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.

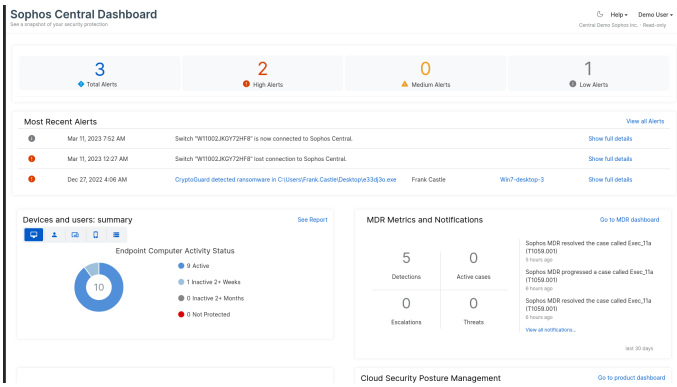
Firewall and VPN: Sophos offers a range of firewall and VPN solutions to help organizations secure their networks and prevent unauthorized access. These solutions include next-generation firewalls, secure web gateways, and virtual private network (VPN) software.

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.

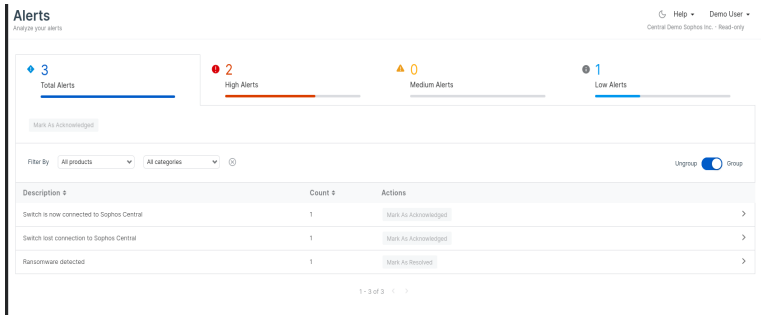
Sophos Central Dashboard



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

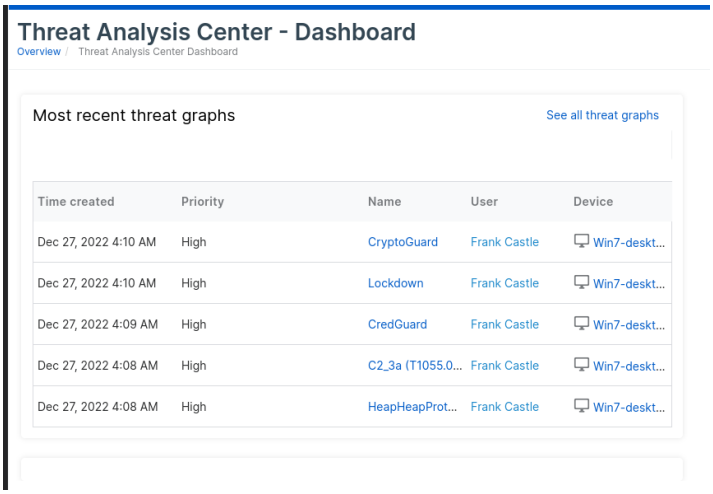
Intrusion Prevention System (IPS) alerts

Web filtering alerts

Endpoint protection alerts

Email protection alerts

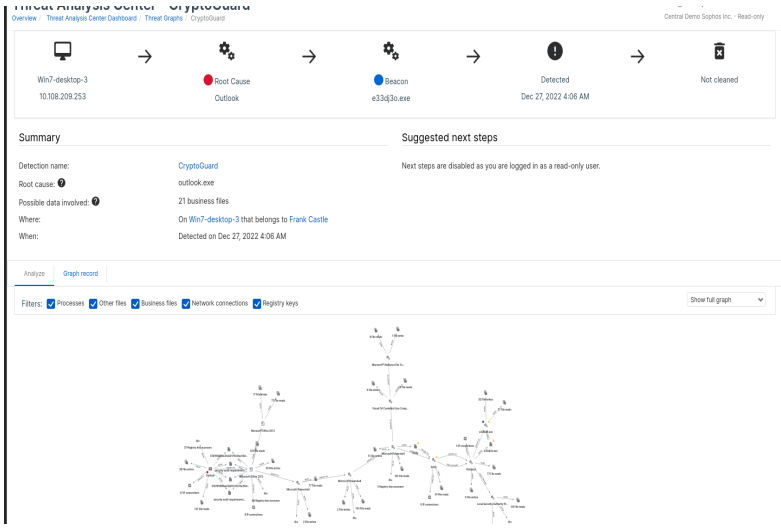
Threat Analysis Center - Dashboard :



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.

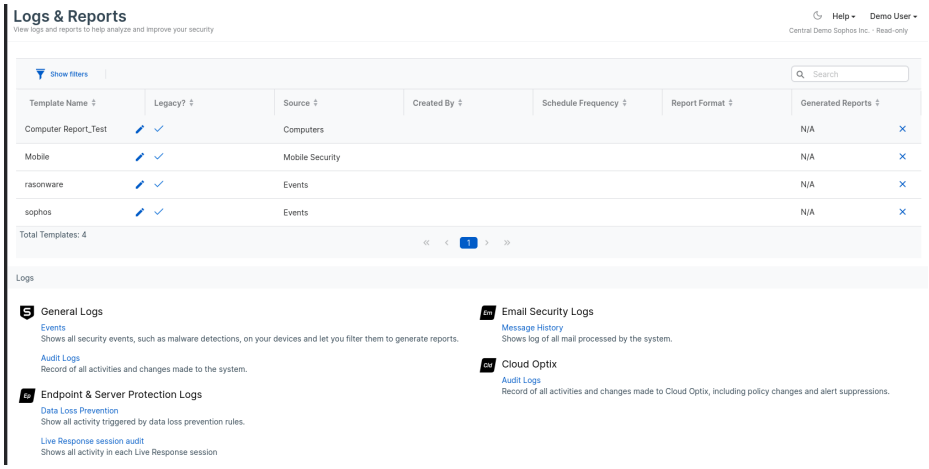
Sophos Threat Analysis Center (TAC) includes a feature called CryptoGuard that helps protect against ransomware attacks

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.

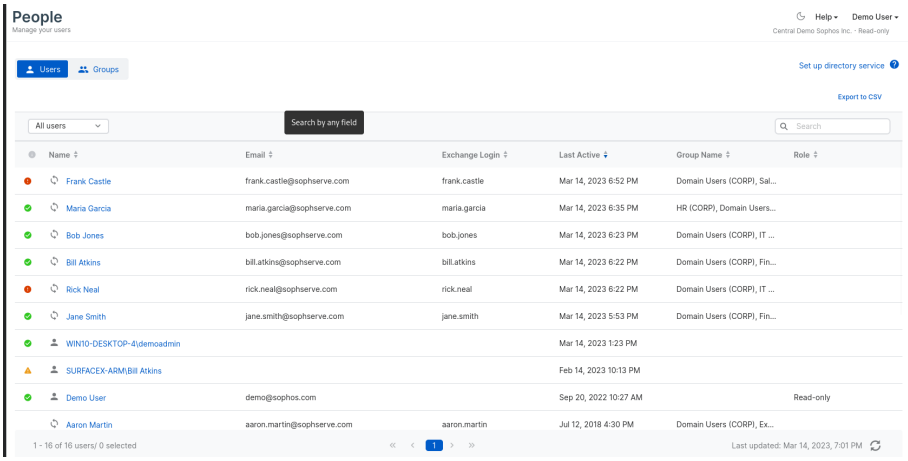
reports can be customized to suit the needs of the organization or user, and can be generated on a scheduled or ad-hoc basis. Reports can be generated for specific devices, users, time periods, or events, and can include information such as

- 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

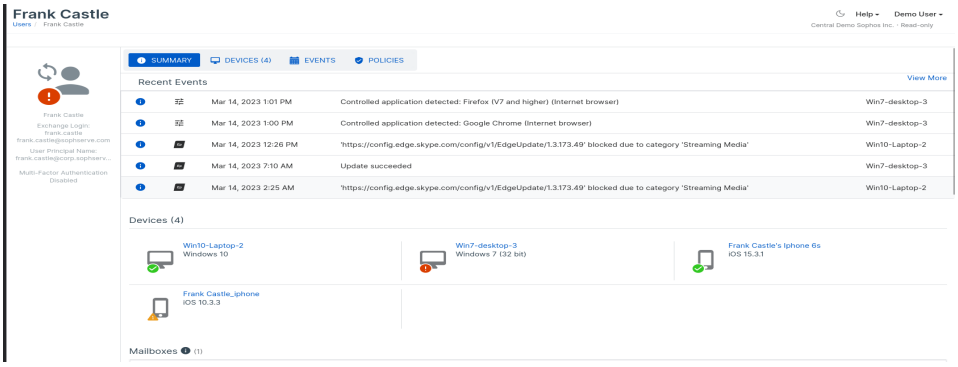
PEOPLE :

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

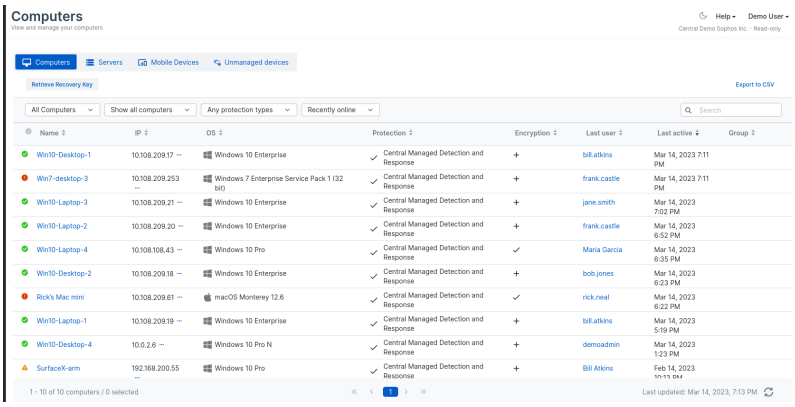


The people dashboard in Sophos Central :

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

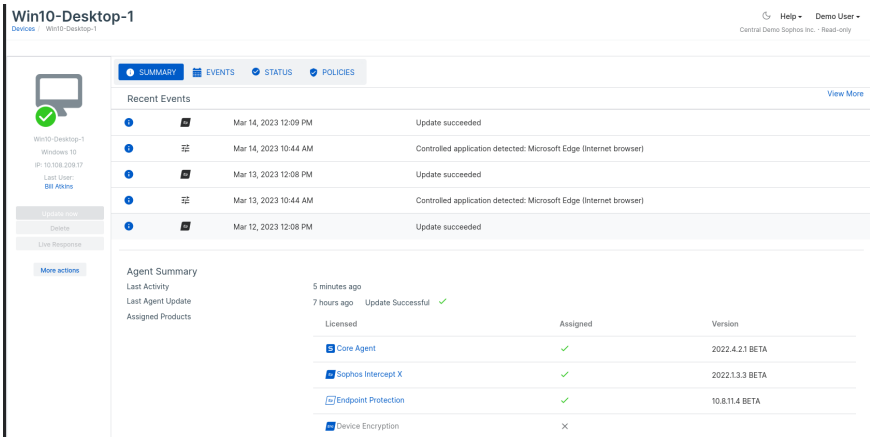


The Devices Dashboard
the overview of all the devices that are connected to the network, including desktops, laptops, servers, mobile devices, and other endpoints. This dashboard is designed to help IT administrators monitor and manage the security of these devices, ensure compliance with company policies,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



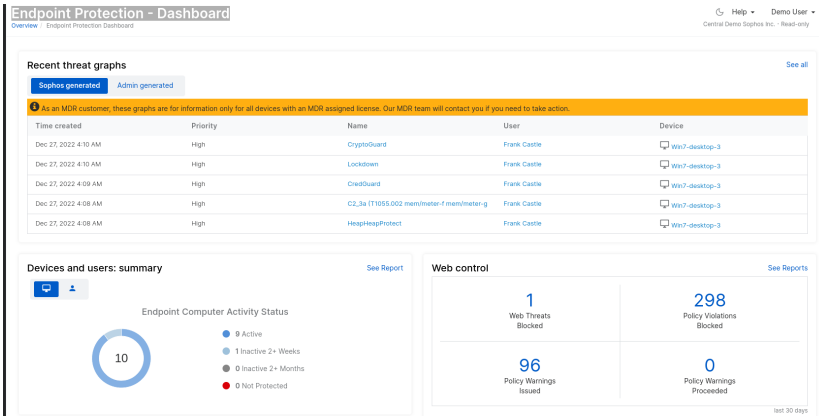
Another important feature of the devices dashboard is the ability to manage devices remotely. Administrators can perform a range of actions on individual devices, including initiating a virus scan, updating security software, or quarantining a device if it is infected with a virus. They can also configure 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. 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

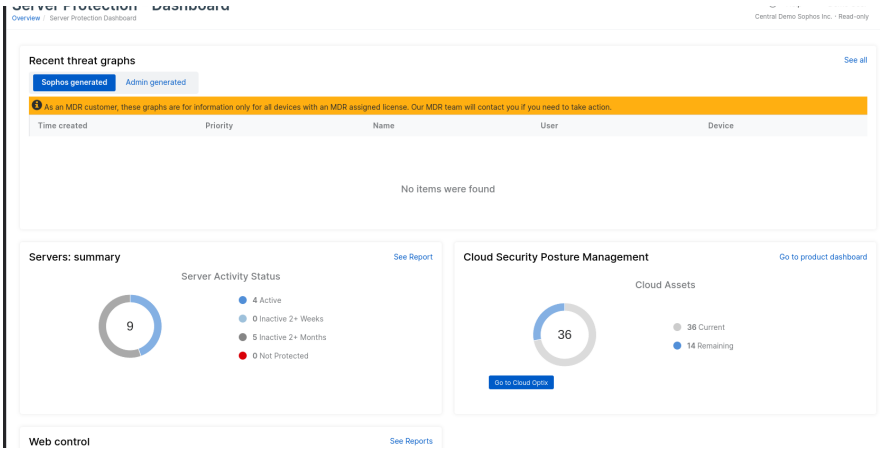
Endpoint Protection dashboard in Sophos provides a comprehensive view of the security status of all endpoints managed by the platform. This includes information on the number of endpoints that are protected, the number of endpoints that are at risk, and the number of endpoints that are unprotected.

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



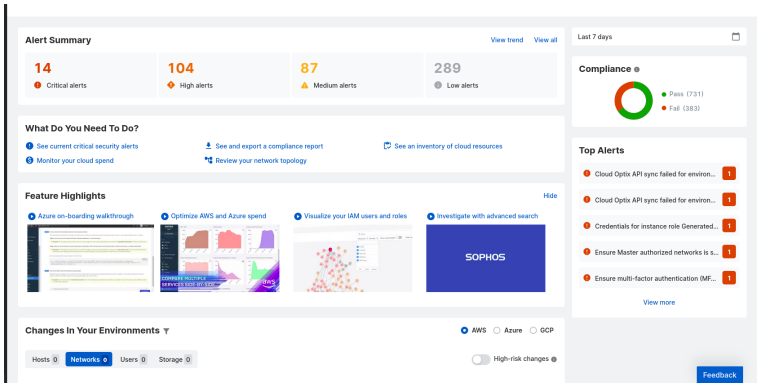
events, including any threats that have been detected and actions that have been taken to mitigate them. Its remote management capabilities, advanced analytics features, and detailed information about individual endpoints make it an essential tool for organizations of all sizes

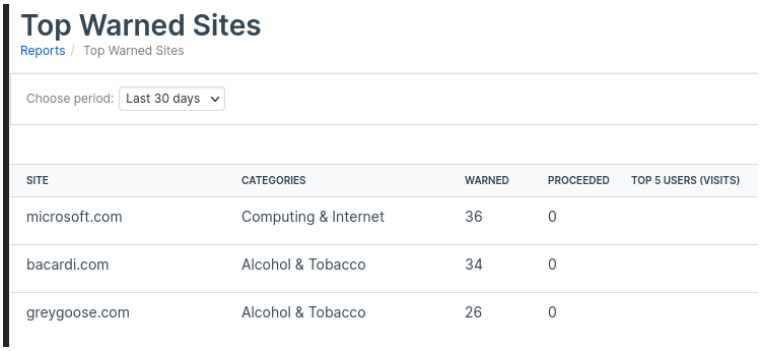
Server Protection – Dashboard:



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.





features :

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