Solución contra código malicioso, Control 44

Evidencia que permita verificar que la solución contra código malicioso protege los activos del monedero electrónico en sus fases de prevención, detección, contención, erradicación, recuperación y seguimiento

1. Resumen del inventario base considerado

Activos físicos

Consecutivo	Nombre	Descripcion	Marca	Modelo	Serie	Direccion IP
3	SW-HP-NGX-01	Switch Core, interconecta todos los dispositivos del centro de datos	Hawlett Packard	FlexFabric 5700	CN79GN302W	10.20.1.2
4	FW-FTNET-NGX-01	Firewall perimetral, gestiona los enlaces de Intrnet, IDS, IPS, Filtrado web, etc	Fortinet	Fortigate 200F	FG200FT921913910	10.20.1.1
5	SW-HP-ASSTEL-01	Switch Core, interconecta todos los dispositivos del centro de datos	Hawlett Packard	FlexFabric 5700	CN79GN3056	10.30.1.2
6	FW-ASSETEL-NGX-01	Firewall perimetral, gestiona los enlaces de Intrnet, IDS, IPS, Filtrado web, etc	Fortinet	Fortigate 300E	FG3H0E5818905944	10.30.1.1
7	SW-ARUBA-2930	Switch Core, interconecta todos los dispositivos del centro de datos	Aruba	Aruba	TW2AHL30WK	10.100.0.14
8	FW-FG200f-03	Firewall perimetral,	Fortinet	Fortigate 200E	FG200FT922930849	10.100.0.1
9	HST-PRLN-01	Host de virtualizacion VMWare	Hawlett Packard	DL 360 G10	MXQ3270X60	10.20.1.4
10	HST-PRLN-02	Host de virtualizacion VMWare	Hawlett Packard	DL 360 G10	MXQ3030ML5	10.20.1.5
11	HST-PRLN-03	Host de virtualizacion VMWare	Hawlett Packard	DL 360 G10	MXQ32812DN	10.20.1.6
12	STR-MSA-01	Dispositivo de Almacenamiento de para las VM de VMWare	Hawlett Packard	MSA 2060	ACV246W2GB	10.20.1.10
13	VLT-SONCE-01	Almacenameinto inmutable de respaldos	Hawlett Packard	HPE StoreOnce 3660 HPE 30TB	2M234801G0	10.20.1.30
14	HST-PRLN-04	Host de virtualizacion VMWare	Hawlett Packard	DL 380 G10	2M282402CZ	10.30.1.13
15	HST-PRLN-05	Host de virtualizacion VMWare	Hawlett Packard	DL 380 G10	2M282402D0	10.30.1.14
16	HST-PRLN-06	Host de virtualizacion VMWare	Hawlett Packard	DL 380 G10	2M282402CY	10.30.1.15
17	STR-MSA-02	Dispositivo de Almacenamiento para las VM de VMWare	Hawlett Packard	MSA 2060 HPE 30TB	ACV247W2LH	10.30.1.18
18	VLT-SONCE-02	Almacenameinto inmutable de respaldos	Hawlett Packard	HPE StoreOnce 3660	2M234801G1	10.30.1.9
28	SRV-NAS-APP	Almancenamiento de red.	N/A	N/A	N/A	10.100.30.9

Activos virtuales

Consecutivo	Nombre	Descripcion	Marca	Modelo	Serie	Direccion IP
1	SRV-ENERGO-AD	Directorio Activo	N/A	N/A	N/A	172.16.52.2
2	SRV-MON-APP-DV	Aplicaion de Monedero Desarrollo	N/A	N/A	N/A	172.16.50.10
3	SRV-MON-APP-PR	Aplicaion de monedero produccion	N/A	N/A	N/A	172.16.52.10
4	SRV-MON-APP-QA	Aplicación de monedero pruebas	N/A	N/A	N/A	172.16.51.10
5	SRV-MON-DB-DV	Base de datos de monedero desarrollo	N/A	N/A	N/A	172.16.50.11
6	SRV-MON-DB-PR	Base de datos de monedero produccion	N/A	N/A	N/A	172.16.52.11
7	SRV-MON-DB-QA	Base de datos de monedero pruebas	N/A	N/A	N/A	172.16.51.11
8	SRV-MON-SER-DV	Servicios de backend desallo	N/A	N/A	N/A	172.16.50.12
9	SRV-MON-SER-PR	Servicios de backend produccion	N/A	N/A	N/A	172.16.52.12
10	SRV-MON-SER-QA	Servicios de backend pruebas	N/A	N/A	N/A	172.16.51.12
11	SRV-NTP	Servidor de tiempo	N/A	N/A	N/A	10.255.248.40
12	SRV-GLPI	Servidor de Tickets	N/A	N/A	N/A	10.255.248.326
13	SRV-GRAFANA	Servidor de Monitoreo	N/A	N/A	N/A	10.255.248.82
14	SRV-WAZUH	Servidor SIEM	N/A	N/A	N/A	10.255.248.15

2. Activos del inventario que deben considerarse en la cobertura contra codigo malisioso

Consecutivo	Nombre	Descripcion	Marca	Modelo	Serie	Direccion IP
1	SRV-ENERGO-AD	Directorio Activo	N/A	N/A	N/A	172.16.52.2
2	SRV-MON-APP-DV	Aplicaion de Monedero Desarrollo	N/A	N/A	N/A	172.16.50.10
3	SRV-MON-APP-PR	Aplicaion de monedero produccion	N/A	N/A	N/A	172.16.52.10
4	SRV-MON-APP-QA	Aplicación de monedero pruebas	N/A	N/A	N/A	172.16.51.10
5	SRV-MON-DB-DV	Base de datos de monedero desarrollo	N/A	N/A	N/A	172.16.50.11
6	SRV-MON-DB-PR	Base de datos de monedero produccion	N/A	N/A	N/A	172.16.52.11
7	SRV-MON-DB-QA	Base de datos de monedero pruebas	N/A	N/A	N/A	172.16.51.11
8	SRV-MON-SER-DV	Servicios de backend desallo	N/A	N/A	N/A	172.16.50.12
9	SRV-MON-SER-PR	Servicios de backend produccion	N/A	N/A	N/A	172.16.52.12
10	SRV-MON-SER-QA	Servicios de backend pruebas	N/A	N/A	N/A	172.16.51.12
11	SRV-NTP	Servidor de tiempo	N/A	N/A	N/A	10.255.248.40
12	SRV-GLPI	Servidor de Tickets	N/A	N/A	N/A	10.255.248.326
13	SRV-GRAFANA	Servidor de Monitoreo	N/A	N/A	N/A	10.255.248.82
14	SRV-WAZUH	Servidor SIEM	N/A	N/A	N/A	10.255.248.15
15	SRv-NAS	NAS Windows Carpetas compartidas	N/A	N/A	N/A	10.100.30.9
15	SW-HP-NGX-01	Switch Core, interconecta todos los dispositivos del centro de datos	Hawlett Packard	FlexFabric 5700	CN79GN302W	10.20.1.2
16	FW-FTNET-NGX-01	Firewall perimetral, gestiona los enlaces de Intrnet, IDS, IPS, Filtrado web, etc	Fortinet	Fortigate 200F	FG200FT921913910	10.20.1.1
17	SW-HP-ASSTEL-01	Switch Core, interconecta todos los dispositivos del centro de datos	Hawlett Packard	FlexFabric 5700	CN79GN3056	10.30.1.2
18	FW-ASSETEL-NGX-01	Firewall perimetral, gestiona los enlaces de Intrnet, IDS, IPS, Filtrado web, etc	Fortinet	Fortigate 300E	FG3H0E5818905944	10.30.1.1
19	SW-ARUBA-2930	Switch Core, interconecta todos los dispositivos del centro de datos	Aruba	Aruba	TW2AHL30WK	10.100.0.14
20	FW-FG200f-03	Firewall perimetral,	Fortinet	Fortigate 200E	FG200FT922930849	10.100.0.1
21	HST-PRLN-01	Host de virtualizacion VMWare	Hawlett Packard	DL 360 G10	MXQ3270X60	10.20.1.4
22	HST-PRLN-02	Host de virtualizacion VMWare	Hawlett Packard	DL 360 G10	MXQ3030ML5	10.20.1.5
23	HST-PRLN-03	Host de virtualizacion VMWare	Hawlett Packard	DL 360 G10	MXQ32812DN	10.20.1.6
24	STR-MSA-01	Dispositivo de Almacenamiento de para las VM de VMWare	Hawlett Packard	MSA 2060	ACV246W2GB	10.20.1.10
25	VLT-SONCE-01	Almacenameinto inmutable de respaldos	Hawlett Packard	HPE StoreOnce 3660 HPE 30TB	2M234801G0	10.20.1.30
26	HST-PRLN-04	Host de virtualizacion VMWare	Hawlett Packard	DL 380 G10	2M282402CZ	10.30.1.13
27	HST-PRLN-05	Host de virtualizacion VMWare	Hawlett Packard	DL 380 G10	2M282402D0	10.30.1.14
28	HST-PRLN-06	Host de virtualizacion VMWare	Hawlett Packard	DL 380 G10	2M282402CY	10.30.1.15
29	STR-MSA-02	Dispositivo de Almacenamiento para las VM de VMWare	Hawlett Packard	MSA 2060 HPE 30TB	ACV247W2LH	10.30.1.18
30	VLT-SONCE-02	Almacenameinto inmutable de respaldos	Hawlett Packard	HPE StoreOnce 3660	2M234801G1	10.30.1.9
31	SRV-NAS-APP	Almancenamiento de red.	N/A	N/A	N/A	10.100.30.9

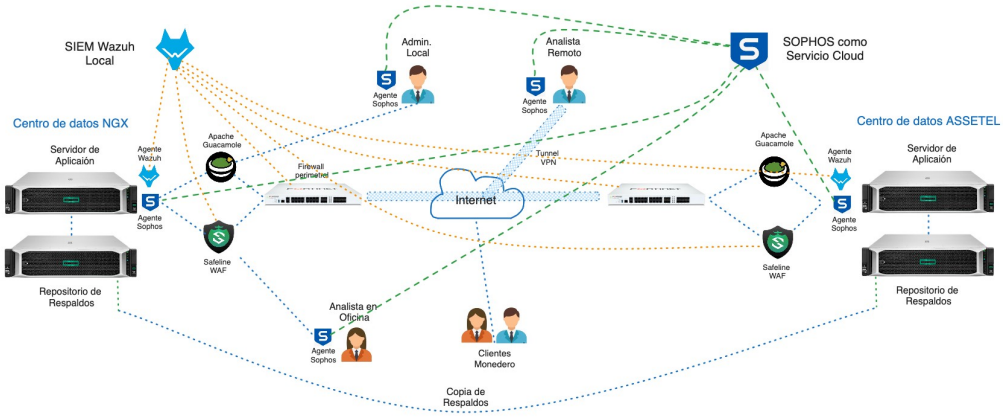
3. Documento maestro de la solución contra código malicioso

Descripción de la solución. Con el fin de minimizar el riesgo de ataque por codigo malicioso se han implementado varios sistemas que operan en conjunto en las diferentes etapas que un evento de esta naturaleza pudiera tener, entre los que destacan, XDR moderno, Firewalls de red perimetrale, Faiwalls de servicios y aplicaiones web, Gestion

de cuentas privilegiadas, SIEM y respaldos en repositorios inmutables. Tratando de reducir las brechas desde cuatro aristas que son: Prevensión, Detección, Contención y Recuperación en el peor de los escenarios.

Arquitectura de protección Para la protección de datos contra ataques de codigo malicioso se ha planteado un escenario con enfoque en la prevención, tratando de impedir inicialmente la entrada, evitando que pueda escalar privilegios, detectando oportunamente los intentos de intrusión o ataques y finalmente asegurando medidas de recuperación o mecanismos de redundancia.

La imagen muestra diagrama con el ecosistema de protección contra codigo malicioso donde se observan Usuarios, Cllientes, Aplicaiones y las diferentes herramientas usadas en las capas de pevención, detección, contención y recuperación



A) Prevención. Agrupa los procesos y herramientas enfocados en evitar que el codigo malicioso entre en los equipos de los ususarios o administradores de sistemas, Atendiendo a la estadistica de que el 85% de estos ataque llegan a traves de correos engañosos se ha implementado el módulo de **seguridad de correo electónico de Sophos** el cual incluye las siguientes funciones:

- Revición de Adjuntos con herramientas anti malware
- Anti Spam
- Reescritura de enlaces
- Politicas de cumplimiento de registros DMARC, DKIM y SPF
- Revición de QRs
- Revisión de listas negras
- Sandbox

Los servidores no se exponen directamente a internet, seresguardan detrás de un firewall de red con IPS, y detrás de un firewall de aplicaciones (WAF) lo que complica a adversarios inyectar código malicioso. Otro sistema que juega un papel vital es la solucion PAM de **Apache guacamole**, la cual permite a los administradores el acceso remoto a los servidores a traves de un proxy reveso sin

contraseñas, previeniendo que estas puedan ser robadas y compartidas con terceros no autorizados.

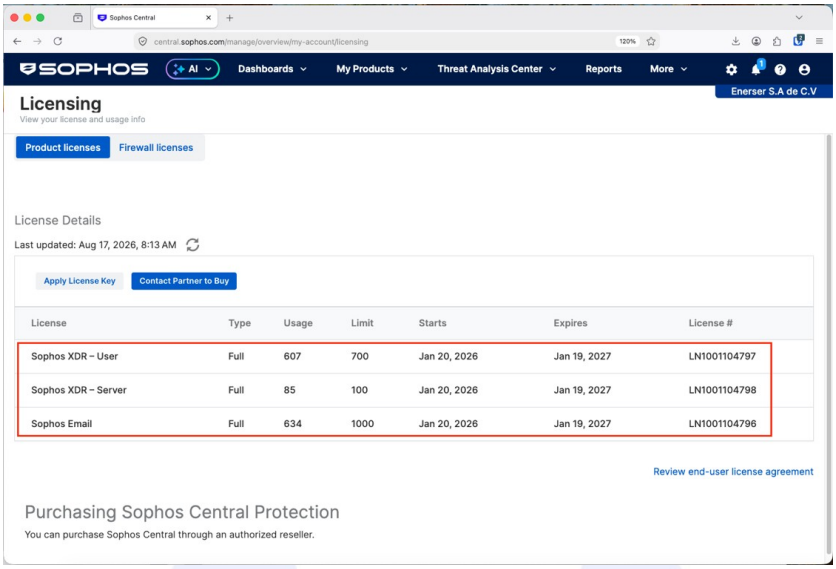
B) Detección. El enfoque de esta capa es evidencial actividades anomalas en etapas tempranas para evitar posibles ataque aquí juegan un papel importante la **Consola de Sophos** quien alaliza el comportamiento de los usuarios, la **Consola de Wazuh** por su parte analiza en tiempo real la actividad en los servidores para encontrar patrones conocidos de ataque como las Tecnicas MITRES&ATK

C) **Contensión.** Entre los motivos de la elección del XDR de sophos, estuvo el hecho de que tienen uno de los módulos de Antiramsomware mejor valorados de la industria, el XDR tambien nos permite Acciones como aislar equipos comprometidos, y ejecutar tareas tras detecciones iniciales. La correlación entre los eventos de La consola de Sophos y Wazuh nos premiten crear incidentes bajo los primeros sintomas de codigo malicioso

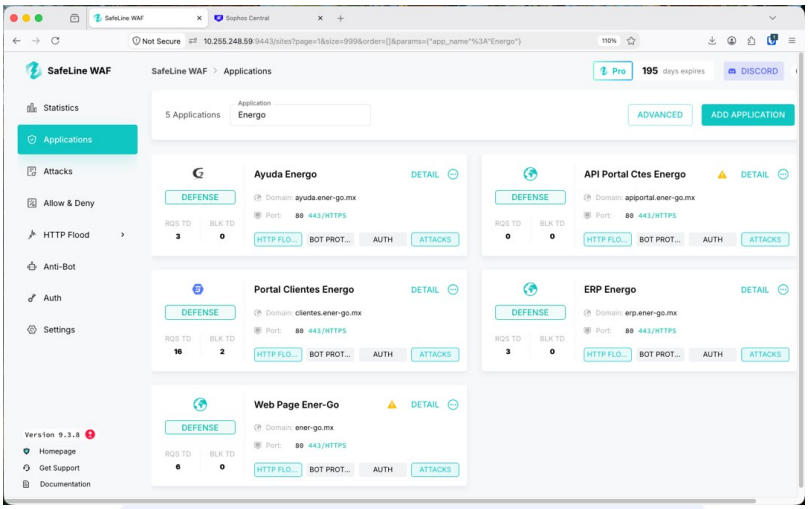
D) **Recuperación**. Para la última linea de defenza hemos diseñado un solido esquema de respaldos de máquinas virtuales utilizando Veeam Backup, Replicas de las mismas en dos centro de datos diferentes, respaldos a repositorios inmutables que se duplican en otro centro de datos, ademas de copias a un servicio de almacenamiento inmutable de nube como es Wasabi. Esto nos permitiría recuperar operaciones en el peor de los casos.

Los servidores de aplicaion del monedero en centro de datos de ASSETEL, ya sean de producción, pruebas o desarrollo, no se consideran en la gestión de código malicioso, por que estan apagados (en sttand-by) a la espera de ser encendidos y son sujetos de sobre escritura diariamente con los cambios que sufren los servidores originales en el centro de datos de NGX, al monendo de encenderlos, empezaran a se monitoreados por sophos y wazuh

Nombre comercial y versión. Para el XDR sistema de detección y respuesta extendida se utiliza Sophos XDR, con los modulos de Usuario, Servidores y Protección de correo electrónico. La imagen inferior muestra captura de pantalla de la consola de administración de sophos en la nube, donde se aprecia, licenciamiento de puntos finales de usuarios, servidores y protección de correo electrónico.


Sophos Central
central.sophos.com/manage/overview/my-account/licensing
SOPHOS
AI
Dashboards
My Products
Threat Analysis Center
Reports
More
Enerser S.A de C.V
Licensing
View your license and usage info
Product licenses
Firewall licenses
License Details
Last updated: Aug 17, 2026, 8:13 AM
Apply License Key
Contact Partner to Buy
License
Type
Usage
Limit
Starts
Expires
License #
Sophos XDR – User
Full
607
700
Jan 20, 2026
Jan 19, 2027
LN1001104797
Sophos XDR – Server
Full
85
100
Jan 20, 2026
Jan 19, 2027
LN1001104798
Sophos Email
Full
634
1000
Jan 20, 2026
Jan 19, 2027
LN1001104796
Review end-user license agreement
Purchasing Sophos Central Protection
You can purchase Sophos Central through an authorized reseller.

Para el WAF se Utiliza Safe Line Pro de Chaitin Tech, en su version 9.3.8, instalado localmente, la imagen muestra capura de pantalla de SafeLine donde se observan los servicios expuestos del monedero.



Alcance de Ambientes. Todos los servidores y estaciones de trabajo con Sistemas operativos (Windows Linux, Mac OSX) capaces instalar un agente de Sophos, estan enrolados al XDR. Lo que incluye Los servidores productivos, los de desarrollo, los de pruebas, el Directorio Activo y el servidor NTP, GLPI, Wazuh. Para los equipos que no pueden instalar agentes, como los Switches, Firewalls, se confirururaron traps de SNPM a Wazuh, se configuraron agentes de Wazuh para la recolección de logs en los servidores Windows y Linux. Finalmente se configuró una integracion via API de Sophos a la consola de Wazuh para centralizar todos los eventos en un solo lugar.

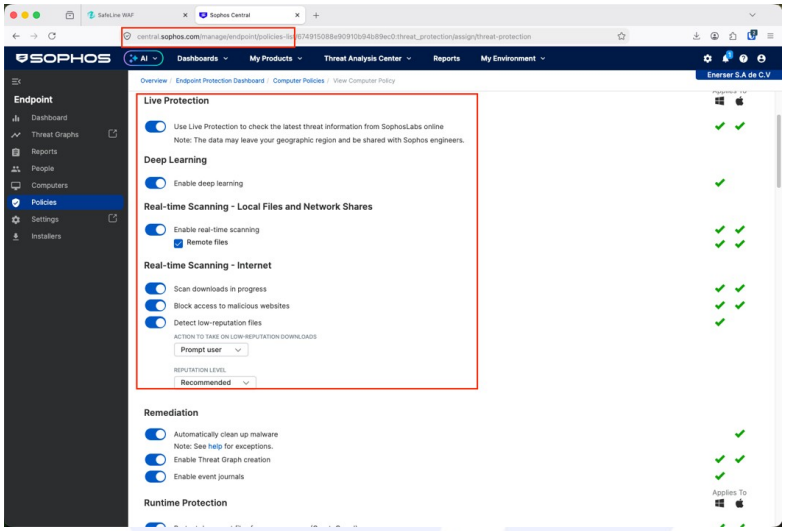
Matriz de responsabilidades. Los Servicios del monedero se operan bajo la supervición de un centro de operaciones deseguridad (SOC), provisto junto con los servicios de centro de datos. Con la sigiuente matriz de responsabilidades.

Nombre	Puesto	Rol	Telefono
Jose Alonso Sánchez	Responsable	Cordinación, supervicion	6642571637
Gerardo López Najera	Coord. Servidores	Windows, Virt. Respaldos	6641748124
Oscar Gutiérrez	Coord. Redes	Redes, Consola de sophos	6642572062
Jesus Isai Cuevas	Analista de ciberseguridad	Consola de Wazuh y sophos	6631272130
Jacsive León	Analista de ciberseguridad	Gestión de incidentes	6672331410

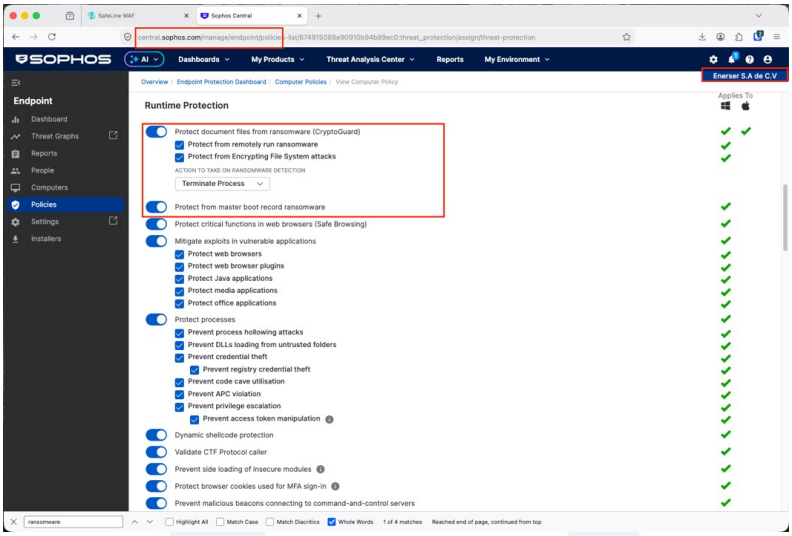
EnerGo

4. Checklist de prevención de código malicioso

Protección en tiempo real habilitada
La imagen muestra captura de pantalla de la politica base por defecto para los usuarios de computadoras de escritorios y laptos, donde se observa, proteccion en tiempo real en el acceso a Internet y en acceso a los archivos en disco.

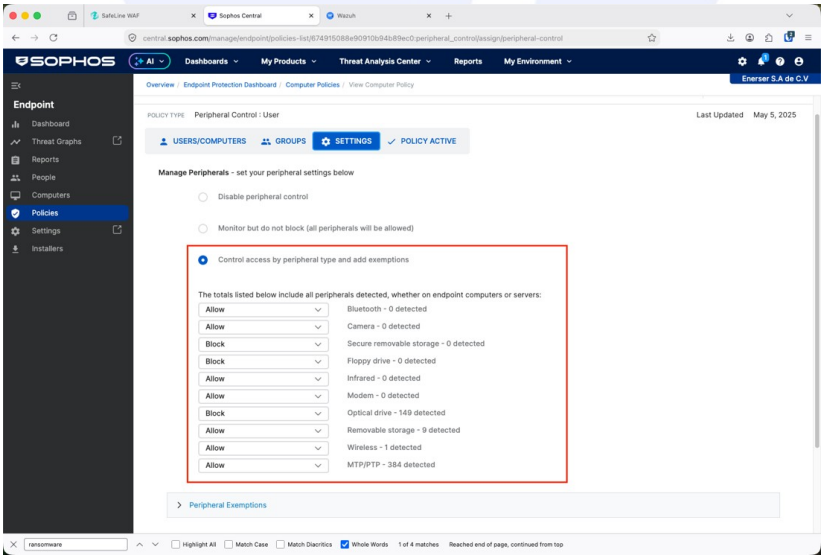


Protección contra ransomware
La imagen muestra captura de pantalla de la politica base por defecto para los usuarios de computadoras de escritorios y laptos, donde se observa, proteccion contra encripción por ransomware habilitada.



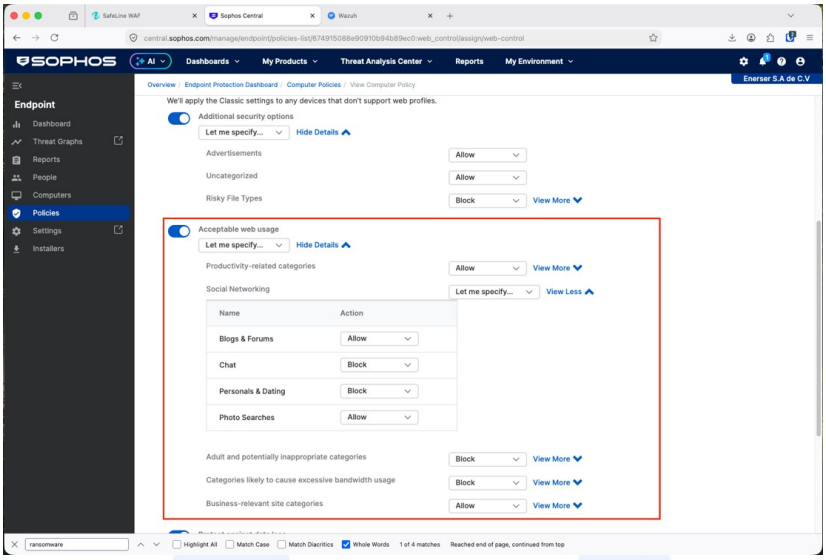
Control del dispositivos removibles

La imagen muestra captura de pantalla de la consola de Sopshos Central donde se observa politica base por defecto para el manejo de dispositivos perifericos, apreciandose el bloqueo dispositivos de almacenamiento removible y discos opticos.

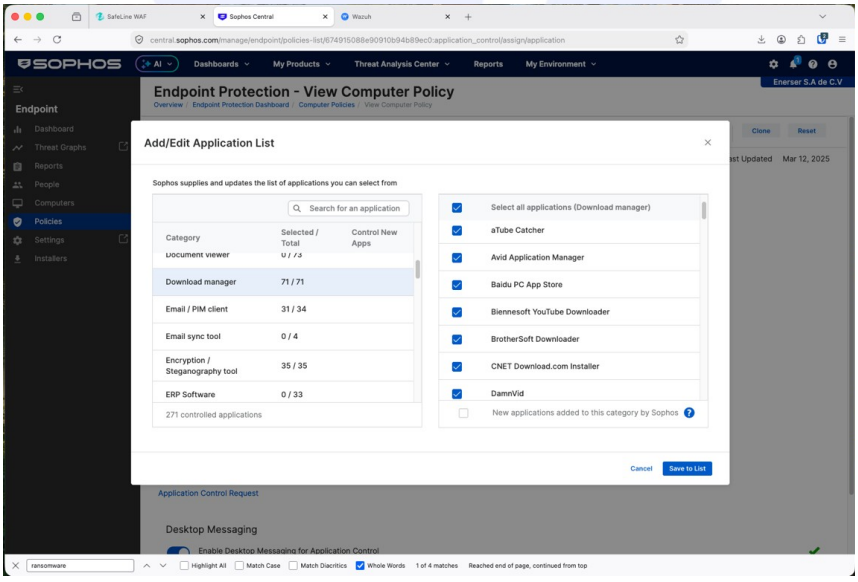


Filtrado web y Reputación

La imagen muestra captura de pantalla de la consola de Sopshos Central donde se observa politica base por defecto para el bloqueo de redes sociales, contenido peligroso, consumo de ancho de banda, sitios de pishing y contenido inapropiado.

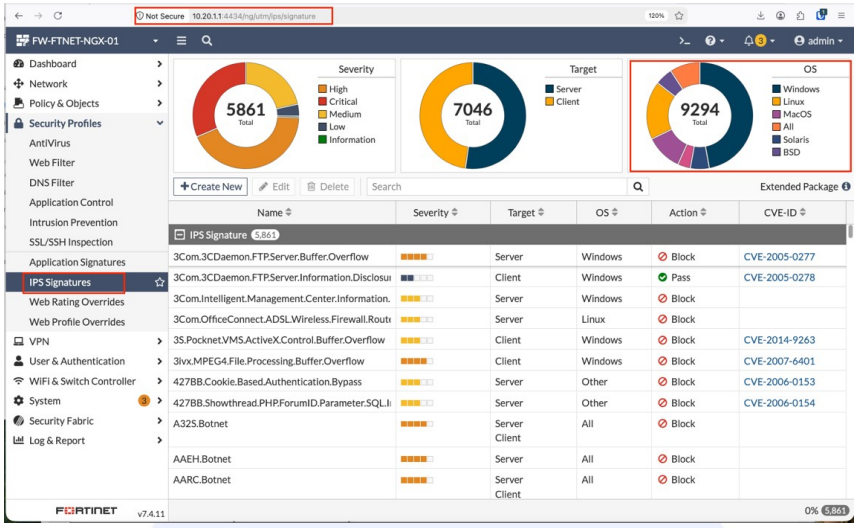


Control de aplicaiones. La imagen muestra captura de pantalla de la consola de Sophos Central donde se obserba politica base por defecto para el manejo de aplicaiones, donde se aprecia el para gestores de descarga clientes de correo, utilerias de encripción, etc.

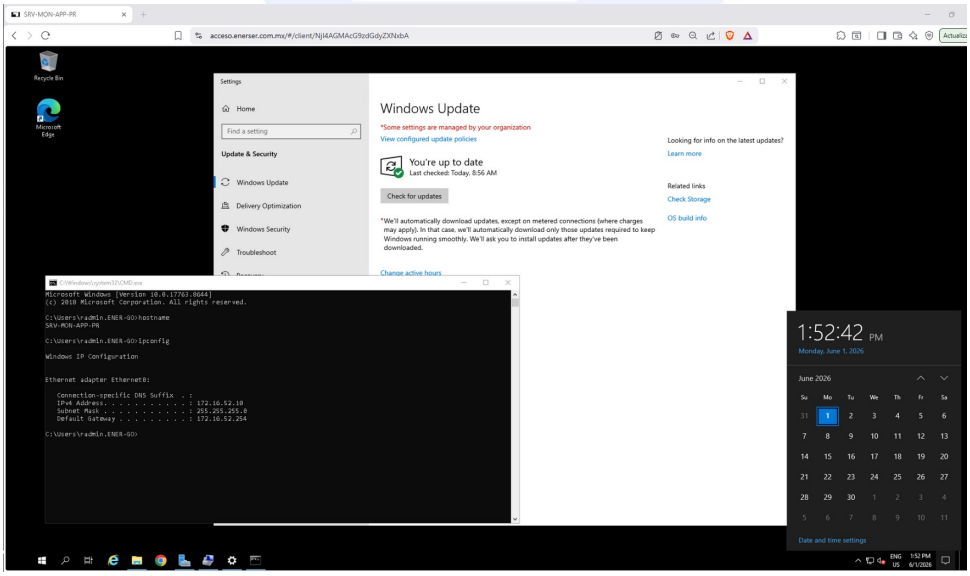


IPS/IDS habilitado en perimetro. La imagen muestra captura de pantalla de la consola del fortigate del centro de datos de NGX con dirección IP 10.20.1.1, donde se observa

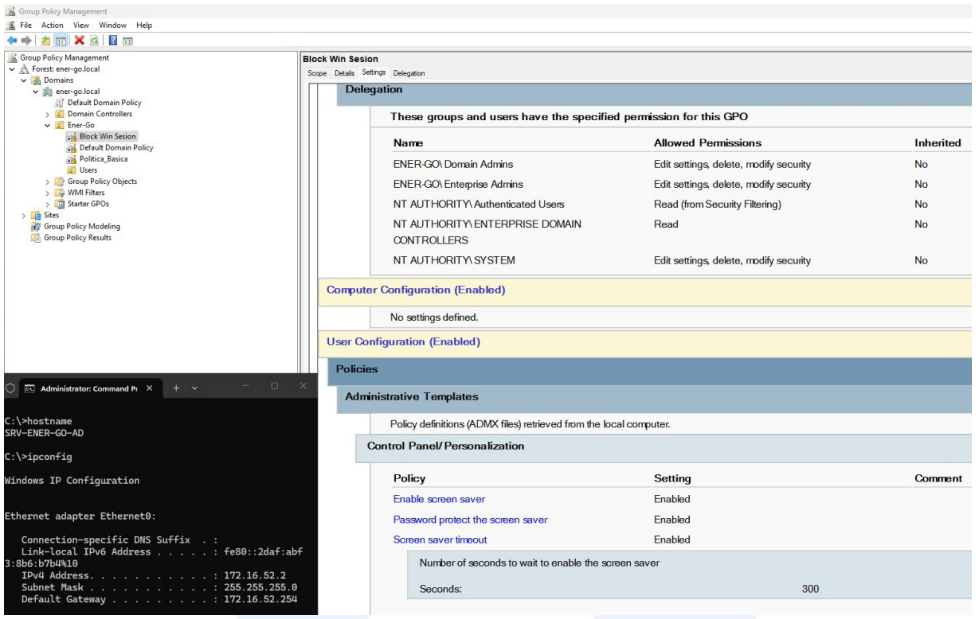
configuracion de un perfil de IPS/IDS para detectar intrusos en brechas conocidas en aplicaiones y sistemas operativos.



Gestión de parches de sistema operativo. La imagen muestra captura de pantalla del servidor de la aplicación del monedero SRV-MON-APP-PR, con direccion IP 17.16.52.10, donde se observa que no existen parches del sistema operativo pendientes de aplicar.

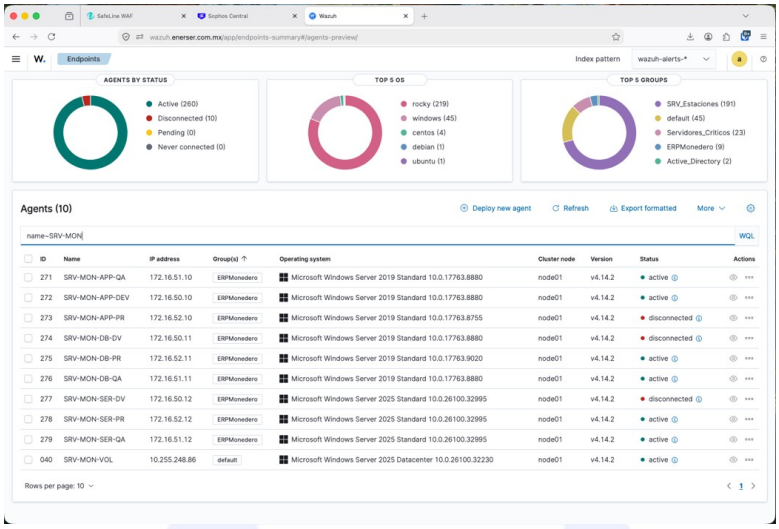


Restricción de privilegios Administrativos. La imagen muestra captura de pantalla del servidor de la aplicación del monedero SRV-ENER-GO-AD, con direccion IP 17.16.52.2, donde se observa politica de restricción para hacer cambios de configuracion e instalación de software para todos los usuarios del dominio.

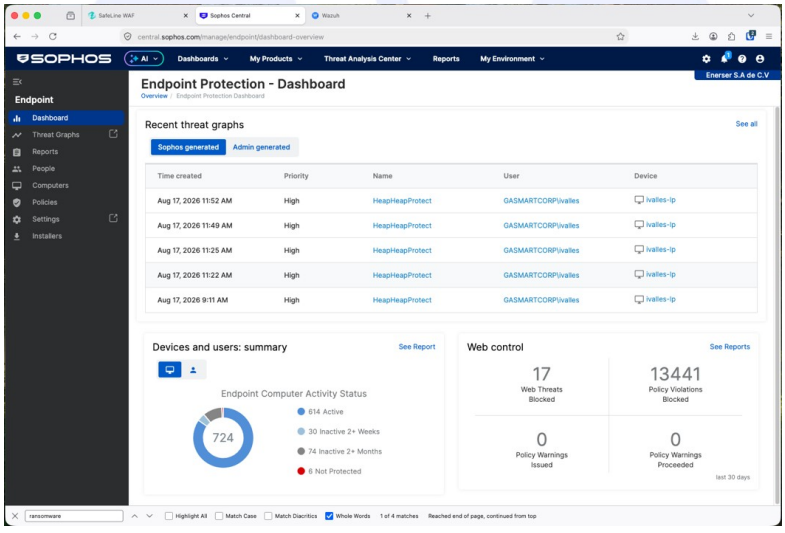


5. Checklist de detección y monitoreo

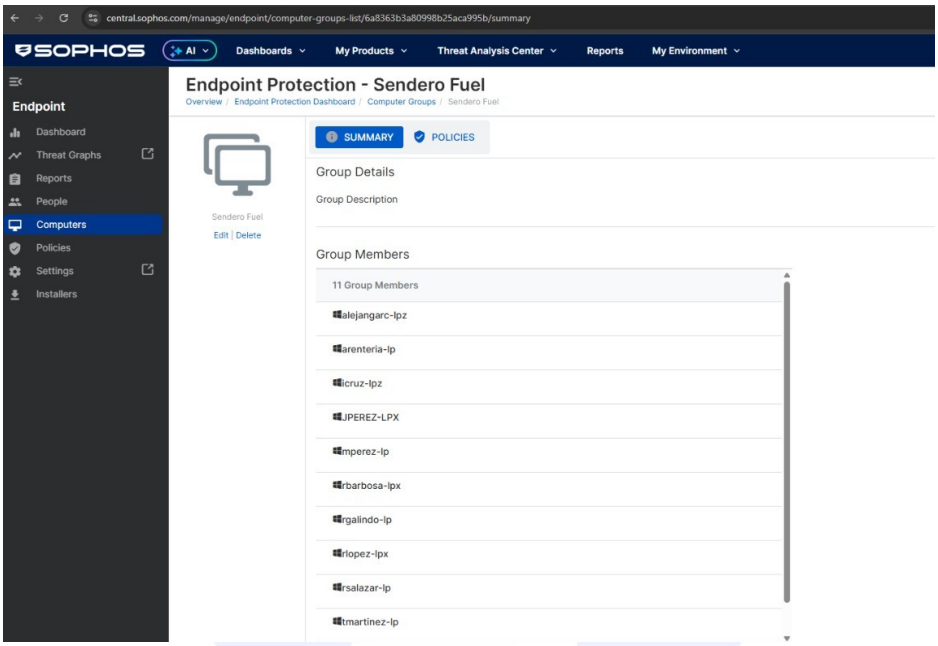
Consola central de monitoreo. La imagen muestra captura de pantalla de la consola de Wazuh, con direción ip 10.255.248.15 donde se observa monitoreo centralizado de logs de servidores, antivirus y Dispositivos de red.

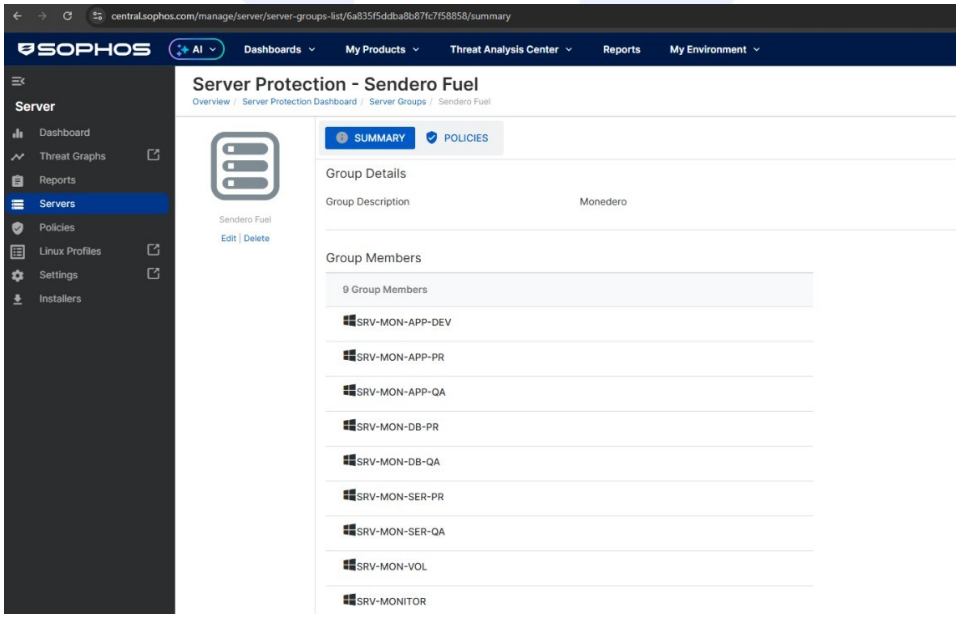


La imagen muestra captura de pantalla de la consola de Sophos central donde se obserba, sumario de dispositivos y ultimas amenazas detectadas



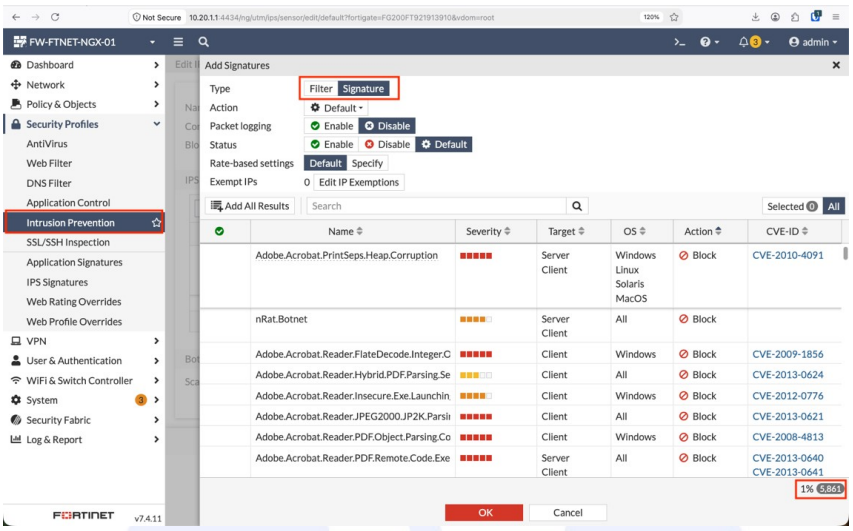
Inventario de agentes instalado. Las siguientes dos imágenes muestra captura de pantalla de la consola de Sophos central donde se obserba el inventario de equipos de usuarios y servidores del monedero.



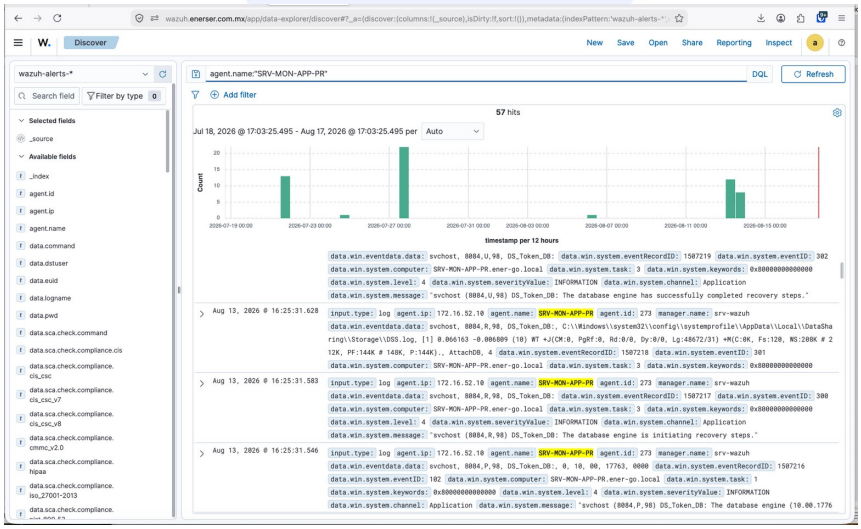


EnerGo

Detección basada en firmas y comportamiento. La imagen muestra captura de pantalla de la iterfaz de gestion del firewall FW-FNET-NGX-01, donde se aprecia perfil de IPS con 5861 firmas.



Alerta de amenazas. La imagen muestra captura de pantalla de la iterfaz de gestion de Wazuh, donde se observan las Alertas relativas a un servidor de monedero, en est caso SRV-MON-APP-PR



EnerGo

Monitoreo de firewalls. La imagen muestra captura de pantalla Grafana, donde se observa monitoreo de los firewalls y switches,observabdose detalle de trafico de las ultimas 3 horas y estatus actual

