Actividad: Análisis de Soluciones de Ciberseguridad Comercial.

Herramientas Analizadas:

- **SentinelOne Singularity Complete**
- **Netskope Intelligent SSE**

Proveedores:

- **SentinelOne**
- **Netskope**

Equipo: Miguel Angel e Ivana

Introducción

El entorno actual de ciberseguridad exige soluciones capaces de defender activos empresariales frente a amenazas cada vez más sofisticadas. SentinelOne Singularity Complete y Netskope Intelligent SSE son dos plataformas líderes en el mercado; la primera, enfocada en la protección y respuesta avanzada en endpoints (EPP/EDR), y la segunda en servicios de seguridad en la nube y acceso seguro (SASE/SSE). Estas soluciones abordan la protección contra amenazas a través de la automatización, inteligencia artificial y una gestión centralizada, adaptándose a organizaciones de diversos tamaños y necesidades.

SentinelOne Singularity Complete

Se trata de una herramienta integrada en la nube enfocada a la seguridad avanzada del correo electrónico bloqueando ataques peligrosos (phishing, BEC, quishing, ransomware, etc.) gracias a algoritmos que le permiten un aprendizaje automático en colaboración con otras herramientas como la IA.

Escalabilidad

SentinelOne Singularity Complete está diseñada para ser **altamente escalable**, lo que la hace adecuada para una amplia gama de organizaciones, desde **pequeñas y medianas empresas (PYMES)** hasta **grandes corporaciones y empresas a nivel empresarial**. Su arquitectura basada en la nube permite una expansión fluida de la protección a medida que crece la infraestructura de la empresa.

El modelo de licenciamiento de SentinelOne se basa principalmente en el **número de endpoints o dispositivos** a proteger, lo que ofrece flexibilidad a las organizaciones al adaptar el costo a sus necesidades específicas. Esto facilita la planificación presupuestaria y asegura que la solución pueda crecer junto con la empresa sin requerir cambios significativos en la infraestructura subyacente. La implementación de nuevos agentes en los endpoints es sencilla y puede automatizarse para grandes despliegues.

Métodos de Detección (Firmas, Comportamiento, IA)

SentinelOne Singularity Complete emplea una **aproximación multicapa y avanzada** para la detección de amenazas, superando con creces los métodos tradicionales basados únicamente en firmas:

- **Detección sin firmas (Machine Learning e IA):** Es uno de sus pilares fundamentales. Utiliza **inteligencia artificial y *machine learning***, tanto en el endpoint como en la nube, para analizar el comportamiento de los procesos, las aplicaciones y el sistema operativo. Esto permite la detección proactiva de amenazas desconocidas (día cero) y ataques sin archivos que no dependen de firmas estáticas. El motor de IA puede identificar patrones maliciosos, anomalías y técnicas de ataque en tiempo real, incluso antes de que causen daño.
- **Análisis de Comportamiento (UEBA):** Incorpora capacidades de **Análisis de Comportamiento de Usuarios y Entidades (UEBA)**. Monitorea y analiza continuamente la actividad del usuario y del sistema en los endpoints para identificar desviaciones del comportamiento normal que podrían indicar una actividad maliciosa. Esto es crucial para detectar amenazas internas o ataques que utilizan credenciales comprometidas.
- **Base de datos de firmas (limitada):** Aunque no es su método principal, puede hacer uso de una base de datos de firmas para amenazas conocidas, pero su enfoque principal es la detección proactiva basada en el comportamiento y la IA.
- **Threat Intelligence:** Se apoya en un **equipo de *Threat Intelligence*** de SentinelOne que alimenta la plataforma con información actualizada sobre nuevas amenazas, tácticas, técnicas y procedimientos (TTPs) de los atacantes. Esto enriquece las capacidades de detección y permite a la plataforma adaptarse rápidamente a la evolución del panorama de amenazas.

Capacidad de Administración y Gestión

La gestión de SentinelOne Singularity Complete se realiza a través de una **consola web centralizada** basada en la nube. Esta consola proporciona una **visión unificada y completa** de la postura de seguridad de todos los endpoints protegidos.

- **Consola en la nube (SaaS):** La solución es inherentemente una **solución SaaS (Software as a Service)**, lo que elimina la necesidad de que el cliente gestione infraestructura de servidor o base de datos. La consola es accesible desde cualquier navegador web y proporciona paneles de control intuitivos.
- **Gestión Centralizada:** Permite la configuración de políticas de seguridad, el despliegue de agentes, la supervisión de eventos, la respuesta a incidentes y la generación de informes desde una única interfaz.
- **Informes y Dashboards:** Ofrece una **amplia gama de informes y *dashboards*** personalizables que proporcionan visibilidad sobre la actividad de amenazas, el estado de los endpoints, las detecciones, los intentos de ataque bloqueados y la conformidad de las políticas. Esto ayuda a los equipos de seguridad a entender su postura, identificar tendencias y cumplir con los requisitos de auditoría.
- **Automatización:** Facilita la automatización de tareas de respuesta, como el aislamiento de endpoints, la eliminación de archivos maliciosos y la reversión de cambios en el sistema.

Estructura de Hardware/Infraestructura

SentinelOne Singularity Complete es una **solución puramente *software*** que no requiere la instalación de hardware específico (appliances) por parte del cliente.

- **Agente en los Endpoints:** Su funcionamiento se basa en la **instalación de un agente ligero** en cada endpoint (ordenadores, servidores) que se desea proteger. Este agente es compatible con una amplia variedad de sistemas operativos (Windows, macOS, Linux).
- **Servicio en la Nube:** La inteligencia y la gestión de la plataforma residen en la **nube de SentinelOne**. Esto significa que la mayor parte de la carga computacional y la infraestructura de procesamiento de datos son gestionadas por el proveedor, liberando al cliente de la necesidad de mantener servidores, bases de datos o infraestructuras complejas dedicadas a la seguridad de los endpoints. El cliente solo necesita desplegar los agentes y acceder a la consola web.

Caso de Uso Ideal

SentinelOne Singularity Complete sería una **elección ideal para organizaciones de tamaño mediano a grande** que buscan una **protección avanzada y proactiva** contra el *ransomware*, *malware* de día cero y ataques sin archivos. Es particularmente adecuada para empresas con:

- **Necesidades de alta seguridad:** Empresas que manejan datos sensibles o regulados, y que no pueden permitirse interrupciones por ataques cibernéticos.
- **Equipos de seguridad limitados:** Aunque la herramienta es potente, su gestión en la nube y la automatización de la respuesta a incidentes pueden ayudar a equipos de seguridad más pequeños a manejar un gran volumen de alertas y amenazas de manera eficiente.
- **Entornos distribuidos o remotos:** La naturaleza basada en la nube y el agente ligero permiten proteger endpoints en cualquier ubicación, ideal para empresas con teletrabajadores o múltiples sucursales.
- **Requerimientos de detección y respuesta avanzadas (EDR):** Organizaciones que necesitan no solo prevenir, sino también detectar y responder activamente a incidentes, realizando *threat hunting* y análisis forense.
- **Poca infraestructura *on-premise*:** Empresas que prefieren soluciones SaaS para reducir la carga de gestión de infraestructura interna.

Por ejemplo, una empresa de **desarrollo de *software*** con un equipo distribuido que maneja propiedad intelectual valiosa se beneficiaría enormemente. Necesitan una protección que no solo bloquee amenazas conocidas, sino que también detecte y neutralice ataques sofisticados dirigidos a sus desarrolladores o repositorios de código, sin requerir una gran inversión en infraestructura de seguridad local.

Netskope Intelligent SSE

Netskope es una plataforma de ciberseguridad cloud-native que proporciona visibilidad, protección de datos y defensa contra amenazas en aplicaciones en la nube, sitios web y tráfico privado. Está diseñada para reemplazar herramientas tradicionales como proxies, firewalls, VPNs y soluciones DLP heredadas, con un enfoque moderno basado en la nube y en el modelo SASE (Secure Access Service Edge).

Escalabilidad

- Diseño cloud-native y SASE: Netskope se basa en una infraestructura global llamada *NewEdge*, con centros de datos en más de 60 regiones, con arquitectura de microservicios que escala automáticamente según la demanda Netskope+15Netskope+15PeerSpot+15.

- Enfoque sin sobresuscripción: Cada PoP opera por debajo del 30 % de su capacidad; al llegar a ese límite, Netskope agrega más capacidad o abre nuevos PoP, garantizando continuidad incluso en picos repentinos .

- Escalable para PYMES y grandes empresas: revisiones en PeerSpot destacan que la plataforma “automatically grows” tanto en entornos de ~500 como 10.000 usuarios, sin necesidad de acción del cliente PeerSpot.

- Modelo de licenciamiento: Netskope ofrece modelos basados principalmente en usuario y volumen de datos/IO, ajustándose según el nivel de servicio (CASB, DLP, ATP, ZTNA, etc.).

Métodos de detección (Firmas, Comportamiento, IA)

- Firma y heurística tradicional: Usa motores de firma y heurísticas en línea para detección rápida.

- Inteligencia artificial y ML avanzada:

    - Usa clasificadores ML inline (PE files, Office, sandboxing dinámico) entrenados con millones de muestras, detectando malware en milisegundos y complementando la detección tradicional Netskope+5Netskope+5Netskope+5.
    - Aplica machine learning para patrones de ransomware, analizando estadísticos de cifrado en archivos y activando alertas en su motor UEBA Netskope+1Netskope+1.

- UEBA: Netskope Advanced UEBA genera análisis basados en comportamiento de usuarios y entidades, con más de 100 detecciones (compromiso interno, exfiltración, ransomware...), incluyendo un “User Confidence Index” que cuantifica el riesgo por usuario community.netskope.com+2Netskope+2Netskope+2.

- Threat Intelligence: Integración continua de feeds TI en tiempo real, reforzada por la arquitectura global y los recursos de Netskope Threat Labs.

Capacidad de Administración y Gestión

- Consola centralizada: Plataforma de administración unificada, basada en la web, con dashboards personalizables que permiten aplicar políticas de seguridad en tiempo real.

- Modelos de despliegue:

    - SaaS (cloud puro): Sin necesidad de infraestructura local.
    - On-premise: Con appliances físicos cuando se requiere procesamiento local.
    - Híbrido: Combinación de nube y elementos locales, ideal para entornos con necesidades de cumplimiento específicas.

- Informes y visualización:
    - Dashboards en tiempo real con métricas de seguridad, cumplimiento, amenazas y actividad de usuarios.
    - Informes programables para auditorías, normativas (GDPR, HIPAA, PCI-DSS), y análisis forense.

- Integración con otras plataformas: Netskope se integra fácilmente con herramientas de terceros como SIEM, SOAR, Microsoft Entra, Okta, etc., para una gestión centralizada de seguridad.

Estructura de Hardware / Infraestructura

- Cloud puro: La mayoría de las funciones (CASB, SWG, DLP, ZTNA, etc.) se ofrecen como servicio desde la nube, eliminando la necesidad de hardware adicional en muchos casos.

- Agente ligero (Netskope Client): Instalado en los endpoints para redireccionar tráfico, aplicar políticas y realizar inspección profunda sin afectar el rendimiento del dispositivo.

- Appliances físicos (opcional): Para clientes con entornos on-premise, Netskope ofrece dispositivos como:
    - NSG-101, NSG-500 y NSG-3000, con capacidades de hasta 10 Gbps y funciones de inspección local.

- Infraestructura mínima en la nube: En escenarios 100 % SaaS, el cliente no necesita mantener ni administrar hardware adicional.

Caso de Uso Ideal para Netskope

Tipo de empresa:
Una empresa global de servicios financieros con miles de empleados distribuidos entre oficinas, sucursales remotas y trabajo híbrido, que maneja información altamente sensible (como datos personales, financieros y regulatorios) y debe cumplir con regulaciones estrictas como GDPR, PCI-DSS, HIPAA o SOX.

¿Por qué Netskope es ideal en este escenario?

- Cobertura multi nube avanzada: Netskope ofrece visibilidad y control granular sobre miles de aplicaciones SaaS y entornos IaaS/PaaS como AWS, Azure y GCP.

- Protección de datos y cumplimiento normativo: Su motor de DLP avanzado permite políticas detalladas, detección de datos sensibles y generación de

informes automatizados para auditorías.

- Modelo Zero Trust con ZTNA: Reemplaza VPNs tradicionales con acceso seguro y contextual basado en identidad, dispositivo y riesgo.

- Usuarios distribuidos y movilidad: Gracias a su arquitectura NewEdge, garantiza bajo nivel de latencia y alta disponibilidad para usuarios remotos, sin necesidad de hardware local.

- Respuesta a amenazas avanzadas: El uso de IA, UEBA, y sandboxing permite detectar y mitigar malware, phishing y comportamiento anómalo incluso en canales cifrados como HTTPS.

- Integración con entornos corporativos existentes: Compatible con SIEM, SOAR, Microsoft Entra ID (Azure AD), soluciones EDR, y herramientas de ticketing como ServiceNow.

Comparativa de las dos herramientas

1. Escalabilidad

Herramienta	**Enfoque de Escalabilidad**	**Modelo de Licenciamiento**	**Adecuación por tamaño de empresa**
SentinelOne Singularity Complete	Diseñada para crecer de manera dinámica y elástica, soportando más de 500,000 agentes por clúster.	Por usuario o dispositivo, licencias escalables en la nube.	PYMES y grandes corporaciones; permite ampliación sin intervención manual elevada.

Netskope Intelligent SSE	Adaptada para despliegues globales y múltiples escenarios (sucursales, nubes múltiples, teletrabajo).	Por usuario, dispositivos o volumen de datos; flexible.	Empresas de cualquier tamaño, ideal para organizaciones con fuerza laboral distribuida.

2. Métodos de Detección (Firmas, Comportamiento, IA)

Herramienta	**Tecnología de Detección**	**Uso de IA/ML**	**Threat Intelligence**
SentinelOne Singularity Complete	Motores de análisis estático, comportamiento y Storyline™ (correlación automática de eventos); EDR avanzado, detección autónoma en el endpoint incluso sin conexión a la nube	Extensivo: IA y ML aplicados a prevención y respuesta, automatización total de acciones	Integrado con fuentes propias y externas, compatible con MITRE ATT&CK. STAR™ para reglas personalizadas.
Netskope Intelligent SSE	Detección de amenazas en tiempo real mediante inspección de tráfico web, cloud y privado; categorización de aplicaciones por IA y	Análisis basado en IA/ML para categorización, control de acceso, y protección ante	Aprovechamiento de inteligencia local y global, integración con plataformas externas de Threat Intelligence

	análisis de comportamiento	amenazas avanzadas	

3. Capacidad de Administración y Gestión

Funcionalidad	**SentinelOne Singularity Complete**	**Netskope Intelligent SSE**
Modelo de Gestión	Consola web centralizada (multi-tenant, SaaS global)	Administración unificada cloud-based para todos los módulos
Personalización/Admin. avanzada	Roles, personalización y autenticación multifactor (MFA)	Gestión de políticas adaptativas
Informes y Paneles	Reports avanzados, paneles de analítica, visibilidad histórica hasta 3 años	Dashboards e informes en tiempo real y personalizados
Automatización / Integraciones	Automatización de flujos y respuestas; integración API con herramientas externas	Integración con soluciones externas; gestión centralizada

Despliegue y Acceso	SaaS global; accesible desde cualquier lugar con gestión centralizada	Consola 100% nube, operación y despliegue ágiles

4. Estructura de Hardware/Infraestructura

Herramienta	**Requisitos de Infraestructura**	**Modalidad**	**Agente/Sensor**
SentinelOne Singularity Complete	Agente software ligero en endpoints (Windows, macOS, Linux, VDI, servidores); no requiere appliances físicos dedicados	SaaS cloud, on-premises en escenarios híbridos	Sentinel Agent; puede operar independiente de hardware específico
Netskope Intelligent SSE	Solución principalmente cloud (NewEdge Network), complementada por gateways virtuales o físicos para ambientes SD-WAN	100% nube para SSE; gateways virtuales/hardware disponibles para integración en ramas/sedes físicas	Netskope One Client (agente unificado), gateways para integración con redes físicas

Conclusión

SentinelOne:

SentinelOne Singularity Complete es una **solución EPP/EDR robusta y de vanguardia** que ofrece una protección integral contra las amenazas cibernéticas modernas.

Ventajas Principales:

- **Detección Proactiva y Avanzada:** Su fuerte enfoque en la **IA y el *machine learning*** permite detectar amenazas desconocidas y ataques complejos (sin archivos, día cero, *ransomware*) que las soluciones tradicionales no pueden.
- **Automatización de Respuesta:** Capacidad para **reaccionar automáticamente** a las amenazas, incluyendo la reversión de acciones maliciosas, lo que reduce significativamente el tiempo de respuesta y el impacto de un ataque.
- **Fácil Gestión (SaaS):** Al ser una solución **SaaS en la nube**, simplifica enormemente la administración y el despliegue, reduciendo la carga de trabajo del personal de TI y seguridad.
- **Visibilidad Completa (EDR):** Proporciona **capacidades EDR** que ofrecen una visibilidad profunda de la actividad en los endpoints, facilitando el análisis forense y el *threat hunting*.
- **Escalabilidad:** Se adapta fácilmente al crecimiento de la organización sin requerir inversiones adicionales en hardware.

Posibles Desventajas:

- **Curva de Aprendizaje:** Aunque la consola es intuitiva, para explotar completamente las capacidades avanzadas de EDR y *threat hunting*, los equipos de seguridad pueden requerir una **curva de aprendizaje** para familiarizarse con todas las funcionalidades.
- **Costo:** Como solución premium con capacidades avanzadas, su **costo** puede ser más elevado en comparación con antivirus tradicionales, lo que podría ser una consideración para PYMES con presupuestos muy ajustados.
- **Dependencia de la Conectividad:** Al ser una solución en la nube, una **conectividad a internet estable** es crucial para la gestión centralizada y la actualización de la inteligencia de amenazas, aunque el agente *offline* sigue proporcionando protección.

En resumen, SentinelOne Singularity Complete es una inversión sólida para organizaciones que buscan una defensa de endpoints de nueva generación, capaz de enfrentar el cambiante panorama de amenazas con inteligencia y automatización.

Netskope:

- Seguridad cloud integral con controles granularizados y análisis basados en IA.
- Cobertura de todo el tráfico (web, cloud, privado) y gestión centralizada 100% nube.
- Adecuado para la protección del entorno de trabajo moderno distribuido.

Desventajas posibles:

- SentinelOne:
  - Dependencia del despliegue de agentes en cada endpoint.
  - Complejidad potencial en entornos sin gestión de endpoints centralizada.
- Netskope:
  - En escenarios puramente locales (sin cloud), su propuesta de valor es menor.
  - Requiere integración adecuada de gateways para entornos híbridos complejos.

Ambas soluciones representan el estado del arte en sus respectivos campos y permiten a las organizaciones protegerse proactivamente ante amenazas emergentes y actuales, cada una potenciando una postura de seguridad robusta y adaptada al contexto digital presente

SentinelOne y Netskope unen fuerzas en una solución