
INVESTIGACIÓN DE RENOVACIÓN SEGURIDAD AMC



Fecha: 13/05/2025

ÍNDICE

1. Introducción

- 1.1. Objetivos principales.
- 1.2. Importancia de una solución de seguridad eficiente

2. Investigación de Alternativas

- 2.1. Opciones en el mercado y sus características
- 2.2. Comparativa de costos y beneficios

3. Prueba de Soluciones Seleccionadas

- 3.1. Criterios para evaluar
- 3.2. Implementación de pruebas

4. Evaluación de Resultados

- 4.1. Comparativa de rendimiento de nuevas alternativas
- 4.2. Comparativa mediante tablas
- 4.3. Análisis de costos a corto y largo plazo

5. Recomendación Final

- 5.1. Mejor opción según los resultados de pruebas
- 5.3. Posibles riesgos de mitigación

6. Conclusión

- 6.1. Beneficios esperados de la migración
- 6.2. Consideraciones finales.

1. Introducción

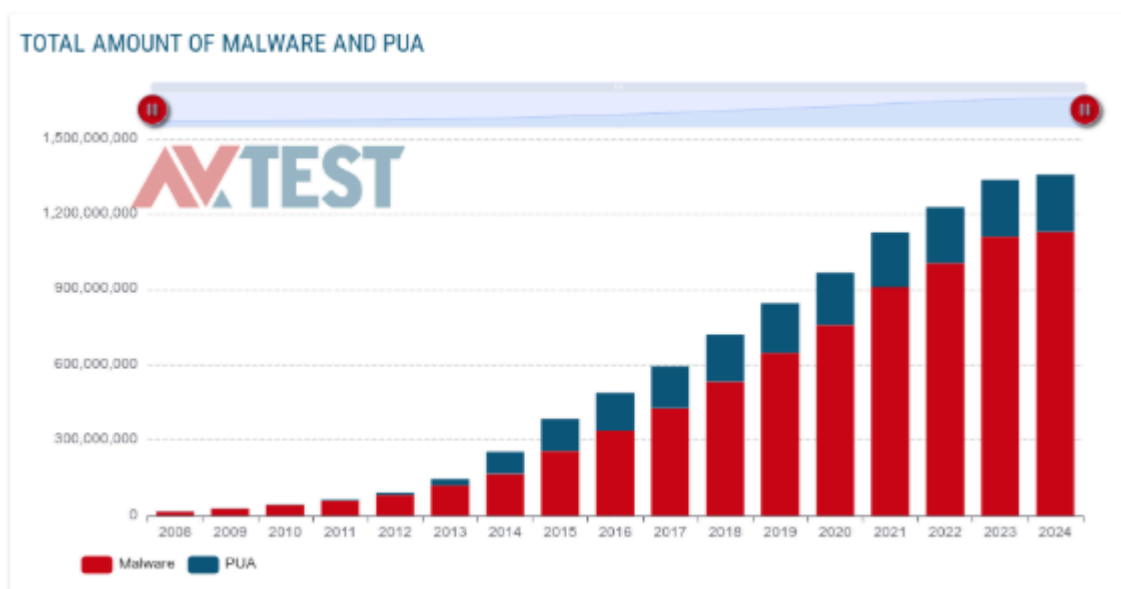
1.1. Importancia de una Solución de Seguridad Eficiente

La seguridad informática es un pilar fundamental en cualquier empresa. Una solución de seguridad eficiente debe garantizar:

- **Protección contra amenazas avanzadas:** Defensa en tiempo real frente a virus, malware, ransomware y ataques dirigidos.
- **Poco impacto en el rendimiento:** Un buen antivirus debe operar en segundo plano sin afectar la productividad de los empleados.
- **Facilidad de gestión:** Un sistema de seguridad bien administrado permite optimizar recursos y reducir la carga del equipo de TI.
- **Escalabilidad y adaptabilidad:** La solución debe ser capaz de crecer junto con la empresa y adaptarse a nuevos desafíos.
- **Cumplimiento normativo:** Garantizar que la empresa cumpla con regulaciones y estándares de seguridad para evitar sanciones legales.

Contar con una solución eficiente **no es un lujo, sino una necesidad** para la protección de la empresa. La evaluación y selección de un nuevo sistema de seguridad garantizará que la empresa esté preparada para enfrentar **los riesgos actuales**.

Cantidad total de malware



Origen: av-atlas.org

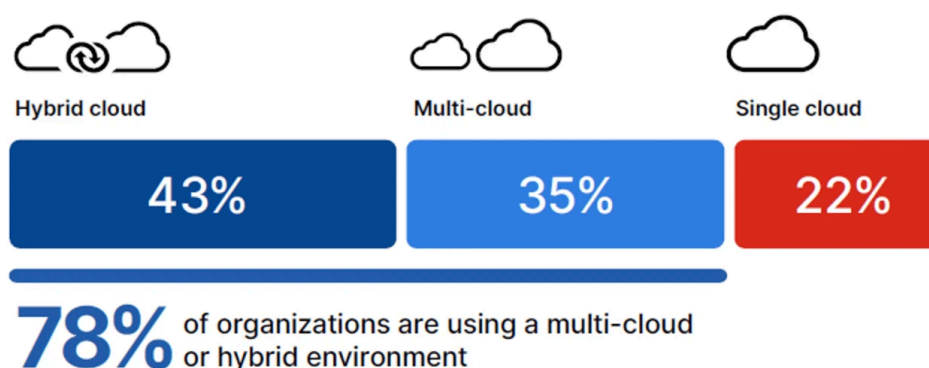
Según el informe *Cybersecurity Ventures 2024*, se estima que:

- El **60% de las pequeñas y medianas empresas (PYMES)** que sufren un ciberataque cierran sus puertas en los 6 meses siguientes debido a las pérdidas.
- Las soluciones de seguridad en la nube tienen un **30-40% menos de costes de mantenimiento** en comparación con soluciones tradicionales locales.

Más estadísticas de ciberseguridad actuales:

- Los **daños del ransomware a nivel mundial** y el pago de rescates sumaron más de 20.000 millones de dólares en 2021. Se espera que esta cifra aumente a más de 265.000 millones de dólares en 2031. ([Fuente](#))
- El 46% de las organizaciones utilizan aplicaciones basadas en la nube creadas específicamente para la nube; el 54% trasladaron aplicaciones desde un entorno local. ([Fuente](#))

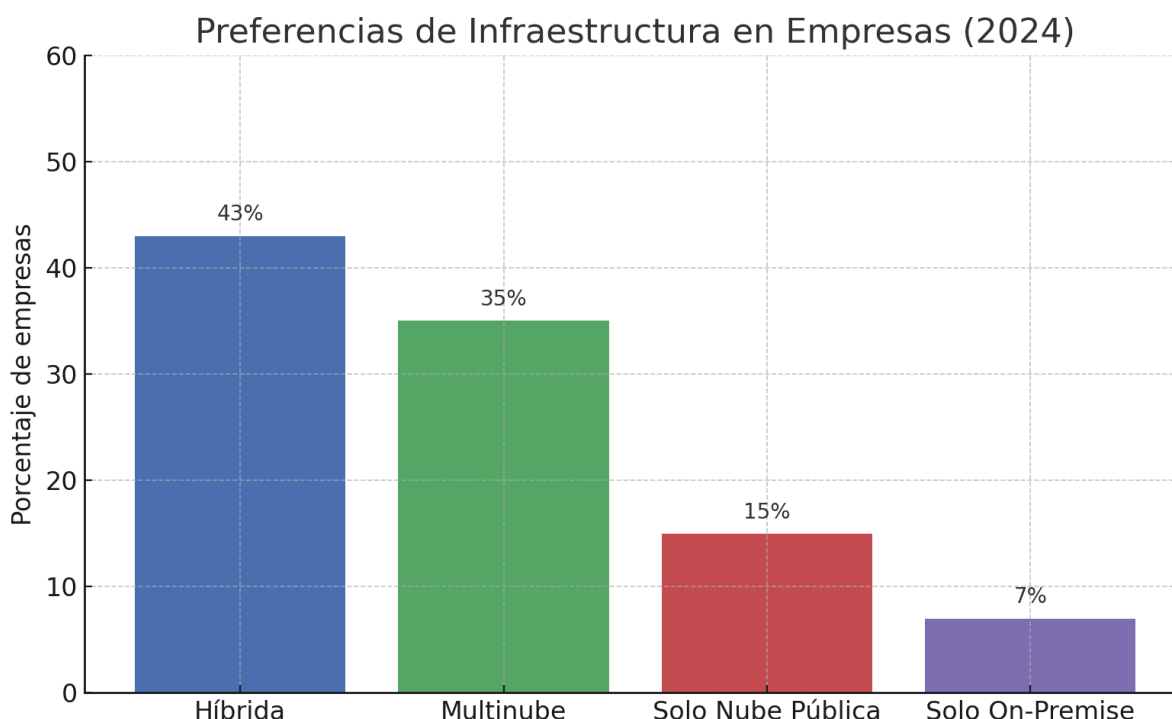
Y también recalcar que según el *2024 Cloud Security Report* de Fortinet, el 78% de las organizaciones optan por estrategias **híbridas o multi-nube**. De estas, el 43% utiliza una combinación de infraestructura en la **nube y on-premise**, mientras que el 35% adopta una estrategia multi-nube. ([Fuente](#))



Estas estadísticas reflejan que las soluciones híbridas permiten combinar lo mejor de ambos mundos: la escalabilidad de la nube y la estabilidad del entorno on-premise. A su vez, la estrategia multinube ofrece redundancia y evita la dependencia de un único proveedor.

Esta tendencia es clave al evaluar nuevas soluciones de seguridad, ya que muchas de ellas están diseñadas específicamente para integrarse en estos entornos mixtos.

Sin embargo, la preocupación por la seguridad y el aumento de incidentes destacan la necesidad de evaluar cuidadosamente las soluciones disponibles. Este trabajo busca identificar la opción que mejor se adapte a las necesidades de la empresa, garantizando una protección eficiente y una gestión centralizada.



Las soluciones híbridas y multinube dominan el mercado, reflejando una tendencia hacia modelos flexibles que combinan la nube con sistemas on-premise. Esta orientación apoya decisiones estratégicas de seguridad y rendimiento.

1.2. Objetivos principales.

El objetivo de este trabajo es evaluar y seleccionar una nueva solución de seguridad informática para **sustituir Trellix (McAfee) en la empresa**, garantizando una **protección más eficiente, gestión centralizada, menor impacto en el rendimiento y si puede ser reducción de costos**.

Para lograrlo, se establecen los siguientes objetivos:

- **Investigar alternativas de antivirus y seguridad en la nube** que ofrezcan mejor protección y facilidad de gestión.
- **Comparar el rendimiento, la seguridad y el costo** de las opciones disponibles en el mercado.
- **Realizar pruebas** en un equipo virtualizado para evaluar el impacto en el funcionamiento y el desempeño dependiendo de la prueba.
- **Determinar la viabilidad de la seguridad basada en la nube** en comparación con soluciones tradicionales.
- **Elaborar una recomendación final** basada en los datos recopilados, asegurando la mejor opción para la empresa.

El resultado esperado es la obtención de un sistema de seguridad **más eficiente, rentable y adaptado a las necesidades de la empresa y basado en nube**.

2. Investigación de Alternativas

2.1. Opciones en el mercado y sus características

Existen diversas soluciones de seguridad que pueden reemplazar a **Trellix**. A continuación, se presentan algunas de las opciones más destacadas del mercado basadas en cloud y mejor seguridad para el caso de la empresa, incluyendo sus principales características.

SentinelOne Singularity

Descripción: Servicio de seguridad gestionada que combina la inteligencia artificial de la plataforma Singularity con la supervisión activa de expertos en ciberseguridad. Proporciona detección y respuesta proactiva frente a amenazas avanzadas en endpoints, servidores y entornos en la nube. Su enfoque automatizado permite contener incidentes en tiempo real, mientras que su consola centralizada facilita la visibilidad y administración.

Trend Micro Vision One

Descripción: Plataforma de seguridad avanzada que correlaciona datos de múltiples entornos (endpoints y servidores) para ofrecer una detección proactiva. Su consola centralizada facilita la administración en empresas medianas. Proporciona inteligencia de amenazas en tiempo real y permite una respuesta automatizada para mitigar incidentes. Su compatibilidad con diversas infraestructuras la hace ideal para entornos híbridos.

Bitdefender GravityZone Business Security Enterprise

Descripción: Solución de seguridad empresarial que combina protección avanzada en endpoints con capacidades EDR, gestionada desde una consola central en la nube. Ofrece prevención proactiva contra malware, ransomware y amenazas en archivos, utilizando inteligencia artificial y tecnologías de comportamiento. Su arquitectura permite una gestión escalable con bajo consumo de recursos, y está pensada para empresas que buscan un equilibrio entre automatización, visibilidad y control.

ESET Protect Complete

Descripción: Es la solución de seguridad empresarial más parecida a Trellix que ofrece protección multicapa contra malware, ransomware y phishing, con gestión centralizada desde la nube o local. Incluye cifrado, control de dispositivos y seguridad para correo y almacenamiento en la nube con un precio muy competente en el mercado y comparándolo con las otras soluciones.

2.2. Comparativa de costos y beneficios

Es esencial un **análisis de los costos y beneficios que ofrecen las distintas alternativas disponibles en el mercado**. Esta comparativa no solo contempla el precio de cada solución, sino también los costos asociados a su implementación, mantenimiento y su total funcionamiento a lo largo del tiempo.

En cuanto a los **costos**, se han considerado los siguientes aspectos:

- Licenciamiento: modalidad de pago (anual, por dispositivo, por usuario, etc.).
- Costos de instalación y despliegue.
- Requerimientos de infraestructura adicional, en caso de ser necesaria.
- Costos de soporte técnico y actualizaciones.

En lo que respecta a los **beneficios**, se han tenido en cuenta:

- Nivel de protección frente a amenazas actuales (malware, ransomware, ataques de día cero, etc.).
- Facilidad de administración y centralización de políticas de seguridad.
- Integración con otros sistemas de la infraestructura de TI existente.
- Ahorro potencial a largo plazo por reducción de incidentes de seguridad.
- Mejor experiencia de usuario y menor impacto en el rendimiento del sistema.

La combinación de estos factores permite establecer una **visión integral de la relación costo-beneficio de cada solución**, con el fin de ver cuál representa una inversión más eficiente y mejor para la empresa.

3. Prueba de Soluciones Seleccionadas

3.1. Criterios de evaluación

♦ 3.1.1. Detección y Prevención de Amenazas

- Instalación de malware de prueba (**EICAR**) para evaluar detección.
- Simulación de ataques de phishing y ransomware en entorno virtual
- Comparación de capacidad de remediación automática.

♦ 3.1.2. Impacto en el Rendimiento

Algunas soluciones pueden afectar la velocidad de los equipos, lo cual es clave si los dispositivos no son muy potentes.

- Medición de **CPU, RAM y disco** durante escaneos completos y segundo plano.
- Comparación del **tiempo de apertura de archivos y aplicaciones** con el agente.
- Evaluación del **impacto en la velocidad de red** al cargar páginas web y descargar archivos.

♦ 3.1.3. Facilidad de Administración

- Configuración de políticas de seguridad en una **consola centralizada**.
- Comparación de opciones de **gestión remota** y automatización de tareas.
- Análisis de reportes y alertas generadas ante detecciones.

♦ 3.1.4. Integración con Infraestructura de la Empresa

- Integración con otras soluciones de seguridad como el **firewall o vpn**.
- Evaluación de la facilidad para realizar **despliegue masivo** en la empresa.

♦ 3.1.5. Evolución de Soporte y Actualizaciones

Es importante asegurarse de que el antivirus tenga un buen soporte técnico y actualizaciones frecuentes.

- Todas las opciones ofrecen equipos especializados 24/7, pero algunos a un costo adicional por resultados premium y de alta disponibilidad.
- Las opciones seleccionadas tienen buena reputación y fiabilidad en actualizaciones y parches rápidos contra nuevas amenazas.

♦ 3.1.6. Coste y Licenciamiento

- Análisis del costo **por licencia y por equipo**.
- Evaluación de **costos adicionales** (soporte, módulos extra, etc.).
- Comparación de la **escalabilidad** al aumentar el número de dispositivos protegidos.

3.2. Implementación de pruebas

Debido a que no todas las soluciones evaluadas ofrecían una versión de prueba completa, se establecieron dos tipos de análisis:

- **Pruebas prácticas** en entorno virtualizado, realizadas únicamente con las opciones que proporcionaron acceso temporal a su plataforma.
- **Evaluación técnica guiada**, basada en **demostraciones comerciales** (de al menos una hora) proporcionadas por los fabricantes, junto con la revisión detallada de documentación técnica y recursos oficiales.

En ambos casos, se utilizaron los mismos criterios de evaluación (ver punto 3.1), permitiendo una comparativa coherente entre todas las soluciones, aun cuando la profundidad de prueba variará. Esta aproximación permite valorar tanto el comportamiento real como la propuesta de valor y capacidades que ofrece cada herramienta según lo que el proveedor demuestra y respalda.



Implementación y puesta en marcha (evaluación basada en demostración):

Durante la sesión de demostración de SentinelOne, se mostró el proceso de gestión simulado, que incluyó la instalación de agentes, la configuración inicial y la integración con otros entornos y su funcionamiento en general. Aunque no fue posible replicar el despliegue en un entorno propio, la información presentada y los casos de uso mostraron un **proceso de automatización de tareas y funcionamiento del entorno**, diseñado para minimizar interrupciones y facilitar la transición desde otras plataformas.

Detección y Prevención de Amenazas:

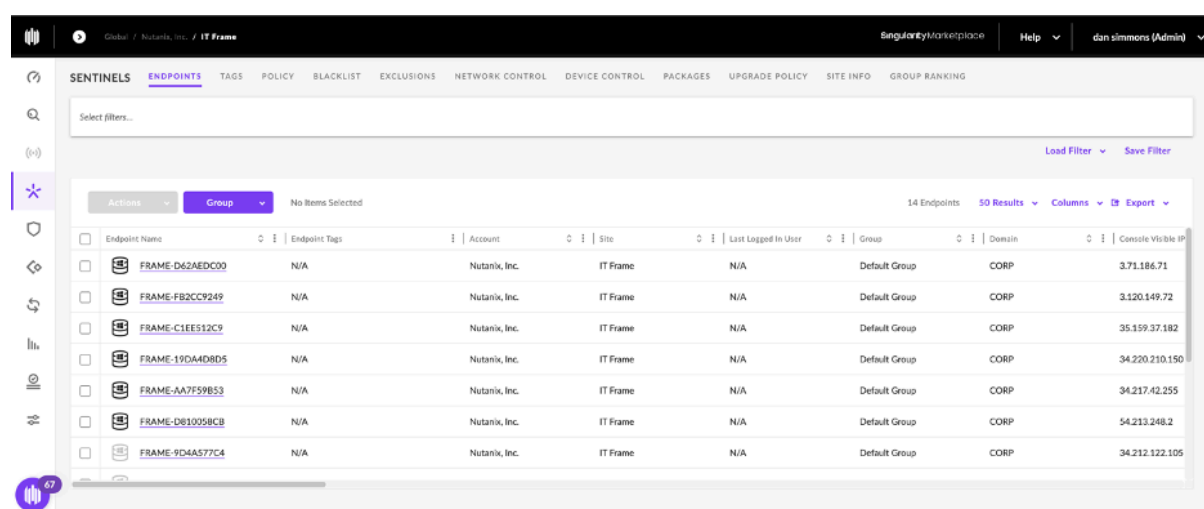
En la demostración se mostró cómo la solución responde a amenazas típicas como **phishing, ransomware y descargas maliciosas**, mediante ejemplos preparados en entornos reales. Se observaron funciones de análisis en tiempo real, alertas automatizadas y flujos de respuesta orquestados. La detección se basa en técnicas de inteligencia artificial y análisis de comportamiento, complementadas por una base de datos de amenazas actualizada constantemente.

Rendimiento:

Según lo mostrado, la solución hace uso de análisis en la nube y automatizaciones que **minimizan el impacto en los dispositivos finales, su uso aproximado es de 2% CPU y 1% RAM**. Aunque no se pudo medir directamente el rendimiento, los indicadores presentados por el proveedor dice que está optimizado para entornos grandes.

Facilidad de Administración:

La consola administrativa fue mostrada en tiempo real, evidenciando una interfaz clara y centralizada. Destaca por su **visualización unificada de incidentes**, herramientas de análisis IA y capacidad de integración con plataformas como SIEM y soluciones de identidad. Se valoró positivamente el resumen generado por IA.



Endpoint Name	Endpoint Tags	Account	Site	Last Logged In User	Group	Domain	Console Visible IP
FRAME-D62AEDC00	N/A	Nutanix, Inc.	IT Frame	N/A	Default Group	CORP	3.71.186.71
FRAME-FB2CC9249	N/A	Nutanix, Inc.	IT Frame	N/A	Default Group	CORP	3.120.149.72
FRAME-C1EE512C9	N/A	Nutanix, Inc.	IT Frame	N/A	Default Group	CORP	35.159.37.182
FRAME-19D4MD8D5	N/A	Nutanix, Inc.	IT Frame	N/A	Default Group	CORP	34.220.210.150
FRAME-AA7F59B53	N/A	Nutanix, Inc.	IT Frame	N/A	Default Group	CORP	34.217.42.255
FRAME-D810058CB	N/A	Nutanix, Inc.	IT Frame	N/A	Default Group	CORP	54.213.248.2
FRAME-9D4A577C4	N/A	Nutanix, Inc.	IT Frame	N/A	Default Group	CORP	34.212.122.105

Integración con Infraestructura de la Empresa:

Durante la sesión, se detalló la compatibilidad de la solución con **entornos híbridos y multi-nube**, así como su integración con herramientas comunes del ecosistema de seguridad empresarial. Se destacó la **versatilidad multiplataforma** (Windows, Linux) y la interoperabilidad con productos de terceros.

Evolución de Soporte y Actualizaciones:

La solución cuenta con **actualizaciones automáticas** y soporte técnico especializado disponible 24/7. Aunque no se verificó su eficacia directamente, el proveedor expuso los mecanismos de actualización continua y los canales de asistencia para resolución de incidentes. También recalcar que tiene wachtower seguro de brecha de hasta 100.000 €.

El coste de SentinelOne **varía según el tamaño de la empresa y el nivel de servicio contratado**. Aunque su precio es superior al de soluciones básicas, el valor añadido del monitoreo continuo con IA y la respuesta gestionada lo posiciona como una solución avanzada. Los presupuestos adjuntados son los siguientes:

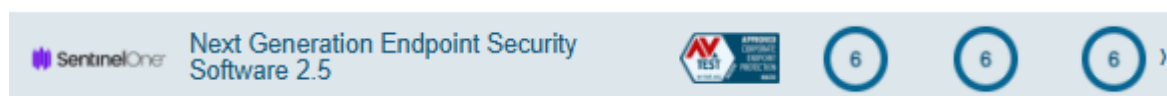
Coste:

Subscription terms:		EURO						EURO	
ANNUALE									
SKU	Description	Tier	Q.ty	List Price	Co-Term (months)	List Price / Seat		Suggested Customer Price	Suggested Customer Price / Seat
PF-PLT-FF-T1-C	Singularity Platform. Access to the Singularity Platform, includes initial 10GB SDL Ingest	1	1	€ 2,000.00	12	€ 2,000.00		400.00 €	400.00 €
S1-CMPAI-EN-T2-C	Complete Protection Platform with AI (Per Workstation)	100-500	262	€ 32,681.88	12	€ 124.74		10,458.20 €	39.92 €
S1-CMPAI-CW-T2-C	Complete Cloud Workload Security with AI (Per Server)	100-500	23	€ 5,687.90	12	€ 247.30		1,763.25 €	76.66 €
SP-RAD-US-T2-C	Singularity Identity Security Posture Management (Per User)	100-500	262	€ 9,170.00	12	€ 35.00		3,484.60 €	13.30 €
SP-RGI-ND-T2-C	Singularity Vulnerability Management (Per Endpoint)	1-500	285	€ 34,200.00	12	€ 120.00		5,643.00 €	19.80 €
Total							83,739.78 €	21,749.05 €	

Con gestión SOC - MDR:

Subscription terms:		EURO						EURO	
ANNUALE									
SKU	Description	Tier	Q.ty	List Price	Co-Term (months)	List Price / Seat		Suggested Customer Price	Suggested Customer Price / Seat
PF-PLT-FF-T1-C	Singularity Platform. Access to the Singularity Platform, includes initial 10GB SDL Ingest	1	1	€ 2,000.00	12	€ 2,000.00		400.00 €	400.00 €
S1-CMPAI-EN-T2-C	Complete Protection Platform with AI (Per Workstation)	100-500	262	€ 32,681.88	12	€ 124.74		9,804.56 €	37.42 €
S1-CMPAI-CW-T2-C	Complete Cloud Workload Security with AI (Per Server)	100-500	23	€ 5,687.90	12	€ 247.30		1,592.61 €	69.24 €
SP-RAD-US-T2-C	Singularity Identity Security Posture Management (Per User)	100-500	262	€ 9,170.00	12	€ 35.00		2,751.00 €	10.50 €
SP-RGI-ND-T2-C	Singularity Vulnerability Management (Per Endpoint)	1-500	285	€ 34,200.00	12	€ 120.00		5,130.00 €	18.00 €
SS-VR-ND-T2-C	Vigilance MDR (Per Endpoint)	100-500	285	€ 7,612.35	12	€ 26.71		6,774.99 €	23.77 €
SS-WAT-ND-T2-C	WatchTower (Per Endpoint)	100-500	285	€ 7,891.65	12	€ 27.69		3,551.24 €	12.46 €
SP-BRWS-FF-T1-C	Breach Response Warranty Small	1	285	€ -	12	€ -		- €	- €
Total							99,243.78 €	30,004.41 €	

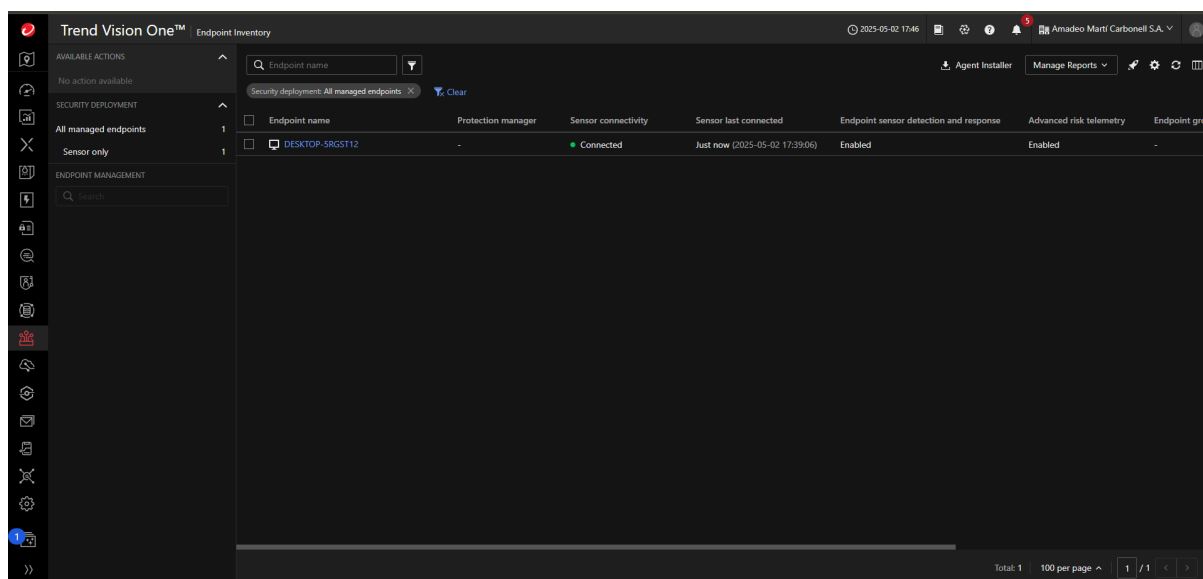
Última valoración av-test:





Implementación y puesta en marcha (investigación de migración):

Trend Micro Vision One se implementa a través de un agente mediano en los endpoints y se **gestiona 100% desde nube**. Su despliegue es flexible y compatible con entornos on-premise, híbridos y en la nube. La plataforma permite una migración escalonada con monitoreo en tiempo real para minimizar riesgos durante la transición.



Tiene varias funciones muy interesantes para su trabajo, estas funciones pueden abarcar desde informes personalizados y preventivas de amenazas hasta simulacros de ataques y phishing.

Detección y Prevención de Amenazas:

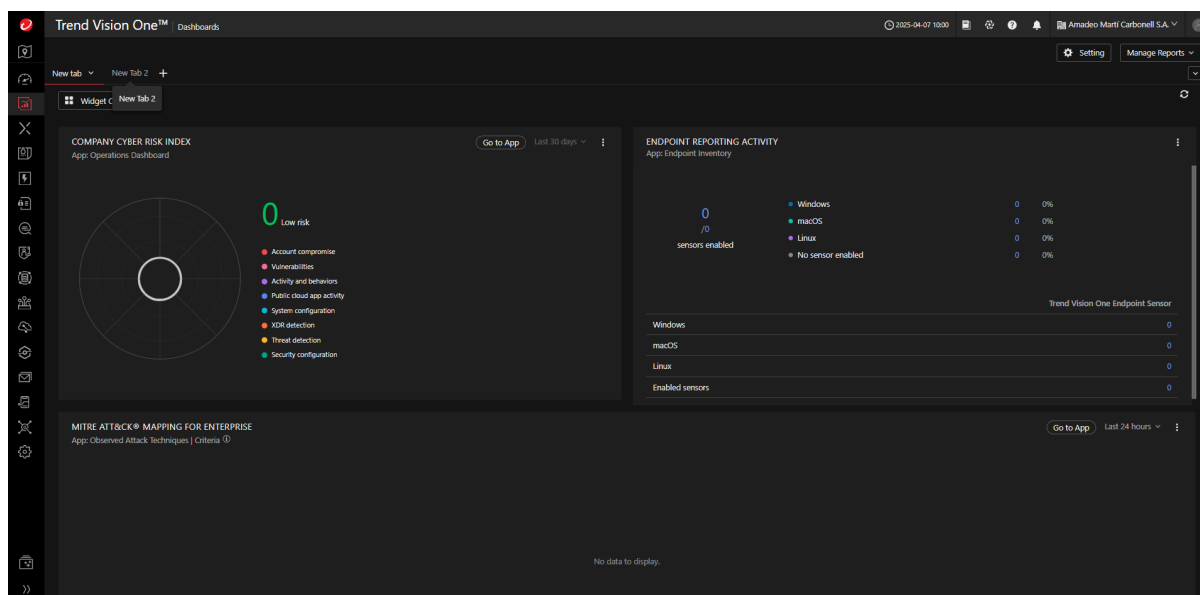
Utiliza análisis de comportamiento, inteligencia artificial y machine learning para detectar y bloquear amenazas avanzadas. Protege contra ransomware, ataques sin archivos, phishing y amenazas persistentes avanzadas. Su enfoque de detección multicapa analiza datos de múltiples fuentes para ofrecer una respuesta proactiva y minimizar el impacto de los ataques.

Rendimiento:

Trend está optimizado para realizar análisis avanzados sin afectar el rendimiento del sistema. Su capacidad de correlación de **eventos en la nube reduce la carga en los dispositivos**, mientras que su arquitectura escalable permite gestionar grandes volúmenes de datos sin ralentizar la operación de los endpoints.

Facilidad de Administración:

Cuenta con una **consola unificada que centraliza la gestión de amenazas**, la respuesta automatizada a incidentes y la administración de políticas de seguridad. Su interfaz intuitiva permite al equipo de TI analizar rápidamente incidentes y aplicar medidas, mejorando la eficiencia operativa.



Integración con Infraestructura de la Empresa:

Trend se **integra con el entorno de la empresa**, permitiendo la conexión con soluciones de seguridad en la nube, firewalls, plataformas de identidad y sistemas de respuesta a incidentes. Compatible con Windows, Linux y dispositivos móviles.

Evolución de Soporte y Actualizaciones:

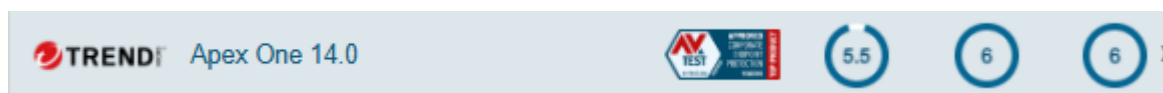
Recibe actualizaciones automáticas con inteligencia de amenazas en tiempo real para mejorar la detección de ataques emergentes. Trend Micro ofrece soporte técnico especializado y acceso a una comunidad de expertos en ciberseguridad en su foro.

Coste:

El coste puede variar del uso y paquetes que queremos darle, Trend Vision One tiene un **sistema de créditos** que dependiendo de, por ejemplo, de cuantos endpoints o soluciones de seguridad de red queramos, poder comprar más funcionalidades o menos.

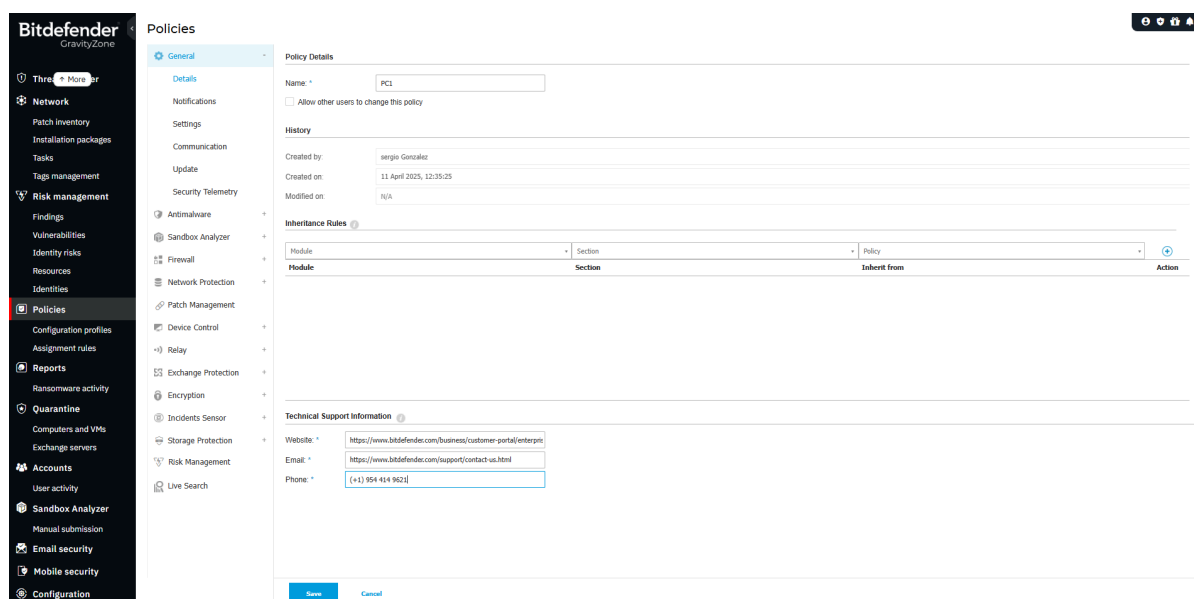
Lamentablemente, no se han podido obtener presupuestos para esta solución de Bitdefender, pero el costo varía dependiendo de las exenciones que se le pueden añadir, la solución costa como una gran propuesta calidad-precio.

Última valoración av-test:



Implementación y puesta en marcha (investigación de migración):

La implementación se realiza mediante la consola en la nube GravityZone o un servidor local, con la posibilidad de desplegar agentes de forma remota en los endpoints. Soporta entornos híbridos, físicos y virtuales. **La migración puede realizarse de forma progresiva**, asegurando la compatibilidad con sistemas existentes y permitiendo pruebas piloto antes del despliegue completo.



Detección y Prevención de Amenazas:

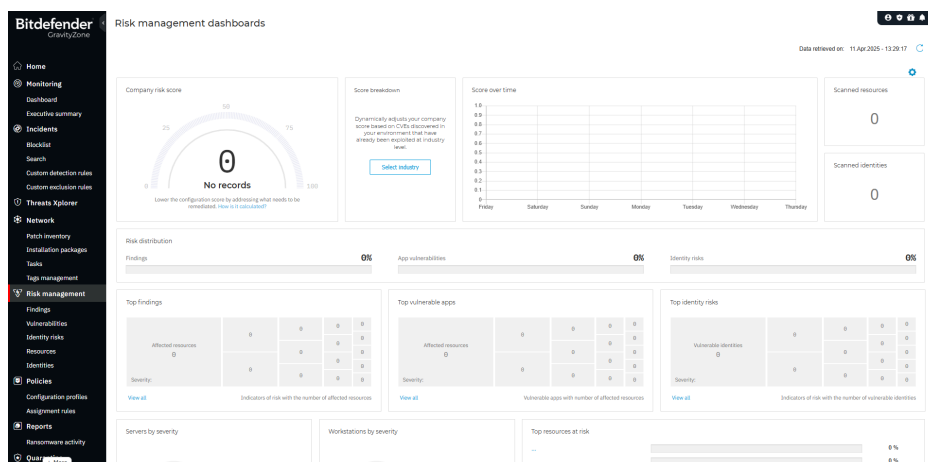
Bitdefender emplea **múltiples capas de seguridad como machine learning, análisis de comportamiento y métodos tradicionales**. Protege frente a ransomware, spyware, ataques de día cero, phishing y exploits. Su motor avanzado detecta anomalías y comportamientos sospechosos antes de que se materialicen como amenazas reales.

Rendimiento:

El impacto sobre los sistemas es mínimo gracias a su **motor de análisis optimizado y a la descarga de procesos pesados**. GravityZone prioriza el rendimiento del usuario final sin comprometer la seguridad, y permite ajustar políticas según el tipo de dispositivo o carga de trabajo.

Facilidad de Administración:

Cuenta con una **consola centralizada desde la que se pueden gestionar políticas, endpoints y alertas**. Incluye informes personalizables y automatización de tareas. La gestión desde una única interfaz permite ahorrar tiempo y facilita el control, incluso en entornos distribuidos o con múltiples sedes.



Integración con Infraestructura de la Empresa:

GravityZone se integra fácilmente con soluciones SIEM, hipervisores como VMware, Hyper-V o Citrix y **plataformas cloud**. También es compatible con Active Directory, herramientas de administración y otras soluciones de seguridad como Fortinet.

Evolución de Soporte y Actualizaciones:

Bitdefender ofrece **soporte 24/7**, base de conocimientos con una persona certifica y acceso a actualizaciones automáticas sin interrupción del servicio. Las firmas de amenazas se actualizan en tiempo real desde su red global de inteligencia, **permitiendo una respuesta rápida** ante amenazas emergentes.

Coste:

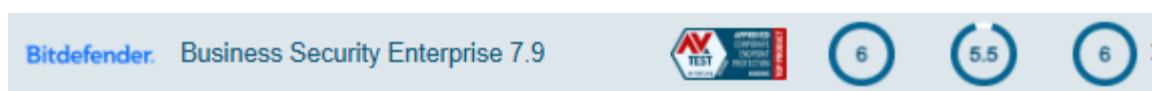
Te paso la oferta del nuestro producto top, que ademas de EDR incluye mucho mas:

- Anomaly Defence
- MITRE Event Tagging
- Endpoint Risk Analytics
- HyperDetect
- Sandbox Analyzer - que es un espacio aislado en nuestro data center donde se analizan los ficheros
- SVA (Security Virtual Appliance)
- Root Cause Analysis
- Incident Visualization
- Application Whitelisting
- Exchange protection

Con respecto a la oferta, al tratarse de un cliente potencial, aplicamos un **30% de descuento** sobre el precio inicial.

Bitdefender Part #	Bitdefender Product	Period	Unit Tiers	Units	Offer type	Unit Price	Subtotal
2892ZZBCN120FLZZ	Bitdefender GravityZone Business Security Enterprise	1 Year	250 - 499	285	Competitive Upgrade	€ 31.91	€ 9,094.35
-						€ -	€ -
-						€ -	€ -
-						€ -	€ -
-						€ -	€ -
-						€ -	€ -
-						€ -	€ -
-						€ -	€ -
-						€ -	€ -
-						€ -	€ -
Total Standard price		€	12,990.30	Special discount from standard price		-30%	Total End User Price
						€	9,094.35

Última valoración av-test:





Implementación y puesta en marcha (investigación de migración):

ESET Protect Complete permite un despliegue ágil mediante su consola web basada en la nube. Se **pueden instalar agentes a través de scripts o políticas de grupo (GPO)**, y la migración desde soluciones anteriores se facilita con herramientas automáticas de desinstalación y detección de software conflictivo. Ofrece opciones de prueba sin interrupciones.

Detección y Prevención de Amenazas:

Esta solución incluye **protección multicapa con detección** de ransomware, malware, ataques sin archivos, phishing y exploits mediante análisis de comportamiento, heurística avanzada y reputación en la nube.

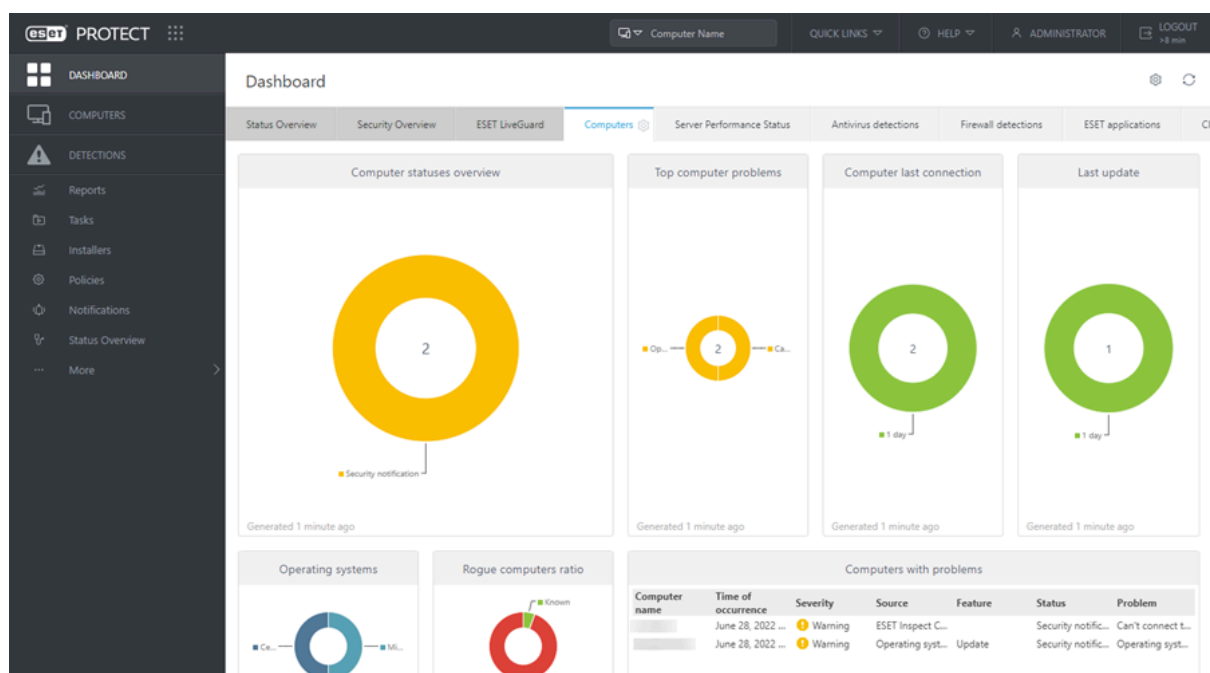


Rendimiento:

Funcionar con un **consumo moderado de recursos**, lo que puede favorecer su uso en equipos con capacidades variadas. En entornos de oficina, esta eficiencia podría contribuir a mantener un equilibrio entre seguridad y rendimiento sin afectar significativamente la experiencia del usuario.

Facilidad de Administración:

La consola ESET Protect permite administrar todos los dispositivos desde una sola ubicación, facilitando la creación de políticas, generación de informes y respuesta rápida a incidentes. Tiene un **diseño intuitivo y se adapta tanto a entornos pequeños como a redes complejas**.



Integración con Infraestructura de la Empresa:

ESET es compatible con entornos **Windows, móviles Android y plataformas como VMware y Citrix**. También se integra con Active Directory para sincronización automática de diversos dispositivos.

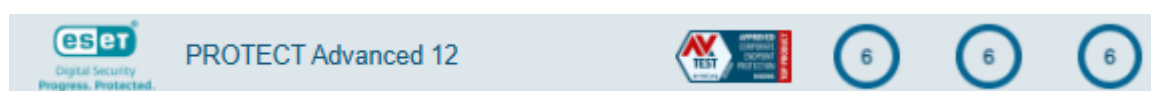
Evolución de Soporte y Actualizaciones:

ESET proporciona **soporte técnico especializado**, acceso a base de conocimientos y actualizaciones automáticas de firmas de virus y módulos de protección. Las actualizaciones no interrumpen el servicio, y los clientes tienen la opción de configurar entornos de actualización locales.

Coste:

ESET Protect Complete es competitivo y ligeramente inferior al de otras soluciones propuestas. Se trata de una opción muy equilibrada en **calidad-precio**, especialmente adecuada para empresas que buscan una protección eficaz en tareas comunes sin realizar una gran inversión. Los presupuestos proporcionados han llegado: sobre 300 endpoints: **11.883 €** (También se puede barajar su hermano menor **ESET PROTECT Advance** con menos funcionalidades, pero a menor precio).

Última valoración av-test:



4. Evaluación de Resultados

4.1. Comparativa de rendimiento de nuevas alternativas.

4.1.1. SentinelOne Singularity

Ventajas:

- Alta automatización y respuesta autónoma.
- Rollback ante ataques como ransomware.
- Buena visibilidad y consola clara.
- Facilidad de escalar y desplegar.
- IA facilitando la gestión.

Desventajas:

- Precio más elevado que otras opciones.
- Curva de aprendizaje moderada.

4.1.2. Trend Vision One

Ventajas:

- Es una opción muy completa por sus funciones que ofrecen.
- Agentes ligeros y sin apenas causa en el rendimiento.
- Interfaz sencilla e intuitiva.

Desventajas:

- Se queda un poco corto de funcionalidades en su versión base.
- Muchos paquetes de pago.
- Curva de aprendizaje de uso más elevada que otras opciones.

4.1.3. Bitdefender GravityZone Business Security Enterprise

Ventajas:

- Interfaz clara e intuitiva.
- Automatización eficiente para tareas comunes.
- Buen rendimiento con bajo consumo de recursos.
- Fácil integración en el entorno.

Desventajas:

- Funcionalidades avanzadas, algo limitadas.
- Requiere configuración adicional para aprovechar todo su potencial.
- Curva de aprendizaje moderada.

ESET Protect Complete

Ventajas:

- Protección multicapa eficaz contra malware, ransomware y phishing.
- Interfaz sencilla y de rápida adopción.
- Gestión centralizada desde consola en la nube o local.
- Incluye funciones útiles como cifrado y control de dispositivos.

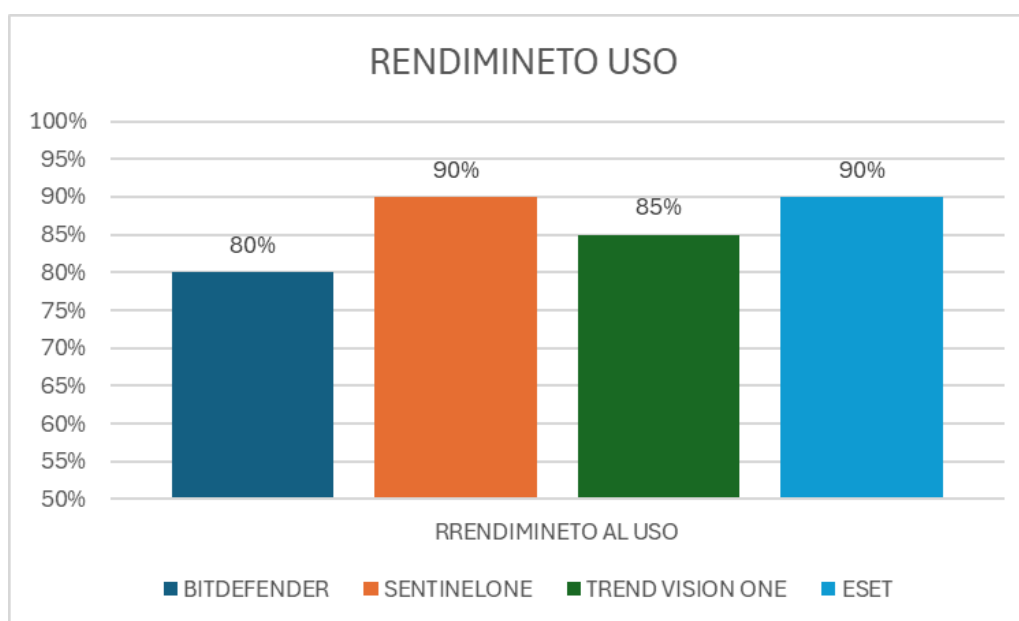
Desventajas:

- Menos opciones de automatización que otras soluciones.
- La personalización de políticas puede ser limitada.
- La opción de configuración son limitadas.

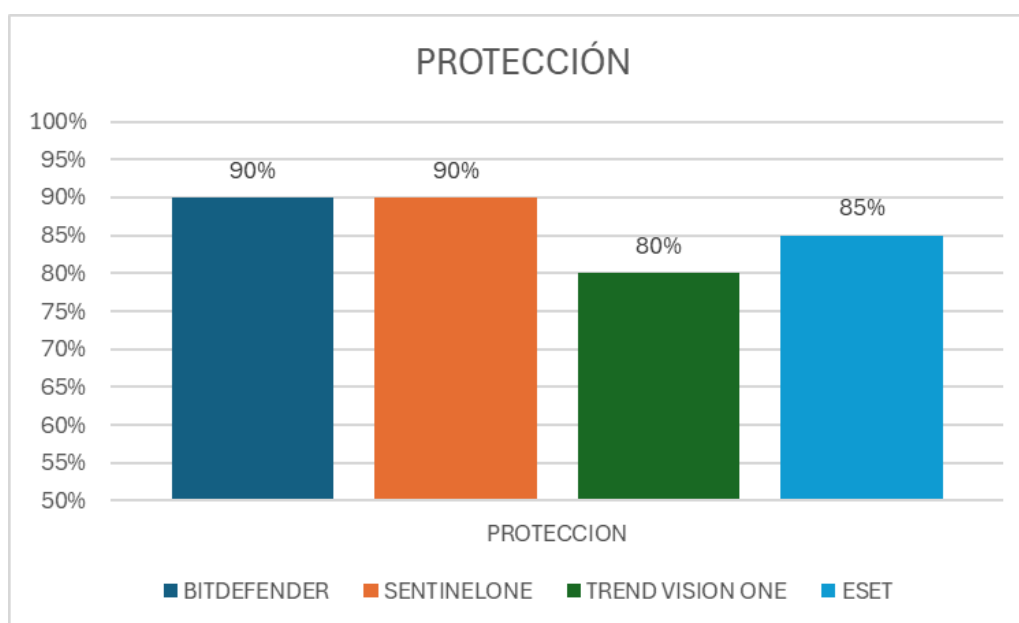
4.2. Comparativa mediante tablas

En este apartado se verá unas tablas de gráficos comparativos para mejor representación de todas las soluciones mostradas en este informe, se mostrarán en tres gráficos, rendimiento al uso, protección y su facilidad de administración midiendo por porcentajes relacionados con av-test y pruebas personales para así tener una mejor visión.

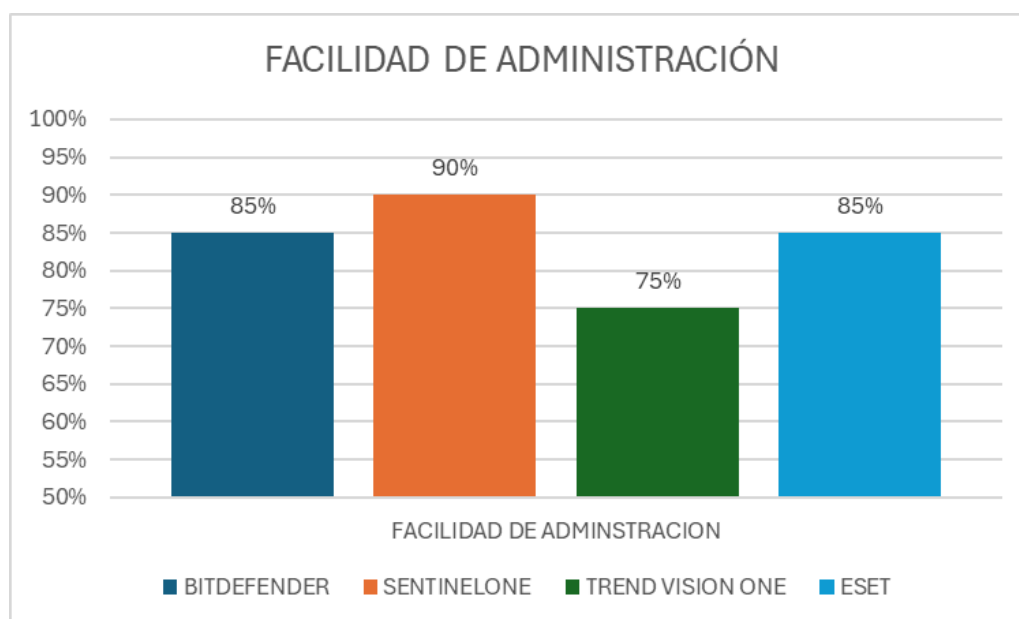
Este gráfico muestra cómo afecta cada solución al rendimiento general de los sistemas, destacando cuáles tienen menor impacto y ofrecen una mejor experiencia para los usuarios.



Este gráfico compara la capacidad de protección entre las distintas soluciones evaluadas, destacando cuál ofrece mayor potencia frente a amenazas.



Aquí se ve qué soluciones permiten una gestión más sencilla, centralizada y eficiente, facilitando el trabajo del equipo de TI y reduciendo esfuerzos manuales.



4.3. Análisis de costos a corto y largo plazo

1. Costos de Licencias

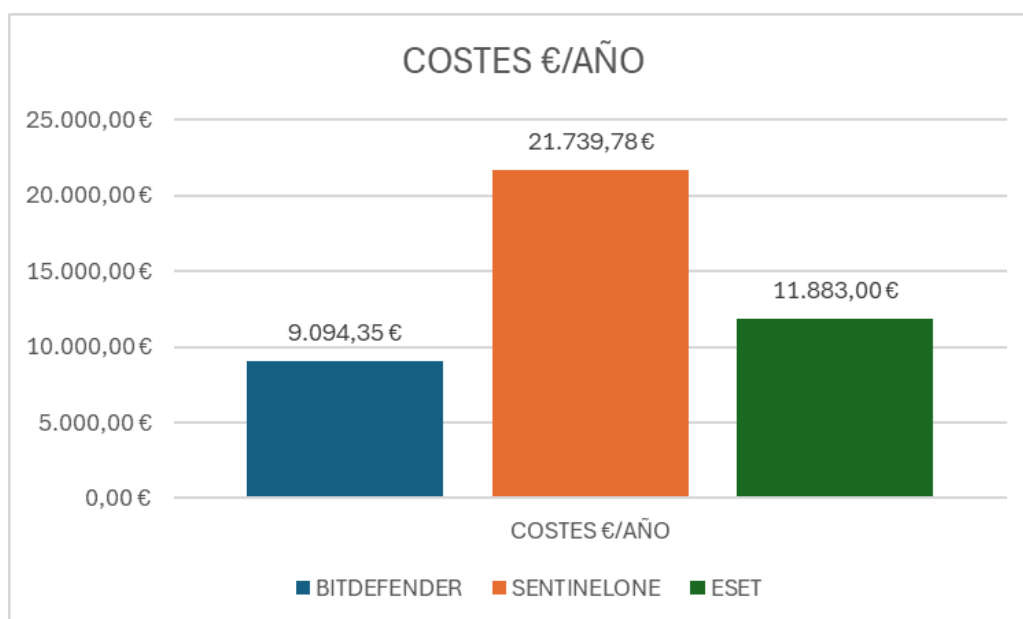
- SentinelOne Singularity: 124.24 €/año por dispositivo → Total: 21.749.05 €
- Trend Vision One: XX €/año por usuario → Total: XX €
- Bitdefender GravityZone: 31.91 €/año por usuario → Total: 9.094.35 €
- ESET Protect Complet: 39,61 €/año por usuario → Total: 11.883 €

2. Costos de Implementación y Migración

- Coste en tiempo del equipo de IT: Dependiendo de la solución de seguridad y el método de implementación, puede llegar a las **12-24 horas** (según datos proporcionados de algunas soluciones).

3. Coste Total en 3-5 años

- **Coste total para 3 años:**
 - SentinelOne Singularity: 65.247.15 €
 - Trend Vision One: XX €
 - Bitdefender GravityZone: 27.283,05 €
 - ESET Protect Complet: 35.649 €
- **Coste total para 5 años:**
 - SentinelOne Singularity: 108.745.25 €
 - Trend Vision One: XX €
 - Bitdefender GravityZone: 45.471,75 €
 - ESET Protect Complet: 59.415 €



5. Recomendación Final

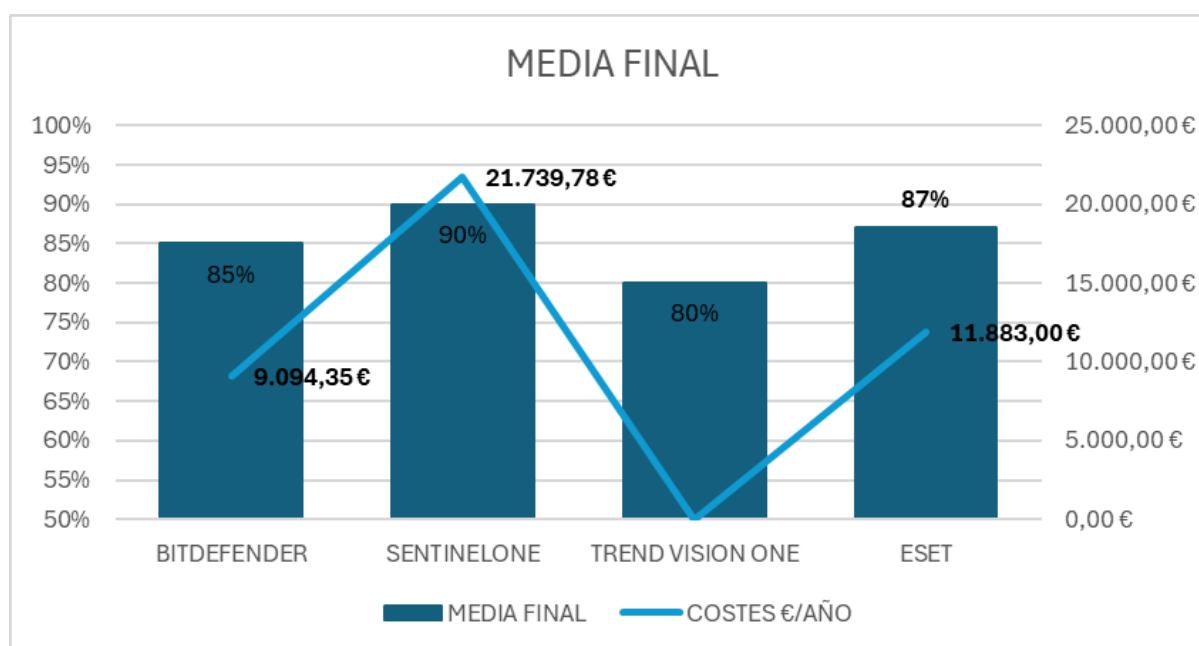
5.1. Mejor opción según los resultados de pruebas.

Tras evaluar las diferentes soluciones de ciberseguridad mediante pruebas prácticas y análisis comparativos, se ha determinado que **SentinelOne** es la mejor opción para los equipos de la empresa.

Las pruebas realizadas y la investigación incluyeron qué SentinelOne destacó en los siguientes aspectos:

- Alta efectividad en la detección de amenazas.
- Bajo impacto en el rendimiento de los equipos
- Gestión centralizada y automatizada,
- Seguro anti brecha
- IA para facilitar el monitoreo.

Los resultados de las pruebas muestran que **SentinelOne** ofrece la mejor combinación de **seguridad, facilidad de administración, rendimiento y precio**, haciendo que su implementación sea la opción más positiva.



5.2. Posibles riesgos de mitigación

La migración a cualquier otra solución de seguridad puede implicar ciertos riesgos que deben ser tenidos en cuenta para asegurar una pasarela efectiva y sin impacto negativo en la protección de los sistemas.

Uno de los riesgos principales es la **interrupción temporal de seguridad** durante el proceso de sustitución. Para minimizar este impacto, se recomienda realizar una **migración por fases**, comenzando con un grupo reducido de equipos en un entorno controlado. Esto permite validar la correcta instalación y funcionamiento del nuevo sistema antes de desplegarlo de forma masiva.

Por otro lado, también puede haber **incompatibilidades con algunas aplicaciones** que no se han tenido en cuenta en las pruebas, por lo que es clave realizar una investigación de compatibilidad antes del despliegue.

Con una planificación adecuada, basada en pruebas y análisis, asegurando una migración estable y una mejora en la ciberseguridad de la empresa.

6. Conclusión

6.1. Beneficios esperados de la migración

La migración de Trellix traerá una serie de beneficios clave para la seguridad, la eficiencia de protección y la administración de los equipos de la empresa. Estos beneficios incluyen mejoras en la protección contra amenazas, una mayor eficiencia y una menor carga administrativa para el equipo de TI.

1. Mejora en la Detección y Respuesta a Amenazas

- Detección avanzada mediante IA.
- Respuesta automatizada ante incidentes, reduciendo tiempos de respuesta.
- Visibilidad completa de endpoints y aplicaciones.

2. Menor Impacto en el Rendimiento

- Optimización de recursos, sin afectar el rendimiento de los equipos.
- Consumo de GPU / RAM baja y mayor eficiencia en equipos, manteniendo la productividad.

3. Facilidad de Administración

- Consola centralizada para gestionar la seguridad de manera eficiente.
- Automatización de tareas repetitivas, reduciendo carga para TI.
- Funcionalidades de ciberseguridad completas.
- Mayor facilidad de visión de lo que ocurre en para el equipo IT
- Equipo de especializado de seguridad 24/7 para el soporte técnico.

4. Protección Multicapa

- Protección integral en endpoints y servidores.
- Detección proactiva de amenazas desconocidas y emergentes (día cero).

5. Reducción de Costos a Largo Plazo

- Menor carga administrativa gracias a la automatización y centralización.

6.2. Consideraciones finales

Cabe resaltar que:

Las soluciones analizadas en este informe muestran un **nivel tecnológico alto y comparten muchas funcionalidades**, como la protección contra amenazas, la gestión centralizada o la capacidad de automatización. Sin embargo, más allá de las diferencias técnicas (como el uso de inteligencia artificial, la arquitectura basada en la nube o la profundidad del análisis en los endpoints).

Uno de los aspectos más importantes a valorar es la calidad de la relación con el proveedor. Mantener una **comunicación buena y contar con un soporte eficaz** puede marcar la diferencia a la hora de resolver incidencias, recibir actualizaciones relevantes para el entorno.

En este sentido, es fundamental no limitar la decisión a las especificaciones del producto, sino considerar también el **acompañamiento que ofrece el fabricante o partner durante la implementación**, el soporte técnico posterior y las oportunidades de evolución del servicio a largo plazo.

También mencionado investigar la opción de cohesity como respaldo de copias de seguridad en encora (partner), aunque su precio es elevado, te da un plus de seguridad en tus backups, y también para barajas más opciones de seguridad para ayudar a mejorar la seguridad informática de la empresa.

Por último, aunque no se ha incluido en el análisis principal de este documento, **Sophos se considera una opción viable a tener en cuenta**. Para llevar una investigación adicional en colaboración con el proveedor **Avanet** con el que se mantuvo la reunión, con el objetivo de comparar sus capacidades y especificaciones frente a las soluciones de este informe y así ver cuál es la mejor alternativa para la empresa.