

# SOPHOS

Sophos is a global cybersecurity company that offers a range of products and services to help protect organizations from various digital threats.

**Endpoint Protection:** Sophos provides a range of endpoint protection solutions to help organizations secure their devices and prevent malware infections. These solutions include antivirus and anti-malware software, as well as advanced threat detection and response capabilities.

**Firewall and VPN:** Sophos offers a range of firewall and VPN solutions to help organizations secure their networks and prevent unauthorized access. These solutions include next-generation firewalls, secure web gateways, and virtual private network (VPN) software.

**Cloud Security:** Sophos provides cloud security solutions to help organizations secure their cloud environments and prevent data breaches. These solutions include cloud access security brokers (CASBs), cloud-based firewalls, and cloud workload protection platforms.

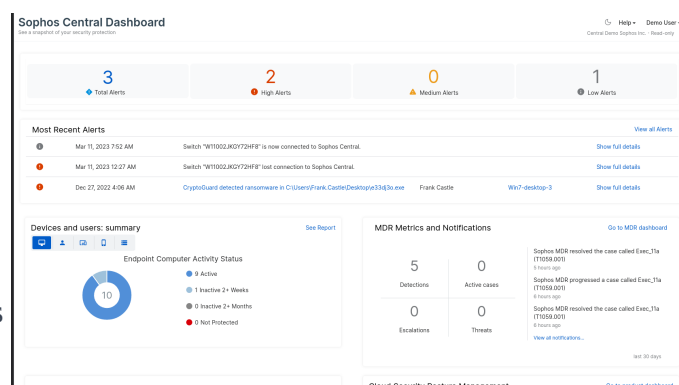
**Email Security:** Sophos offers email security solutions to help organizations prevent email-based attacks such as phishing and spam. These solutions include email gateways, anti-spam and anti-phishing software, and email encryption tools.

**Mobile Security:** Sophos provides mobile security solutions to help organizations protect their mobile devices from cyber threats. These solutions include mobile device management (MDM) software, mobile threat defense tools, and secure app development platforms.

## Sophos Central Dashboard

the Sophos Central Dashboard provides a comprehensive view of an organization's security posture and allows users to respond quickly to potential threats. Its customizable and unified approach to security management simplifies security management and reduces the risk of security breaches.

- Unified Security Management
- Automated Response and Remediation
- Real-time Threat Intelligence
- Compliance Monitoring such as PCI DSS, HIPAA, and GDPR.
- User Management and Reporting and Analytics



**Alerts :** Sophos offers a variety of alerts for its endpoint protection, firewall, and other security solutions. These alerts help users stay informed about potential security threats

### common alerts:

Malware detection

Firewall alerts

Intrusion Prevention System (IPS) alerts

Web filtering alerts

Endpoint protection alerts

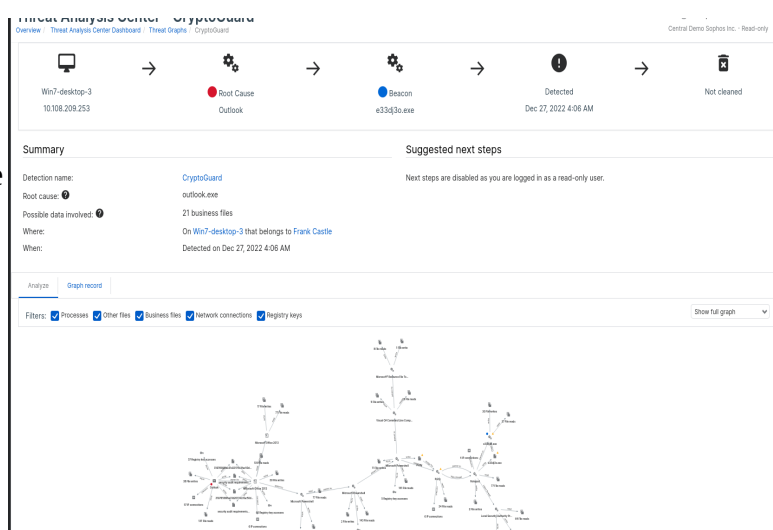
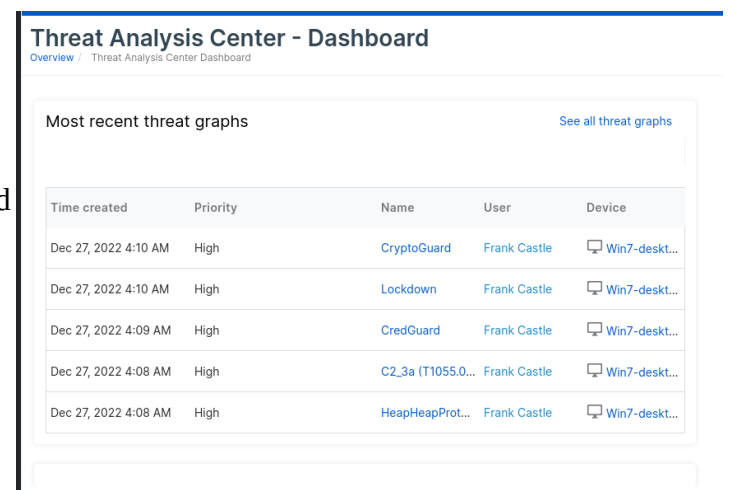
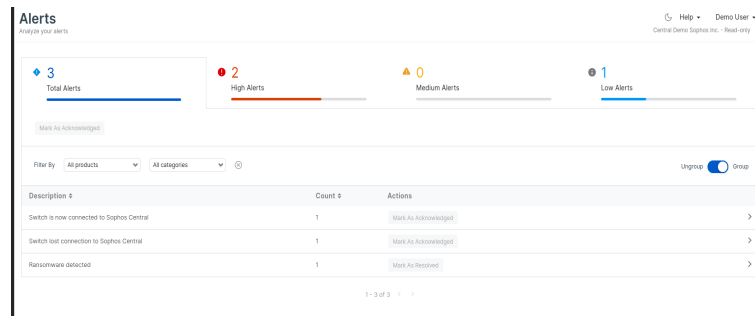
Email protection alerts

### Threat Analysis Center - Dashboard :

The TAC Dashboard displays real-time information about the threat landscape, including the number of active threats, the top detected malware families, and the countries with the most security events. The dashboard also provides a summary of security events detected by Sophos products, such as antivirus detections, firewall events, and intrusion prevention system alerts.

Sophos Threat Analysis Center (TAC) includes a feature called CryptoGuard that helps protect against ransomware attacks

CryptoGuard is a behavior-based technology that works by monitoring the system for suspicious behavior patterns that are commonly associated with ransomware attacks. When CryptoGuard detects suspicious activity, it immediately stops the process and quarantines any affected files. This helps prevent the ransomware from encrypting additional files and minimizes the damage caused by the attack.



## LOGS and Reports :

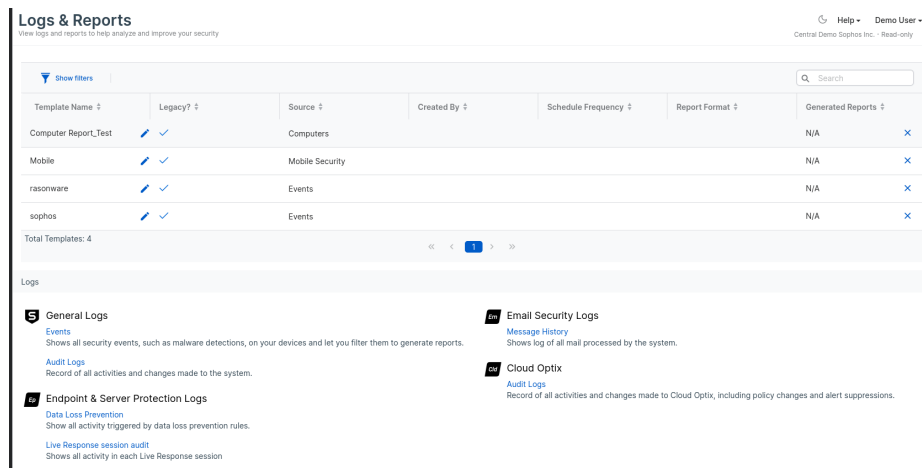
Sophos generates logs automatically, which are detailed records of activities and events that occur on the network and its devices. These logs include information such as the time and date of an event, the type of event, the device or user involved, and any relevant details or context. The logs generated by Sophos can be viewed and analyzed in real-time or stored for later reference.

By monitoring the logs generated by Sophos, administrators can quickly detect security threats, such as malware infections, unauthorized access attempts, and policy violations.

reports can be customized to suit the needs of the organization or user, and can be generated on a scheduled or ad-hoc basis. Reports can be generated for specific devices, users, time periods, or events, and can include information such as

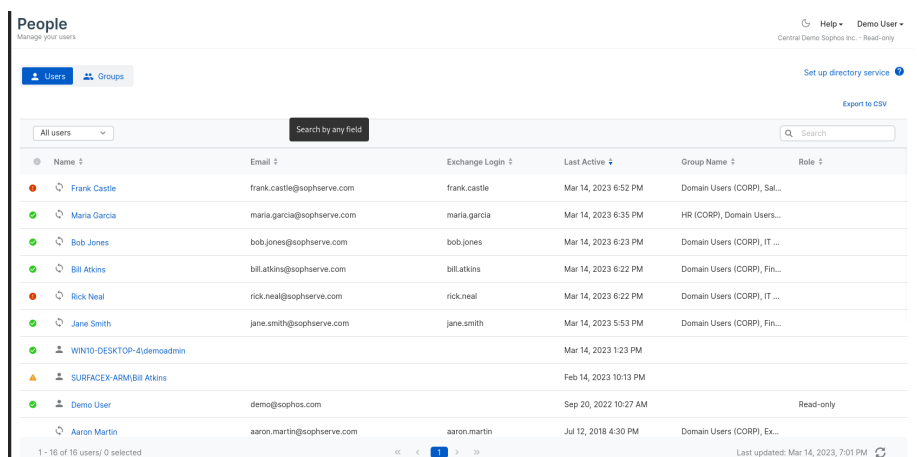
- threat detection and mitigation,
- system updates,
- policy violations, and
- user activity.

Logs provide detailed records of network activity, while reports provide summarized and organized information extracted from the logs. Together, logs and reports help administrators to identify potential security risks, take proactive measures to mitigate them, and demonstrate compliance with regulatory standards



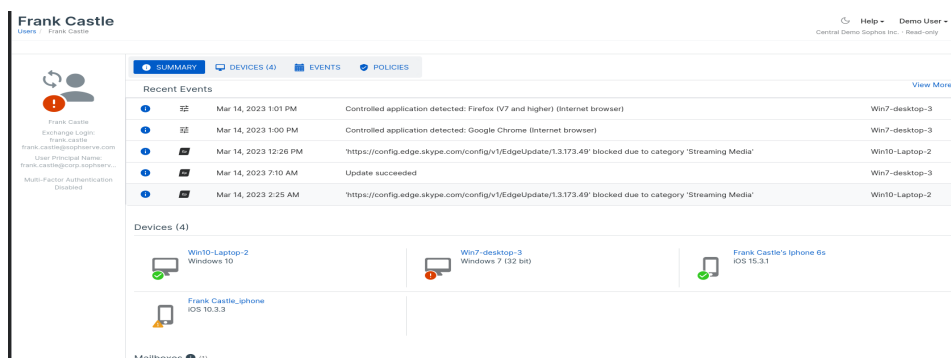
## PEOPLE :

people dashboard as part of its Sophos Central platform. The people dashboard provides a comprehensive view of an organization's employees and their activities, allowing administrators to manage their security posture



## The people dashboard in Sophos Central :

- User and Device Management
- Security Status
- Threat Detection
- Customizable Filters



The Devices Dashboard provides the overview of all the devices that are connected to the network, including desktops, laptops, servers, mobile devices, and other endpoints. This dashboard is designed to help IT administrators monitor and manage the security of these devices, ensure compliance with company policies, and detect any potential security risks.

## The device dashboard in sophos central

- Device Inventory
- Real-time Monitoring
- Policy Enforcement
- Automated Threat Response
- Reporting and Analytics

Another important feature of the devices dashboard is the ability to manage devices remotely. Administrators can perform a range of actions on individual devices, including initiating a virus scan, updating security software, or quarantining a device if it is infected with a virus. They can also configure security policies for individual devices or groups of devices, ensuring that all devices are configured to meet the organization's security requirements.

The devices dashboard also includes advanced analytics capabilities, allowing administrators to gain insights into the security status of their devices over time. They can view trends in threat detection, vulnerability management, and compliance, allowing them to identify areas where additional security measures may be required. The devices dashboard is the ability to drill down into the security status of individual devices. Administrators can view detailed information about a specific device, including the operating system, the installed applications, and the security software that is running. Detailed history of the device's security events, including the number of threats detected and the actions that were taken to mitigate them.

## Endpoint Protection – Dashboard

Endpoint Protection dashboard in Sophos provides a comprehensive view of the security status of all endpoints managed by the platform. This includes information on the number of endpoints that are protected, the number of endpoints that are at risk, and the number of endpoints that are unprotected.

Administrators can view detailed information about a specific endpoint, including its operating system, its hardware configuration, and the security software that is installed. They can also view the endpoint's recent security

**Computers**  
View and manage your computers

Help Demo User  
Central Demo Sophos Inc. Read-only

Computers Servers Mobile Devices Unmanaged devices

Refresh Recovery Key Export to CSV

Name	IP	OS	Protection	Encryption	Last user	Last active	Group
Win10-Desktop-1	10.108.209.17	Windows 10 Enterprise	Central Managed Detection and Response	+	bill.atkins	Mar 14, 2023 7:11 PM	
Win7-desktop-3	10.108.209.253	Windows 7 Enterprise Service Pack 1 (32 bit)	Central Managed Detection and Response	+	frank.castle	Mar 14, 2023 7:11 PM	
Win10-Laptop-3	10.108.209.21	Windows 10 Enterprise	Central Managed Detection and Response	+	jane.smith	Mar 14, 2023 7:02 PM	
Win10-Laptop-2	10.108.209.20	Windows 10 Enterprise	Central Managed Detection and Response	+	frank.castle	Mar 14, 2023 6:52 PM	
Win10-Laptop-4	10.108.108.43	Windows 10 Pro	Central Managed Detection and Response	✓	Maria Garcia	Mar 14, 2023 6:35 PM	
Win10-Desktop-2	10.108.209.18	Windows 10 Enterprise	Central Managed Detection and Response	+	bob.jones	Mar 14, 2023 6:23 PM	
Rick's Mac mini	10.108.209.61	macOS Monterey 12.6	Central Managed Detection and Response	✓	rick.neal	Mar 14, 2023 6:22 PM	
Win10-Laptop-1	10.108.209.19	Windows 10 Enterprise	Central Managed Detection and Response	+	bill.atkins	Mar 14, 2023 5:19 PM	
Win10-Desktop-4	10.0.2.6	Windows 10 Pro N	Central Managed Detection and Response	+	demoadmin	Mar 14, 2023 1:23 PM	
SurfaceK-arm	192.168.200.55	Windows 10 Pro	Central Managed Detection and Response	+	Bill Atkins	Feb 14, 2023 10:11 AM	

1 - 10 of 10 computers / 0 selected

Last updated: Mar 14, 2023, 7:13 PM

**Win10-Desktop-1**  
Devices Win10-Desktop-1

Help Demo User  
Central Demo Sophos Inc. Read-only

SUMMARY EVENTS STATUS POLICIES

Recent Events View More

Mar 14, 2023 12:09 PM	Update succeeded
Mar 14, 2023 10:44 AM	Controlled application detected: Microsoft Edge (Internet browser)
Mar 13, 2023 12:08 PM	Update succeeded
Mar 13, 2023 10:44 AM	Controlled application detected: Microsoft Edge (Internet browser)
Mar 12, 2023 12:08 PM	Update succeeded

Agent Summary

Last Activity 5 minutes ago  
Last Agent Update 7 hours ago Update Successful ✓  
Assigned Products

Product	Assigned	Version
Core Agent	✓	2022.4.21 BETA
Sophos Intercept X	✓	2022.1.3.3 BETA
Endpoint Protection	✓	10.8.11.4 BETA
Device Encryption	X	

**Endpoint Protection - Dashboard**  
Overview Endpoint Protection Dashboard

Help Demo User  
Central Demo Sophos Inc. Read-only

Recent threat graphs See all

Sophos generated Admin generated

As an MDR customer, these graphs are for information only for all devices with an MDR assigned license. Our MDR team will contact you if you need to take action.

Time created	Priority	Name	User	Device
Dec 27, 2022 4:10 AM	High	CryptoGuard	Frank Castle	Win7-desktop-3
Dec 27, 2022 4:10 AM	High	Lockdown	Frank Castle	Win7-desktop-3
Dec 27, 2022 4:09 AM	High	CryptoGuard	Frank Castle	Win7-desktop-3
Dec 27, 2022 4:08 AM	High	C2_3a (T1055.002 meminjector+meminjector-g	Frank Castle	Win7-desktop-3
Dec 27, 2022 4:08 AM	High	HeapdumpProtect	Frank Castle	Win7-desktop-3

Devices and users: summary See Report

Endpoint Computer Activity Status

10

- 9 Active
- 1 Inactive 2+ Weeks
- 0 Inactive 2+ Months
- 0 Not Protected

Web control See Reports

1 Web Threats Blocked	298 Policy Violations Blocked
96 Policy Warnings Issued	0 Policy Warnings Proceeded

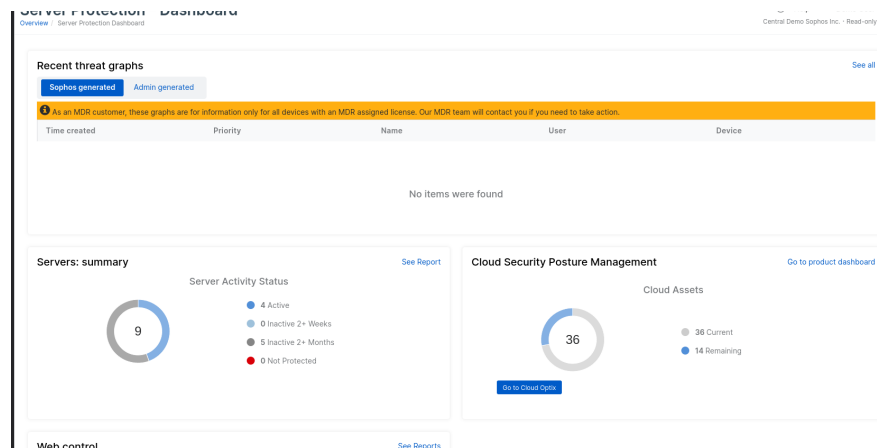
test 30 days

events, including any threats that have been detected and actions that have been taken to mitigate them. Its remote management capabilities, advanced analytics features, and detailed information about individual endpoints make it an essential tool for organizations of all sizes

## Server Protection – Dashboard:

The Server Protection dashboard in Sophos Central is a comprehensive view of all the servers that are managed by the platform. This includes physical and virtual servers running on-premises or in the cloud. The dashboard provides a summary of the security status of each server, including the number of threats detected, the number of threats blocked, and the number of servers that are currently unprotected

Administrators can view detailed information about a specific server, including its operating system, the applications and services that are running, and the security software that is installed. They can also see a detailed history of the server's security events, including the number of threats detected and the actions that were taken to mitigate them.



## Server Protection - Top Malware Downloaders

[Overview](#) / [Server Protection Dashboard](#) / [Reports](#) / [Top Malware Downloaders](#)

Choose period:

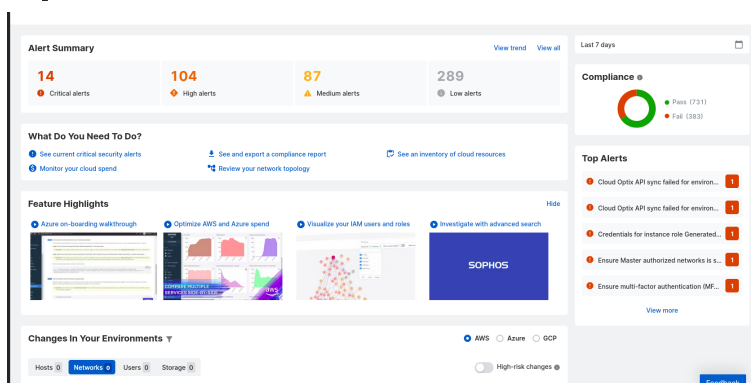
USER	COMPUTER	VISITS	TOP 5 MALWARE (VISITS)
CORP\bill.atkins	Win10-Laptop-1	1	High Risk (1)

## Server Protection - Policy Violators

[Overview](#) / [Server Protection Dashboard](#) / [Reports](#) / [Policy Violators](#)

Choose period:

VIOLATOR	VISITS	TOP 5 VIOLATIONS (VISITS)
CORP\bob.jones	137	Alcohol & Tobacco (2) Alcohol & Tobacco (2) Proxies & Translators (2) Proxies & Translators (2) Proxies & Translators (2)
CORP\bill.atkins	98	Weapons (2) Weapons (2) Adult/Sexually Explicit (1) Adult/Sexually Explicit (1) Adult/Sexually Explicit (1)
CORP\frank.castle	63	Blogs & Forums (5) Shopping (5) Blogs & Forums (3) Blogs & Forums (2) Entertainment (2)



## Top Warned Sites

[Reports](#) / [Top Warned Sites](#)

Choose period:

SITE	CATEGORIES	WARNED	PROCEEDED	TOP 5 USERS (VISITS)
microsoft.com	Computing & Internet	36	0	
bacardi.com	Alcohol & Tobacco	34	0	
greygoose.com	Alcohol & Tobacco	26	0	

features :

- policy violations
- malware downloads
- Top warned Sites
- Cloud Security Posture Management with optix