

**INFORME DE ESTADO ACTUAL
SOLUCIONES DE SEGURIDAD TRELLIX
SOFTSECURITY**



**SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
2023**

El material incluido en este documento es propiedad exclusiva de SOFTSECURITY SAS. Este documento no puede ser divulgado de cualquier manera o a cualquier persona a excepción del destinatario y los empleados o representantes de la firma a quien va dirigido, quienes son los directamente responsables de la evaluación de su contenido. Este documento no puede ser utilizado en cualquier forma diferente al propósito con el que fue distribuido. Se prohíbe terminantemente cualquier uso, reproducción o transmisión no autorizada.



TABLA DE CONTENIDO

1. OBJETIVO	2
2. DATOS GENERALES.....	2
3. VERSIONAMIENTO DE PRODUCTOS TRELLIX.....	3
4. ESTADO ACTUAL.....	4
4.1 Base de Datos	4
4.2 Aplicación	5
4.2.1 Trellix Agent	27
4.2.2 Endpoint Security (ENS)	29
4.2.3 Data Loss Prevention (DLP)	35
5. LOGS DE SEGURIDAD DE LA APLICACIÓN TRELLIX EPO	36
6. RECOMENDACIONES	40

1. OBJETIVO

Dar a conocer el estado actual de los productos pertenecientes a la suite Trellix adquirida por la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO – SIC

2. DATOS GENERALES

Actualmente en la entidad, se tiene implementado una consola ePolicy Orchestrator para la administración centralizada de los productos Trellix instalados en los equipos terminales de la SIC; la consola de administración se encuentra instalada en un servidor destinado para la base de datos y la aplicación, con los siguientes parámetros:

Servidor de base de datos

Sistema operativo:	Windows server 2012 R2
Nombre del servidor:	SRVEPOPROD
Dirección IP:	10.20.100.239
Versión SQL server:	SQL server 2012
Instancia de base de datos:	SQLMCALEE
Nombre de la base de datos:	ePO_SRVEPOPROD
Puerto de conexión:	1433
Usuario base de datos:	sa
Contraseña:	Administrada por la entidad

Tabla 1. Servidor base de datos

Servidor de aplicación

Sistema operativo:	Windows Server 2012 R2
Nombre del servidor:	SRVEPOPROD
Dirección IP:	10.20.100.239

Tabla 2. Servidor aplicación

3. VERSIONAMIENTO DE PRODUCTOS TRELLIX

Las versiones implementadas en la entidad para la administración de los productos pertenecientes a la suite de Trellix son:

Producto	Versión
ePolicy Orchestator	5.10.2028 (Update 15)
EndPoint Security Adaptive Threat protection	10.7.0.6393
Endpoint Security Firewall	10.7.0.6078
Endpoint Security platform	10.7.0.6149
Endpoint Security Threat Prevention	10.7.0.6177
Endpoint Security Web Control	10.7.0.5773
Endpoint Security for Linux Firewall	10.7.16.37
Endpoint Security for Linux Threat prevention	10.7.16.27
Endpoint Security kernel modules for linux	10.7.16.10.27
McAfee Client Proxy	3.2.0.189
Data Loss Prevention	11.3.2.82
Data Loss Prevention for MacOS	11.9.100.182.1
Trellix Agent For Linux	5.7.9.182
Trellix Agent for Mac	5.7.9.139
Trellix Agent for Windows	5.8.0.161
Rogue System Detection (RSD)	5.0.7.44
SIEM Collector	11.1.9952.62126
VirusScan Enterprise (VSE)	8.8.0.2300
Host Intrusion Prevention	8.0.0.5316

Tabla 3. versiones de producto

4. ESTADO ACTUAL

4.1 Base de Datos

La base de datos perteneciente a la consola de administración ePO tiene un tamaño de 9 Gb aproximadamente como lo demuestra la siguiente imagen:

Database	
Name	ePO_SRVEPOPROD
Status	Normal
Owner	sa
Date Created	23/03/2016 9:27:12 a. m.
Size	9927,56 MB
Space Available	2739,88 MB

Imagen 1. Tamaño de base de datos

En esta base de datos, se destacan los 10 ID con mayor número de eventos

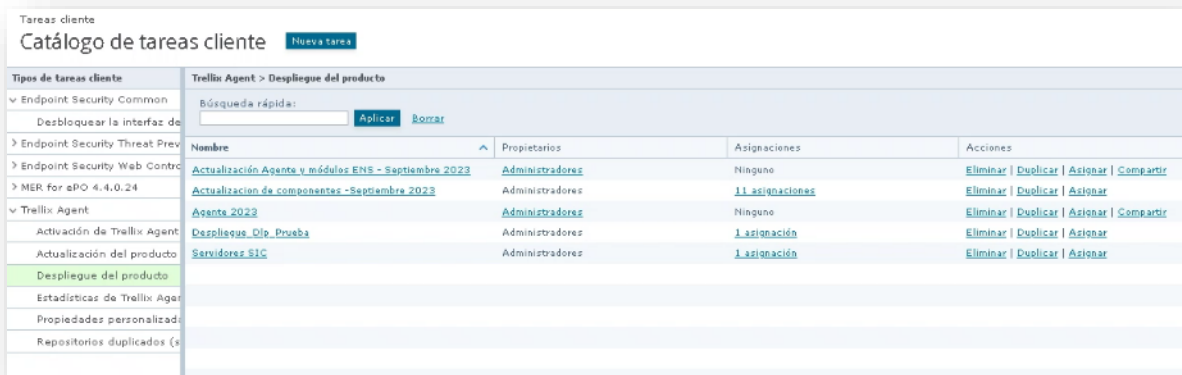
	Count	EventID	Event Description	Event Source
1	108653	1119	The update failed; see event log	McAfee Endpoint Security
2	83464	19115	Device Plug	Data Loss Prevention
3	60996	1027	The file %FILENAME% is infected with ...	McAfee Endpoint Security
4	46830	18060	Exploit Prevention Files/Process/Regist...	McAfee Endpoint Security
5	23378	1120	The update is running.	McAfee Endpoint Security
6	19267	1118	The update was successful. Scan versi...	McAfee Endpoint Security
7	7734	18054	An exploit was detected.	McAfee Endpoint Security
8	5088	35104	Endpoint Security Adaptive Threat Prot...	McAfee Endpoint Security
9	4563	1027	The file %FILENAME% is infected with ...	Trellix Endpoint Security
10	4061	1119	The update failed; see event log	Trellix Endpoint Security

Imagen 2. Top 10 eventos en base de datos

4.2 Aplicación

La consola ePO instalada en la entidad corresponde a la versión 5.10.2028 (Update 15), la cual administra los productos de Trellix Agent, Trellix Endpoint Security (ENS), Trellix Endpoint Security for Linux (ENSL), VirusScan Enterprise (VSE), Rogue System Detection (RSD), McAfee Client Proxy, McAfee Data Loss Prevention (DLP), SIEM Collector y Host Intrusion Prevention

Dentro de la configuración de la consola se observa que se encuentra un total de **1422** equipos gestionados y existen **181** equipos los cuales se encontraban gestionados, pero dejaron de comunicarse hace más de 90 días. por otro lado, se evidencia una gran cantidad de tareas cliente como se muestra en la siguiente imagen:



Tareas cliente

Catálogo de tareas cliente [Nueva tarea](#)

Tipos de tareas cliente		Trellix Agent > Despliegue del producto		
Búsqueda rápida:		Aplicar Borrar		
Nombre	Propietarios	Asignaciones	Acciones	
Actualización Agente v módulos ENS - Septiembre 2023	Administradores	Ninguno	Eliminar Duplicar Asignar Compartir	
Actualización de componentes - Septiembre 2023	Administradores	11 asignaciones	Eliminar Duplicar Asignar	
Agente 2023	Administradores	Ninguno	Eliminar Duplicar Asignar Compartir	
Despliegue Clp Prueba	Administradores	1 asignación	Eliminar Duplicar Asignar	
Servidores SIC	Administradores	1 asignación	Eliminar Duplicar Asignar	

Imagen 3. Tareas cliente

los equipos de la entidad tienen asignado por medio del árbol de sistemas, las tareas anteriormente mostradas con las cuales se ejecutan los procedimientos de instalación de productos de manera automática que se activan posterior a la instalación del agente de Trellix en los equipos cliente; las tareas asignadas son:

Sistemas

Árbol de sistemas

Sistemas nuevos

Nuevos subgrupos

Árbol de sistemas

Sistemas

Directivas asignadas

Tareas cliente asignadas

Detalles de grupo

Despliegue de agente

✓ Mi organización

Comware

Controladores de Dominio

Desactivar ENS

DLP

Equipos Pruebas

Escaneos Programados

Instalación-DLP

MONITOREO

Servidores

Servidores_Linux

Tecnología

Recolector

Valor predefinido: Sin filtro

Búsqueda rápida:

Aplicar

Borrar

Nombre de tarea

Tipo de tarea

Estado

Planificación

Fecha y hora de inicio

Herencia interrumpir

Herencia de

Escaneo Analisis Bajo Demanda ENS

Análisis bajo demanda personal

Activada

Ejecutar inmediatamente

11/02/21 0:00

11 no heredado

Este nodo

Servidores SIC

Despliegue del producto

Activada

Ejecutar inmediatamente

25/09/23 0:00

Ninguno

Este nodo

Imagen 4. Tareas asignadas

Para la automatización de procesos en la consola de administración, está cuenta con las tareas de servidor que llevan a cabo diferentes actividades como los son la actualización diaria de firmas de reconocimiento de amenazas en el repositorio principal, la replicación de las actualizaciones descargadas a los repositorios distribuidos, sincronización con el directorio activo de la entidad, envío de informes automáticos entre otros; en la siguiente imagen se observan **27** tareas de servidor activas:

Automatización						
Tareas servidor						
<div>Nueva tarea Importar tareas</div>						
<div>Tareas servidor</div> <div> <div>Búsqueda rápida: <input type="text"/></div> <div>Aplicar</div> <div>Borrar</div> <div>☐ Mostrar filas seleccionadas</div> </div>						
☐	Nombre	Estado	Tipo	Planificación	Próxima ejecución	Última ejecución
☒	Generate Records for Trellix Agent Compliance History Reporting	Activada	Usuario	Semanal	15/10/23 1:00	8/10/23 1:00
☐	Deployment Agent	Activada	Usuario	Cada hora	12/10/23 16:00	12/10/23 12:00
☐	DLP Purge History of Operational Events and Incidents	Activada	Sistema	Semanal	13/10/23 22:00	6/10/23 22:00
☐	DLP Send Email for Operational Events and Incidents	Activada	Sistema	Diaria	12/10/23 15:00	12/10/23 14:00
☐	DLP Set Reviewer for Operational Events and Incidents	Activada	Sistema	Diaria	12/10/23 15:00	12/10/23 14:00
☐	REPORTE DE ANTIVIRUS	Activada	Usuario	Mensual	6/11/23 9:00	2/10/23 9:00
☐	REPORTE ANTIVIRUS 3	Activada	Usuario	Mensual	6/11/23 10:00	2/10/23 10:00
☐	REPORTE ANTIVIRUS 4	Activada	Usuario	Semanal	13/10/23 9:19	12/10/23 9:19
☐	Equipos sin agente de McAfee	Activada	Usuario	Semanal	16/10/23 9:00	9/10/23 9:00
☐	Envío Reporte "Estado de Herramientas Implementadas"	Activada	Usuario	Diaria	13/10/23 8:00	12/10/23 8:00
☐	LdapSync: Sync across users from LDAP	Activada	Sistema	Diaria	12/10/23 16:00	12/10/23 8:00
☐	ePO Database Index Maintenance	Activada	Sistema	Semanal	15/10/23 4:00	8/10/23 4:00
☐	Download Software Product List	Activada	Usuario	Diaria	13/10/23 1:28	12/10/23 1:28
☐	DLP delete systems that were removed from ePO system tree	Activada	Sistema	Semanal	13/10/23 4:00	6/10/23 4:00
☐	DLP purge evidences	Activada	Sistema	Semanal	14/10/23 4:00	7/10/23 4:00
☐	DLP events conversion 9.4 and above	Activada	Sistema	Diaria	12/10/23 22:00	11/10/23 22:00
☐	EUA Analyze Environment	Activada	Usuario	Semanal	14/10/23 1:08	8/10/23 1:08

☐	EUA Download XML	Activada	Usuario	Semanal	14/10/23 1:11	8/10/23 1:11
☐	Detect Discovery Servers	Activada	Sistema	Avanzada	12/10/23 14:50	La tarea no se ha ejecutado nunca
☐	Actualizar repositorio principal	Activada	Usuario	Diaria	13/10/23 0:00	12/10/23 0:00
☐	ENS	Activada	Usuario	Diaria	13/10/23 0:00	12/10/23 0:00
☐	DLP Sync event users from LDAP	Activada	Sistema	Diaria	13/10/23 0:00	12/10/23 0:00
☐	Trellix Endpoint: Alert Policies Not Synced Task	Activada	Sistema	Avanzada	12/10/23 14:55	12/10/23 13:55
☐	Trellix Endpoint Update Task	Activada	Sistema	Diaria	13/10/23 2:34	12/10/23 2:34
☐	Manage DXL Breakers	Activada	Sistema	Diaria	13/10/23 0:00	12/10/23 0:00
☐	Send DXL Certificate Revocations	Activada	Sistema	Diaria	13/10/23 0:00	12/10/23 0:00
☐	Busqueda de equipos duplicados	Activada	Usuario	Semanal	14/10/23 9:00	9/10/23 9:00
☐	Disaster Recovery Snapshot Server	Desactivada	Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca
☐	Send DXL State Event	Desactivada	Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca
☐	Case Migration from DLP 10.0	Desactivada	Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca
☐	DLP Import Skyhigh Security Cloud Evidences	Desactivada	Sistema	Avanzada	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca
☐	Endpoint Security Firewall Property Translator	Desactivada	Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca
☐	Eliminar equipos inactivos	Desactivada	Usuario	Semanal	Ninguna hora de próxima ejecución	1/05/23 1:00
☐	DLP incident migration from 9.3.x to 9.4.100 and above	Desactivada	Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca

Imagen 7. Tareas de servidor activas

En la revisión efectuada sobre las tareas de servidor, se evidencian **4** tareas con errores que impiden su ejecución. No obstante, también se evidencian algunas otras tareas las cuales no poseen ningún error en su ejecución. A continuación, la evidencia de lo descrito:

Detalles de tarea servidor	
Nombre:	Generate Records for Trellix Agent Compliance History Reporting
Notas:	This default task stores the results of the "Trellix Agent Compliance Summary" query for use in reporting on compliance history.
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 23/03/16 Fecha de finalización: Sin fecha de finalización Hora planificada: Semanal Domingo a las 1:00 Hora de próxima ejecución: 15/10/23 1:00 22/10/23 1:00 29/10/23 1:00
Acciones:	1. Ejecutar consulta Nombre de consulta: Resumen de conformidad de McAfee Agent, Idioma: Inglés 1.1 Generar evento de conformidad Si el elemento sujeto a conformidad es un sistema gestionado, generar un evento de notificación cuando el porcentaje de sistemas no conformes llegue a: 20%

Imagen 8. Tarea de servidor 1 sin errores

Detalles de tarea servidor	
Nombre:	Deployment Agent
Notas:	No hay notas disponibles
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	<p>Fecha de inicio: 29/03/16</p> <p>Fecha de finalización: Sin fecha de finalización</p> <p>Hora planificada: Cada hora cada 4 horas pasados 00 minutos de la hora</p> <p>Hora de próxima ejecución: 12/10/23 16:00 12/10/23 20:00 13/10/23 0:00</p>

Acciones:	1. Ejecutar consulta Nombre de consulta: Sistemas no gestionados , Idioma: Inglés
	1.1 Desplegar Trellix Agent Versión de agente: Trellix Agent for Windows 5.8.0.161 (Actual) Instalar solo en sistemas que todavía no tienen un agente gestionado por este servidor de Trellix ePO: falso Forzar instalación sobre versión existente: verdadero Ruta de instalación: <PROGRAM_FILES_DIR>\McAfee\Commen Framework Dominio: SIC.LOCAL Nombre de usuario: administrador Número de intentos: Continuos Intervalo entre reintentos: 30 seconds Cancelar después de: 5 minutes Insertar agente mediante: Todos los controladores de agentes

Imagen 9. Tarea de servidor 2 sin errores

Detalles de tarea servidor	
Nombre:	DLP Purge History of Operational Events and Incidents
Notas:	Runs the purge task
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 24/08/16 Fecha de finalización: Sin fecha de finalización Hora planificada: Semanal Viernes a las 22:00 Hora de próxima ejecución: 13/10/23 22:00 20/10/23 22:00 27/10/23 22:00
Acciones:	1. Ejecutor de tareas de eventos (Purgar) No se ha definido ninguna regla

Imagen 10. Tarea de servidor 3 sin errores

Detalles de tarea servidor	
Nombre:	DLP Send Email for Operational Events and Incidents
Notas:	Runs the send email task
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 24/08/16 Fecha de finalización: Sin fecha de finalización Hora planificada: Diaria entre 0:00 y 23:59, con repetición cada 1 horas Hora de próxima ejecución: 12/10/23 15:00 12/10/23 16:00 12/10/23 17:00
Acciones:	1. Ejecutor de tareas de eventos (Notificación de correo automática) No se ha definido ninguna regla

Imagen 11. Tarea de servidor 4 sin errores

Detalles de tarea servidor	
Nombre:	DLP Set Reviewer for Operational Events and Incidents
Notas:	Runs the set reviewer task
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 24/08/16 Fecha de finalización: Sin fecha de finalización Hora planificada: Diaria entre 0:00 y 23:59, con repetición cada 1 horas Hora de próxima ejecución: 12/10/23 15:00 12/10/23 16:00 12/10/23 17:00
Acciones:	1. Ejecutor de tareas de eventos (Definir revisor) No se ha definido ninguna regla

Imagen 12. Tarea de servidor 5 sin errores

Detalles de tarea servidor	
Nombre:	REPORTE DE ANTIVIRUS
Notas:	No hay notas disponibles
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 24/08/16 Fecha de finalización: Sin fecha de finalización Hora planificada: Mensual 1.º Lunes a las 9:00 Hora de próxima ejecución: 6/11/23 9:00 4/12/23 9:00 1/01/24 9:00

Acciones:	1. Ejecutar consulta
	Nombre de consulta: Consulta no válida
	1.1 Enviar archivo por correo electrónico
	Destinatarios: dc.dba@sic.gov.co
	Cco:
	Asunto: 10 principales amenazas detectadas
	Formato: PDF
	Exportar: Datos de gráfico y tablas de acceso a información detallada
	Tamaño: Carta USA
	Orientación: Vertical

Imagen 13. Tarea de servidor 6 con errores

Detalles de tarea servidor	
Nombre:	REPORTE ANTIVIRUS 3
Notas:	No hay notas disponibles.
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	<p>Fecha de inicio: 24/08/16</p> <p>Fecha de finalización: Sin fecha de finalización</p> <p>Hora planificada: Mensual 1.º Lunes a las 10:00</p> <p>Hora de próxima ejecución: 6/11/23 10:00 4/12/23 10:00 1/01/24 10:00</p>

Acciones:	1. Ejecutar consulta
	Nombre de consulta: Consulta no válida
	1.1 Enviar archivo por correo electrónico
	Destinatarios: dc.dba@sic.gov.co
	Cco:
	Asunto: Los 10 usuarios con más detecciones
	Formato: PDF
	Exportar: Datos de gráfico y tablas de acceso a información detallada
	Tamaño: Carta USA
	Orientación: Vertical

Imagen 14. Tarea de servidor 7 con errores

Detalles de tarea servidor	
Nombre:	REPORTE ANTIVIRUS 4
Notas:	No hay notas disponibles
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 24/08/16 Fecha de finalización: Sin fecha de finalización Hora planificada: Semanal Días entre semana a las 9:19 Hora de próxima ejecución: 13/10/23 9:19 16/10/23 9:19 17/10/23 9:19

Acciones:	1. Ejecutar consulta Nombre de consulta: Consulta no válida 1.1 Enviar archivo por correo electrónico Destinatarios: dc.dba@sic.gov.co Cco: Asunto: Resumen de comunicaciones del agente Formato: PDF Exportar: Datos de gráfico y tablas de acceso a información detallada Tamaño: Carta USA Orientación: Vertical
-----------	--

Imagen 15. Tarea de servidor 8 con errores

Nombre:	Equipos sin agente de McAfee
Notas:	No hay notas disponibles
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 10/11/16 Fecha de finalización: Sin fecha de finalización Hora planificada: Semanal Lunes a las 9:00 Hora de próxima ejecución: 16/10/23 9:00 23/10/23 9:00 30/10/23 9:00

Acciones:	1. Ejecutar consulta Nombre de consulta: Consulta no válida 1.1 Enviar archivo por correo electrónico Destinatarios: dc.dba@sic.gov.co Cco: Asunto: Equipos sin agente de McAfee Formato: PDF Exportar: Datos de gráfico y tablas de acceso a información detallada Tamaño: Carta USA Orientación: Vertical
------------------	---

Imagen 16. Tarea de servidor 9 con errores

Detalles de tarea servidor	
Nombre:	Envío Reporte "Estado de Herramientas Implementadas"
Notas:	No hay notas disponibles
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 22/06/17 Fecha de finalización: Sin fecha de finalización Hora planificada: Diaria a las 8:00 Hora de próxima ejecución: 13/10/23 8:00 14/10/23 8:00 15/10/23 8:00
Acciones:	1. Ejecutar informe Resumen de informe para Estado de Herramientas Implementadas , Idioma: Español 1.1 Enviar archivo por correo electrónico Destinatarios: dc.dba@sic.gov.co Cco: Asunto: Reporte Estado de Herramientas Implementadas Formato: Exportar:

Imagen 17. Tarea de servidor 10 sin errores

Detalles de tarea servidor	
Nombre:	LdapSync: Sync across users from LDAP
Notas:	Syncs users from an LDAP server to the database.
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	<p>Fecha de inicio: 31/07/19</p> <p>Fecha de finalización: Sin fecha de finalización</p> <p>Hora planificada: Diaria entre 0:00 y 23:59, con repetición cada 8 horas</p> <p>Hora de próxima ejecución: 12/10/23 16:00 13/10/23 0:00 13/10/23 8:00</p>
Acciones:	<p>1. LdapSync: sincronizar los usuarios de LDAP</p> <p>[] se sincronizará con la planificación deseada.</p>

Imagen 18. Tarea de servidor 11 sin errores

Detalles de tarea servidor	
Nombre:	ePO Database Index Maintenance
Notas:	ePO Database Index Maintenance and statistics update
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	<p>Fecha de inicio: 31/07/19</p> <p>Fecha de finalización: Sin fecha de finalización</p> <p>Hora planificada: Semanal Domingo a las 4:00</p> <p>Hora de próxima ejecución: 15/10/23 4:00 22/10/23 4:00 29/10/23 4:00</p>
Acciones:	<p>1. Mantenimiento de índice de base de datos de ePO</p> <p>Esta tarea no requiere ninguna configuración.</p>

Imagen 19. Tarea de servidor 12 sin errores

Detalles de tarea servidor	
Nombre:	Download Software Product List
Notas:	Downloads the list of software your license key has access to.
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 31/07/19 Fecha de finalización: Sin fecha de finalización Hora planificada: Diaria a las 1:28 Hora de próxima ejecución: 13/10/23 1:28 14/10/23 1:28 15/10/23 1:28
Acciones:	1. Descargar lista de productos de software Se va a descargar la lista de productos a los que tiene acceso la clave de licencia introducida.

Imagen 20. Tarea de servidor 13 sin errores

Detalles de tarea servidor	
Nombre:	DLP delete systems that were removed from ePO system tree
Notas:	Deletes DLP system information and user session information for systems that were removed from ePO system tree
Propietario de tarea:	system
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 23/02/23 Fecha de finalización: Sin fecha de finalización Hora planificada: Semanal Viernes a las 4:00 Hora de próxima ejecución: 13/10/23 4:00 20/10/23 4:00 27/10/23 4:00
Acciones:	1. Eliminar sistemas de DLP que se han quitado del árbol de sistemas de ePO

Imagen 21. Tarea de servidor 14 sin errores

Detalles de tarea servidor	
Nombre:	DLP purge evidences
Notas:	Delete evidence files that were marked for deletion. Recommended to run on weekly basis.
Propietario de tarea:	system
Estado de planificación:	Activada
Planificación:	<p>Fecha de inicio: 23/02/23</p> <p>Fecha de finalización: Sin fecha de finalización</p> <p>Hora planificada: Semanal Sábado a las 4:00</p> <p>Hora de próxima ejecución: 14/10/23 4:00 21/10/23 4:00 28/10/23 4:00</p>
Acciones:	<p>1. Purgar pruebas de DLP</p> <p>Se ejecuta automáticamente</p>

Imagen 22. Tarea de servidor 15 sin errores

Detalles de tarea servidor	
Nombre:	DLP events conversion 9.4 and above
Notas:	This task converts operational events and incidents from 9.4 and above to the latest schema. Run this task once after upgrading from 9.4 and above
Propietario de tarea:	admin
Estado de planificación:	Activada
Planificación:	<p>Fecha de inicio: 23/02/23</p> <p>Fecha de finalización: Sin fecha de finalización</p> <p>Hora planificada: Diaria a las 22:00</p> <p>Hora de próxima ejecución: 12/10/23 22:00 13/10/23 22:00 14/10/23 22:00</p>
Acciones:	<p>1. Migración de eventos de incidentes de DLP de una versión anterior desde la 9.4 a la versión actual</p>

Imagen 23. Tarea de servidor 16 sin errores

Detalles de tarea servidor	
Nombre:	EUA Analyze Environment
Notas:	Analyzes the environment to determine what percentage is ready to upgrade to McAfee Endpoint Security using the Endpoint Upgrade Assistant extension.
Propietario de tarea:	sec (Monitoreo SOC)
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 23/02/23 Fecha de finalización: Sin fecha de finalización Hora planificada: Semanal Fin de semana a las 1:08 Hora de próxima ejecución: 14/10/23 1:08 15/10/23 1:08 21/10/23 1:08
Acciones:	1. Analizar sistemas para la ampliación a ENS Analiza el entorno para determinar qué porcentaje está preparado para la ampliación a McAfee Endpoint Security mediante la extensión Endpoint Upgrade Assistant.

Imagen 24. Tarea de servidor 17 sin errores

Detalles de tarea servidor	
Nombre:	EUA Download XML
Notas:	Downloads an xml file containing the latest McAfee Endpoint Security product information for the Endpoint Upgrade Assistant extension.
Propietario de tarea:	sec (Monitoreo SOC)
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 23/02/23 Fecha de finalización: Sin fecha de finalización Hora planificada: Semanal Fin de semana a las 1:11 Hora de próxima ejecución: 14/10/23 1:11 15/10/23 1:11 21/10/23 1:11
Acciones:	1. Descargar archivo XML para EUA Descarga un archivo XML que contiene la información de producto más reciente sobre McAfee Endpoint Security para la extensión Endpoint Upgrade Assistant.

Imagen 25. Tarea de servidor 18 sin errores

Detalles de tarea servidor	
Nombre:	Detect Discovery Servers
Notas:	Detects newly installed discovery servers and enabled them to run discovery scans
Propietario de tarea:	admin
Estado de planificación:	No válida
Planificación:	Fecha de inicio: 23/02/23 Fecha de finalización: Sin fecha de finalización Hora planificada: Avanzada sintaxis cron: 0 0/10 * * * ? Hora de próxima ejecución: 12/10/23 15:10:00 12/10/23 15:20:00 12/10/23 15:30:00
Acciones:	1. Detectar servidores de descubrimiento
Errores de validación:	Esta tarea no se puede ejecutar ni editar por estas razones: • El usuario no está autorizado a ejecutar el comando "Detectar servidores de descubrimiento"

Imagen 26. Tarea de servidor 19 sin errores

Detalles de tarea servidor	
Nombre:	Actualizar repositorio principal
Notas:	No hay notas disponibles
Propietario de tarea:	sec (Monitoreo SOC)
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 2/03/23 Fecha de finalización: Sin fecha de finalización Hora planificada: Diaria a las 0:00 Hora de próxima ejecución: 13/10/23 0:00 14/10/23 0:00 15/10/23 0:00
Acciones:	1. Extracción de repositorio Sitio de origen: TrellixHttp Rama: Actual Mover el paquete existente a la rama Anterior: Falso Seleccionar paquetes: Todos los paquetes

Imagen 27. Tarea de servidor 20 sin errores

Detalles de tarea servidor	
Nombre:	ENS
Notas:	No hay notas disponibles
Propietario de tarea:	sec (MonitoreoSOC)
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 31/05/23 Fecha de finalización: Sin fecha de finalización Hora planificada: Diaria a las 0:00 Hora de próxima ejecución: 13/10/23 0:00 14/10/23 0:00 15/10/23 0:00
Acciones:	1. Migrar a Endpoint Security Solamente para uso por parte de la tarea de migración de Endpoint Security.

Imagen 28. Tarea de servidor 21 sin errores

Detalles de tarea servidor	
Nombre:	DLP Sync event users from LDAP
Notas:	Sync event user information from LDAP servers registered on ePO
Propietario de tarea:	sec (MonitoreoSOC)
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 24/09/23 Fecha de finalización: Sin fecha de finalización Hora planificada: Diaria entre 0:00 y 3:59, con repetición cada 1 horas Hora de próxima ejecución: 13/10/23 0:00 13/10/23 1:00 13/10/23 2:00
Acciones:	1. Sincronizar los usuarios de eventos desde LDAP de DLP Sincronizar los usuarios de eventos desde LDAP de DLP

Imagen 29. Tarea de servidor 22 sin errores

Detalles de tarea servidor	
Nombre:	Trellix Endpoint: Alert Policies Not Synched Task
Notas:	Adds, updates or removes the message center alert which warns about Trellix Endpoint policy settings not being synched on endpoints
Propietario de tarea:	sec (MonitoreoSOC)
Estado de planificación:	Activada
Planificación:	<p>Fecha de inicio: 24/09/23</p> <p>Fecha de finalización: Sin fecha de finalización</p> <p>Hora planificada: Avanzada sintaxis cron: 0 55 * * * ?</p> <p>Hora de próxima ejecución: 12/10/23 15:55:00 12/10/23 16:55:00 12/10/23 17:55:00</p>
Acciones:	<p>1. Directivas de alerta de Trellix Endpoint no sincronizadas</p> <p>No hay ninguna configuración para este comando</p>

Imagen 30. Tarea de servidor 23 sin errores

Detalles de tarea servidor	
Nombre:	Trellix Endpoint Update Task
Notas:	Check for new updates to Trellix Endpoint
Propietario de tarea:	sec (MonitoreoSOC)
Estado de planificación:	Activada
Planificación:	<p>Fecha de inicio: 24/09/23</p> <p>Fecha de finalización: Sin fecha de finalización</p> <p>Hora planificada: Diaria a las 2:34</p> <p>Hora de próxima ejecución: 13/10/23 2:34 14/10/23 2:34 15/10/23 2:34</p>
Acciones:	<p>1. Actualización de Trellix Endpoint</p> <p>There is no configuration for this command</p>

Imagen 31. Tarea de servidor 24 sin errores

Detalles de tarea servidor	
Nombre:	Manage DXL Brokers
Notas:	Evaluate each system against the DXLBROKER tag criteria and update DXL Broker Policies
Propietario de tarea:	sec (Monitoreo SOC)
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 24/09/23 Fecha de finalización: Sin fecha de finalización Hora planificada: Diaria a las 0:00 Hora de próxima ejecución: 13/10/23 0:00 14/10/23 0:00 15/10/23 0:00
Acciones:	1. Gestionar Brókers de DXL Esta tarea asignará la etiqueta DXLBROKER a todos los Brókers de DXL completamente configurados y actualizará las directivas.

Imagen 32. Tarea de servidor 25 sin errores

Detalles de tarea servidor	
Nombre:	Send DXL Certificate Revocations
Notas:	Sends the full list of certificates revoked by the administrator. This task should be run after every new broker deployment.
Propietario de tarea:	sec (Monitoreo SOC)
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 24/09/23 Fecha de finalización: Sin fecha de finalización Hora planificada: Diaria a las 0:00 Hora de próxima ejecución: 13/10/23 0:00 14/10/23 0:00 15/10/23 0:00
Acciones:	1. Enviar revocaciones de certificados de DXL Enviar las revocaciones

Imagen 33. Tarea de servidor 26 sin errores

Detalles de tarea servidor	
Nombre:	Busqueda de equipos duplicados
Notas:	No hay notas disponibles
Propietario de tarea:	soc (Monitoreo SOC)
Estado de planificación:	Activada
Planificación:	Fecha de inicio: 6/10/23 Fecha de finalización: Sin fecha de finalización Hora planificada: Semanal Sábado a las 9:00 Hora de próxima ejecución: 14/10/23 9:00 21/10/23 9:00 28/10/23 9:00
Acciones:	1. Exportar consultas Nombre de consulta: Nombres de sistemas duplicados , Idioma: Español 1.1 Enviar archivo por correo electrónico Destinatarios: soc@sic.gov.co Cco: Asunto: Equipos Duplicados Formato: CSV Exportar: Datos de gráfico y tablas de acceso a información detallada

Imagen 34. Tarea de servidor 27 sin errores

Dentro de las tareas de servidor se observan algunas tareas que se encuentran desactivadas y las cuales pueden proporcionar un mejor aprovechamiento de las capacidades de la consola ePO, a continuación, se muestran las tareas de servidor que se encuentran desactivadas:

☐	Nombre	Estado	▼	Tipo	Planificación	Próxima ejecución	Última ejecución	Acciones
☐	Send DDL State Event	Desactivada		Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Eliminar equipos inactivos	Desactivada		Usuario	Semanal	Ninguna hora de próxima ejecución	1/05/23 1:00	Ver Editar Ejecutar
☐	DLP Import Skyhigh Security Cloud Evidences	Desactivada		Sistema	Avanzada	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Case Migration from DLP 10.0	Desactivada		Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Endpoint Security Firewall Property Translator	Desactivada		Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	NSP: Dashboard Data Updating Task	Desactivada		Usuario	Avanzada	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	DLP Import MVision Cloud Events	Desactivada		Sistema	Avanzada	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	DLP operational events migration from 9.3.x to 9.4.100 and above	Desactivada		Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	DLP Incident migration from 9.3.x to 9.4.100 and above	Desactivada		Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Migrate Data to New Tables	Desactivada		Sistema	Semanal	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Purge Threat and Client Events Older than 90 Days	Desactivada		Usuario	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Endpoint Security Migration	Desactivada		Sistema	Manual	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	VSE: Compliance Over the Last 30 Days	Desactivada		Usuario	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	DLP Policy Conversion	Desactivada		Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Roll Up Data (Local ePO Server)	Desactivada		Usuario	Semanal	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Synchronize Shared Tasks	Desactivada		Usuario	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Synchronize Shared Policies	Desactivada		Usuario	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar

☐	Duplicate Agent GUID - clear error count	Desactivada	Usuario	Semanal	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Duplicate Agent GUID - remove systems with potentially duplicate	Desactivada	Usuario	Semanal	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Disaster Recovery Snapshot Server	Desactivada	Sistema	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	RSD: Update Sensor Deployment Client Tasks	No válida	Usuario	Maneja	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	RSD: Default Delete Detected Systems Task	No válida	Usuario	Diaria	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	VSE: DAT Adoption Over the Last 24 Hours	Desactivada	Usuario	Avanzada	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar
☐	Inactive Agent Cleanup Task	Desactivada	Usuario	Semanal	Ninguna hora de próxima ejecución	La tarea no se ha ejecutado nunca	Ver Editar Ejecutar

Imagen 35. Tareas de servidor desactivadas

La consola de administración centralizada de McAfee, cuenta con un sistema para responder de forma automática al generarse algún evento definido por el administrador, esta facultad se conoce como **respuestas automáticas**; actualmente las respuestas automáticas se encuentran desactivadas como se muestra en la imagen

Respuestas automáticas					
Valor predefinido: Todas		Búsqueda rápida:	<input type="text"/>	<input type="button" value="Aplicar"/>	<input type="button" value="Borrar"/>
			Mostrar filas seleccionadas		
☐	Nombre	Estado	Categoría de evento	Tipo de evento	Acciones
☐	Master Repository Update failed	Activada	Eventos de notificación de ePO	Servidor	Ver Editar Duplicar
☐	Software Manager new product update available	Desactivada	Eventos de notificación de ePO	Servidor	Ver Editar Duplicar
☐	Non-compliant computer detected	Desactivada	Eventos de notificación de ePO	Servidor	Ver Editar Duplicar
☐	Distributed Repository Replication failed	Desactivada	Eventos de notificación de ePO	Servidor	Ver Editar Duplicar
☐	Malware detected and not handled	Desactivada	Eventos de notificación de ePO	Amenaza	Ver Editar Duplicar
☐	Master Repository Update succeeded	Desactivada	Eventos de notificación de ePO	Servidor	Ver Editar Duplicar
☐	Send Threat Event via DXL	Desactivada	Eventos de notificación de ePO	Amenaza	Ver Editar Duplicar
☐	RSD: Query Nav Rogue Detection	No válida		rsdAddDetectedSystemEvent	Ver Editar Duplicar

Imagen 36. Respuestas automáticas

Para la administración de la consola ePO se está destinado un conjunto de usuarios, algunos usuarios tienen asignado los privilegios de Global reviewer, Admin y algunos otros usuarios se encuentran desactivados de la herramienta; los usuarios creados para la administración de la consola son:



Imagen 37. Usuarios de administración

En la configuración de la consola ePO se evidencia, la configuración de los métodos de conexión con los agentes de Trellix instalados en los equipos de la entidad, los puertos de comunicación por medio de los cuales la consola lleva a cabo la comunicación con los agentes instalados y la configuración del servidor del correo electrónico; este último se utiliza para el envío de reportes básicos de la consola ePO de manera automática a los destinatarios elegidos por el administrador de la herramienta, en las siguientes imágenes se puede observar las configuraciones antes mencionadas:



Imagen 38. Métodos de conexión con Trellix Agent

Puerto de comunicación agente-servidor:	8000
Puerto seguro de comunicación agente-servidor:	Activado en puerto 443
Puerto de comunicación de activación de agente:	9081
Puerto de comunicación de difusión de agente:	9082
Puerto de comunicación consola-servidor de aplicaciones:	9443
Puerto de comunicación cliente-servidor autenticada:	8444

Imagen 39. Puertos de Comunicación

Nombre del servidor SMTP:	10.20.100.70
Puerto del servidor SMTP:	25
Cifrado de correo electrónico (compatibilidad con TLS):	Disabled
Nombre de usuario:	
Dirección del remitente:	soc@sic.gov.co
Correo electrónico de prueba:	Destinatario: <input type="text"/> <input type="button" value="Probar"/>

Imagen 40. Configuración servidor de correo

En el módulo de servidores registrados se encuentran las conexiones seguras con otras aplicaciones, que mejoran el funcionamiento y los procedimientos de la consola ePO; entre los que se encuentra la lectura de los usuarios pertenecientes al dominio de la entidad o el envío de información para el monitoreo de la aplicación. Estas configuraciones se muestran en seguida:

Servidores registrados

Generador de servidores registrados		1 Descripción	2 Detalles
Tipo de servidor LDAP:	Active Directory		
Nombre del servidor:	☐ Nombre de dominio: <input type="text"/> Usar un nombre de dominio DNS. ☒ Nombre del servidor: <input type="text" value="10.20.1.190"/> Usar un nombre de servidor o una dirección IP.		
Utilizar catálogo global:	☐		
Obtener referencias:	☐		
Utilizar SSL:	☐		
Nombre de usuario:	<input type="text" value="sic\usr_mcafee_dlp"/> Utilice dominio\nombre de usuario para las cuentas de Active Directory.		
Contraseña:	☐ Cambiar contraseña: Contraseña: <input type="text"/> Confirmar contraseña: <input type="text"/>		
Nombre de sitio:	<input type="text"/> <input type="button" value="Examinar"/>		

Imagen 41. Configuración conexión controlar de dominio

Servidores registrados

Generador de servidores registrados		1 Descripción	2 Detalles
El servidor de Trellix ePO registrado está disponible para la generación de informes de acumulación.			
Versión de Trellix ePO:	5.3		
Servidor de base de datos:	Nombre DNS <input type="text" value="srvepoprod"/>		
Instancia de SQL Server:	☒ Predeterminada ☐ Nombre de instancia: <input type="text"/>		
Nombre de base de datos:	<input type="text" value="ePO_SRVEPOPROD"/> (normalmente empieza por "ePO_")		
Puerto de base datos:	<input type="text" value="1433"/>		
Tipo de autenticación:	☐ Autenticación de Windows ☒ Autenticación de SQL		
Utilizar NTLMv2	☒		
Comunicación SSL con el servidor de base de datos:	<input type="text" value="Intentar utilizar SSL"/>		
Nombre de usuario:	<input type="text" value="sa"/> (para la autenticación de Windows: dominio\usuario)		

Contraseña:	☐ Cambiar contraseña Nueva contraseña: <input type="password"/> Confirmar contraseña: <input type="password"/>
Probar conexión:	<input type="button" value="Probar conexión"/>
Uso compartido de directivas:	☐ Activar ☒ Desactivar
Uso compartido de tareas cliente:	☐ Activar ☒ Desactivar
Transferir sistemas:	☐ Activar Para transferir correctamente un sistema, antes debe importar al servidor remoto la clave agente-servidor que utiliza dicho sistema. ☒ Importación automática de Sitelist ☐ Importación manual de Sitelist: <input type="button" value="Examinar..."/> No se ha seleccionado ningún archivo. ☒ Desactivar

Imagen 42. Configuración servidor de monitoreo

A continuación, se muestra el estado actual de cada uno de los productos Trellix gestionados por la consola ePO

4.2.1 Trellix Agent

La herramienta Trellix Agent, es el medio por el cual la consola ePO administra los productos de Trellix instalados en los equipos cliente de la entidad, por medio de este, se lleva a cabo la actualización de las diferentes tareas o directivas implementadas para la organización desde la consola de administración. Actualmente, en la entidad se observa un total de 1.422 equipos gestionados, divididos de la siguiente manera según la versión de esta herramienta:

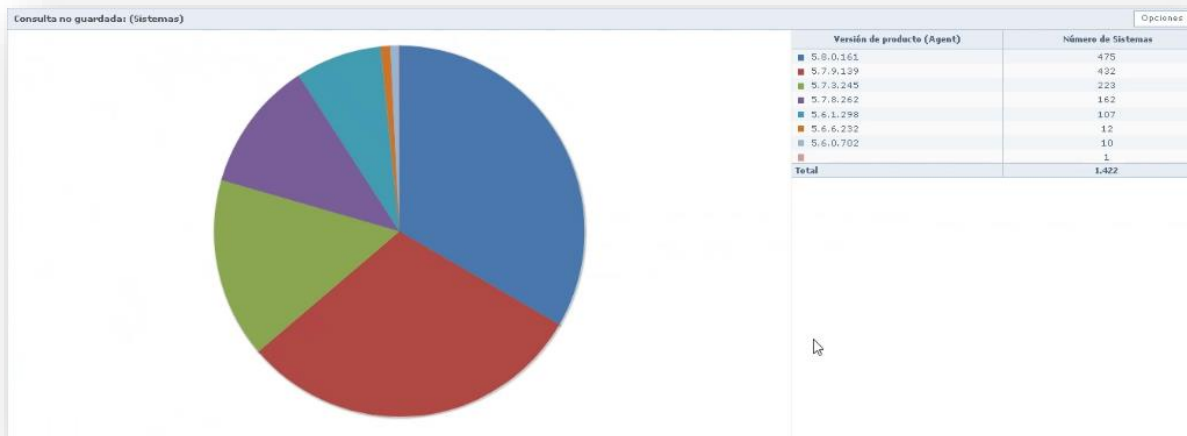


Imagen 43. Versiones McAfee Agent

De los equipos gestionados se puede evidenciar que un total de 586 equipos no se encuentran en estado de conformidad con la comunicación que se debe realizar con la consola ePO para la actualización de tareas, directivas y políticas, como se muestra en la siguiente gráfica:

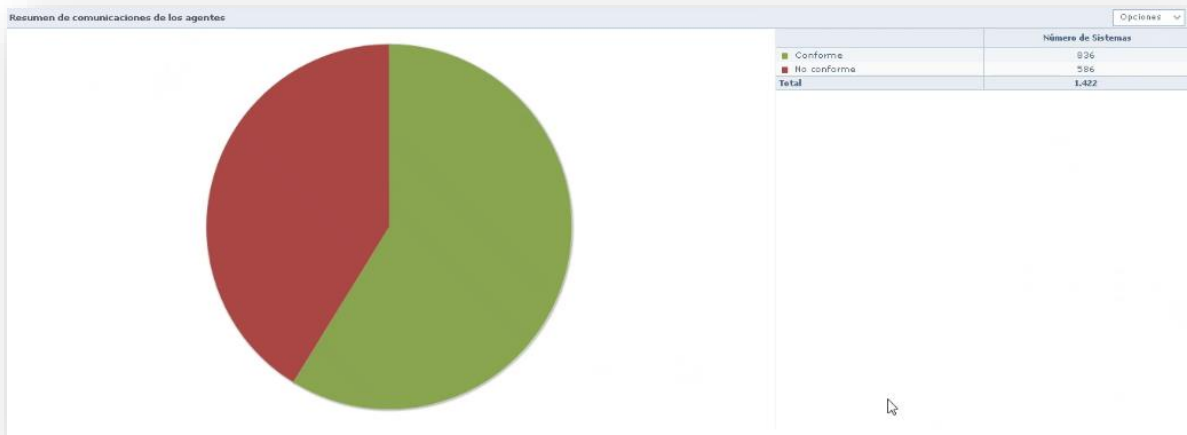


Imagen 44. Conformidad de McAfee Agent

Las directivas aplicadas sobre el agente de McAfee son:



Trellix Agent			
Buscar			
☐ Ocultar directivas no asignadas			
General			
Nombre	Asignaciones de reglas	Asignados a	Acciones
Large Organization Default	Ninguno	Ninguno	Ver
My Default	Ninguno	Mi organización	Editar
Trellix Default	Ninguno	Rafz global	Ver

Imagen 45. Directivas McAfee Agent categoría general

4.2.2 Endpoint Security (ENS)

Endpoint Security (ENS), es la nueva plataforma de protección para los equipos cliente, que ofrece un menor consumo de recurso con una mejor efectividad en la mitigación de amenazas; las tareas de instalación de este producto desde la consola ePO se componen de la instalación de 5 subproductos que son: Trellix Endpoint Security Platform, Trellix Endpoint Security Threat Prevention, Trellix Endpoint Security Adaptive Threat Protection, Trellix Endpoint Security Web Control y Trellix Endpoint Security Firewall.

De esta manera, se verifica las versiones y la cantidad de equipos de la entidad que actualmente tienen instalados estos productos de manera individual

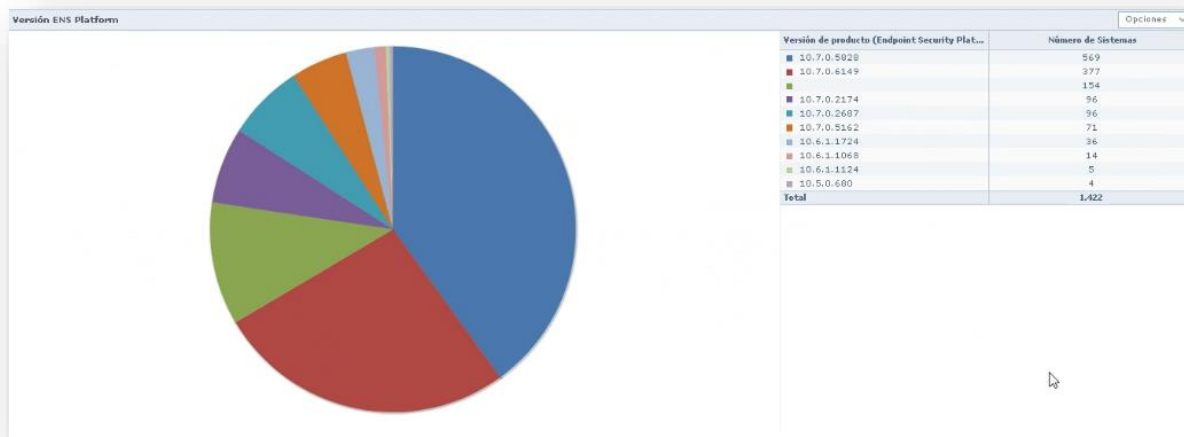


Imagen 46. Trellix Endpoint Security Platform

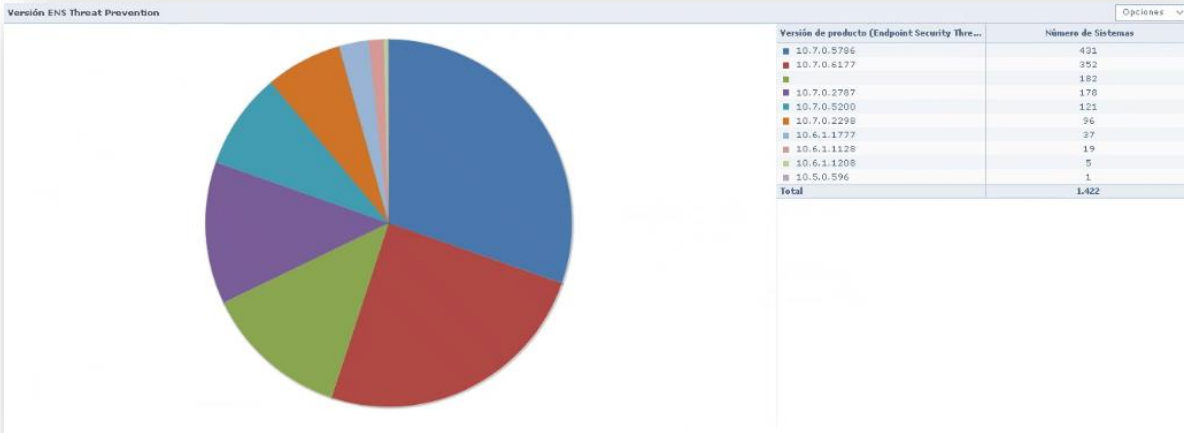


Imagen 47. Trellix Endpoint Security Threat Prevention

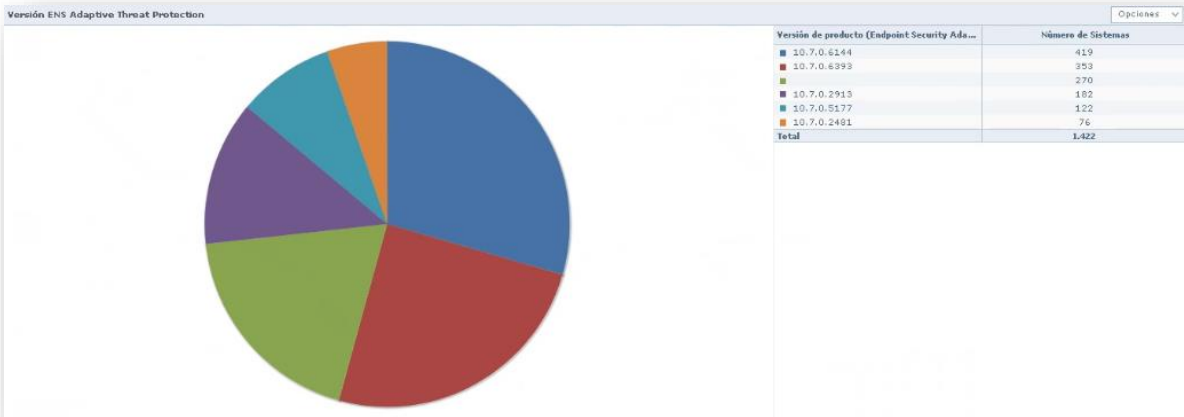


Imagen 48. Trellix Endpoint Security Adaptive Threat Protection

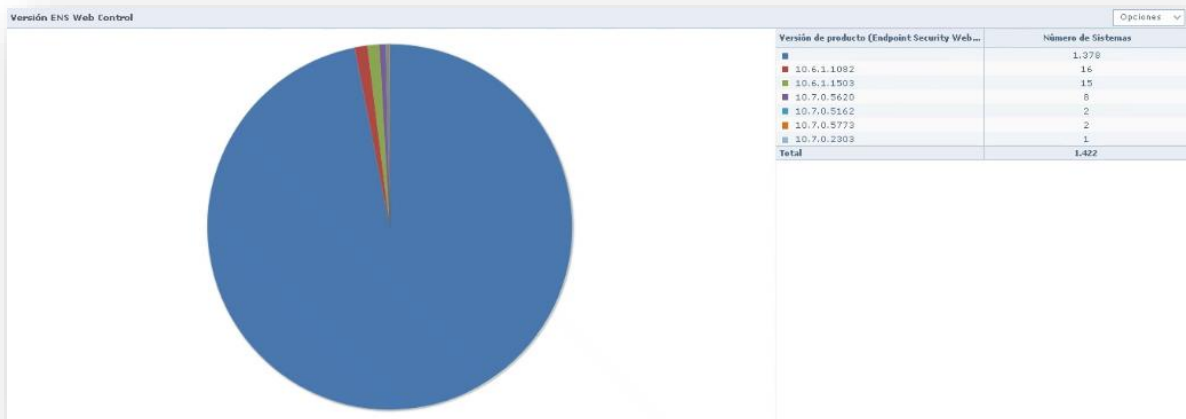


Imagen 49. Trellix Endpoint Security Web Control

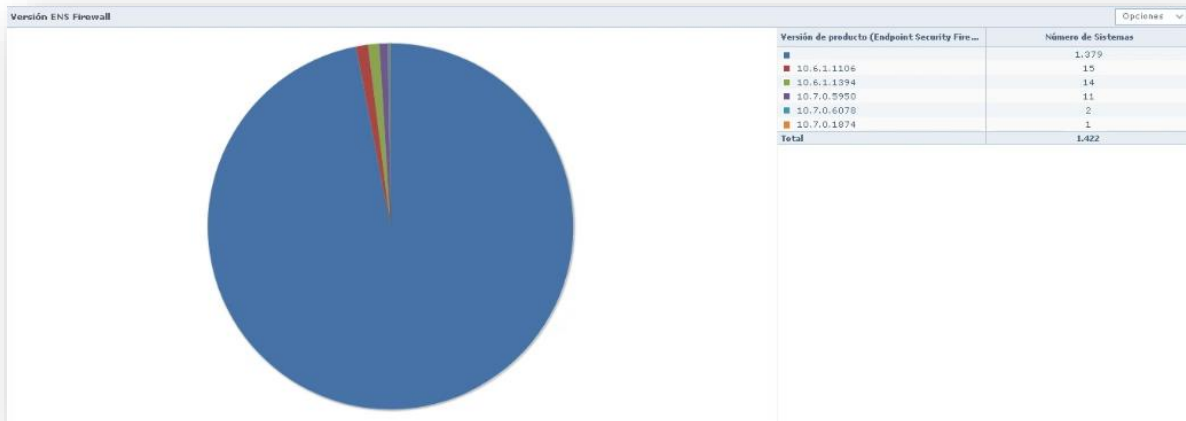


Imagen 50. Trellix Endpoint Security Firewall

De los equipos de la entidad que tienen instalados los productos de ENS, se puede evidenciar que el **32%** no están tomando las directivas correctamente, de esta forma están aplicando directivas antiguas

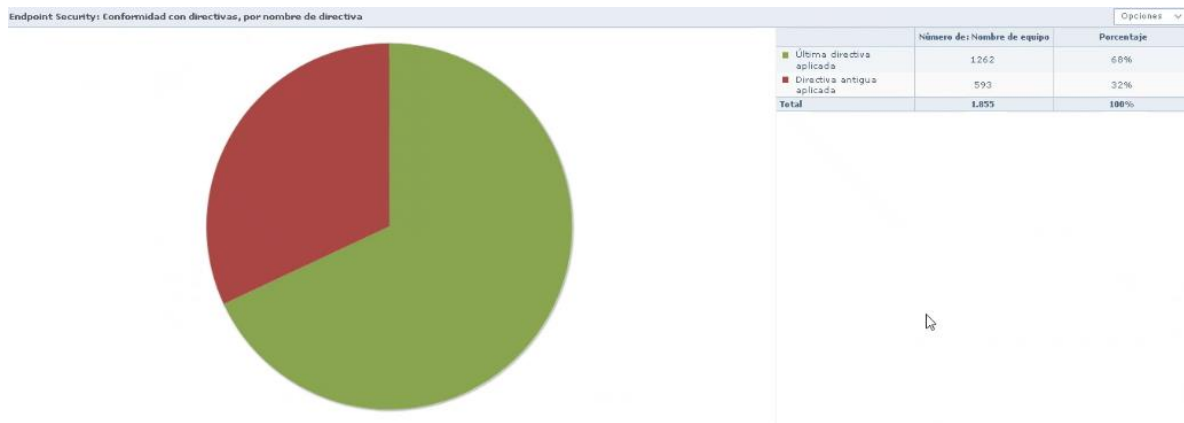


Imagen 51. Conformidad de directivas ENS

Por otro lado, la herramienta ENS debe tener habilitados algunos parámetros que proporcionen los mejores niveles de seguridad en los equipos de la entidad; se evalúa el estado actual de estos parámetros obteniendo resultados de inconformidad como se muestran en la siguiente imagen:

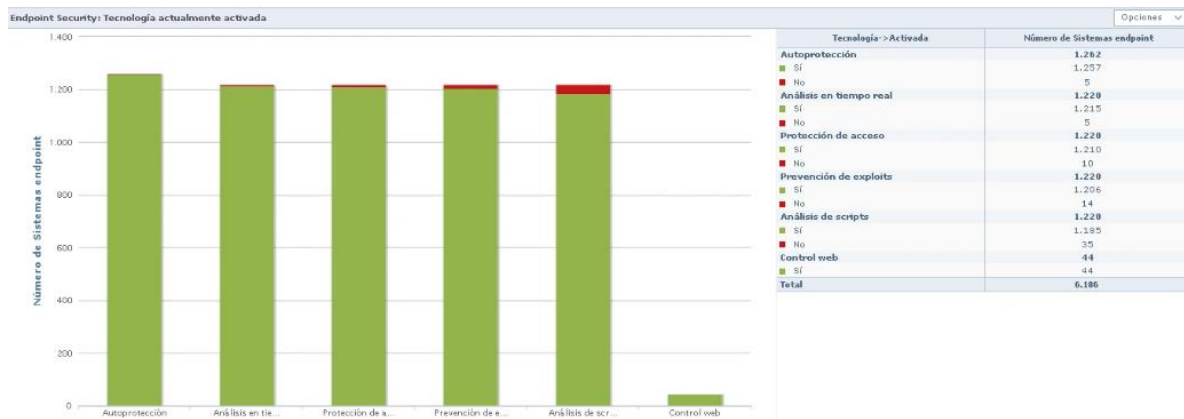


Imagen 52. Conformidad parámetros de ENS

Las directivas pertenecientes a los diferentes módulos de esta herramienta que están aplicando a los equipos de la entidad se relacionan a continuación:

Endpoint Security Common

Buscar

☐ Ocultar directivas no asignadas

Nueva directiva

Opciones

Nombre	Asignaciones de reglas	Asignados a	Acciones
Migrated_EGS_Product_Configuratio...	Ninguno	Ninguno	Editor
My Default	Ninguno	Mi organización	Editor
SIC	Ninguno	Ninguno	Editor
SIC-1	Ninguno	Ninguno	Editor
Test Server	Ninguno	Ninguno	Editor
Trellix Default	Ninguno	Raíz global	Ver

Imagen 53. Directiva ENS Common

Endpoint Security Threat Prevention

Buscar

☐
Ocultar directivas no asignadas

Nueva directiva

▼

Análisis en tiempo real

Nombre	Asignaciones de reglas	Asignados a	Acciones
Antivirus desactivado	Ninguno	Desactivar Antivirus	Editar ▼
Análisis en tiempo real para Exchange	Ninguno	Ninguno	Ver ▼
Disable_SIC	Ninguno	Disable_Endpoint,Disable_Endpoint_Linu...	Editar ▼
Exclusiones JAR	Ninguno	Tecnología	Editar ▼
My Default	Ninguno	Ninguno	Editar ▼
prueba	Ninguno	Ninguno	Editar ▼
PRUEBA2	Ninguno	Ninguno	Editar ▼
Ptojob	Ninguno	Ninguno	Editar ▼
RUBRIK	Ninguno	Servidores_SIPI_NUEVOS	Editar ▼
Servidores SIC	Ninguno	Escaneos Programados	Editar ▼
SIC	Ninguno	Mi organización	Editar ▼
SIC - DC	Ninguno	Controladores de Dominio	Editar ▼
SIC_ACSEPTO	Ninguno	Servidores_exclusionesACSEPTO	Editar ▼

SIC_ACSEPTO_SERVIDOR 0.63	Ninguno	Exclusiones_Especiales_ACSEPTO_63	Editar
SIC_SERVIDORES	Ninguno	Servidores	Editar
SIC_SIPI	Ninguno	Servidores_SIPI	Editar
SIPI	Ninguno	Ninguno	Editar
Trellix Default	Ninguno	Raíz global	Ver

Imagen 54. Directivas ENS análisis en tiempo real

Opciones			
Nombre	Asignaciones de reglas	Asignados a	Acciones
My Default	Ninguno	Ninguno	Editar ▼
SIC	Ninguno	Mi organización	Editar ▼
Trellix Default	Ninguno	Raíz global	Ver ▼

Imagen 55. Directivas ENS opciones

Prevención de exploit			
Nombre	Asignaciones de reglas	Asignados a	Acciones
Antivirus desactivado	Ninguno	Desactivar Antivirus,Disable_Endpoint_Li...	Editar ▼
disable_linux	Ninguno	Ninguno	Editar ▼
Exploit	Ninguno	Ninguno	Editar ▼
My Default	Ninguno	Ninguno	Editar ▼
Prueba	Ninguno	Disable_Endpoint	Editar ▼
Servidores SIC	Ninguno	Escaneos Programados	Editar ▼
SIC	Ninguno	Mi organización	Editar ▼
SIC -Server	Ninguno	Servidores	Editar ▼
Trellix Default	Ninguno	Raíz global	Ver ▼

Imagen 56. Directivas ENS prevención de exploit

Protección de acceso			
Nombre	Asignaciones de reglas	Asignados a	Acciones
.wory	Ninguno	Ninguno	Editar ▼
Antivirus desactivado	Ninguno	Desactivar Antivirus,Desactivar ENS	Editar ▼
Disable	Ninguno	Disable_Endpoint,Disable_Endpoint_Linux	Editar ▼
My Default	Ninguno	Ninguno	Editar ▼
Protección de acceso - SIC	Ninguno	Mi organización	Editar ▼
Protección de acceso - SIC - HASH	Ninguno	Ninguno	Editar ▼
Protección de acceso - SIC Server	Ninguno	Servidores,Servidores_exclusionesACSEP...	Editar ▼
Servidores SIC	Ninguno	Escaneos Programados	Editar ▼
SIC	Ninguno	Ninguno	Editar ▼
Trellix Default	Ninguno	Raíz global	Ver ▼

Imagen 57. Directivas ENS protección de acceso

4.2.3 Data Loss Prevention (DLP)

Actualmente, la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO cuenta con un total de 1.422 máquinas reportadas en la consola ePO en donde 1.306 máquinas no poseen instalado el producto Trellix DLP, por lo tanto, solo 116 máquinas están siendo gestionadas por el producto Data Loss Prevention como se puede observar a continuación

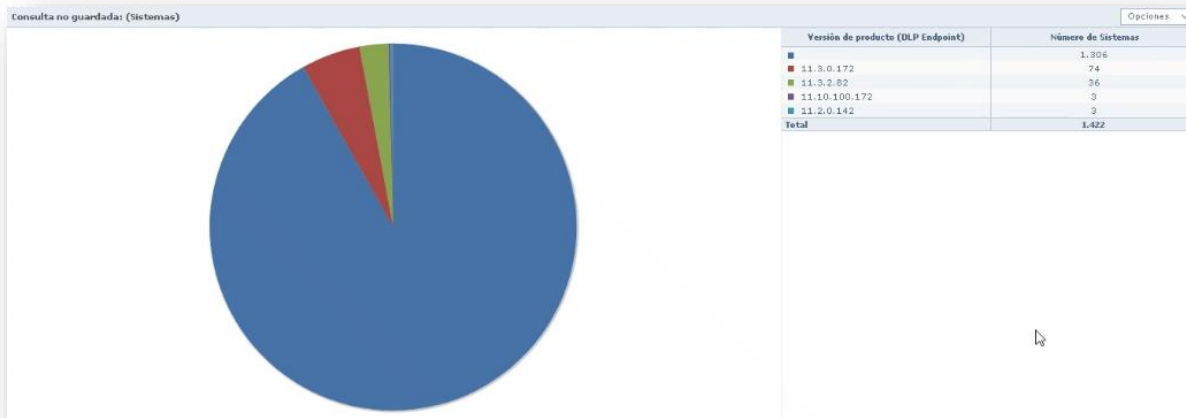


Imagen 58. Consultas e informes – Versiones DLP implementadas

Los módulos de control de dispositivos y protección de datos del producto Trellix DLP, se encuentran implementados en un total de 43 máquinas, es decir, que solo esta cantidad de equipos, están aplicando la reacción de monitoreo de datos y acciones realizadas por los usuarios de la SIC. Por otro lado, existen 73 equipos que no se encuentran aplicando ninguna de estas reglas.

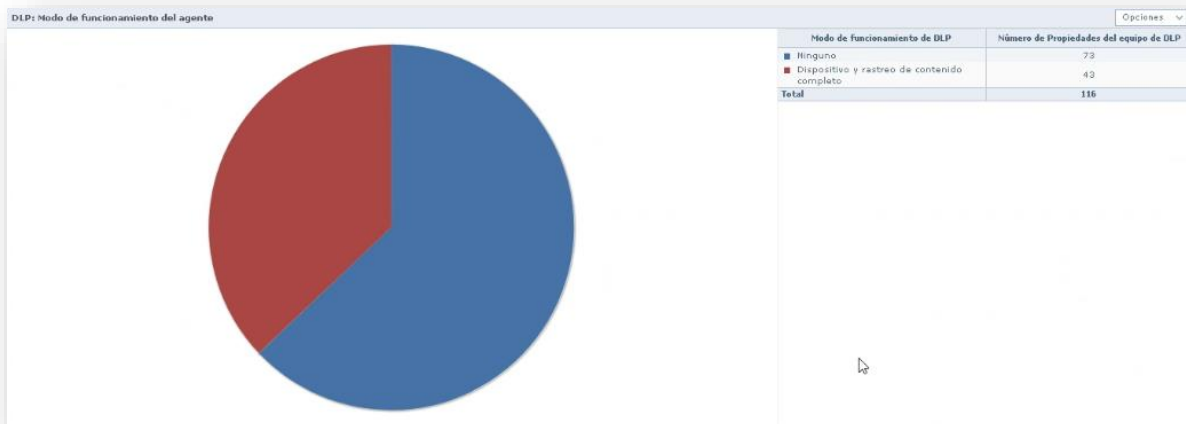


Imagen 59. Modo de funcionamiento del agente DLP

5. LOGS DE SEGURIDAD DE LA APLICACIÓN TRELLIX EPO

Es importante tener en cuenta que el servidor de la consola de administración Trellix ePolicy Orchestrator, en la cual, se logran administrar varios productos de seguridad en la entidad, incluyendo las políticas de protección de datos por medio del software Trellix DLP, debe tener una alta disponibilidad para un óptimo funcionamiento durante la ejecución de funciones de seguridad con la cual cumple cada herramienta Trellix.

Teniendo en cuenta que un funcionamiento adecuado del servidor donde se encuentra instalada la consola ePO de la entidad es necesario, se logra evidenciar lo siguiente a nivel de software y hardware

Servicios consola ePO:

Durante el mes de octubre, los 3 servicios de la consola ePO, los cuales son esenciales para el funcionamiento correcto de la herramienta, se encuentran operando satisfactoriamente



Imagen 60. Logs de seguridad de aplicación – McAfee ePolicy Orchestrator Services

Espacio en disco del servidor ePO:

Dentro de las revisiones efectuadas, se observa que el servidor aún cuenta con espacio en disco suficiente para un rendimiento óptimo de la consola Trellix ePolicy Orchestrator.

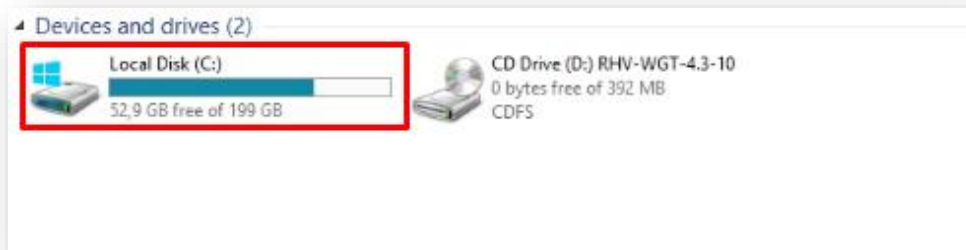
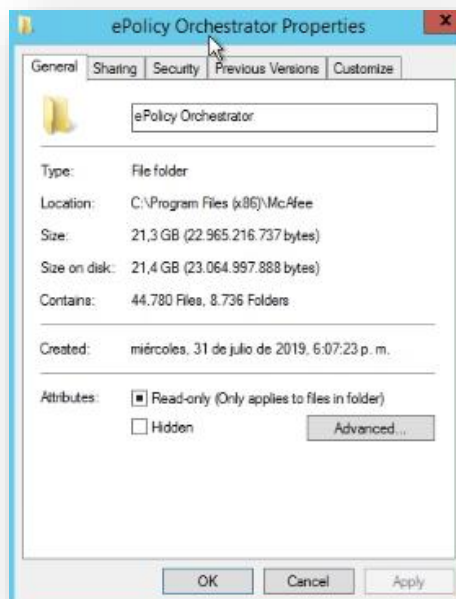


Imagen 61. Logs de seguridad de aplicación – Espacio en disco del servidor ePO

Tamaño de la carpeta de instalación de la consola ePO:

Actualmente, durante el mes de octubre de 2023, el tamaño con el cual cuenta la carpeta donde se encuentran instaladas las librerías, servicios y otra data perteneciente a la consola Trellix ePolicy Orchestrator es de 21.4gb.



Características del servidor de la consola ePO:

El servidor donde se encuentra instalada la consola cumple con las siguientes características las cuales cumplen con los requerimientos mínimos de acuerdo a la información establecida por el fabricante y la cual se puede comprobar en el siguiente enlace

[Product Documentation | Trellix](#)

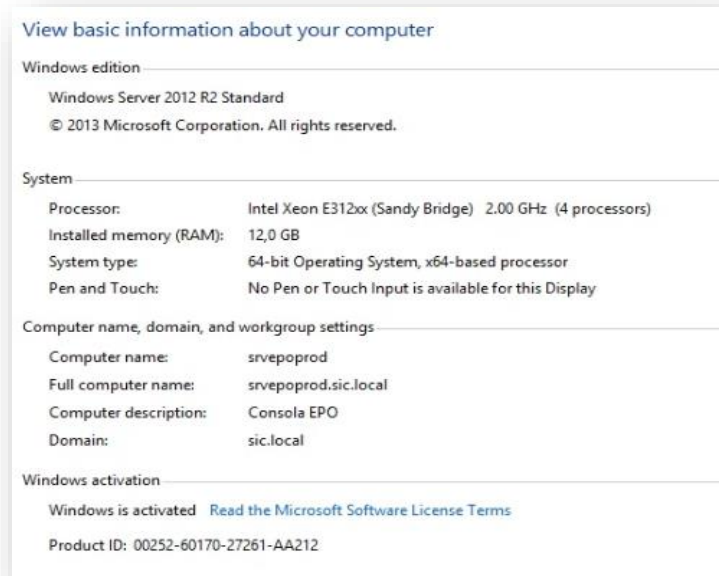


Imagen 62. Logs de seguridad de aplicación – Características servidor ePO

CPU y memoria del servidor ePO:

Lo máximo de uso en CPU que se logró evidenciar está en 20% lo cual indica que el servidor se encuentra funcionando correctamente ya que no se presenta un crecimiento exponencial en la unidad central de proceso

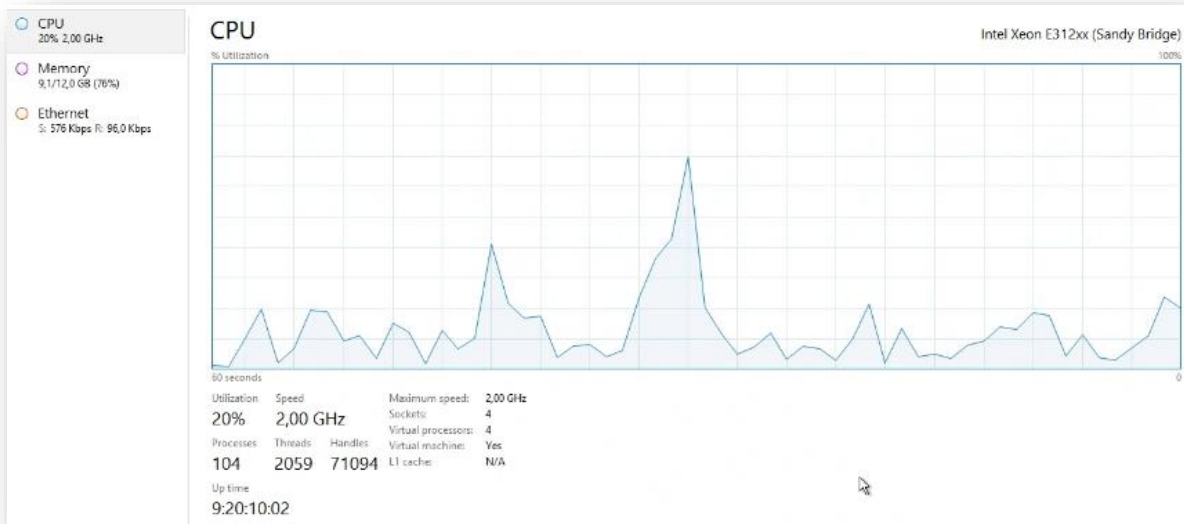


Imagen 63. Logs de seguridad de aplicación – CPU servidor ePO

Por otro lado, pudimos comprobar que, a nivel de memoria, esta se encuentra utilizando un 76% que equivale a 9,1 Gb de 12 Gb con las cuales cuenta el servidor

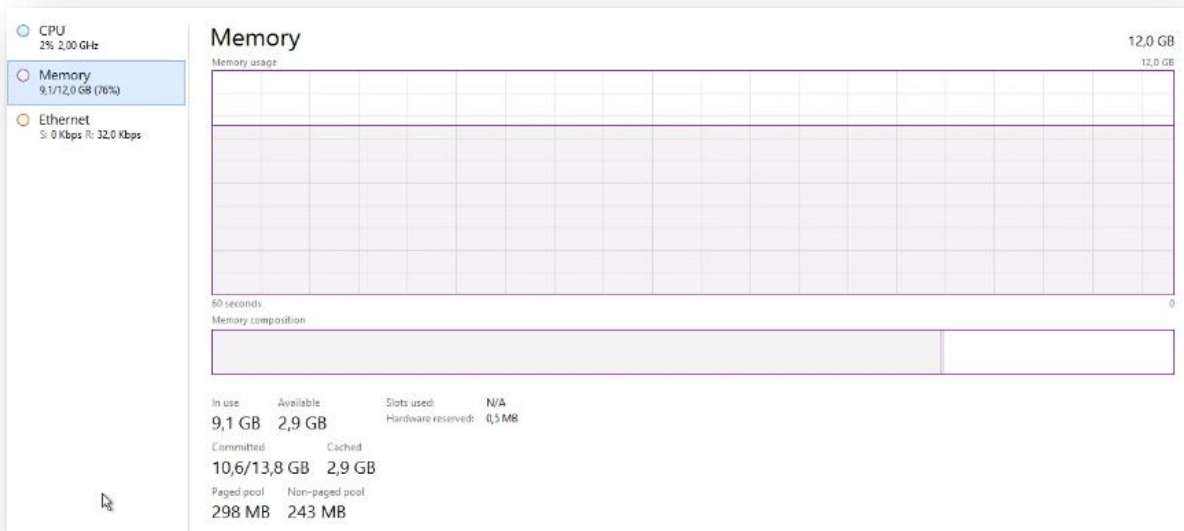


Imagen 64. Logs de seguridad de aplicación – Memoria servidor ePO

6. RECOMENDACIONES

Una vez realizada la revisión general de la configuración actual de la consola de administración centralizada Trellix ePO, se encuentran aspectos que deben ser mejorados con el fin de mitigar la probabilidad de explotación de amenazas para proporcionar un mayor nivel de seguridad en los equipos cliente de la entidad. A continuación, se relacionan las recomendaciones:

- Se recomienda la depuración de la base de datos ya que esta tiene un tamaño considerablemente alto, entre lo que se destacan registros de eventos de nivel bajo.
- Se debe realizar la verificación de las máquinas registradas en la consola de administración que tienen más de 90 días sin comunicación y eliminar los registros de máquinas que no estén activas en el parque tecnológico de la entidad.
- Se recomienda la actualización de los sistemas operativos no soportados de las máquinas que se encuentren activas en la entidad.
- Activar tareas de servidor que sirvan para automatizar el mantenimiento y los procesos de la consola de administración.
- Activar las respuestas automáticas que permitan visualizar inconvenientes con las actualizaciones diarias o eventos de amenazas continuos sobre las máquinas de la entidad.
- Se recomienda la actualización del producto Trellix DLP, a la última version en los equipos de la entidad.
- Se recomienda efectuar la depuración de los paquetes de productos McAfee que se encuentran en versiones obsoletas.
- Se recomienda implementar la herramienta Trellix DLP tanto a nivel de control de dispositivos con el fin de evitar cualquier inserción de virus provenientes de unidades de almacenamiento extraíble como también implementar dicha herramienta a nivel de protección de datos y así poder mitigar la fuga de información de datos que sean de clasificación sensible o confidencial para la entidad.
- Se recomienda validar las 4 tareas de servidor ("REPORTE DE ANTIVIRUS", "REPORTE DE ANTIVIRUS 3", "REPORTE DE ANTIVIRUS 4" Y "EQUIPOS SIN AGENTE DE MCAFEE") las cuales están presentando errores a la hora de su ejecución.



Daniel Eduardo Hernandez Toro.
Especialista en Seguridad de la Información
SOFTSECURITY S.A.S.
Teléfonos: 57-1 7030397 / 57-1 2698731 / 57-1 2694875
Celular: 57-3143304677