ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

POLITICAS DE CIBERSEGURIDAD -SOPHOS CENTRAL

2022

Alcaldía Distrital de Cartagena de Indias - Bolívar

Centro Diag. 30 # 30 - 78 Plaza de la Aduana.
(57) + (5) 6411370 - Línea Gratuita: 018000 415 393.
alcalde@cartagena.gov.co / atencionalciudadano@cartagenagov.co

Contenido

Consola Administración Centralizada de Sophos 3

Tecnologías next-gen 3

Análisis de datos en profundidad 3

Potentes paneles de control 3

Implementación de políticas de restricción 4

Implementación de políticas generales 4

Restricción de Aplicaciones 4

Control de periféricos 6

Control Web 7

Consola Administración Centralizada de Sophos

Sophos Central es la consola de administración de ciberseguridad en la nube la cual te permite tener control de todos los dispositivos y gestionar los eventos e incidente de cibersegurdiad de manera fácil

Tecnologías next-gen

- Prevención predictiva con IA
- Detección de nivel empresarial
- Respuesta automatizada a incidentes

Análisis de datos en profundidad

- Telemetría entre productos sincronizados
- Información sobre amenazas de SophosLabs Intelix
- Investigaciones entre productos

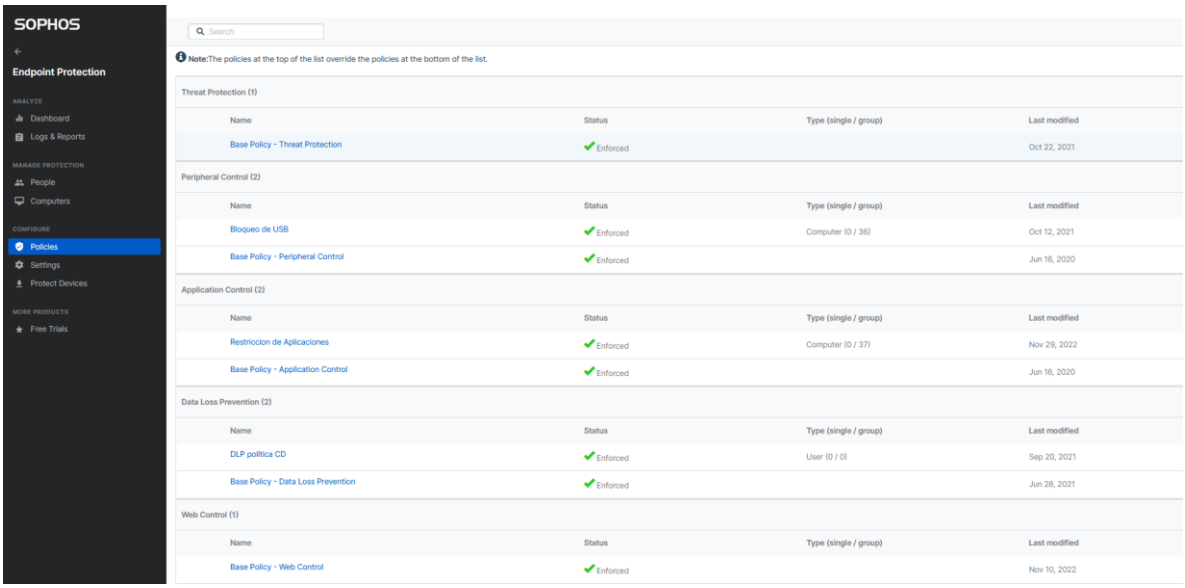
Potentes paneles de control

- Potentes paneles de control, generación de informes y notificaciones
- Acceda a resúmenes rápidos con paneles de control visuales
- Profundice en la información con potentes informes y análisis

Implementación de políticas de restricción

Implementación de políticas generales

Mediante la consola de administración centralizada de Sophos Central podemos implementar políticas de control sobre los dispositivos que tiene instalado la solución de EndPoint de Sophos como mecanismo de prevención protección contra Ramsomware



Control de Políticas Generales

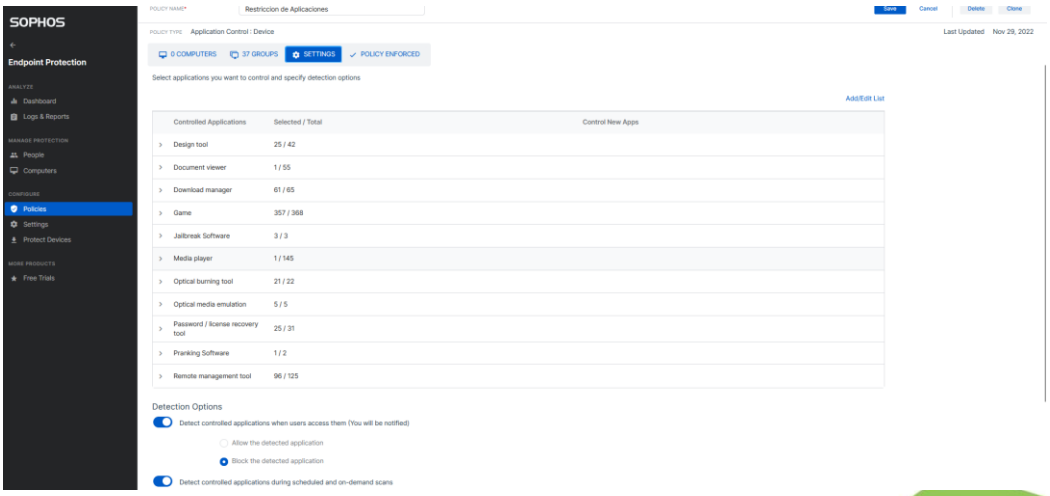
Restricción de Aplicaciones

A continuación de describe algunas aplicaciones que podemos controlar atraves de la gestión del antivirus, tales como:

- 710 Gauge Utility
- Adobe Dreamweaver
- Allplan
- ArtiosCAD
- AutoCAD
- Autodesk Application Manager
- Autodesk Inventor 2017

- Autodesk Inventor 2018
- Autodesk Revit
- Autodesk Windows Components
- Corel Video Studio Pro X
- Creo
- Dassault Systmes SolidWorks
- Draftsight
- Gates Design Flex Pro
- GaugeTools
- Google SketchUp
- LibreCAD
- Maple
- Maxon Cinema 4D
- Micromine 2016
- MityGUI
- NetFabb
- Photo Pos Pro
- PlanGrid
- Rhinoceros
- SketchBook Express
- Sparx Systems
- The Print Shop
- UniGraphics
- Webots Robot Simulator

Mecanismo de control evidenciado en la siguiente imagen



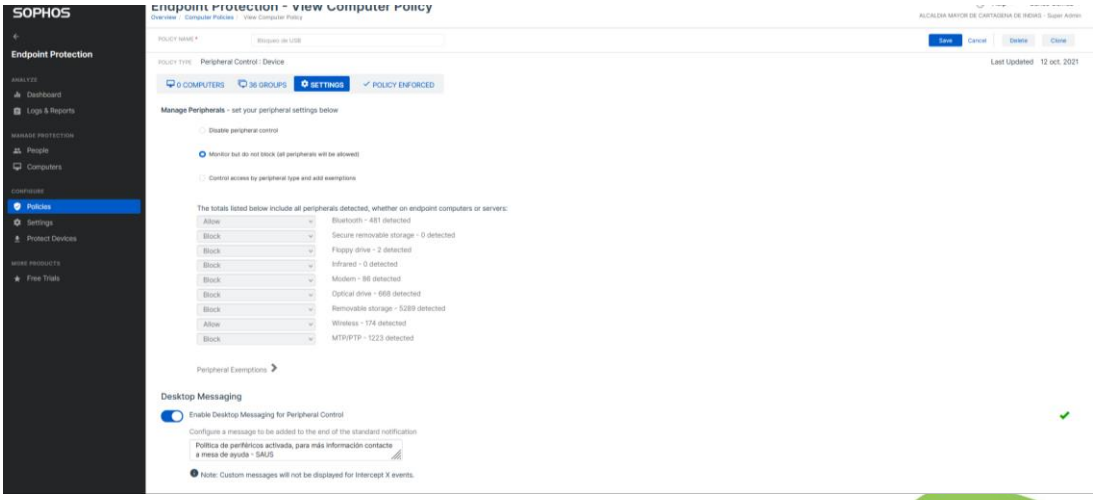
Restricción de aplicaciones

Control de periféricos

Los totales que aparecen a continuación incluyen todos los periféricos detectados, ya sea en estaciones de trabajo o servidores:

- AutorizarBloquear
- Bluetooth - 0 detectados
- AutorizarSolo lecturaBloquear
- Proteger almacenamiento extraíble - 0 detectados
- AutorizarSolo lecturaBloquear
- Disquete - 0 detectados
- AutorizarBloquear
- Infrarrojo - 0 detectados
- AutorizarBloquear
- Módem - 0 detectados
- AutorizarSolo lecturaBloquear
- Unidad óptica - 0 detectados
- AutorizarSolo lecturaBloquear
- Almacenamiento extraíble - 0 detectados
- AutorizarBloquear puenteBloquear
- Inalámbrico - 0 detectados
- AutorizarBloquear
- MTP/PTP - 0 detectados

Mecanismo de control evidenciado en la siguiente imagen



Control de periféricos

Control Web

Se establecerá políticas para bloquear o permitir las siguientes acciones de acceso web para las estaciones de trabajo.

Detalle	Acción
Categorías relacionadas con la productividad	Permitir
Redes sociales	Permitir
Categorías de adultos y potencialmente inapropiadas	Bloquear
Categorías susceptibles de provocar un uso excesivo del ancho de banda	Bloquear
Categorías de sitios relativas al trabajo	Permitir

Mecanismo de control evidenciado en la siguiente imagen