Transporte

ANEXO No. 1

FICHA TECNICA

OBJETO: RENOVAR EL LICENCIAMIENTO DE LA SOLUCIÓN DE SEGURIDAD PARA ENDPOINTS, ASÍ COMO DEL MÓDULO RESPUESTA PARA XDR ((EXTENDED DETECTION AND RESPONSE), COMO PARTE DE LA SEGURIDAD TECNOLÓGICA DE LOS DATOS EN EL MINISTERIO DE TRANSPORTE.

ESPECIFICACIONES TÉCNICAS MINIMAS.

A continuación, se establecen las condiciones mínimas técnicas exigidas que debe cumplir el contratista:

Línea	PRODUCTO	CANTIDAD	ADQUISICIÓN Y RENOVACIÓN
Renovación	**Trend Micro Smart Protection for Endpoint** licencias a 1.050 para usuario	1050 LICENCIAS	Renovación de Licenciamiento de la **Suite Trend Micro Smart Protection** for Endpoint incluyendo los siguientes módulos o funciones: 1 APEX CENTRAL ONPREMISE 2.APEX CENTRAL 2.1 PLUGIN IDF 2.2 PLUGIN VDI 2.3 PLUGIN MAC 3.SERVER PROTECT 4.PLUGIN DE VULNERABILITY PROTECTION EN ENDPOINT 5.WORRY-FREE SERVICE 6.PLUGIN APPLICATION CONTROL 7.ENDPOINT ENCRYPTION/FILE ENCRIPTION 8. MOBILE SECURITY 9. SCAN MAIL (EXCHANGE/DOMINO) Por cada producto de la suite del Antivirus y para la solución de detención de amenazas avanzadas, el proveedor debe ofrecer la última versión disponible en el mercado o la que el Ministerio requiera y esté soportada por la casa Matriz.
Renovación	**Trend Micro Vision One Pro** (Protección de Servidores Avanzada)	300 LICENCIAS	Renovación de Licenciamiento de Trend Micro Vision One Pro que incluye los siguientes módulos o funciones: 1. CLOUD ONE WORKLOAD SECURITY 2. ANTIMALWARE PROTECTION 3. FILE INTEGRITY MONITORING 4. INTRUSION PREVENTION CON PARCHADO VIRTUAL 5. FIREWALL DE HOST 6. CONTROL DE APLICACIONES
Renovación	**Trend Micro Vision One Credits** que cubra la totalidad de los end	38500 licencias del componente de XDR	Renovación de Licenciamiento de Trend Micro Vision One Credits que incluya las funciones XDR para EndPoints, usuarios y

	points, usuarios y Servidores con XDR	(Detección y respuesta a amenazas e incidentes cibernéticos proactivamente)	de la misma marca de la protección de EndPoints y servidores de la entidad
Renovación	**Trend Micro Vision One Credits ASRM** que cubra la totalidad de los End points y Servidores con ASRM	27000	Renovación de Licenciamiento de Trend Micro Vision One Credits para la funcionalidad de visibilidad Avanzada ASRM 1. VISION ONE ASRM PARA LA TOTALIDAD DE ENDPOINTS Y SERVIDORES DE LA ENTIDAD.
Renovación	**Trend Vision One Email and Collaboration Security** - Core que cubra la totalidad de los usuarios de O365	1250	Renovación del licenciamiento para la protección de las herramientas ofimáticas y de colaboración que componen la suite de MICROSOFT 365 que cumpla con mínimo las siguientes características: que incluya como mínimo las siguientes características: 1. Protección avanzado y completo de amenazas a través de capacidades de protección en el tenant de colaboración de Microsoft 365 para los servicios de correo, One Drive, SharePoint, Teams y Chat de Teams teniendo como premisa las capacidades avanzadas de protección que permitan la identificación de suplantación a través de BEC y logrando capacidades. 2. Capacidad de integración a través de API con Microsoft 365 para garantizar que no existan retrasos en la entrega de correos por saltos adicionales en el flujo de correo y protección avanzada de amenazas vía API para la protección de amenazas y prevención de fuga de información en los servicios de SharePoint, y OneDrive en Microsoft 365. 3. Implementación granular y segmentación por grupos para garantizar que se puedan tener diferentes políticas a usuarios dependiendo su rol y función dentro de la entidad, así como fácil administración centralizada con múltiples componentes. 4. La solución debe integrarse nativamente en la misma consola de ASRM para entregar telemetría a la consola unificada y permitir calcular el nivel de riesgo de los usuarios en Microsoft 365 a partir de su

			comportamiento, amenazas recibidas, entre otros; esto con el fin de aumentar la precisión en el cálculo de riesgo corporativo.
Instalación, Configuración y puesta en funcionamiento.			El contratista debe realizar la instalación, configuración y puesta en funcionamiento de toda la solución (equipos de cómputo, servidores, consolas, etc) Entiéndase por instalación la validación de la solución, es decir que se encuentre debidamente desplegada en la totalidad de los equipos de punto final (PC y portátiles de usuario final) así como en los servidores centralizados en el Datacenter y en el servicio de correo electrónico, para alcanzar los objetivos de protección ante las ciberamenazas que surgen diariamente.
Soporte	- Soporte 8x5 para atención de incidentes no críticos - Soporte reactivo ante incidentes cibernéticos sin restricción de tiempo		Entiéndase como soporte técnico el soporte que el contratista debe brindar cuando la solución presente algún tipo de falla. El contratista deberá garantizar el soporte técnico para la solución integral de Trend Micro, si es necesario en sitio (8x5) de lunes a viernes, sea en modalidad presencial o remota desde la consola del producto, a todas las estaciones conectadas que tengan el producto instalado. Del mismo modo debe garantizar el soporte y la actualización desde las instalaciones físicas del Ministerio de Transporte a los servidores y PC's que utilicen el producto Trend Micro instalado durante el término de vigencia y de garantía de las licencias adquiridas. El proveedor debe contar con un plan de atención y respuesta a incidentes que apoye cualquier ataque cibernético que pueda ocurrir en el Ministerio y en caso de materialización de un incidente cibernético (esto incluye un ataque de ransomware) debe adjuntar o describir el contenido del Plan de Respuesta a Incidentes en este sentido Para lo anterior el contratista deberá disponer de mínimo el siguiente personal: Presentar al supervisor del contrato dentro de los **dos (2) días hábiles siguientes a la**

		suscripción del acta de inicio el equipo mínimo de trabajo para la ejecución: **Perfil: Dos (2) técnicos**. **Formación académica**: dos (2) técnicos, tecnólogos o profesionales en sistemas, en telecomunicaciones, electrónico o afines con certificados requeridos en los niveles "Expert" o "Elite" en las soluciones del fabricante Trend Micro. **Experiencia: mínimo dos años de experiencia en la administración, soporte y resolución de problemas de soluciones de TrendMicro** **Actividades para desarrollar:** que Atenderán casos de soporte, para lo cual el contratista deberá allegar una matriz de comunicaciones con lo que disponga la entidad para la atención de casos de soporte de acuerdo con su nivel de criticidad. Para la valoración y aprobación del personal se debe presentar junto con la propuesta los siguientes documentos: 1. Hoja de vida. 2. Actas de grado. 3. Tarjeta Profesional 4. Diplomas. 5. Las certificaciones solicitadas.
ANS para el esquema de soporte	Todo el soporte a la solución se regirá bajo el siguiente ANS:	

Nivel de atención	Características del evento	Tipo de soporte	Efecto	Tiempo de respuesta	Penalidad
5	Crítico	Soporte reactivo	Afecta la operación del negocio. Ej. Servidor de base de datos caído.	Atención inmediata Tiempos de respuesta: **telefónica 30 minutos** **Asistencia en sitio 2 horas siguientes**	Si no se tiene respuesta en el tiempo requerido se remite NOTA al fabricante, para su evaluación como canal de distribución
4	Urgente	Soporte reactivo	Puede afectar la operación del negocio si no se resuelve en un plazo razonable de tiempo. Requiere atención urgente: Ej. No entran correos	Atención correctiva con prioridad Tiempos de respuesta: **Telefónica 2 horas** **Asistencia en sitio 4 horas siguientes**	Deberá otorgar una charla de sensibilización al personal de GTIC de 1 hora máximo al siguiente mes del incumplimiento.

				desde un dominio especifico.		
	3	Importante	Soporte 8x5	No afecta la operación del negocio, pero se requiere dar solución.	**Telefónica 4 horas** **Asistencia en sitio el transcurso de la semana**	Deberá parametrizar un informe personalizado en la consola, según lo requiera el Ministerio
	2	Monitoreo	Soporte 8x5	No afecta la operación del negocio Ej: Una prueba.	Atención en la semana siguientes al evento	No Aplica
	1	Información	Soporte 8x5	No requiere urgencia y es una verificación Ej. una consulta.	Durante el mes siguiente	No Aplica

Health Check	- Revisión general de configuraciones de toda la solución, esta revisión debe ser basada en las mejores prácticas sugeridas directamente por el fabricante Trend Micro)	Health Check - El contratista debe garantizar que la fábrica de la solución de Trend Micro realice dos (2) evaluaciones (assessments) en el año, una cada seis (6) meses, en las cuales se verifique el despliegue y configuración de la solución para el mejor uso de las funcionalidades disponibles, nuevas o actualizadas, para lo que entregará informe con lo realizado en cada revisión.
ATENCIÓN REACTIVA ANTE INCIDENTES CIBERNÉTICOS		Ante eventuales incidentes o ataques cibernéticos sin restricción de tiempo ataques de virus o cualquiera de sus derivados en el ámbito de seguridad que esté contenido dentro de la solución licenciada por Ministerio de Transporte y que llegue a afectar la solución informática implementada, GENERANDO INDISPONIBILIDAD, el contratista deberá proporcionar todo el recurso humano y tecnológico necesario, hasta el restablecimiento del servicio en un 100% sin restricción de tiempo y horario.
MANTENIMIENTO		El contratista deberá realizar mantenimiento preventivo presencial o remoto para verificar el correcto funcionamiento de la consola principal, una vez cada 30 días y/o cada vez aparezcan nuevos parches o actualizaciones importantes relacionadas con la solución, verificando la correcta actualización del software instalado y revisar los equipos que más reportes de virus estén presentando y hacer las respectivas recomendaciones referentes a últimos parches de seguridad y procedimientos contra: virus, gusanos, troyanos, entre otros, durante el tiempo de

	vigencia del contrato y de la garantía de la licencia, por el periodo de 12 meses.
MEMBRESIA DEL OFERENTE	El oferente debe tener membresía como distribuidor autorizado en uno de los dos niveles más altos (ELITE O EXPERT) según el programa de canales del fabricante y para certificar esto deberá adjuntar carta emitida por el fabricante de la solución con fecha de emisión no superior a 30 días al cierre de este proceso de contratación. El contratista debe mantener la membresía solicitada durante todo el plazo del contrato. En caso de oferentes plurales uno de los miembros deberá cumplir con este requisito.
ACTUALIZACIÓN DEL AGENTE:	Además de lo anterior, el contratista deberá proporcionar actualización automática y silenciosa de versiones, motores, políticas y últimas definiciones de virus en el Ministerio de Transporte durante los 12 meses de igual forma el proveedor debe también realizar recomendaciones sobre políticas de seguridad a la entidad vía telefónica, correo electrónico, chat, foro, o in situ.
SOPORTE IPV6	La suite de productos debe tener soporte nativo para funcionar en IPV6 y soporte para trabajar en IPV4 O DUAL STACK
Transferencia de conocimiento (A los funcionarios designados de los detalles de la implementación de la solución integral en la Entidad)	Efectuar la transferencia de conocimiento por un mínimo de 8 horas para mínimo dos funcionarios que designe el supervisor del contrato, dicha transferencia de conocimiento podrá dictarse durante la etapa de implementación y afinamiento de toda la solución de Trend micro que tiene la entidad y sobre las nuevas funciones que se adquieren en virtud del presente proceso a los funcionarios, que durante la ejecución del contrato que serán designados el supervisor del contrato. Finalizada la transferencia de conocimiento se debe entregar el respectivo certificado de asistencia.
GARANTÍAS	Las soluciones cuentan con garantía de 1 año y que en caso de actualizaciones de las soluciones se garantiza el funcionamiento del software sin que la entidad deba incurrir en costos adicionales.

Para cumplir el objeto del contrato, el contratista deberá en cumplir y satisfacer las especificaciones técnicas en cada licencia y que a continuación se relacionan.

REQUERIMIENTOS BASE PROCESO RENOVACIÓN Y OPTIMIZACIÓN DE TRENDMICRO
CARACTERISTICAS
La solución de protección de Antimalware se debe poder desplegar 100% en Nube y debe permitir como mínimo las características de Antimalware, Control de Aplicaciones y de dispositivos, protección avanzada contra Ransomware, mitigación de vulnerabilidades a través de parches virtuales y protección de fuga de información a través de expresiones regulares, diccionarios y características de los archivos.
La solución de protección Antimalware debe permitir la implementación de protección antimalware, control de aplicaciones, control de dispositivos, prevención de fuga de información, reputación web, mitigación de vulnerabilidades a través de parches virtuales en un solo agente.
La solución debe permitir hacer backup y restauración automática de archivos ante intentos de cifrado no autorizados, con el fin de generar una protección proactiva contra Ransomware.
La solución debe tener la capacidad de brindar protección contra malware, virus de red, conexiones sospechosas, amenazas web, spyware, análisis de archivos adjunto de correo POP3, monitoreo de comportamiento, ataques combinados y ataques de día cero para equipos de punto final (Endpoint).
La solución debe contar con firewall (reglas de conexiones de aplicación, IP, puerto y protocolo), reputación de archivos y/o reputación web, que permita la creación de políticas a través de aplicaciones, aplicaciones específicas, llaves de registro de aplicaciones y estas se podrán aplicar a través de UDP, TCP y ICMP con puertos y direcciones IP definidas según las necesidades.
La solución debe tener la capacidad de aislar los equipos o ponerlos en cuarentena cuando se detecta algún ataque para evitar la propagación de este dentro de la red.
La solución debe bloquear procesos comúnmente asociados a Ransomware y debe finalizar los programas que muestren un comportamiento anormal asociado con ataques de explotación.
La solución debe tener un módulo de monitoreo de eventos que permita monitorear permitir, denegar y preguntar cuando sea posible cambios en los archivos host de las maquinas, nuevos servicios, modificación de archivos de sistema, modificación de la política de seguridad entre otros.
La consola de administración debe tener un módulo de monitoreo de comportamiento, reputación web, conexiones sospechosas, protección de vulnerabilidades, control de dispositivos y control de aplicaciones.
La solución debe tener la capacidad de analizar la reputación de archivos y recuperarlos cuando sean enviados a cuarentena. Además, debe permitir realizar escaneos de los Endpoint de forma manual, programada y en tiempo real.
La solución debe permitir la configuración de los tipos de eventos que serán notificados y visualizados en el agente, y adicionalmente configurar el mensaje de las alertas dependiendo de la criticidad del evento (High, Medium, Low), además se debe tener la capacidad de eliminar de los logs de los eventos del sistema, servidor y agentes con una frecuencia especifica.
La solución de protección de endpoints debe permitir crear políticas de protección y descubrimiento de información confidencial a través de DLP en el mismo agente de protección de malware para agentes internos y externos las cuales permitirán bloquear la fuga de información a través de clientes de correo, ftp, http, https, mensajería instantánea, web mails, protocolo SMB, impresiones, dispositivos removibles, Windows clipboard y servicios de almacenamiento cloud. Todo esto se debe hacer sobre el mismo agente de protección de Endpoints, device control y reputación web.
La solución debe permitir crear identificadores de datos a través de palabras claves, atributos de archivos y expresiones regulares; además la solución debe permitir probar las expresiones regulares directamente en la plataforma.
Los templates de DLP de la solución deberán permitir definir la severidad de alto, medio, bajo como mínimo.
La solución deberá permitir tener políticas de control de aplicaciones en el mismo agente de DLP, control de dispositivos, XDR y protección de Endpoints, donde se puedan crear políticas para permitir las aplicaciones o bloquearlas y también debe permitir un modo de evaluación.
El control de aplicaciones debe permitir, bloquear o importar aplicaciones para la configuración de las políticas y deberá tener por defecto como mínimo las siguientes categorías de aplicaciones: Browsers y herramientas de browser, mensajería instantánea, productividad, P2P, cifrado, aplicaciones altamente

REQUERIMIENTOS BASE PROCESO RENOVACIÓN Y OPTIMIZACIÓN DE TRENDMICRO
CARACTERISTICAS
riesgosas y en esta última como mínimo debe tener la posibilidad de bloquear key loggers, Crackers de contraseñas y proxys anónimos.
El control de aplicaciones de la solución debe tener un score de las aplicaciones basado en popularidad y reputación y deberá tener un campo del uso global de la aplicación.
La solución de seguridad EDR – XDR que el Ministerio de Transporte debe renovar, es una combinación de servicios desplegados en nube pública y de agentes que se deben instalar en los dispositivos de punto final. Esta solución consta de los siguientes módulos: *Tabla 1. Detalle de los módulos que se deben renovar de la solución de EDR-XDR de TrendMicro*

Módulo	Unidad	Cantidad
Smart Protection for Endpoint suite (Equipos de Usuario final). Conformado por: • Worry-Free™ Services • Apex One Virtual Device Infrastructure add-on • Apex Central Advanced Edition - Multi-lingual • ServerProtect for Microsoft Windows/Novell NetWare • ServerProtect for Linux • Apex One Endpoint Protection • Trend Micro Apex One™ as a Service • Apex One and Apex Central Full Feature for Windows and Mac • Mobile Security • Apex One DLP add-on • Apex One Application Control add-on • Trend Micro Endpoint Encryption - Full Disk Encryption and File Encryption • Security for Mac • Apex One Vulnerability Protection add-on • Advanced Endpoint Security • Sandbox Submission	Agente por Endpoint	1050
Trend Vision One Endpoint Security – Pro (Servidores)	Agente por Endpoint	300
Trend Vision One Email and Collaboration Security – Core (Protección de servicios colaborativos y buzones de correo electrónico en nube)	Licencia por cuenta de usuario	1250
Trend Vision One Credits (Créditos para acceder a los servicios de nube)	Crédito	65500

Por tratarse de servicios desplegados en la nube pública de TrendMicro, a la fecha este tipo de servicios solo cuenta con versionamiento de agentes para usuario final, es decir los instaladores que se deben desplegar en cada computados y servidor que se proteja con la solución. Cuando estos agentes son presentados a la consola principal pueden ser actualizados y llevados hasta las versiones más recientes que el fabricante libere en el mercado, razón por la cual no se habla de versiones de la solución para los módulos de nube relacionados en la tabla.
La solución de protección de endpoints debe permitir tener un módulo de control de dispositivos que permita aplicar políticas a agentes internos y externos teniendo en cuenta si la maquina esta fuera o dentro de la red interna. El módulo de control de dispositivos debe como mínimo permitir los siguientes dispositivos: Floppys, CD/DVD, unidades de red, unidades de almacenamiento USB, adaptadores bluetooth, dispositivos de

REQUERIMIENTOS BASE PROCESO RENOVACIÓN Y OPTIMIZACIÓN DE TRENDMICRO
CARACTERISTICAS
imagen, dispositivos infrarrojos, módems, NICs Wireless y debe permitir bloquear la tecla Print Screen para optimizar los niveles de protección.
El módulo de control de dispositivos debe permitir tener un listado de USB permitidas y de aplicaciones permitidas para que interactúen con dispositivos bloqueados. Además, debe tener la opción de bloquear la función AutoRun en dispositivos de almacenamiento USB.
La solución debe permitir tener reglas de prevención de intrusos de host y debe mostrar como mínimo el identificador, el nombre de la regla, el tipo de aplicación, la severidad, el tipo, el CVE al que está asociado la regla, la última actualización y estas reglas se deben poder aplicar en modo detección y prevención.
La solución deberá ser capaz de realizar una inspección profunda de los paquetes bidireccionalmente para analizar y prevenir ataques a vulnerabilidades en las aplicaciones instaladas en cada servidor, incluidas vulnerabilidades conocidas y de día cero.
La solución debe permitir tener capacidades diferenciales para servidores y debe poder incluir módulos de Antimalware, File Integrity Monitoring, Control de aplicaciones, Firewall, prevención de Intrusiones en host, escaneos de vulnerabilidades recomendados y deben ser administrado sobre una única consola de la solución usando un único agente.
La Consola debe permitir para los servidores proporcionar monitoreo continuo para visibilidad instantánea y completa del entorno, notificaciones en tiempo real de las actividades y eventos que ocurran; permitir la generación de reportes customizables y desde el mismo dashboard de la consola de la solución poder administrar entornos físicos, virtuales y en la nube.
La solución deberá detectar automáticamente nuevos servidores en los diferentes sistemas de infraestructuras de servidores públicas y privadas en vCenter, AWS, Microsoft Azure, vCloud Air, Directorio Activo.
Las vulnerabilidades deberán ser protegidas frente aquellas descubiertas recientemente y aplicando la protección en los servidores sin tener que reiniciar el sistema o modificar el código fuente de la(s) aplicación(es) o sistema operativo.
La solución deberá contar con la capacidad de realizar escaneos de recomendaciones bajo demanda y programados para servidores, sin límite de escaneos, para detectar vulnerabilidades relacionadas con la plataforma (sistema operativo, aplicativo de servidor web y aplicativo de servidor de aplicaciones) sobre la cual están montados los sitios web expuestos a Internet.
PROTECCIÓN DE CORREO Y HERRAMIENTAS DE COLABORACIÓN
La solución de protección de correo debe ser mono marca con la solución de protección para endpoints y la solución de XDR para garantizar la visibilidad y protección en múltiples puntos.
La solución deberá tener la capacidad para proteger correos internos de la organización que provengan de la plataforma de Microsoft Office 365 y Google WorkSpace.
La solución deberá tener la capacidad para proteger correos de dominios externos y ajenos a la empresa que provengan de la plataforma de Microsoft Office 365 y Google WorkSpace.
La solución deberá tener motores para la detección de malware con la capacidad de identificar Exploits en documentos y archivos de Office.
La solución deberá tener escaneo de URL en el cuerpo de los correos y en los archivos adjuntos, además debe tener protección para OneDrive, SharePoint, Google Drive, Box y Dropbox entre otros, esto se debe hacer sin requerir enrutamiento de los registros MX.
La solución deberá tener plantillas customizables de DLP para controlar la fuga de información permitiendo realizar pruebas de expresiones regulares y listados de palabras para nuevas plantillas, estas políticas se deben poder aplicar a los servicios de Microsoft 365 de correo, OneDrive, SharePoint, Google Drive y correo en Google WorkSpace con la capacidad de descubrir y reportar violaciones a las políticas.

REQUERIMIENTOS BASE PROCESO RENOVACIÓN Y OPTIMIZACIÓN DE TRENDMICRO
CARACTERISTICAS
La solución deberá tener la capacidad desde la consola en la nube, de crear políticas basadas en reglas según el correo entrante o saliente y a los cuales se les pueda personalizar las acciones a tomar en categorías de (Clean, Delete, Tag, encriptar, notificar).
La solución deberá tener la capacidad de analizar los enlaces que se encuentren en el cuerpo del mensaje de los correos electrónicos, igualmente debe tener la capacidad de analizar los enlaces que se encuentren ocultos en el cuerpo del mensaje, ya sea en botones, banners o imágenes en el momento en el que el usuario le dé clic en el enlace.
La solución debe proporcionar protección contra ataques de BEC (Bussiness Email Compromise) con el análisis de los mensajes.
La solución debe tener la capacidad de realizar un análisis avanzado de los archivos usando Machine Learning, para identificar amenazas que aún no han sido reportadas, pero que pueden generar una afectación sobre los datos o el sistema que está utilizando el usuario.
La solución debe permitir a los administradores configurar la lista de excepciones, de los archivos detectados mediante Machine Learning como maliciosos o sospechosos.
La solución debe permitir restaurar archivos que sean enviados a cuarentena ya sea por fueron detectados como maliciosos o que no cumplen con las políticas de Prevención de filtración de datos de la organización.
La solución debe permitir realizar un escaneo manual en modo de evaluación para permitir a los administradores verificar las reglas que serán aplicadas para proteger Office 365 sin tomar ninguna acción sobre dichos correos o archivos.
CONSOLA DE ADMINISTRACION
La consola de administración debe 100% cloud y debe permitir la protección de Endpoints, servidores, correo y XDR.
La solución debe permitir tener consolas adicionales que se pueden desplegar Onpremise o SaaS para cifrado y protección de móviles del mismo fabricante. Estas consolas se deben poder administrar de manera independiente a las consolas de Endpoints, servidores y XDR.
La solución debe permitir la creación, modificación y eliminación de roles y usuarios para la administración de esta.
La consola de administración debe permitir administrar los agentes instalados en la red de equipos. Permitiendo conocer el estado de los agentes.
La consola de administración debe estar en la Nube para garantizar la administración en todo el tiempo sin importar el lugar donde estén las maquinas administradas.
La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de estos.
La consola de administración debe permitir configurar notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de estos.
La consola de administración debe proporcionar un Dashboard que brinde información global sobre los agentes, eventos de reputación web, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.
La consola de administración debe permitir consultar los Logs de instalación tanto del agente como el del servidor de administración.
La consola de administración debe permitir visualizar estadísticas de históricos de actualizaciones de patrones de análisis de antivirus, antispyware, análisis de comportamiento, conexiones sospechosas, y exploits de los navegadores de internet.

REQUERIMIENTOS BASE PROCESO RENOVACIÓN Y OPTIMIZACIÓN DE TRENDMICRO
CARACTERISTICAS
La consola de administración debe permitir visualizar los logs de los eventos sobre los equipos donde se encuentra instalado el agente, dichos eventos deben estar relacionados a temas de malware, spyware, Reputación web, conexiones sospechosas, archivos sospechosos, Command & Control Callbacks, Behavior Monitoring, Machine Learning, control de dispositivos, DLP, y escaneos. Adicionalmente la solución debe permitir filtrar dichos logs por periodos de tiempo preestablecidos, por rangos de fechas y por tipo de escaneo.
La consola de administración debe permitir la visualización de los logs de registro de los eventos de la actualización del servidor de actualizaciones.
La solución debe tener un componente específico para la protección de servidores y equipos legados que contenga como mínimo protección de Antimalware, Monitoreo de Integridad de Archivos (FIM), inspección avanzada de logs, control de aplicaciones, Parchado virtual, firewall y XDR en un único agente y una consola unificada. Adicionalmente a esto la solución debe tener más de 8300 políticas de parchado virtual y debe como mínimo permitir crear reglas de monitoreo de integridad para archivos, llaves de registro y políticas personalizadas. Finalmente, la protección de amenazas para servidores debe hacer backup y restauración automática de archivos ante intentos de cifrado no autorizados y debe soportar más de 2000 kernels de Linux y sistemas operativos Windows 2003 en adelante. Un punto importante es que con el fin de mantener la disponibilidad de los servicios la solución no debe exigir reinicio en ningún momento del servidor cuando se instalen los agentes.
La consola de administración debe permitir la visualización de los logs de registro de los eventos del servidor de administraciones.
La solución debe contar con Dashboard que muestre las detecciones de Spam/Graymail y debe indicar el total de cuentas de Email en Microsoft y Google WorkSpace que tienen el sensor de XDR activado.
La consola de administración debe permitir tener un inventario de activos de correo donde se muestre la cuenta de usuario, la dirección de correo, ver si el sensor de XDR está activo, el nombre de los dominios protegidos, cuentas no administradas, entre otra información, para el acceso de esto no se debe requerir el acceso a consolas adicionales.
La consola de administración debe tener la capacidad de generar reporte en formato PDF, DOCX y XLSX y también en formato PDF protegidos con contraseña para los reportes de los servidores.
La consola de administración debe permitir visualizar a través de un Dashboard el riesgo corporativo y este debe calcularse como mínimo con las cuentas comprometidas, vulnerabilidades en los Endpoints y Servidores, actividad y comportamientos, actividad Cloud, configuraciones del sistema entre otro.
La consola de administración debe permitir visualizar el nivel de criticidad de los Endpoints y servidores a través de una marca y debe permitir personalizar el nivel de criticidad del riesgo para los activos, ver las vulnerabilidades que tiene el Endpoint y/o servidor, actividad cloud, usuarios y en general tener un perfil del activo, esto desde el mismo Dashboard.
La solución debe permitir marcar los usuarios críticos basados en su nivel de riesgo, la actividad por ubicación, dispositivos en los que trabaja e indicadores de riesgo y debe permitir la actividad de la cuenta por ubicación.
La plataforma debe mostrar listado de dispositivos descubiertos, dispositivos con agentes administrados y esto se debe poder filtrar por mes.
La solución debe tener un Dashboard donde se vea una descripción general de exposición, ataques y configuraciones de seguridad.
El dashboard de la descripción general de exposición debe mostrar una gráfica con el cubrimiento de vulnerabilidades, métricas y un listado del porcentaje de Endpoints vulnerables.
La plataforma debe permitir el envío de hasta 20 muestras de archivos diarios al SandBox dentro de la misma plataforma integrada de manera manual y esto deberá entregar un reporte en formato .pdf descargable.
AGENTES

REQUERIMIENTOS BASE PROCESO RENOVACIÓN Y OPTIMIZACIÓN DE TRENDMICRO
CARACTERISTICAS
Los agentes deben ser instalados mediante instalación web, link de instalación por correo, instalación por script, instalación remota, y/o paquete de instalación.
Los agentes deben requerir contraseña de administración para ser desinstalados de los equipos.
Las políticas de seguridad deben aplicarse en los agentes de forma individual y/o por grupos.
El agente debe tener la capacidad de eliminar los archivos sospechosos de forma automática.
La solución debe usar solo un agente para los endpoints para realizar la protección antimalware, parcheo virtual, DLP, control de aplicaciones y EDR.
Los agentes de EPP deben poder instalarse en sistemas operativos Windows desde Windows 2003 y deben soportar más de 2000 kernels de Linux
El agente de protección no debe requerir reinicio en servidores para garantizar la disponibilidad de los servicios.
Los agentes deben tener la capacidad de conectarse a múltiples fuentes de actualización (patrones, firmas, url sospechosas, etc.), si alguna de estas es inaccesible para el agente.
El licenciamiento debe permitir la instalación de agentes para móviles y cifrado diferentes a los usados para la protección de Endpoints y Servidores
Los agentes de cifrado deben integrarse con las soluciones de cifrado que vienen en los sistemas operativos. Microsoft BitLocker, Apple FileVault.
XDR
La solución debe permitir la detección de amenazas tipo Fileless a través de la exploración de memoria mejorada para detectar comportamientos de procesos sospechosos. El agente debe tener la capacidad de terminar los procesos sospechosos antes de que se pueda hacer cualquier daño.
La solución debe permitir evaluar el alcance del daño causado por un ataque dirigido, proporcionar información sobre la llegada y progresión del ataque y ayudar en la planificación de una respuesta efectiva a incidentes de seguridad.
La solución deberá permitir graficar toda la cronología de los eventos generados en una investigación por medio de un gráfico de anillos que muestra el número total de puntos finales clasificados ya sea estén relacionados, o no relacionados a otros procesos, en cola o cancelados. La información debe estar siendo actualizada en tiempo real y de forma automática mientras avanza una investigación.
La solución debe permitir la búsqueda de Indicadores de Compromiso (IoC) en búsqueda de comunicaciones específicas, actividad de registro, actividad de la cuenta autenticada en el sistema y procesos en curso. Además, debe permitir la integración con información externa de IoC (Indicators Of Compromises) como reglas STIX, TAXII
La solución debe permitir el análisis de comportamiento de un malware, actividades específicas de IoC y conexiones de comando a control.
La interfaz de la solución debe estar integrada con la consola de administración de las soluciones de seguridad para tener desde un solo punto el análisis, el contexto completo de los eventos y la línea de tiempo de los sucesos.
La solución debe escanear documentos en busca de códigos de exploits integrados y vulnerabilidades conocidas y controlar los programas que demuestran un comportamiento anormal asociado con ataques de exploits.
La solución debe analizar los archivos desconocidos de baja prevalencia utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso y debe ser capaz de recopilar datos y barrido del sensor en los endpoints (IOC) y almacenarlos de forma centralizada para su posterior análisis.
La solución debe tener la capacidad de asociar los datos de registro y logs de los procesos con otros artefactos de disco y/o memoria.
La solución debe tener la capacidad de identificar amenazas aun cuando usen PowerShell codificado y debe detectar tareas programadas maliciosas además se debe mostrar todos los dispositivos en los que un proceso principal (padre) inicia otros procesos (hijos) especialmente de tipo PowerShell y cmd.

REQUERIMIENTOS BASE PROCESO RENOVACIÓN Y OPTIMIZACIÓN DE TRENDMICRO
CARACTERISTICAS
La solución debe contar con la capacidad de mostrar la línea de tiempo de incidentes y mostrar en una sola vista todo el ciclo de vida del ataque de la amenaza y debe revelar la cadena completa de procesos afectados por el malware/comportamiento malicioso.
La solución permitirá que el trabajo de investigación continúe en el dispositivo aislado sin permitir que se extienda la actividad maliciosa por medio de cuarentena y/o aislamiento de los sistemas infectados.
La solución de EDR no debe requerir un agente adicional a los agentes de Endpoint Protection instalados en las máquinas de la compañía y debe permitir la correlación entre, endpoints y servidores en la misma consola unificada.
XDR debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques y estos deben tener la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad.
Los modelos de correlación deben combinar múltiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.
XDR debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos y estos gráficos deben mostrar una representación visual de los objetos que levantaron la alerta y la relación entre ellos.
Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las accionas que una amenaza llevó a cabo en un servidor, Endpoint, o carga de trabajo en la nube.
Debe permitir la búsqueda proactiva a través de Endpoint, correo y servidores (como telemetría, NetFlow, meta data, etc.) usando un simple constructor de consultas sobre una consola unificada.
La solución debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros y filtrar los resultados añadiendo criterios adicionales de búsqueda, también debe detectar proactivamente con búsquedas automáticas de IoC publicados por el “vendor”.
Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz, además las búsquedas deben permitir construir, guardar y reutilizar búsquedas para Threat Hunting básico.
La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.
En una sola ubicación debe poder ver el estado de respuestas en Endpoint, email, servidores y red y con mínimo debe mostrar la siguiente información: identificador de la tarea ejecutada, acción, objetivo, usuario que la creo, desde donde fue creada y fecha de la última actualización. Además, la solución debe permitir la creación de scripts personalizados en (power Shell script) .ps1 y (bash Script).
Debe permitir ejecutar acciones de respuesta rápidamente haciendo clic derecho en el incidente y desde los resultados de búsqueda de Threat Intelligence. Las respuestas como mínimo deben ser: aislar un Endpoint, ejecutar un script personalizado, iniciar un Shell remoto, adicionar a una lista negra, entre otros.
La solución debe exponer una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR y debe permitir obtener un listado con los detalles de los Endpoints, obtener un listado de alertas con sus detalles y modificar su estado, adicionar y remover objetos sospechosos de una lista negra, entre otras.
Las alertas deben permitir ver un análisis de causa raíz para identificar el alcance del impacto y permitir tomar acciones de respuesta.
La solución debe tener modelos avanzados de detección y respuesta para correo y como mínimo debe permitir tener modelos de Spear Phishing, Acceso web sospechoso después de un correo electrónico sospechoso, detección de Ransomware por correo, Ataques via Link, Correo electrónico sospechoso con enlace de redireccionamiento detectado, entre otros, estos modelos se deben poder activar o desactivar según las necesidades de la entidad

REQUERIMIENTOS BASE PROCESO RENOVACIÓN Y OPTIMIZACIÓN DE TRENDMICRO
CARACTERISTICAS
Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado)
La solución de protección de correo y XDR debe permitir seleccionar los grupos y usuarios a los que se les quiere activar la protección y sensor de XDR
La solución de XDR debe mostrar un score del riesgo corporativo y se debe integrar como mínimo con las soluciones de firewall de Checkpoint, Palo Alto y Fortinet y debe permitir integrar fuentes de terceros como TAXII y MISP, y permitir la integración como mínimo con 25 fabricantes dentro de los que deben estar AWS, AttackIQ, Cymulate, Elastic, Okta, Microsoft, NetSkope, OpenLDAP, Picus, Qualys, Securonix, ServiceNow, Splunk, Tanium, Tenable y VMware, también debe proveer un conector para Splunk nativo.
CIFRADO
La solución de cifrado debe ser mono marca con la solución de protección de Endpoints, Servidores, móviles y XDR
La solución de cifrado nativo debe estar soportada para Windows 8, 8.1 y 10 para Windows 11 y superiores debe permitir la administración de llaves de Microsoft BitLocker y no será requerido cifrado nativo del fabricante
La solución de cifrado nativo debe estar soportada para MacOS 10.8, 10.9, 10.10, 10.11, 10.12, 10.13, 10.14 en versiones superiores debe permitir la administración de llaves de Apple FileVault y no será requerido cifrado nativo del fabricante
La solución debe permitir la administración de las claves de cifrado, y la sincronización de políticas con todos los equipos en los sistemas operativos soportados
La solución debe garantizar el cifrado de archivos, carpetas y medios extraíbles.
La solución debe tener capacidad de implementar comandos remotos, recuperar datos perdidos y una sincronización de políticas en tiempo real
La solución debe tener integración con UEFI (Unified Extensible Firmware Interface), responsable de inicializar el hardware de los equipos antes de dar el control al sistema operativo.
La solución debe cifrar todas las unidades de disco físicas que tenga disponibles el equipo.
La solución debe contar con varios métodos de autenticación para el inicio de sesión en los equipos. • ColorCode: Una secuencia única de colores. • Domain Authentication: Sincronización LDAP de Active Directory para inicio de sesión único (SSO). • Fixed Password: Una cadena de caracteres, números y símbolos. • PIN: Un número de identificación personal estándar. • Remote Help: Autenticación interactiva para usuarios que olvidan sus credenciales o dispositivos que no tienen políticas sincronizadas dentro de un período de tiempo predeterminado. • Self Help: Combinaciones de preguntas y respuestas que permiten a los usuarios restablecer una contraseña olvidada sin ponerse en contacto con el Soporte técnico. • Smart Card: Una tarjeta física utilizada junto con un PIN o una contraseña fija.
La consola debe proporcionar la capacidad de administrar los usuarios para agregar o eliminar cuentas, restablecer contraseñas, cambiar permisos, configurar prioridad de políticas, importar usuarios es de Active Directory y buscar cuentas de usuario específicas.
La consola debe mostrar un estado actual de los discos cifrados de cualquier equipo con las fechas de última sincronización y política aplicada.
La consola debe brindar la posibilidad de mostrar en todos los dispositivos los intentos fallidos de inicio de sesión.
La consola debe mostrar los dispositivos que se encuentran bloqueados debido a restricciones de políticas.
La consola cuenta con una lista de políticas donde muestra la información y el estado de las políticas creadas para todos los usuarios.

Transporte

REQUERIMIENTOS BASE PROCESO RENOVACIÓN Y OPTIMIZACIÓN DE TRENDMICRO
CARACTERISTICAS
La solución debe permitir el cifrado completo de disco incluyendo aplicaciones, configuraciones de registro, archivos temporales, archivos de intercambio, spoolers de impresión y archivos eliminados.
La solución debe contar con un cifrado de archivos en el cual se pueda establecer una clave para cada archivo en específico sin importar que se encuentren en el mismo equipo.
La solución debe usar cifrado AES
La solución debe permitir a los usuarios restablecer una contraseña olvidada o una cuenta bloqueada antes de poder iniciar sesión el dispositivo.
La consola debe generar un reporte en el que se muestren todas las posibles violaciones de seguridad en relación con conexiones fallidas, intento de manipulación de las políticas o intentos de modificación de los logs.
La solución debe permitir la generación de informes donde se muestren datos como estados de cifrado, versiones de dispositivos, últimos usuarios conectados a los dispositivos.
La solución debe utilizar los estándares de cifrado OPAL y OPAL 2.
El agente para el cifrado debe proteger los archivos y las carpetas ubicados en cualquier dispositivo que aparezca como una unidad dentro del sistema operativo.
MOVILES
La solución de protección de móviles debe ser mono marca con la solución de protección de Endpoints, servidores y cifrado.
La consola de administración debe contar con dashboard que permitan monitorear los dispositivos de forma sencilla y estos pueden ser personalizados por el administrador
La consola de administración deberá permitir control y visibilidad de los dispositivos móviles que cuenten con un agente instalado.
La solución deberá permitir la creación, modificación y eliminación de grupos, los cuales servirán para estructurar los agentes y poderlos administrarlos más fácilmente.
La solución deberá permitir estructurar los dispositivos administrados en grupos para facilitar su administración.
La solución deberá tener la capacidad de crear, modificar o eliminar políticas y asignarlas a un dispositivo o a un grupo de dispositivos.
La solución deberá permitir configurar los escaneos de para un solo dispositivo o para múltiples dispositivos.
La solución deberá permitir la eliminación de un dispositivos o eliminación de múltiples dispositivos
La solución deberá permitir la administración de las aplicaciones permitidas para ser instaladas en los dispositivos.
La solución debe permitir la creación, modificación y eliminación de cuentas de usuarios y roles, para la consola de administración y gestión.
La solución deberá tener la capacidad de realizar la búsqueda de los dispositivos permitiendo el uso de filtros como (Teléfono, IMEI, Numero del Serial, Dirección MAC, etc.) para búsquedas avanzadas.
La solución deberá tener la capacidad de recuperar las licencias de las aplicaciones desde los dispositivos.
La consola de administración debe tener la capacidad de generar reportes relacionados a las vulnerabilidades recomendadas a proteger, así como identificar cuales vulnerabilidades ya fueron parchadas en el servidor y que deben ser deshabilitadas.
La solución deberá permitir la carga de certificados en formatos como .pfx, .p12, .cer, .crt o .der para ser utilizados por el Servidor de Administración, e igualmente deberá permitir la eliminación de los mismos.
La solución deberá tener la capacidad de visualizar mediante la consola de administración las aplicaciones sospechosas, certificados maliciosos instalados en los dispositivos que estan siendo administrados por la solución.

REQUERIMIENTOS BASE PROCESO RENOVACIÓN Y OPTIMIZACIÓN DE TRENDMICRO
CARACTERISTICAS
La solución deberá tener la capacidad de enviar notificaciones (Detecciones de Malware, Certificados Maliciosos, Errores de Sistema, etc) y reportes via email a los administradores y/o usuarios.
La consola de administración deberá ser capaz de integrarse con Microsoft Active Directory para la administración de usuarios de acceso a la consola y realizar búsqueda de nuevos dispositivos en el dominio
La solución deberá permitir localizar un dispositivo y acceder remotamente para reiniciar contraseñas, bloquearlo o eliminar toda la información en caso de pérdida del dispositivo.
La solución deberá ser capaz de generar reportes desde la consola de administración, permitiendo generarlos por rango de tiempo (máximo 30 días).
La solución deberá tener la capacidad de programar la generación de reportes (diario, semanal, mensual)
La solución debe tener la capacidad de realizar las actualizaciones de los componentes de forma programada o manual, y notificar a los dispositivos cuando las actualizaciones estén disponibles.
La solución debe tener la capacidad de conectarse con el servicio de Microsoft Exchance Server para permitir administrar los dispositivos que user Exchange ActiveSync.
La solución debe permitir integración con aplicaciones de terceros como AirWatch, y/o Mobile Iron.
La solución debe tener la capacidad de realizar un análisis estático de los archivos sospechosos con el uso de Predictive Machine Learning.
La solución debe permitir el registro de dispositivos mediante enlaces web, códigos QR o una descarga desde iTunes.
La solución debe permitir que los agentes tengan la capacidad de conectarse con el servidor de administración ya sea que este se encuentre implementado dentro de la organización o este implementado en un ambiente en la nube

ACEPTACIÓN CUMPLIMIENTO DE REQUERIMIENTOS TÉCNICOS

Señor proponente, al remitir la propuesta, usted está aceptando que la misma cumple con la totalidad de los requerimientos incluidos en el presente documento y que incluye la totalidad de costos y gastos, directos e indirectos, así como los impuestos, asociados a la ejecución del contrato. Así mismo, que, en caso de resultar adjudicatario del proceso de selección correspondiente, podrá prestar el servicio y/o entregar el bien, con las condiciones técnicas descritas en el presente documento.

El valor de la oferta deberá contener todos los costos e impuestos en los que incurra el Contratista por la suscripción, legalización y ejecución del contrato que se pretende suscribir, como impuestos, constitución Garantía Única, transportes, operarios, etc.

Los valores que se expresen en la oferta deben ser dados en moneda legal colombiana.



GUSTAVO ADOLFO VÉLEZ ACHURY

Coordinador Grupo Tecnologías de la Información y las Comunicaciones.