Tracelay Networks

Report

SOPHOS XDR Platform

Prepared for-

Mr. Arun Dev

Prepared by-

Harsh Sharma

Overview

XDR stands for Extended Detection and Response which is an proactive alternative to all the reactive traditional security tools like EDR,MDR,SIEM and NDR.

XDR increases productivity and manages security tools within. Making it easier and time efficient for security professionals working under SOC operations.

SOPHOS XDR consists of following services:

- Endpoint Protection
- Server Protection
- Mobile
- Encryption
- Wireless
- Email Security
- Firewall Management
- Phish Threat
- Cloud Native Security
- Switches
- Managed Detection and Response (MDR)

With the help of Automation , Machine Learning and User Behaviour Analytics (UBA), XDR analyse every activity and details out activities. Making it more easier for investigation and being an single tool which helps to organize all the other tools leading to more time efficiency.

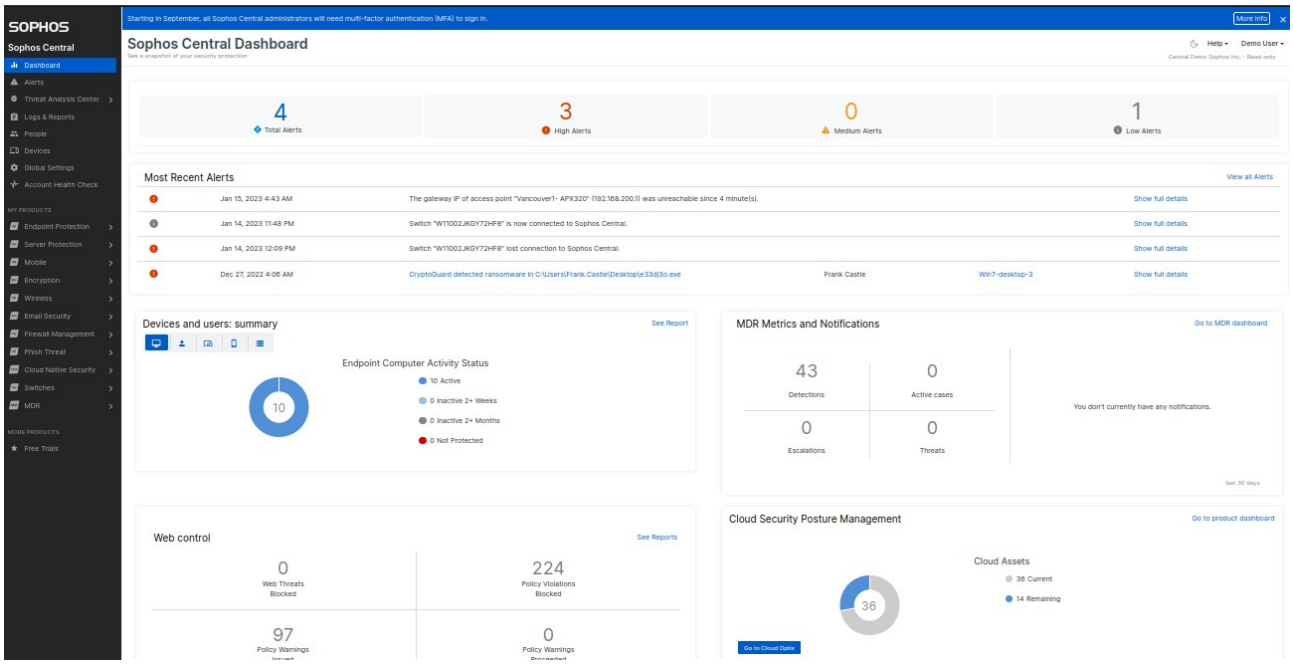
Benefits of SOPHOS XDR

1. Block known and unknown attacks with enpoint protection : Block malware, exploits and fileless attacks with integrated AI-driven antivirus.

2. Faster Detection and Responding : Review and control every endpoint in your organization on a cloud ecosystem.

3. Risk Reduction – XDR combined with high protection stops threat before it becomes an incident.

DASHBOARD



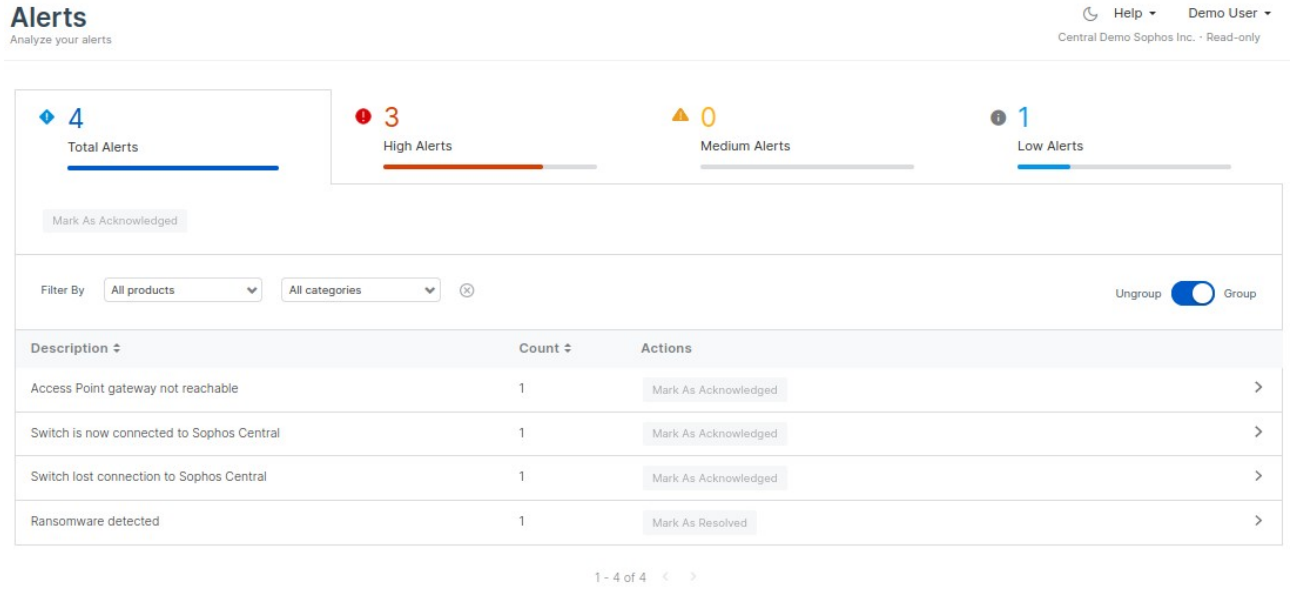
Dashboard briefly provides the information about all the services for example:
1. Most recent alerts captured categorised in High,Med and Low alerts
2. Devices and Users : No of endpoints and their status
3. MDR metrics : shows no of detections , active cases and threats.
4. Web Control : Breifs about web activities and warnings flagged to websites and users who violates polices.
5. Cloud assets Information
6. Email security – provides information on all emails categorised in spam , virus, threats etc.
7. Global security news : briefs latest news in security

To get more detailed version of all the services click on the respective service.

All the information can be generated in a csv format.

Alerts

Alerts are shown in a specific tab where we can investigate and review.



Alerts are classified in three categories:
1. High Alerts
2. Medium Alerts
3. Low Alerts

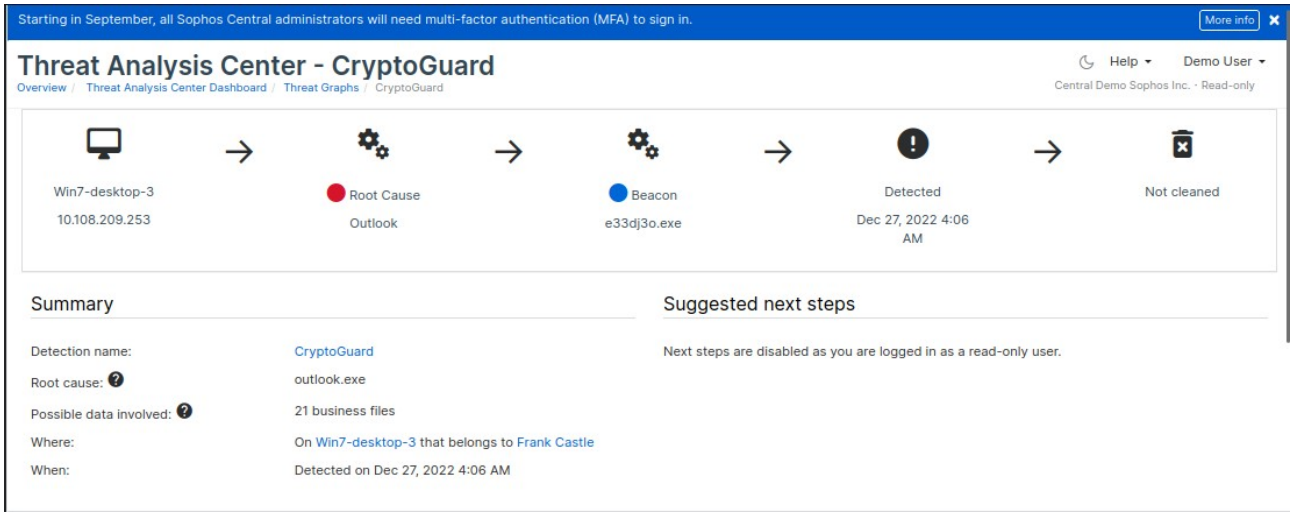
We can acknowledge the alerts and review them.

Threat Analysis Center

In this section threats are logged and gets investigated.

From which tool detected the activity to beacon name i.e malicious executable everything is summarised in threat analysis center

In the image, malicious activity is detected by CryptoGuard



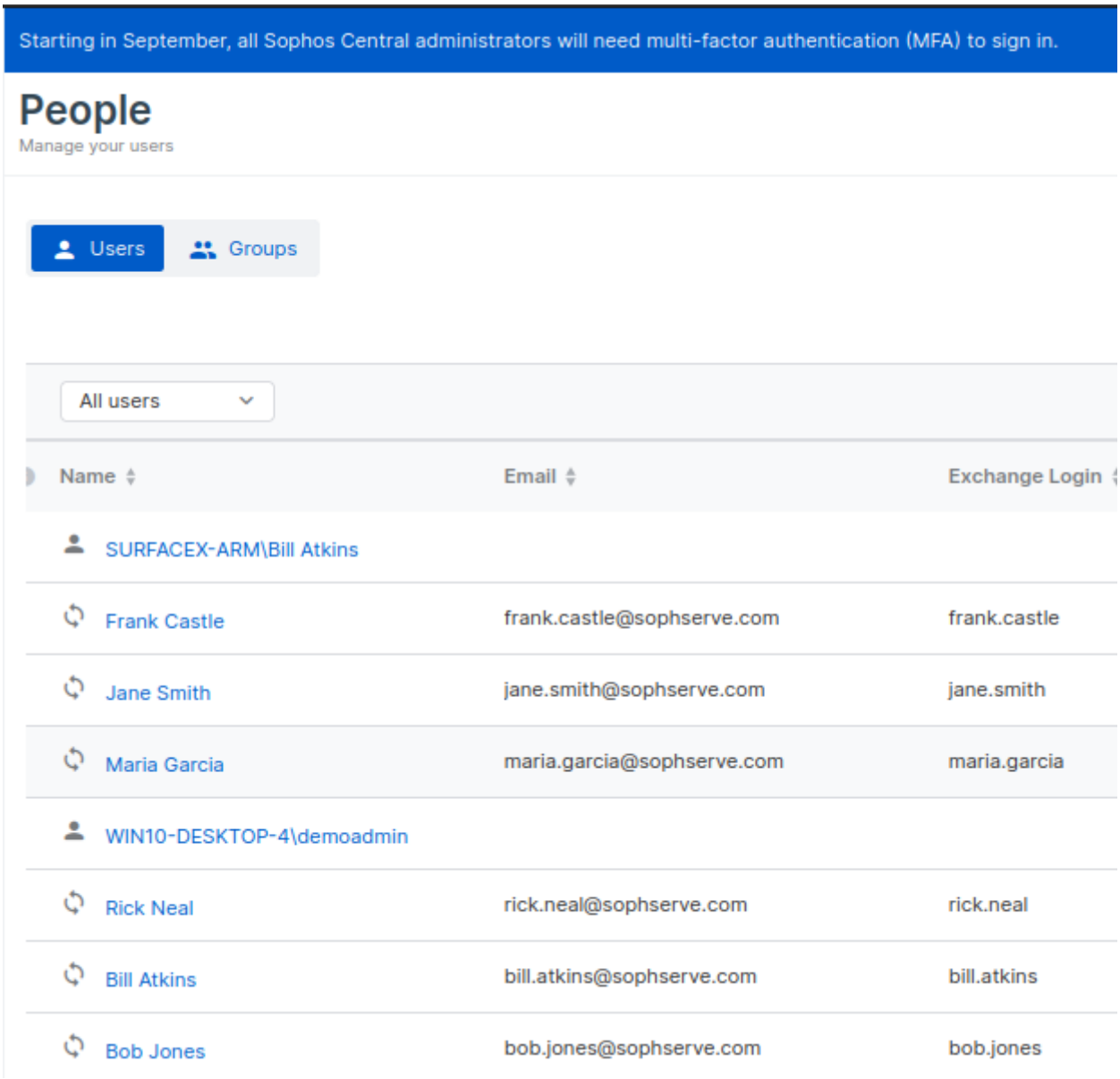
Logs and Reports

To improve and analysis of logs is done here. Every single log and reports are generated here.
Logs such as:
1. General Logs : Events and Audit Logs
2. Endpoint & Server Protection Logs : Data Loss Prevention adn Live Reponse session audits

Reports such as:
1. Endpoint & Server Protection : Malwares and PUAs , peripheral , Blocked application , allowed application, windows firewalls
2. Unifeid Endpoint Management & Sophos Intercept X for Mobile : Unified Endpoint management , Sophos Intercept X mobile.

People

People tab helps to organize and review all the members in the SOPHOS XDR.



Details of the members can be viewed here including their email address and usernames.

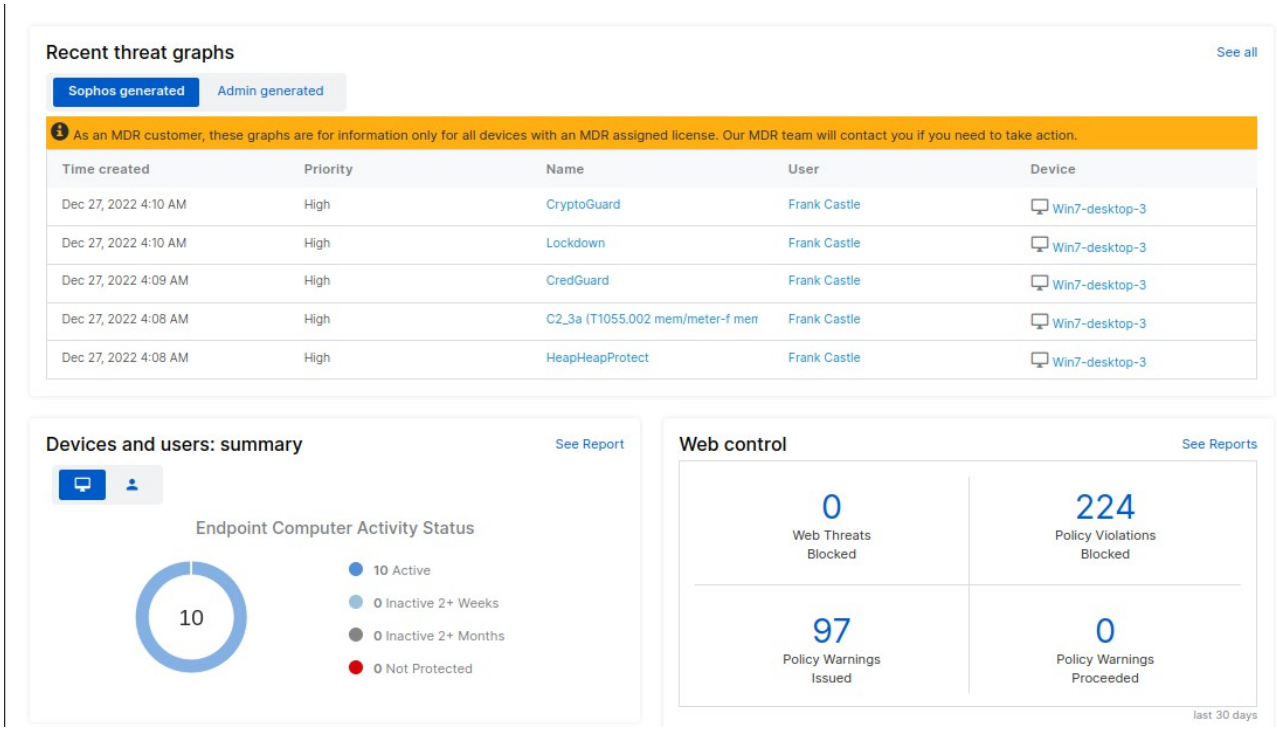
Devices

Devices dashboard gives all the information about all the devices connected with the services.

Devices are categorised in different types:
1. Computers
2. Servers
3. Mobile Devices
4. Unmanaged Devices

Endpoint Protection

Activity status of all the endpoints, threat reports and summaries of an endpoint is stored here.



Server Protection – Dashboard

Information about servers and cloud assets is stored here. Reports on web control having policy violations blocked, warnings can be reviewed here.

Server protection helps to manage servers and cloud assets.