miércoles, 21 de julio de 2021

PROPUESTA TECNICA

Procedimiento de Compra menor "**RENOVACIÓN LICENCIA DE ANTIVIRUS PARA USO DE LA PGR**".

Referencia No.: PROCURADURIA-DAF-CM-2021-0102.

Atención:

Comité de Compras y Contrataciones
Procuraduría General de la República (PGR)
Santo Domingo
Distrito Nacional

Tarja Software, SRL

Kevin Rosario **Móvil (829) 974 1692** **krosario@tarjasoft.com**
San Carlos, C/ Pena y Reynoso #10, Santo Domingo, Rep. Dom. RNC: 131850103

Tabla de Contenido

Referencia No. 1
Cláusula de Confidencialidad 3
Introducción 3
Perfil y Reseña histórica de TARJA SOFTWARE, SRL (TARJASOFT) 3
Dentro de nuestras soluciones podemos citar algunas alianzas estratégicas con fabricantes reconocidos de tecnología 4
Servicios que ofrecemos: 4
Certificación personal del proyecto: 5
Objetivo del Proyecto 6
Metodología para ejecución de proyecto: 6
Proceso de Soporte Local TARJASOFT 7
Contrato de Soporte con FABRICANTE 7
Sophos Central 9
Funciones de Sophos Intercept X. 17
Descripción de los bienes y servicios: 18
Cumplimiento especificaciones técnicas del pliego 18
Plazo de entrega del licenciamiento 19
Servicios profesionales. 20
Condiciones de pago 20
Referencia de Proyectos Similares: 20

Cláusula de Confidencialidad

TARJA SOFTWARE, SRL en lo adelante **TARJASOFT**, presenta este documento con la premisa de que su contenido no será discutido, analizado o divulgado por otra entidad ajena a la **Procuraduría General de la República** en lo adelante **PGR**.

Es preciso aclarar que el contenido de la presente propuesta, no podrá reproducirse parcial o totalmente a terceros, sin previa autorización escrita de **TARJASOFT**, debido a que el diseño y logística de esta propuesta es propiedad de **TARJASOFT**.

Introducción

La información contenida en este documento está basada en la experiencia adquirida por **TARJASOFT** en la ejecución de proyectos similares. Consideramos que la participación de **TARJASOFT** constituye una garantía razonable para el éxito de este proyecto y en la consecución de los objetivos que persigue la renovación de antivirus para uso de la **PGR**.

TARJASOFT es una compañía especializada en el desarrollo e implementación de sistemas y plataformas tecnológicas de Infraestructura de TI y seguridad de la información.

En el mundo cambiante de la tecnología, **TARJASOFT** pone a disposición de su empresa la experiencia y el conocimiento de las tecnologías avanzadas y de vanguardia, necesarias para lograr valor de negocio y eficiencia operativa.

Perfil y Reseña histórica de TARJA SOFTWARE, SRL (TARJASOFT)

Tarja Software, fue fundada en noviembre 2018, y registrada según normas establecidas en la Ley No. 479-08, con el respaldo financiero de la Banca Local e inversionistas 100% dominicanos. Nos caracterizamos desde nuestros inicios en ofrecer servicios profesionales de alto nivel y confiables, así como soluciones tecnológicas de renombre a través de los fabricantes internacionales que representamos e implementadas por Ingenieros con más de 5 años de

TARJA SOFTWARE, S.R.L. RNC: 131-85010-3

experiencia, certificados en cada una de las tecnologías que ofrecemos.

Basándonos en la experiencia que hemos adquirido en diversas implementaciones de proyectos estratégicos, podemos poner a su disposición las mejores prácticas y tecnologías eficientes para ayudar a lograr sus objetivos de negocio. **TARJASOFT** es una agrupación de emprendedores que hoy día cuenta con 5 profesionales de distintas áreas de la tecnología.

Dentro de nuestras soluciones podemos citar algunas alianzas estratégicas con fabricantes reconocidos de tecnología:

- **SOPHOS,** soluciones de seguridad cibernética.
- **UBIQUITI,** redes inalámbricas avanzadas.
- **Microsoft,** licenciamiento para sistemas operativos y nube (OFFICE365).
- **VMWare,** solución para virtualización.
- **Teramind,** herramienta para Monitoreo de la actividad del usuario, prevención de fuga de datos y Análisis del comportamiento del usuario.
- **HPE,** infraestructura para su centro de datos y comunicaciones.
- **VEEAM,** respaldo para infraestructura virtual.
- **FastVUE,** reportes avanzados para tecnologías de syslog.
- **ZENTYAL,** alternativa completa para reemplazar su infraestructura de servidores Windows.
- **ManageEngine,** gestión y administración simplificada de su entorno de TI.

Servicios que ofrecemos:

- Consultoría en Seguridad de la información.
- Continuidad de negocio.
- Gestión tercerizada del centro de operaciones de seguridad (SOC).
- Diseño de arquitectura para Infraestructura de TI.
- Cableado estructurado para redes y centro de datos.
- Servicios para Seguridad de TI, Gestión de Riesgos y Vulnerabilidades.
- Pruebas de penetración.

Certificación personal del proyecto:

TARJASOFT, cuenta con personal altamente calificado para la implementación de este y cualquier otro proyecto requerido por nuestros clientes, como parte del equipo seleccionado para este proyecto se encuentra:

Irvin Rosario, profesional de alto nivel en informática con más de 7 años de experiencia en Seguridad de la información y cumplimiento.

Entrenamientos y certificaciones:

- Sophos and Synchronized Security – Sales Consultant.
- Sophos and Synchronized Security – Certified Engineer.
- Sophos and Synchronized Security – Certified Architect.
- Sophos XG Firewall v17.5 – Technician.
- Sophos XG Firewall v18 – Architect.
- Sophos Central Endpoint and Server v2.0 – Engineer.
- Sophos Central Endpoint and Server v1.0 – Engineer.
- Cisco CCNA.
- ManageEngine ADAudit Certified Product Associate.
- ManageEngine Eventlog Analyzer Certified Product Associate.
- Imperva SecureSphere System Administration v12.0.
- Imperva Specialist Database Security & Compliance v12.0 (IDSS).

Johnattan Pérez, profesional de alto nivel en informática con más de 10 años de experiencia en Infraestructura, Redes y Seguridad de la Información.

Entrenamientos y certificaciones:

- Sophos and Synchronized Security – Sales Consultant.
- Sophos and Synchronized Security – Certified Engineer.
- Juniper Networks – Certified Advanced Firewall Administrator.
- FORTINET - NSE4.
- ETHICAL HACKING.
- ISACA - CERTIFIED INFORMATION SECURITY MANAGER.
- Kaspersky Technical Certification.

- CCNA.
- CCNP.

Alan Rosario, profesional de alto nivel en informática con más de 4 años de experiencia en Infraestructura y Seguridad de la Información.

Entrenamientos y certificaciones:

- Sophos and Synchronized Security – Sales Consultant.
- Sophos and Synchronized Security – Certified Engineer.
- Sophos Central Endpoint and Server v2.0 – Engineer.
- Sophos XG Firewall v18 – Engineer.

Objetivo del Proyecto

Brindar una solución llave en mano confiable y con niveles avanzados de seguridad, para la protección de la información, clientes finales y usuarios del **PGR**. En tal sentido **TARJASOFT** propone una opción que cumplen al 100% con las necesidades planteadas en el proceso **PROCURADURIA-DAF-CM-2021-0102**.

Con la entrega de las licencias de antivirus corporativo, **TARJASOFT** garantiza el apoyo total para bridarles soporte técnico y todo lo concerniente al cumplimiento del funcionamiento de la plataforma.

Metodología para ejecución de proyecto:

La metodología aplicada muestra todos los aspectos a considerar para la entrega de las licencias solicitadas en dicho proceso, desde su gestión hasta su activación, basándose en el estudio realizado a los requerimientos de la **PGR**.

1. Gestión con el fabricante.
2. Activación de las licencias de solución de antivirus.
3. Documentación y administración (guía para la administración de la plataforma).

TARJA SOFTWARE, S.R.L.
RNC: 131-85010-3

Proceso de Soporte Local TARJASOFT

Las solicitudes de soporte serán asignados a un técnico especialista en la herramienta contratada para servirles de apoyo 9x5. Donde contamos con los siguientes SLA por niveles de Urgencia:

- Low: NBD
- Normal: 12 horas
- High: 4 horas
- Critical: 1 hora

Nota: Podríamos extender el soporte hasta los sábados dependiendo de la urgencia/prioridad reportado por el cliente.

Nuestros contactos para soporte son:
- Correo: soporte@tarjasoft.com
- Teléfonos: 829-959-6079 y 829-974-1692

Contrato de Soporte con FABRICANTE:

INTERCEPT X:

	Severity Level	Target Response Time	Target Status Update Frequency
Enhanced	Critical	Within 4 hours	Daily, or as agreed with the customer/partner
	High	Within 8 hours	Every business day, or as agreed with the customer/partner
	Medium	Within 24 hours	As agreed with the customer/partner
	Low	Within 24 hours	As agreed with the customer/partner

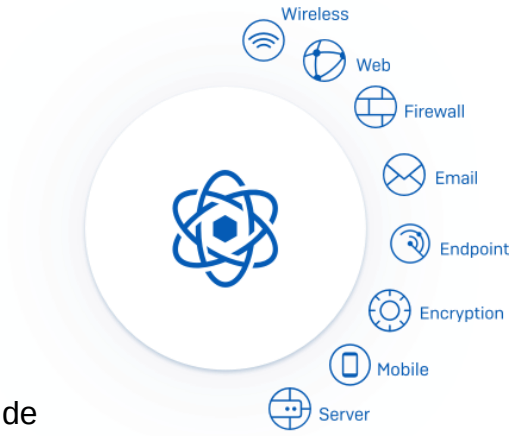
SOPHOS
Security made simple.

Support level	Enhanced (Included with Endpoint)*
24/7 multi-channel support	✓
Software downloads, updates, and maintenance	✓
Access to support knowledgebase and support forums	✓
Warranty (Appliances only)	Warranty valid as long as support contract active (5 year EOL)
Hardware replacement (Appliances only)	Advanced
Remote assistance support	✓
Remote consulting	
Priority case and sample handling	
VIP Access to Senior Technical Resource team	
Named Technical Account Manager (TAM)	
Front of the line access to product information	
Personalized communications and alerts	
Performance and feature optimization	
Enhanced escalation	
Emergency Onsite Support	

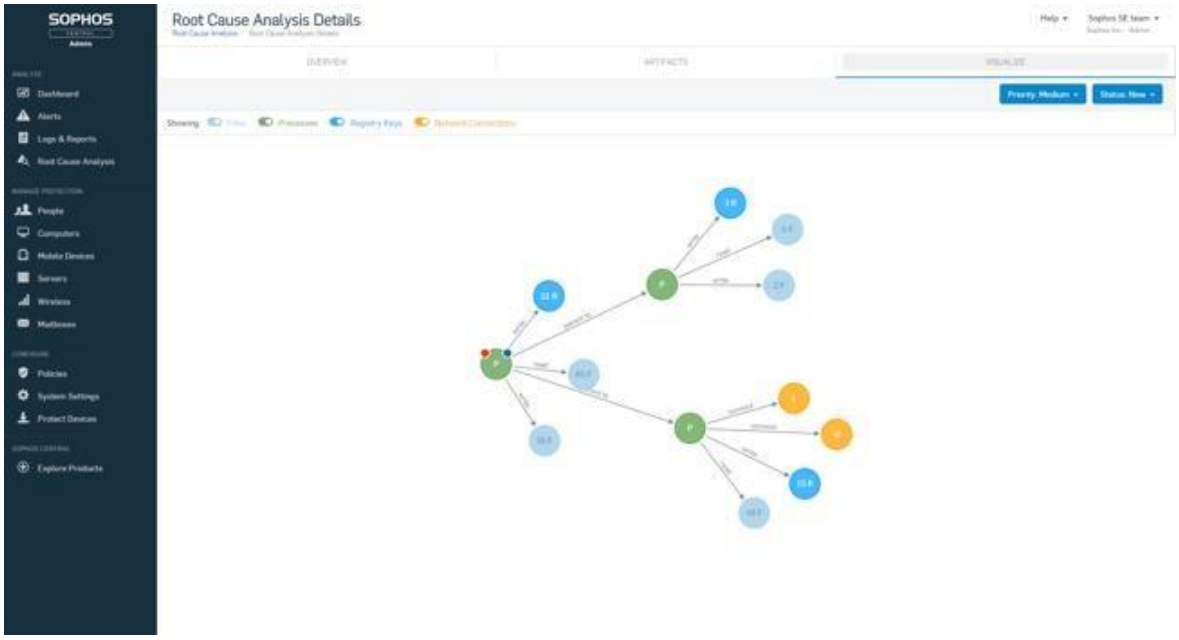
Descripción Técnica

Sophos Central

La consola unificada para administrar sus productos de Sophos

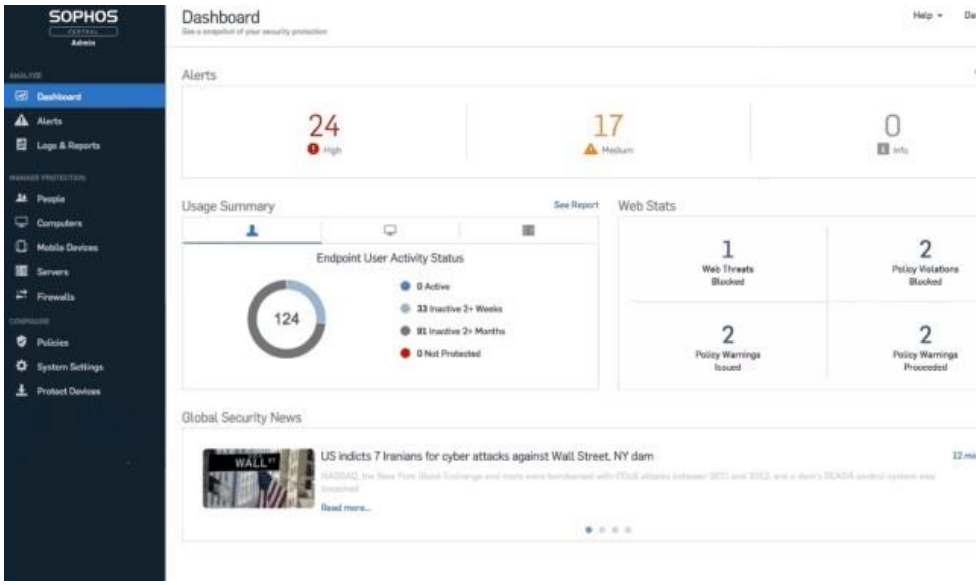


Intercept X
Solución anti-vulnerabilidades y anti-ransomware sin firmas y análisis de causa raíz para proteger sus estaciones de trabajo de amenazas avanzadas.

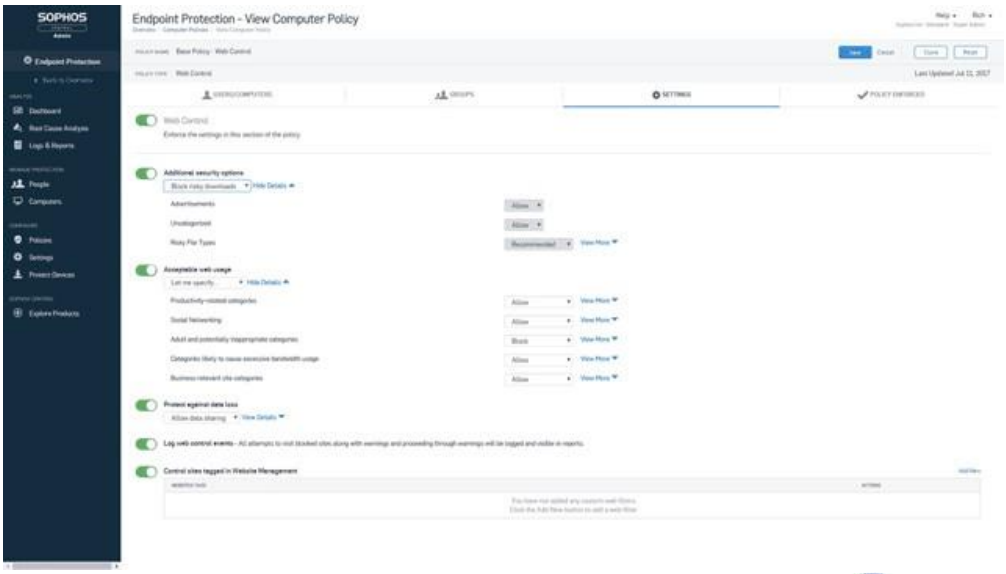


TARJA SOFTWARE, S.R.L.
RNC: 131-85010-3

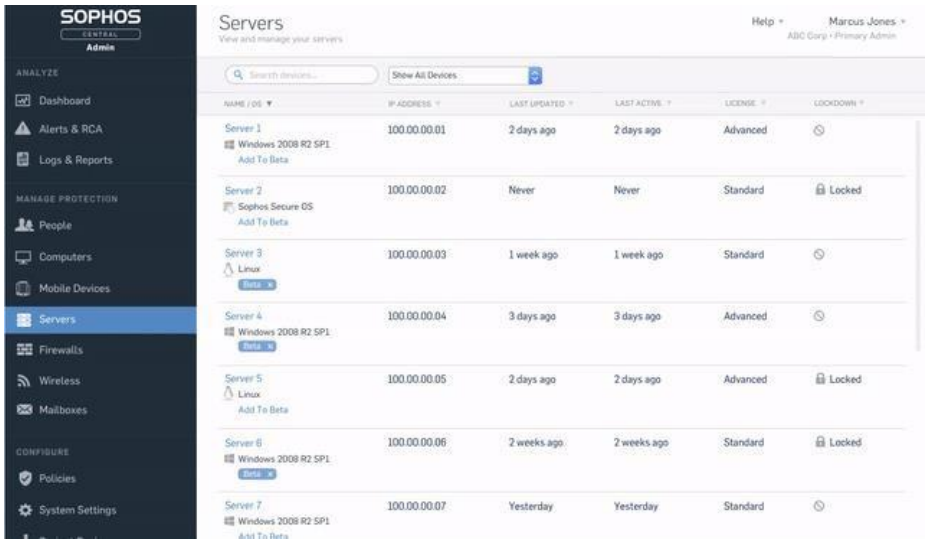
Endpoint Protection
Protección avanzada para estaciones de trabajo con una interfaz de usuario simple e intuitiva.



Protección web
Protección web segura de nivel empresarial avanzada a la vez que fácil de usar.
Server Security

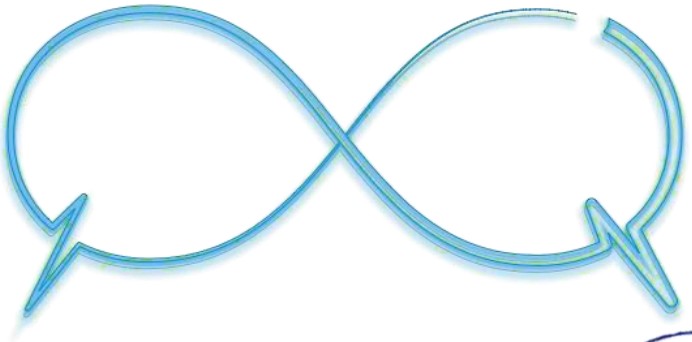


Proteja sus servidores virtuales y físicos sin sacrificar el rendimiento, incluida la función Server Lockdown con un clic.



Seguridad Sincronizada

Sophos Central le permite administrar nuestra plataforma galardonada de Synchronized Security. Los ataques avanzados están más coordinados que nunca. Ahora, sus defensas también lo están. Nuestro revolucionario Security Heartbeat™ garantiza la comunicación entre su protección de endpoints y su firewall (cortafuegos). Es una idea sencilla pero eficaz que le proporciona una mayor protección contra amenazas avanzadas y le permite responder a incidentes de forma más rápida. Es tan sencilla que se preguntará por qué nadie antes lo había hecho.

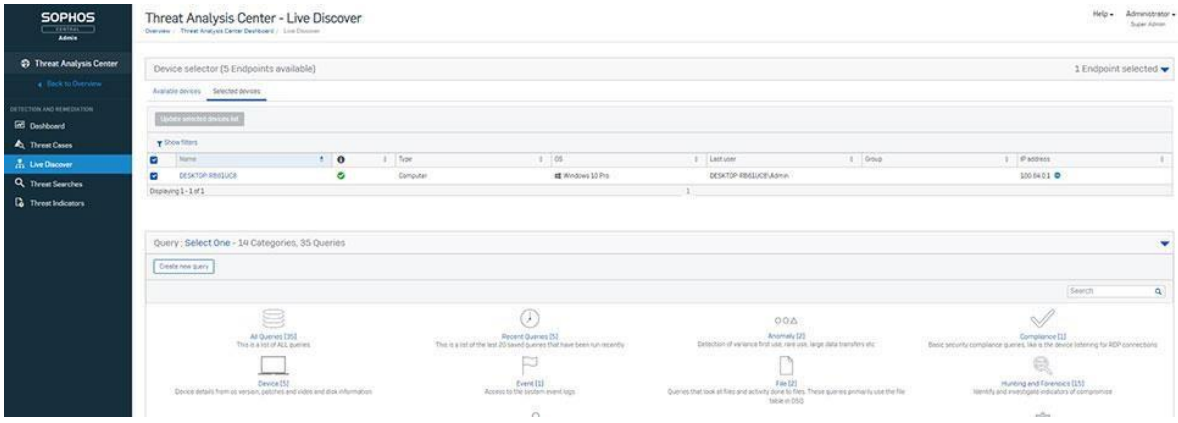


SOPHOS
Security made simple.

INTERCEPT X

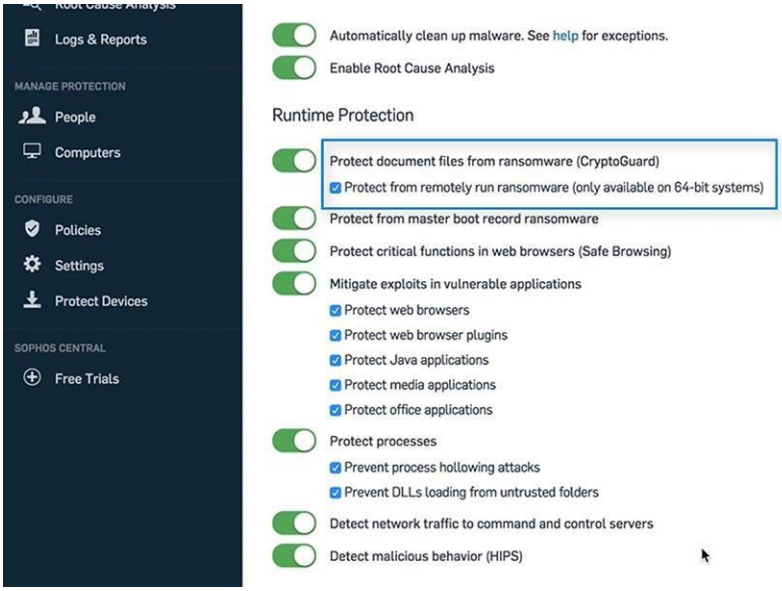
LA MEJOR PROTECCIÓN PARA ENDPOINTS DEL MUNDO
Malware • Ransomware • Exploits • Virus

Detección y respuesta para endpoints (EDR)
Integra una potente detección y respuesta para endpoints (EDR) con la protección para endpoints mejor valorada del mercado. Intercept X, diseñado tanto para las operaciones de seguridad TI como para la búsqueda de amenazas, detecta e investiga la actividad sospechosa con un análisis basado en IA. A diferencia de otras herramientas de EDR, añade experiencia, no personal, al replicar las habilidades de analistas difíciles de encontrar.



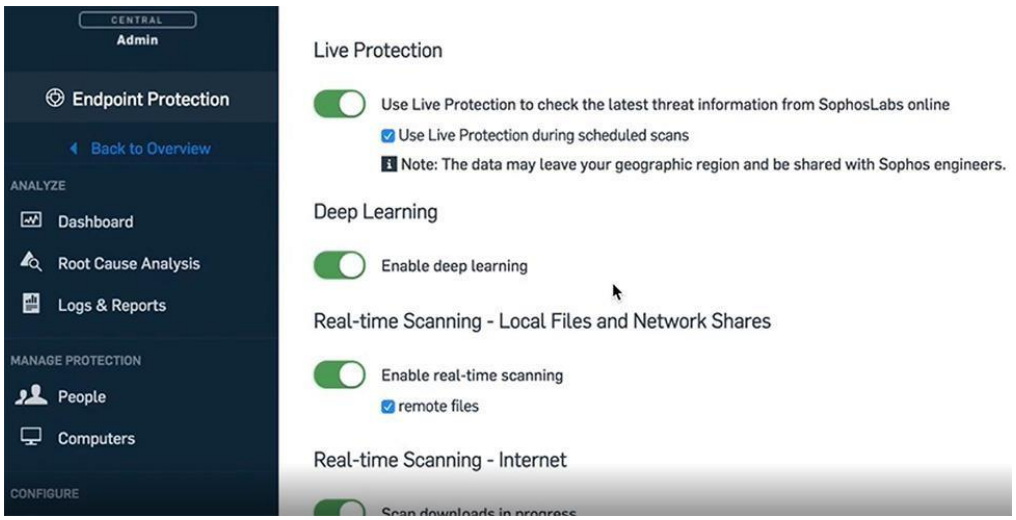
Antiransomware
Los ataques de ransomware actuales a menudo combinan múltiples técnicas avanzadas con hacking en tiempo real. Para minimizar el riesgo de caer víctima, necesita una protección avanzada que monitorice y proteja toda la cadena de ataque.

Sophos Intercept X le proporciona tecnologías de protección avanzada que desestabilizan toda la cadena de ataque, incluido el Deep Learning para prevenir los ataques de forma predictiva y CryptoGuard para revertir el cifrado no autorizado de archivos en segundos.



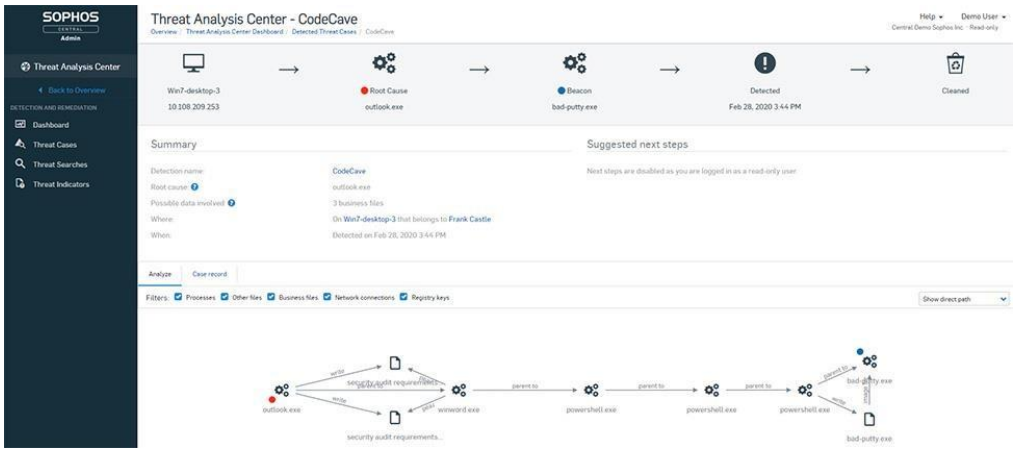
Tecnología de Deep Learning

una forma avanzada de Machine Learning, Intercept X está cambiando la seguridad de los endpoints de un enfoque reactivo a uno predictivo a fin de proteger contra amenazas tanto conocidas como nuevas. Aunque muchos productos afirman utilizar el aprendizaje automático, no todo el aprendizaje automático se crea de la misma manera. El Deep Learning ha superado sistemáticamente otros modelos de Machine Learning en la detección de malware.



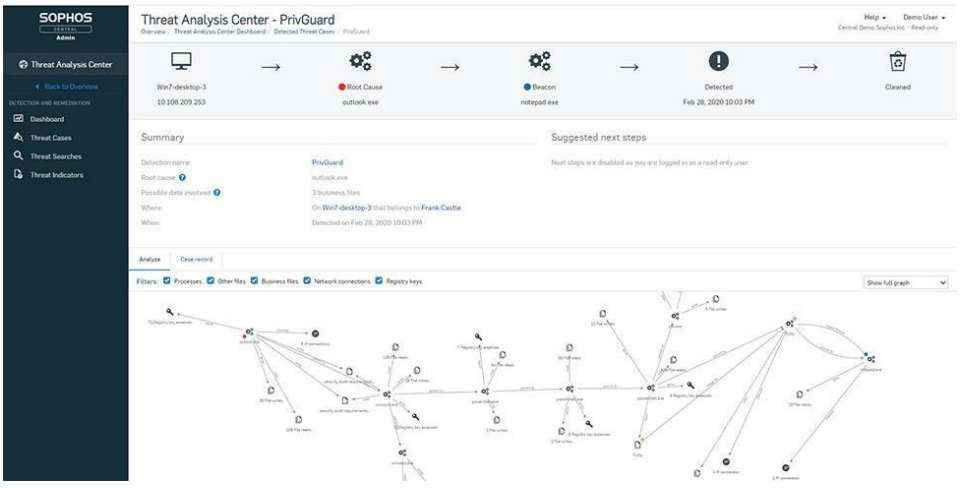
Prevención de exploits

La prevención de exploits detiene las técnicas utilizadas en los ataques basados en exploits sin archivos y sin malware. Aunque hay millones de aplicaciones de malware y miles de vulnerabilidades de software esperando a ser explotadas, solo existen unas pocas técnicas de exploits de las que se sirven los hackers como parte de la cadena de ataque. Al arrebatar a los hackers las herramientas clave que tanto les gusta utilizar, Intercept X detiene los ataques de día cero antes de que puedan iniciarse.

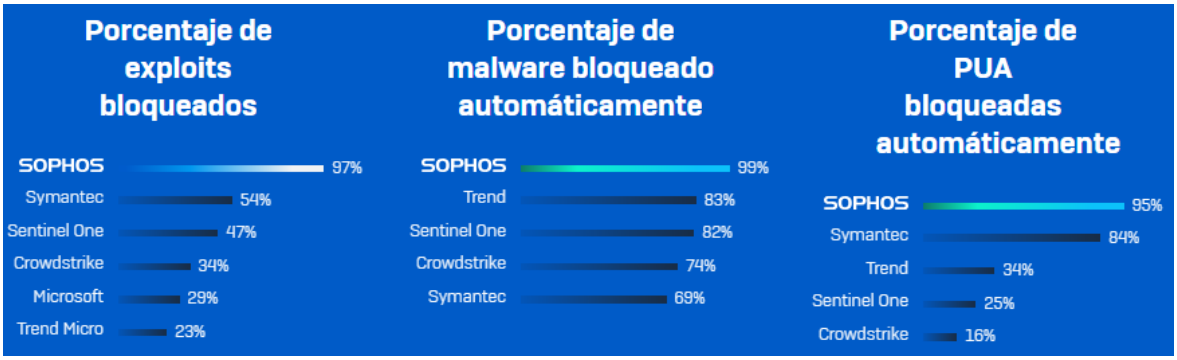


Mitigaciones de adversarios activos

Intercept X utiliza diversas técnicas, entre ellas, la prevención de robos de credenciales, la detección del uso de cuevas de código y la protección de llamadas a procedimientos de aplicaciones (APC) que usan los atacantes para hacerse presentes y pasar inadvertidos en las redes de la víctima. Ahora que los atacantes se centran cada vez más en técnicas que van más allá del malware para moverse entre sistemas y redes como usuarios legítimos, Intercept X detecta y previene este comportamiento a fin de impedir que los atacantes lleven a cabo su misión.



N.º 1 en protección
En pruebas de terceros independientes, Sophos bloquea sistemáticamente más malware y exploits que las soluciones de la competencia. Pero compruébelo usted mismo.



Benefíciese del poder de una red neuronal de Deep Learning
Consiga una prevención de amenazas para endpoints inigualable. Intercept X utiliza Deep Learning, una forma avanzada de Machine Learning, para detectar malware tanto conocido como desconocido sin depender de firmas.

El Deep Learning hace que Intercept X sea más inteligente, escalable y efectivo contra las amenazas desconocidas. Intercept X se sirve del Deep Learning para superar a aquellas soluciones de seguridad que utilizan únicamente el Machine Learning tradicional o la detección basada en firmas.

Detenga el ransomware al instante
Bloquee los ataques de ransomware antes de que causen estragos en su empresa. Intercept X incluye tecnología antiransomware que detecta procesos de cifrado malicioso y los neutraliza antes de que puedan propagarse por la red. Evita tanto el ransomware de registro de arranque maestro como el basado en archivos.

Cualquier archivo que se haya cifrado se revierte a un estado seguro, lo que significa que sus empleados pueden seguir trabajando sin interrupciones, con un impacto mínimo en la continuidad empresarial. Recibirá información detallada posterior a la limpieza para que pueda ver cómo entró la amenaza, a qué afectó y cuándo se bloqueó.

Detección y respuesta para endpoints (EDR)
La primera EDR diseñada para analistas de seguridad y administradores de TI

Intercept X Advanced with EDR le permite hacer cualquier pregunta sobre lo que ha ocurrido en el pasado y lo que está ocurriendo ahora en sus endpoints. Busque amenazas para detectar adversarios activos o aplíquelo a sus operaciones de TI a fin de mantener la higiene de su seguridad informática. Cuando se encuentre un problema de forma remota responda con precisión. Al empezar con la protección más sólida, Intercept X detiene las filtraciones antes de que comiencen. Reduce el número de elementos que investigar y le ahorra tiempo.

- La protección más sólida combinada con una potente EDR.
- Añada experiencia, no personal.
- Diseñada para la operación de TI y la búsqueda de amenazas.

TARJA SOFTWARE, S.R.L.
RNC: 131-85010-3

SOPHOS
Security made simple.

Funciones de Sophos Intercept X.

	Características	
EXPLOIT PREVENTION	Aplicación de la prevención de ejecución de datos	✓
	Selección aleatoria del diseño del espacio de direcciones obligatoria	✓
	ASLR de abajo a arriba	✓
	Página NULL (Protección de desreferencia NULL)	✓
	Asignación de pulverización del montón	✓
	Pulverización dinámica del montón	✓
	Eje de la pila	✓
	Ejecución de la pila (MemProt)	✓
	Mitigaciones de ROP basadas en pilas (Autor de llamada)	✓
	Mitigaciones de ROP basadas en ramas (Asistidas por hardware)	✓
	Sobrescritura del controlador de excepciones estructurado (SEHOP)	✓
	Filtrado de tabla de direcciones de importación (IAF)	✓
	Carga de bibliotecas	✓
	Inyección de DLL reflectiva	✓
	Shellcode	✓
	Modo Dios de VBScript	✓
	Wow64	✓
	Syscall	✓
	Vaciado de procesos	✓
	Secuestro de DLL	✓
	Omisión de AppLocker Squiblydoo	✓
	Protección de APC (Double Pulsar / AtomBombing)	✓
	Aumento de privilegios de procesos	✓
	Protección shellcode dinámica	✓
	EFS Guard	✓
	CTF Guard	✓
	ApiSetGuard	✓
MITIGACIONES DE ACTIVE ADVERSARY	Protección contra robos de credenciales	✓
	Mitigación de cuevas de código	✓
	Protección contra Man-in-the-Browser (Navegación segura)	✓
	Detección de tráfico malicioso	✓
	Detección de shell Meterpreter	✓

	Características	
ANTI-RANSOMWARE	Protección contra archivos de ransomware (CryptoGuard)	✓
	Detección automática de archivos (CryptoGuard)	✓
	Protección del registro de arranque y disco (WipeGuard)	✓
BLOQUEO DE APLICACIONES	Navegadores web (incluido HTA)	✓
	Complementos de navegadores web	✓
	Java	✓
	Aplicaciones multimedia	✓
	Aplicaciones de Office	✓
PROTECCIÓN CON DEEP LEARNING	Detección de malware con Deep Learning	✓
	Bloqueo de aplicaciones no deseadas (PUA) con Deep Learning	✓
	Supresión de falsos positivos	✓
RESPONDER INVESTIGAR ELIMINAR	Casos de amenazas (Análisis de causa raíz)	✓
	Sophos Clean	✓
	Seguridad sincronizada con Security Heartbeat	✓

7

TARJA SOFTWARE, S.R.L. PIVC: 131-85010-3

Descripción de los bienes y servicios:

Licencias de Antivirus-PGR				
ITEMS	BIENES Y/O SERVICIOS	CANTIDAD	CUMPLE	NO CUMPLE
1	Solución de antivirus para estación de trabajo	850	Si	

Confirmamos que los productos ofertados cumplen al 100% todas las funcionalidades requeridas en este pliego. Los productos ofertados son:

1. SOPHOS Central Intercept X Advanced with EDR/XDR: Protección para usuarios.
    a. Enlace: https://www.sophos.com/es-es/products/endpoint-antivirus.aspx
    b. Specs: https://www.sophos.com/es-es/products/endpoint-antivirus/tech-specs.aspx
2. Soporte del fabricante 24x7.

Plazo de entrega del licenciamiento.

Las licencias serán entregadas vía correo electrónico en un periodo de 24 a 48 horas a partir de la emisión de la orden de compra.

El periodo de vigencia de las licencias ofertada es de **d o c e (12) m e s e s** para la solución de antivirus.

CRONOGRAMA ENTREGA DE LICENCIA	Duration
Generar licencia Antivirus	**2 dias**
Pre-requisitos para la entrega	**0.5 dia**
Orden de compra	0.5 dia
Gestión con fabricante	**1.5 dias**
Entrega de licenciamiento Antivirus	1.5 dias

Servicios profesionales.

Los servicios profesionales serán coordinados con el departamento de tecnología para iniciar los trabajos. Estos servicios contemplan el despliegue de hasta (15) agentes y (10) políticas requeridos por la PGR. Adicionalmente, incluimos las certificaciones que nos avalan como técnicos expertos en las herramientas ofertadas en este proceso.

Condiciones de pago.

Validamos como bueno y valido las condiciones de pago, según las especificaciones de los términos de referencia en el punto **6. Condiciones de pago. Pagos realizados en un periodo de treinta (30) días.**

Referencia de Proyectos Similares:

- **Banco de Ahorro y Crédito del Caribe**
  Sr. Wayner Castillo
  Encargado de Seguridad
  Móvil (809) 904-9668
  wcastillo@bancobacc.com.do

- **COOP ECLOF**
  Sr. Omar Concepción
  Director de TI
  Móvil (809) 333-5273
  opconcepcion@coopeclof.com

TARJA SOFTWARE, S.R.L. RNC: 131-85010-3

- **Minino Abogados**
  Sr. Ariel Almonte
  Consultor de tecnología
  Móvil (809) 566-7414
  itsupport@minino.com.do

- **CORAAPPLATA**
  Sr. Felipe Diaz
  Encargado de tecnología
  Móvil (809) 586-2461
  felipediaz@coraapplata.gob.do

Cordialmente

TARJA SOFTWARE, SRL **PGR**