SOPHOS
Security made simple.

Pocket Guide

Synchronized Security in Discover (TAP) Mode

Product: Sophos XG Firewall

Contents

Overview

This document describes how you can deploy Sophos XG Firewall in Discover (TAP) mode, and install Sophos Central Endpoint Advanced (CEA) protection with Intercept X (CIX) on endpoint computers to gain synchronized security and network visibility on the Admin Console of XG Firewall:

- **Security Heartbeat** provides visibility into the health status and identity information of Sophos Endpoints based on the Security Heartbeat sent by them to XG Firewall. Bringing anti-exploit zero-day defense, anti-ransomware CryptoGuard technology and root cause analysis through signature-less technologies on top of traditional endpoint security, Intercept X with Sophos Endpoint Advanced protection scans Sophos Endpoints for threats and vulnerabilities, based on which it sends Security Heartbeat.

- **Synchronized Application Control** (SAC) provides visibility into all previously unknown applications, which are identified and automatically categorized by Sophos Synchronized Security based on users, hosts, and destination countries. This consists of application information from Sophos Endpoints for traffic that does not match current application control signatures, or which is using generic HTTP or HTTPS connections.

- **Network Threat and Usage Reports** enable you to monitor user, web, and application usage, and intrusions in the network, including inappropriate web and application usage, user behaviour, and advanced malware and intrusions.

Prerequisites

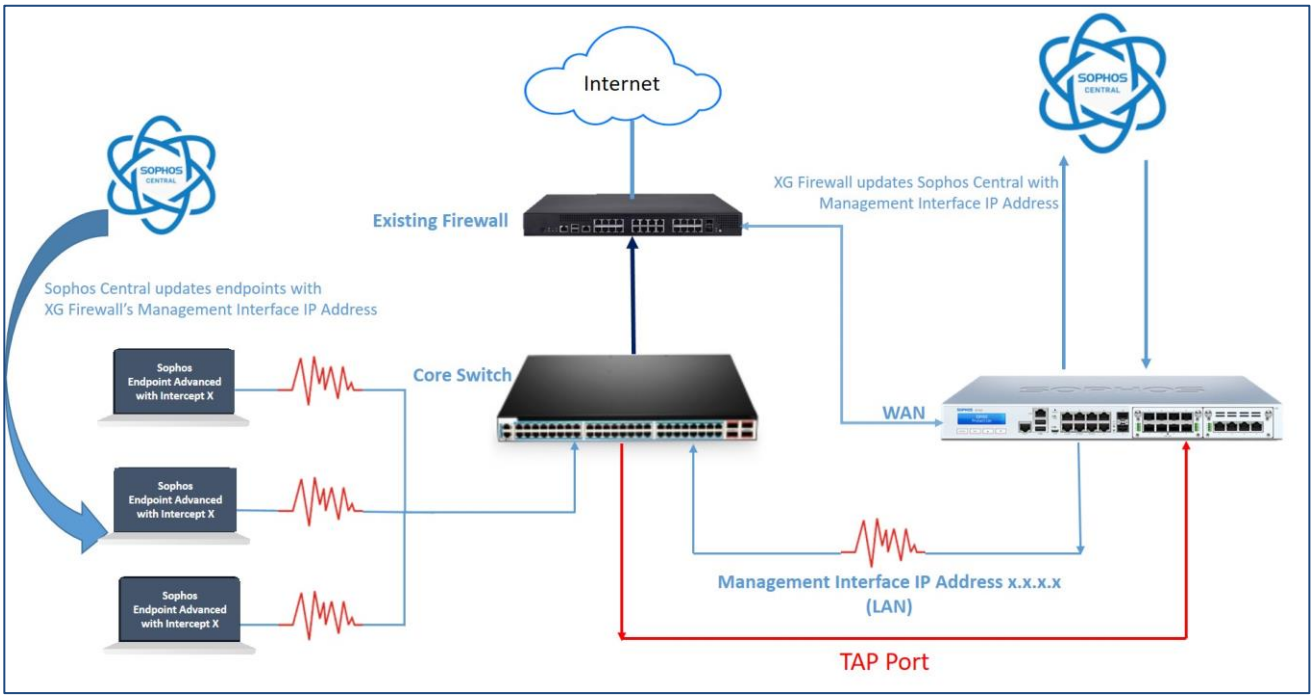
- You must have read-write permissions on the SFOS Admin Console and Command Line Interface for the relevant features.
- XG Firewall must be connected to a switch that supports SPAN or mirror port configuration.
- Choose the endpoint computers on which you wish to install the following:
    - Sophos Central Endpoint Advanced (CEA)
    - Intercept X (CIX)
- Set IPS Max Packets to the default 8 packets. (CLI command: **set ips maxpkts default**)
- XG Firewall should be able to reach all Sophos Endpoints.

Note:

- SAC works only in active-passive high availability mode. It does not support active-active mode.
- In Discover mode, XG Firewall device cannot support dynamic DNS, multicast routing, DHCP client functions, IPsec VPN, VLAN and PPPoE.

Network Diagram

In Discover mode, the XG Firewall device enables passive monitoring of traffic flow in your network. When you connect an interface of the device to a SPAN or mirror port on a switch, traffic from the other switch ports is copied and provided to the device. The device can work with any existing firewall, and does not displace or disrupt existing IT security infrastructure.



Deploy Synchronized Security

Step 1: Deploy XG Firewall

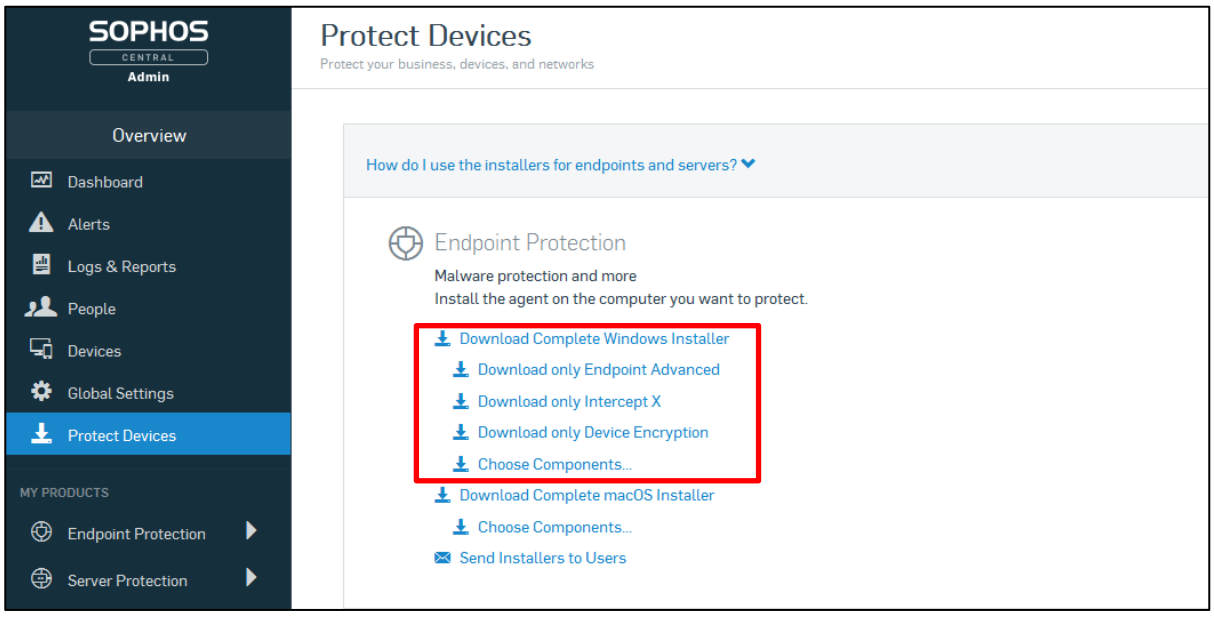
For details of how to deploy XG Firewall in Discover Mode, click Configure Discover (TAP) Mode and Security Audit Report.

Note:

- You require subscription to Network Protection and Web Protection modules for the analysis of IPS, Web Filter and Application Filter policies. Trial version gives you access to these modules.
- You can create custom categories for Web and Application Filter to receive reports specific to your network.

Step 2: Install CEA and CIX

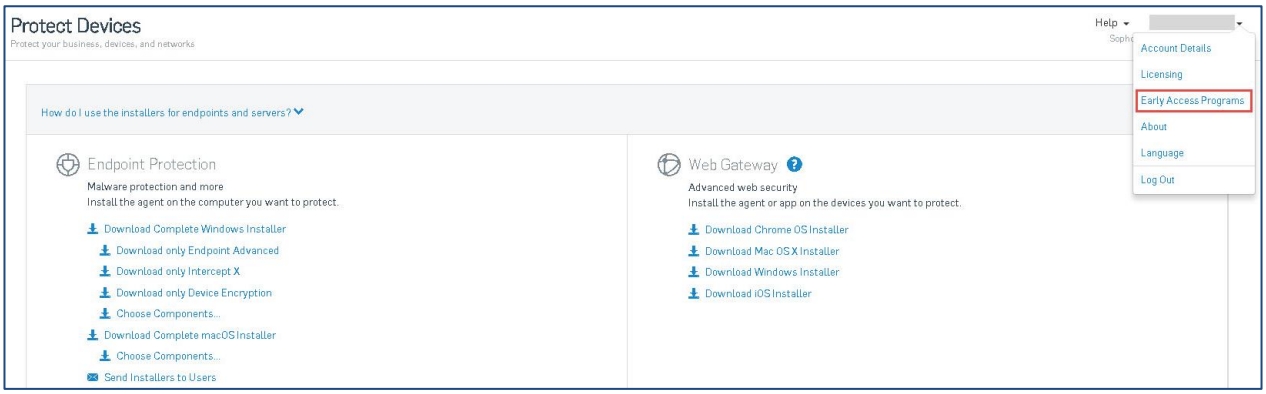
- Log in to your Sophos Central account (https://central.sophos.com). If you do not have one, take a 30-day trial of Sophos Central. It will give you access to the trial version of all modules available from Sophos Central.
- On the left menu, click **Protect Devices**.
- Click **Download Complete Windows Installer** or click **Choose Components** and select **Endpoint Advanced** and **Intercept X**. Click **Download Installer** and save file.



Note:

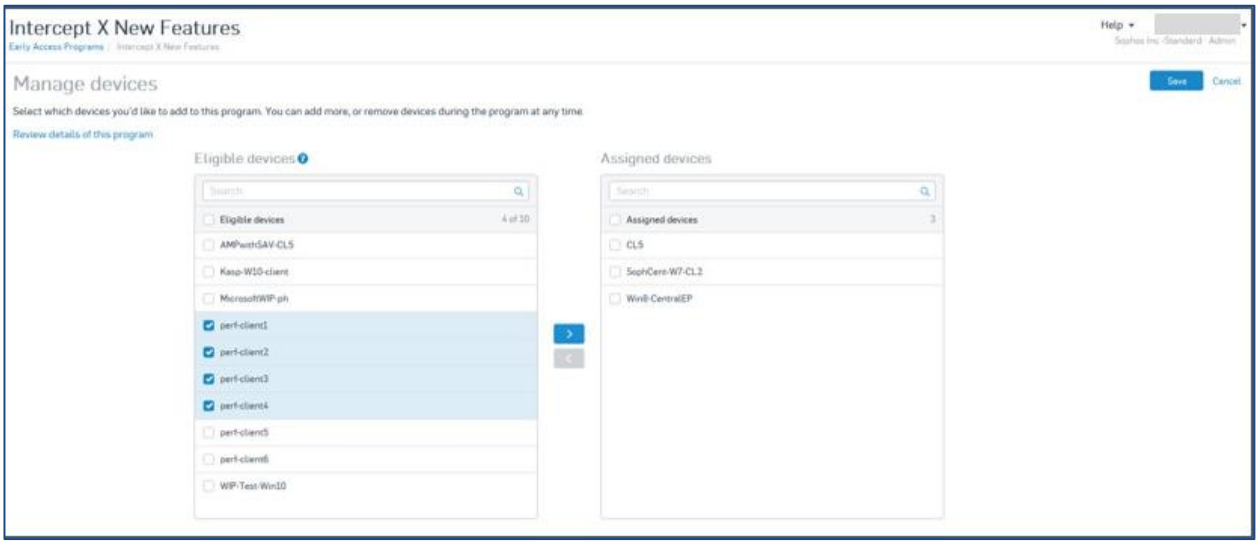
- Installing Sophos CEA protection will uninstall your current anti-virus.
- To enable Security Heartbeat and Synchronized Application Control, you require Sophos CEA and CIX of version 11.x.

- Go to the upper-right corner, and click the tab next to your name. Click **Early Access Programs**.



- Under **Intercept X New Features**, click **Manage**.

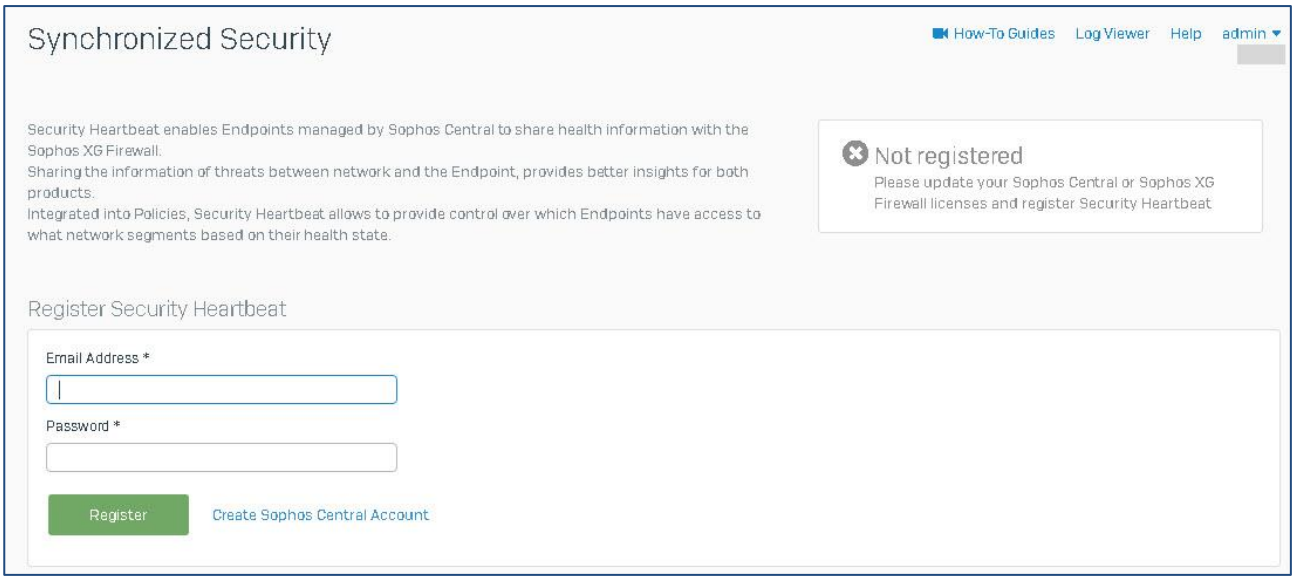
- Under **Eligible devices**, select the endpoint computers and add them to **Assigned devices**.
- On the upper-right corner, click **Save**.



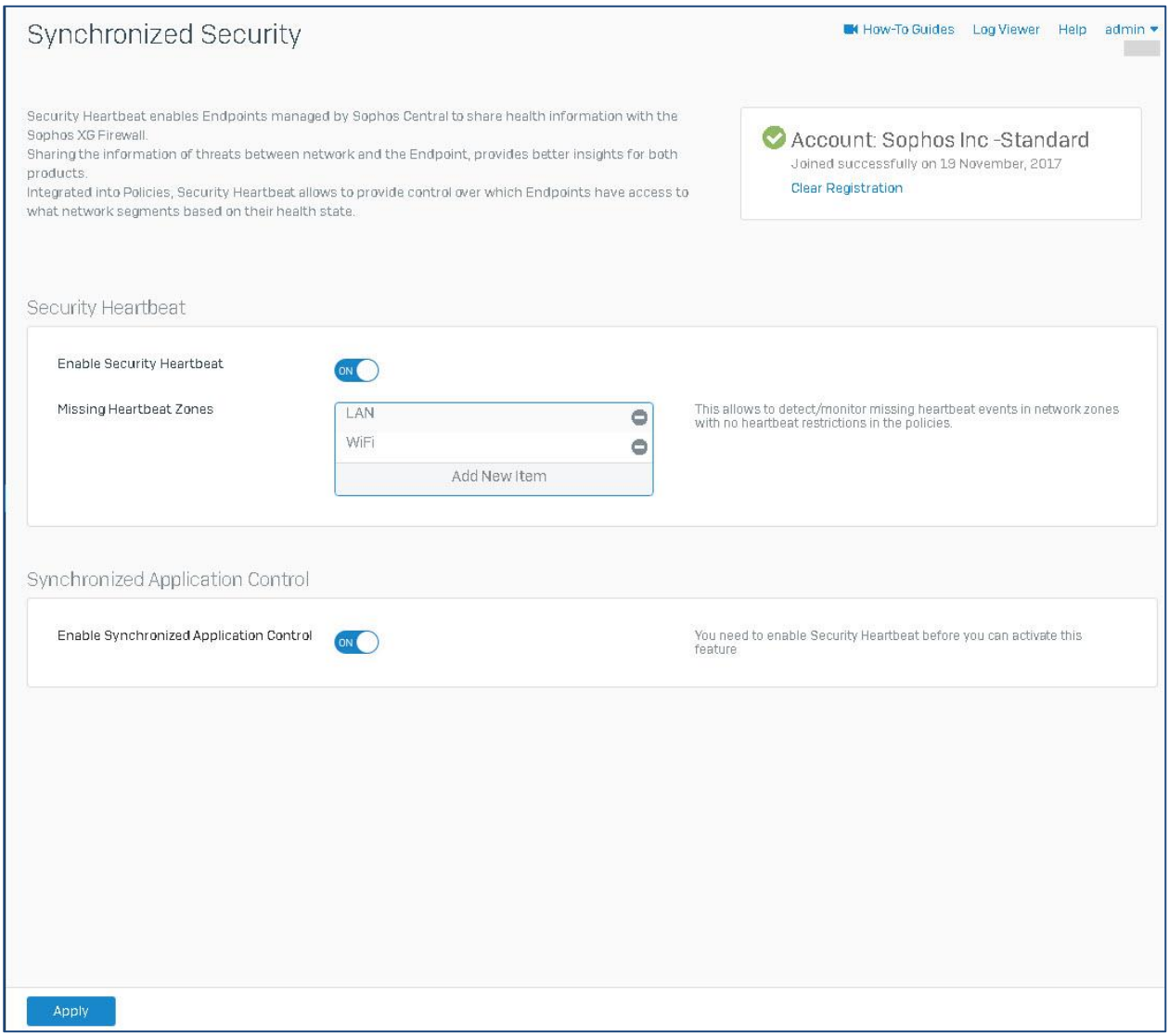
Result: You have installed Sophos Central Endpoint Advanced and Intercept X on the **Assigned devices**.

Step 3: Connect XG Firewall to Sophos Central and Enable Security Heartbeat

- Log in to the Admin Console of XG Firewall. Go to **Protect > Synchronized Security** and enter the Sophos Central admin credentials to register the XG Firewall with Sophos Central.



- Turn on **Enable Security Heartbeat**.
- For **Missing Heartbeat Zones**, select the zones in which you wish to monitor the endpoint Heartbeats.
- Turn on **Enable Synchronized Application Control**.
- Click **Apply**.



Result

- XG Firewall device will become visible in Sophos Central.
- XG Firewall will update its LAN management interface IP address on all endpoints in the heartbeat.xml file via Sophos Central.
- Once the endpoint receives this updated information, it will initiate Security Heartbeat with the management interface of XG Firewall.

- The following health status will appear on the XG Firewall dashboard:
  - **Green:** Endpoint is healthy.
  - **Yellow:** Potentially unwanted application (PUA) was detected, or inactive malware was found on the endpoint.
  - **Red:** Active malware or ransomware was found on the endpoint and one or more Sophos Endpoint Services are not running or are missing.
  - **Missing Heartbeat:** Endpoint is no longer sending Heartbeat, but XG Firewall still receives traffic from the endpoint.

  Note: Additionally, Sophos Central dashboard displays the endpoint health status.

- XG Firewall also identifies network intrusions, web and application usage by users and hosts, and automatically categorizes the information.

What you can Monitor in Discover Mode

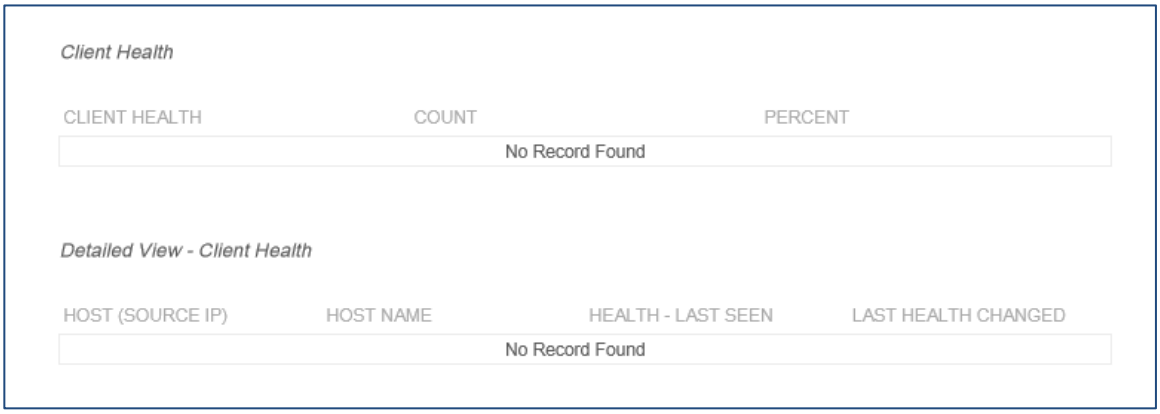
A. Security Audit Report (SAR)

Security Audit Report provides key observations, users with risk-prone behavior, including User Threat Quotient (UTQ), user application risks and usage, including Application Risk Score, high risk applications and application categories by data transfer, synchronized applications, web risks based on objectionable domains, web usage based on data transfer and hits, intrusion attacks, Advanced Threat Protection (ATP) visibility, and Security Heartbeat of endpoints.

The following are representative reports available in SAR:

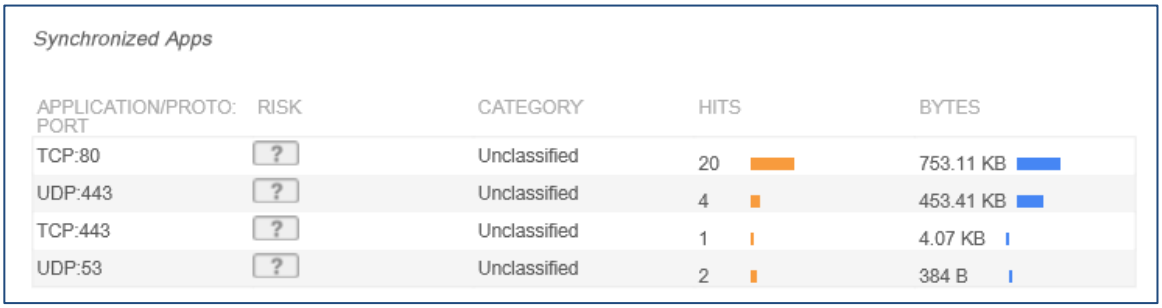
Security Heartbeat

If an endpoint is running unwanted applications or is infected, it will appear as yellow or red. You can also view endpoints with missing Heartbeats. Red indicators should be dealt with immediately, while yellow indicates risk but not urgency.



Synchronized Apps

Synchronized Applications report displays applications which are identified and classified by Sophos Endpoints. Uncategorized applications appear based on port and protocol.



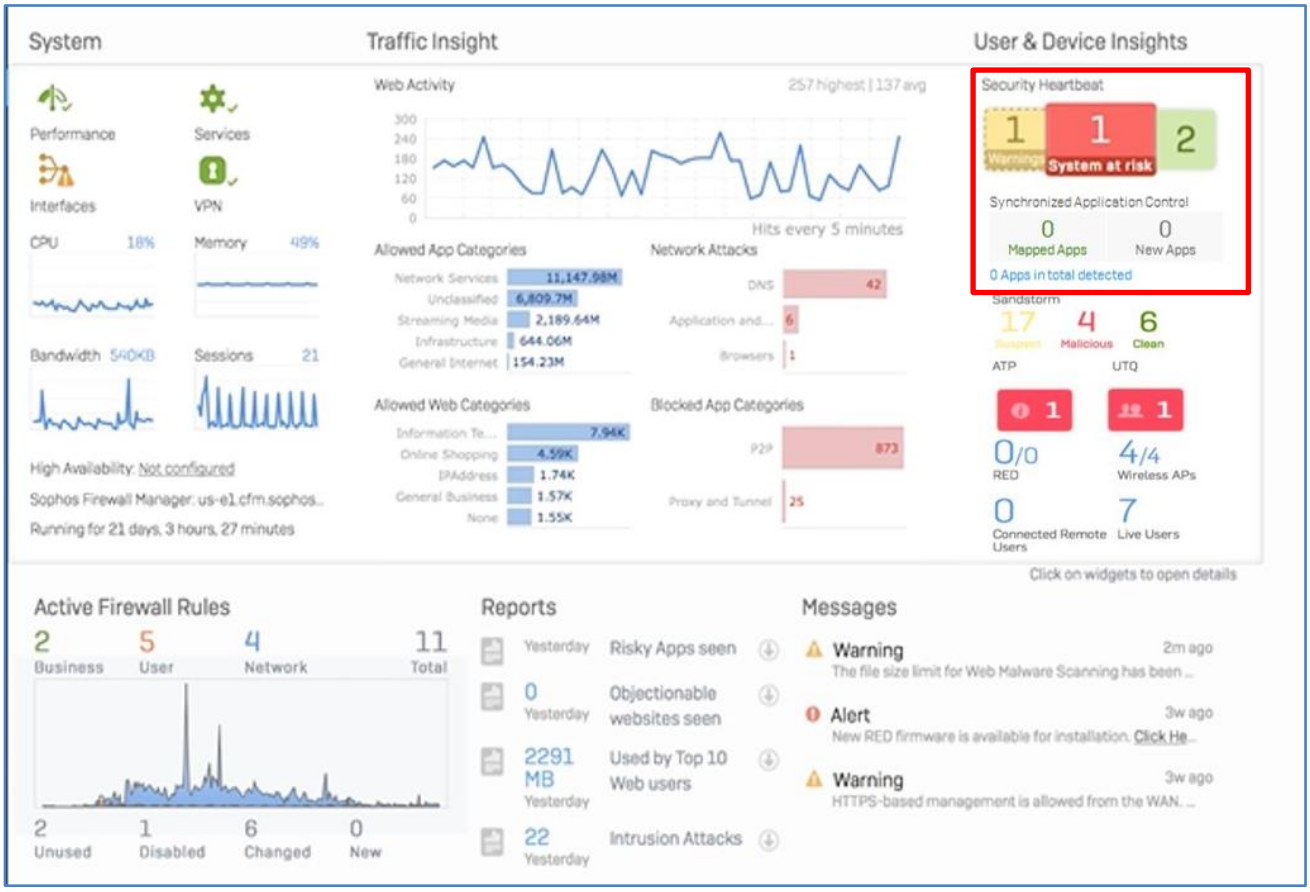
B. View Reports on Admin Console

The following are representative reports on the Admin Console of XG Firewall:

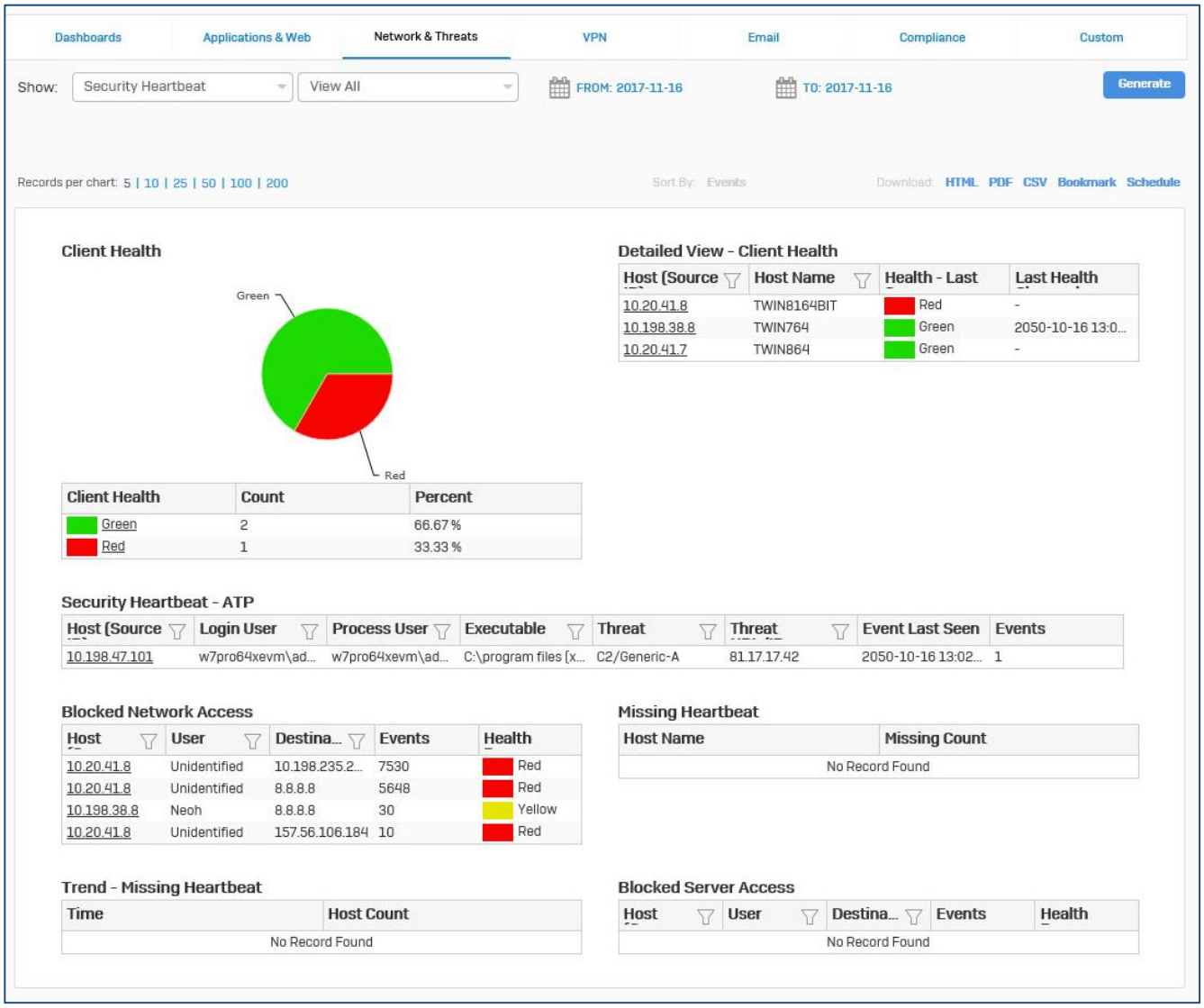
1. Security Heartbeat
2. Synchronized Applications
3. Network Threat & Usage Reports

Security Heartbeat

On the XG Firewall dashboard (**Monitor & Analyze > Control Center**), the Sophos Security Heartbeat widget displays the health status of all your Sophos Central-managed endpoints.



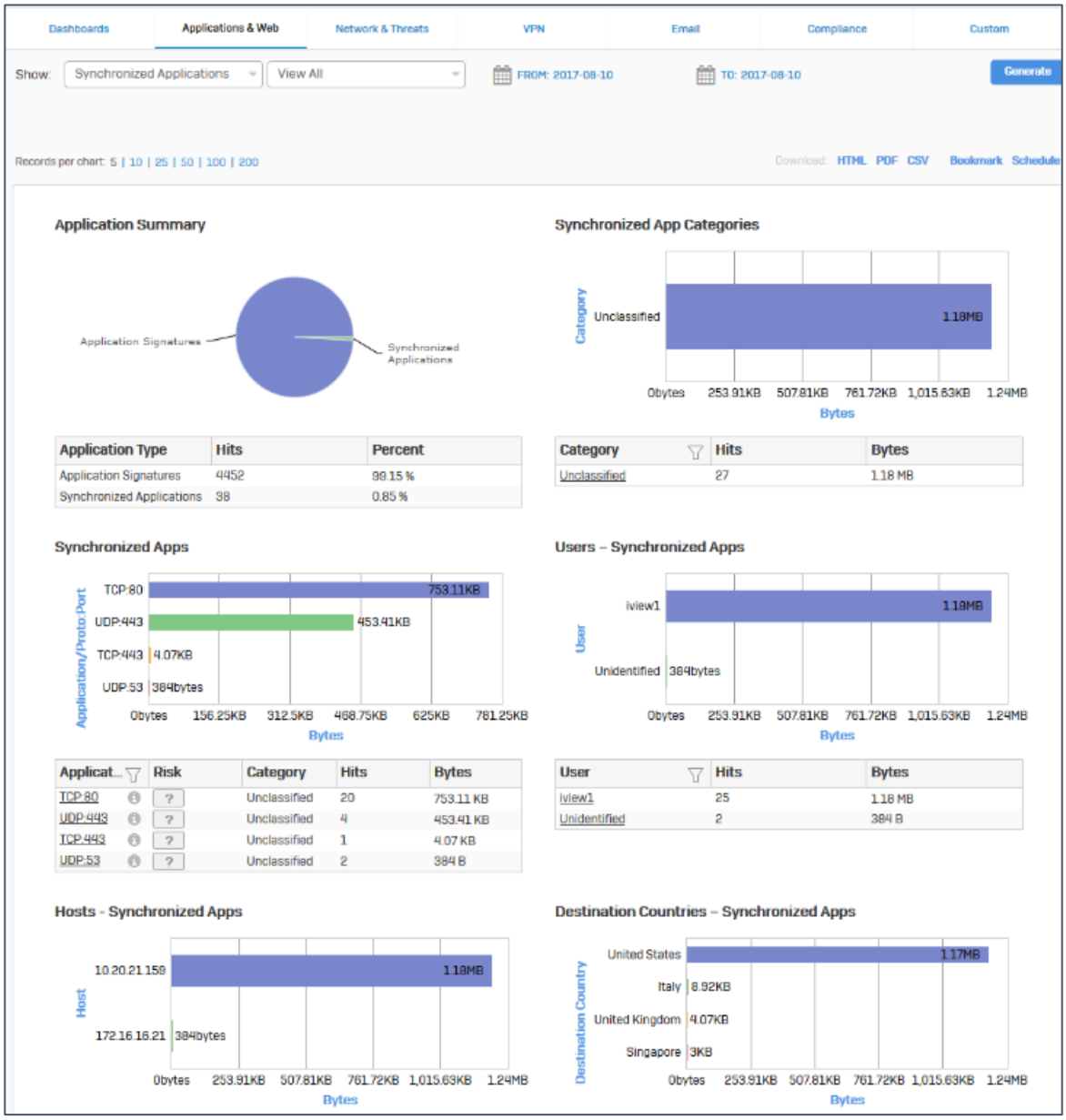
Dashboard



Security Heartbeat

Synchronized Applications

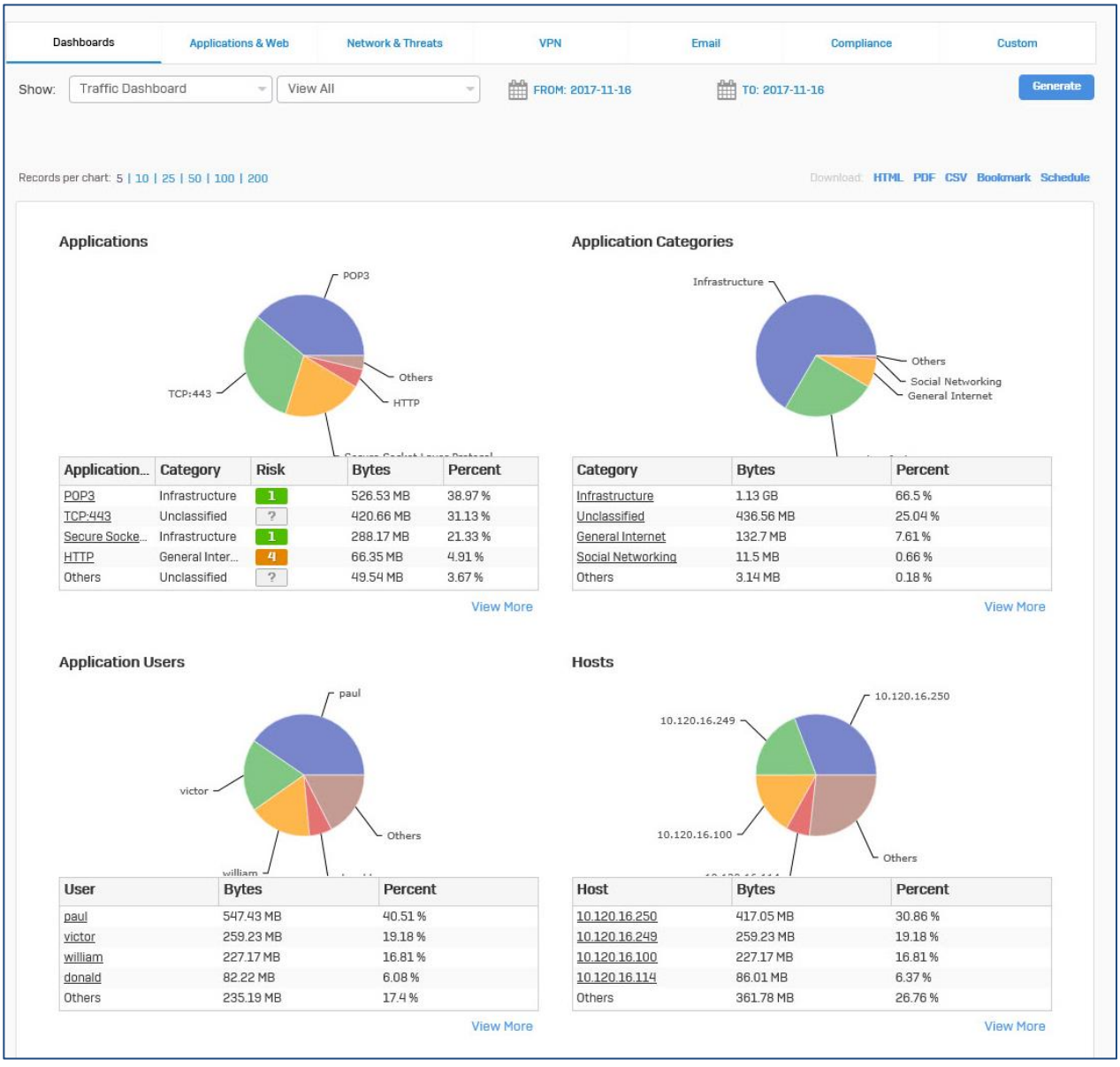
Synchronized Applications reports offer complete historical reporting of all applications, which are identified by Sophos Endpoints. These applications appear based on users, hosts, destination countries.



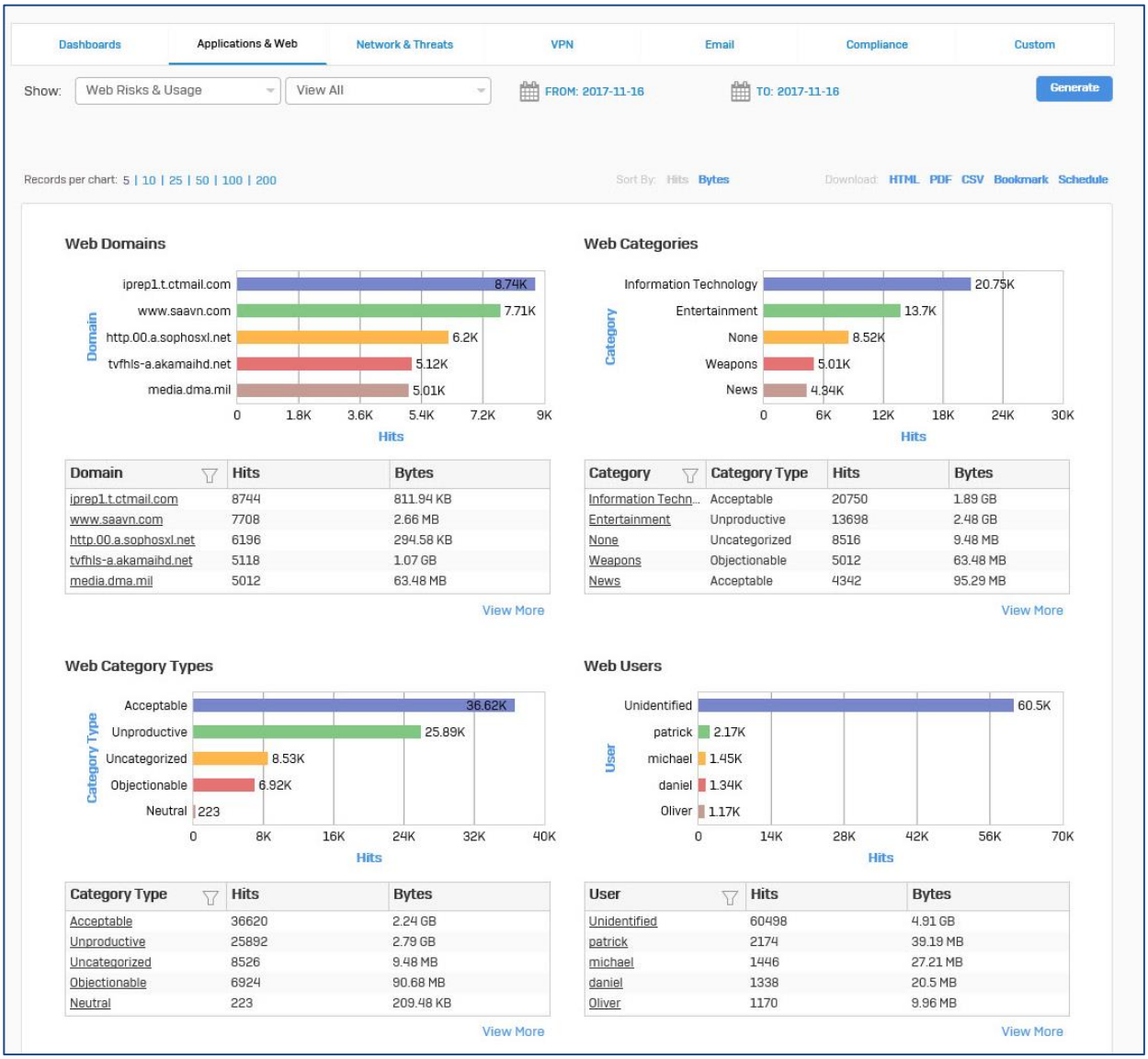
Synchronized Applications

Network Threat & Usage Reports

You will gain access to Traffic and Security Dashboards, Executive Report and User Threat Quotient, in addition to Application & Web reports, Network & Threats, and Compliance reports.



Dashboard



Web Risks & Usage

Suggested Reading

Synchronized Security in Bridge Mode

(In Bridge mode, you can create security policies and firewall rules in XG Firewall to take action automatically on endpoints based on Security Heartbeat and Synchronized Applications.)

Copyright Notice