladol Integrated - HQ network and explains potential risks prevailing within the network such as application and web risks, risky users, and intrusion risks that can be addressed by Ladol Integrated - HQ.

Sophos Firewall with Layer 8 Identity-based technology offers actionable security intelligence and controls to enterprises, giving complete control over user-level policy enforcement for future-ready security. Sophos Firewall integrates multiple features over a single platform, eliminating the need to manage multiple solutions and reducing complexity.

This report provides a high level overview of Ladol Integrated - HQ's network that covers:

- Report Findings
- User Behavior
- User-Application Risks & Usage
- Synchronized Applications
- Web Risks & Usage
- Business Application Risks & Usage
- Mail Risks & Usage
- Intrusion Attacks
- Active Threat Response
- Security Heartbeat

Server Time : Sun Mar 23 04:08:19 WAT 2025

Report Findings

Key Observations

Key Observations on Top High-Risk Applications:

APPLICATION CATEGORY	NUMBER OF "RISK-5 & RISK-4" APPLICATIONS FOUND
No Record Found	

User Behavior

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

The Layer 8 Technology over Sophos Firewalls treats user identity as the eighth layer or the "human layer" in the network protocol stack. This allows administrators to uniquely identify users, control Internet activity of these users in the network, and enable policy-setting and reporting by username.

Users with Risk-Prone Behavior

User Threat Quotient (UTQ) helps security administrators spot users posing risk, based on suspicious web behavior and advanced attacks triggered from their hosts. The risk could be a result of unintended actions due to lack of security awareness, a malware infected host, or the intended actions of a rogue user. Knowing the user and the activities that caused risk can help the network security administrator take required actions to avoid such risks.

Users with Risk-Prone Behavior

RELATIVE RISK RANKING	USER	RELATIVE THREAT SCORE
No Record Found		

SOPHOS

User Data Transfer

This report helps track User Data Transfer and further investigation can help understand how efficiently corporate resources are utilized and whether any modification is warranted in User Access Policies.

Users

USER	CLIENT TYPE	DATA TRANSFER	UPLOADED	DOWNLOADED	USED TIME
No Record Found					

Reported only when user logs out.

Server Time : Sun Mar 23 04:08:19 WAT 2025

SOPHOS

User Application Risks & Usage

Today, it is crucial for an organization to be aware about the applications traversing the network and potential risks they pose in order to effectively manage related business risks. Sophos Firewall Application Visibility & Control offers complete visibility on which applications are being accessed within the network irrespective of their ports and protocols. This stops sophisticated application-layer threats right at the network perimeter.

Application Risk Score

This risk calculator indicates the overall risk associated with various applications and is calculated on the basis of individual risk associated with a specific application and the number of hits on that application.

Risk: ?

Blocked Applications

Number of User Applications Blocked by Risk Level

RISK	NO OF APPLICATION
No Record Found	

Blocked Applications (by Risk Level)

APP NAME	RISK LEVEL	CATEGORY	TECHNOLOGY	HITS
No Record Found				

Server Time : Sun Mar 23 04:08:19 WAT 2025

High-Risk Applications in Use

The table below listshigh risk applications (risk rating 5 or 4 in this order) along with risk level, application category, characteristics, and technology to help understand potential application risks faced by the network. If these applications are not intentionally allowed or appear to serve no business need, then a recommended practice is to block such high risk applications.

High Risk Applications

<table>
<tr><th>RISK LEVEL</th><th>APP NAME</th><th>CATEGORY</th><th>TECHNOLOGY</th><th>HITS</th><th>BYTES</th></tr>
<tr><td colspan="6">No Record Found</td></tr>
</table>

Application Categories & Applications

Knowing top app categories and applications help understand how efficiently corporate resources are utilized and also app filtering policies. These reports provide a snapshot of various application categories and applications accessed by users, and the amount of traffic generated.

Known Application Categories by Data Transfer

APPLICATION CATEGORY	HITS	BYTES
No Record Found		

Known Applications by Data Transfer

APPLICATION	APPLICATION RISK	APPLICATION CATEGORY	HITS	BYTES
No Record Found				

SOPHOS

Synchronized Applications

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. i.e. it cannot control what it cannot see.
Sophos Firewall utilizes Synchronized Security to automatically identify, classify, and control unknown applications. It allows administrators to easily block the unwanted apps and prioritize the ones they do.
The Endpoint inherently knows exactly what applications are generating traffic and shares that information with the firewall. The firewall automatically categorizes endpoint reported applications and applies Application Control and Traffic Shaping policy.

Synchronized Apps

APPLICATION/PROTO:PORT	CATEGORY	HITS	BYTES
No Record Found			

Blocked Synchronized Apps

APPLICATION/PROTO:PORT	CATEGORY	HITS
No Record Found		

Cloud Applications

Organizations want visibility on which cloud storage services like Dropbox, Box, OneDrive, iCloud, Google Drive, or others are used to store company or customer data. e.g. If the company has a corporate Box account and one user is consistently uploading data to OneDrive, that could be a red flag that needs further investigation or policy enforcement. This practice of using unsanctioned cloud services is called "Shadow IT" and organizations want to discover such usage.
CASB in Sophos Firewall helps identify risky behavior by providing insights into what cloud services are being used, and how they are being used – flagging unsanctioned high risk usage. Administrators can then take appropriate action by educating users or implementing app control or traffic shaping policies to control or eliminate potential risky or unwanted behavior.

New Cloud Applications

APPLICATION	CATEGORY	USERS	UPLOADS	DOWNLOADS	BYTES
No Record Found					

Unsanctioned Cloud Applications

APPLICATION	CATEGORY	USERS	UPLOADS	DOWNLOADS	BYTES
No Record Found					

Tolerated Cloud Applications

APPLICATION	CATEGORY	USERS	UPLOADS	DOWNLOADS	BYTES
No Record Found					

Sanctioned Cloud Applications

APPLICATION	CATEGORY	USERS	UPLOADS	DOWNLOADS	BYTES
No Record Found					

SOPHOS

Web Risks & Usage Visibility

Organizations need a strong security mechanism, which is able to block access to harmful websites and prevent malware, phishing, pharming attacks, and undesirable content that could lead to legal liability and direct financial losses. Being able to do so also enables them to manage productivity of their users and helps them achieve effective utilization of bandwidth.
Sophos Firewall Web Filtering offers one of the most comprehensive URL databases with millions of URLs providing web security, HTTPS controls, and a comprehensive web and content filtering solution.

By Hits

By Bandwidth

SOPHOS

Blocked Web Categories and Domains

Blocked Web Domains

WEB DOMAIN	WEB CATEGORY	HITS
No Record Found		

Blocked Web Categories

WEB CATEGORY	NO OF BLOCKED WEB DOMAINS	HITS
No Record Found		

Blocked Web Viruses

VIRUS	COUNT
No Record Found	

Server Time : Sun Mar 23 04:08:19 WAT 2025

Objectionable Web Categories & Domains Being Accessed

These reports help Administrator monitor objectionable web categories and domains. If these web categories and web domains are not intentionally allowed or appear to serve no business need, then a recommended practice is to configure Sophos Firewall to block them.

Objectionable Web Categories

CATEGORY	NO OF DOMAINS	BYTES	HITS
No Record Found			

Objectionable Web Domains

WEB DOMAINS	WEB CATEGORY	BYTES	HITS
No Record Found			

Web Categories & Domains

These reports offer insights into the users' browsing habits that can help understand how efficiently corporate resources get utilized and the efficacy of web-filtering policies.
This report displays a list of top web categories along with the number of hits.

Known Web Categories by Hits

CATEGORY	BYTES	HITS
No Record Found		

Known Web Categories by Data Transfer

CATEGORY	HITS	BYTES
No Record Found		

Web Domains by Hits

WEB DOMAIN	WEB CATEGORY	BYTES	HITS
No Record Found			

Web Domains by Data Transfer

WEB DOMAIN	WEB CATEGORY	HITS	BYTES
No Record Found			

Business Application Risks & Usage

Information assets and business applications that reside on web servers remain prone to various threats such as cross-site scripting, parameter tampering, and more. Findings from this report capture security risk assessment for business applications and web servers while providing useful guidance with regard to usage, bandwidth consumption, and risks found during assessment.

Attacked Web Server Domains

WEB SERVER DOMAIN	HITS
No Record Found	

Blocked Web Server Requests

BLOCKED REASON	HITS
No Record Found	

Web Server Attack Source

SOURCE IP	HITS
No Record Found	

Web Server Virus

VIRUS	COUNT
No Record Found	

Web Servers by Data Transfer

WEB SERVER DOMAIN	REQUESTS	BYTES
No Record Found		

Web Server Users

USER	REQUESTS
No Record Found	

Mail Risks & Usage

Email continues to be an attack vector to be addressed by businesses. This section provides an analysis of mail usage and protection with reports like Top Mail Users, Spam Senders, Mail Recipients, and Mail Viruses.

Mail Senders

SENDER	HITS	BYTES
No Record Found		

Mail Recipients

RECIPIENT	HITS	BYTES
No Record Found		

Mail Applications Used for Spam

MAIL APP NAME	HITS
No Record Found	

Spam Recipients

RECIPIENT	HITS	PERCENT
No Record Found		

Spam Senders

SENDER	HITS	PERCENT
No Record Found		

Mail Applications Used for Viruses

MAIL APP NAME	COUNT
No Record Found	

Mail Viruses

VIRUS	COUNT
No Record Found	

Intrusion Attacks

Detection and protection against network and application-level attacks like intrusion attacks, malicious code transmission, and backdoor activity is critical to protect the network from hackers. Sophos Firewall's Intrusion Prevention System helps strengthen defenses against network-level and application-level attacks.

Number of Attacks by Severity Level

Total Attacks

SEVERITY	TOTAL
No Record Found	

Attacks Blocked

SEVERITY	TOTAL
No Record Found	

Attacks Detected and Allowed

SEVERITY	TOTAL
No Record Found	

It is recommended that administrators evaluate "Attacks Detected and Allowed" based on the network environment to configure necessary action in Sophos Firewall for related IPS signatures.

Intrusion Attacks

This report fetches details for the top attacks that have hit the system with information about their severity level, category, platform, target and attack count.

Intrusion Attacks by Severity

SEVERITY-LEVEL	ATTACK	CATEGORY	PLATFORM	TARGET	ATTACK COUNT
No Record Found					

Attack Categories

ATTACK CATEGORY	VARIETY OF ATTACKS	ATTACK COUNT
No Record Found		

SOPHOS

Active Threat Response

Made simple to use, Sophos Active threat response protects enterprise networks from falling prey to botnet risks and helps identify infected endpoints, so the administrator can take immediate action.

Summary

THREAT COUNT	HOST COUNT	EVENTS
No Record Found		

Advanced Threats

THREAT	HOST COUNT	MODULE	EVENTS
No Record Found			

Hosts - Threat source

HOST (SOURCE IP)	THREAT COUNT	EVENTS
No Record Found		

Synchronized IoC

HOST (SOURCE IP)	LOGIN USER	PROCESS USER	EXECUTABLE	THREAT	THREAT URL/IP	EVENT LAST SEEN	EVENTS
No Record Found							

Security Heartbeat

Exchange of security heartbeat messages between Ladol Integrated - HQ and Sophos Central managed endpoints enables monitoring of health/security posture of these endpoints (red, yellow or green). A Ladol Integrated - HQ administrator can enforce a policy to allow only compliant endpoints to access the network thereby isolating the compromised end-points.
Security Heartbeat Report provides visibility into the health status (red, yellow, green) of cloud-managed endpoints along with details.

Client Health

CLIENT HEALTH	COUNT	PERCENT
No Record Found		

Detailed View - Client Health

HOST (SOURCE IP)	HOST NAME	HEALTH - LAST SEEN	LAST HEALTH CHANGED
No Record Found			

Blocked Network Access

HOST (SOURCE IP)	USER	DESTINATION	ATTEMPTS	HEALTH REASON
No Record Found				

Missing Heartbeat

HOST NAME	MISSING COUNT
No Record Found	