Protección de punto final
de Seqrite

SEQRITE | sp source point

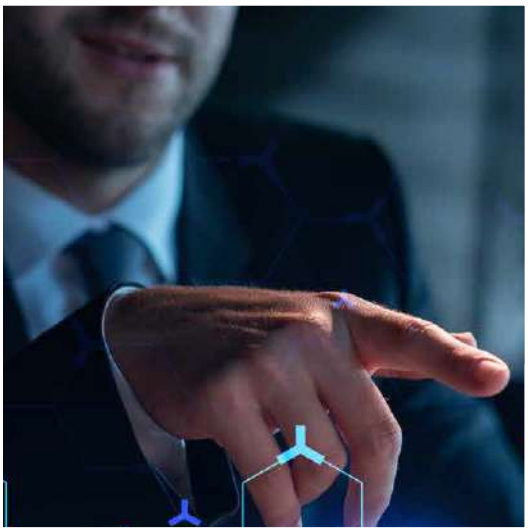
Protección integral de punto final, que incluye prevención, detección, respuesta y caza de amenazas de nivel empresarial para estaciones de trabajo, portátiles y servidores.

www.seqrite.com

¿Por qué proteger los puntos finales **es el futuro de la ciberseguridad?**

A medida que evolucionan los ciberataques y las empresas adoptan cada vez más los servicios en la nube y las operaciones remotas, los métodos tradicionales de protección de punto final se quedan cortos a la hora de proporcionar una seguridad adecuada. A pesar de las considerables inversiones en ciberseguridad, las organizaciones suelen tener dificultades para proteger sus activos digitales y sus datos frente a los ataques iniciados desde los puntos finales. Por lo tanto, es necesario proteger las tecnologías utilizadas por los trabajadores remotos.

Para lograr una protección completa de los puntos finales, las empresas necesitan una solución de red que trascienda los límites geográficos y abarque todos los puntos finales móviles modernos. Ya sea en la nube o en las instalaciones, la elección es suya. Ofrecemos una solución de seguridad integral diseñada para una eficiencia óptima del rendimiento, garantizando la protección de todos los puntos finales.



Seqrite

Protección de puntos finales para empresas

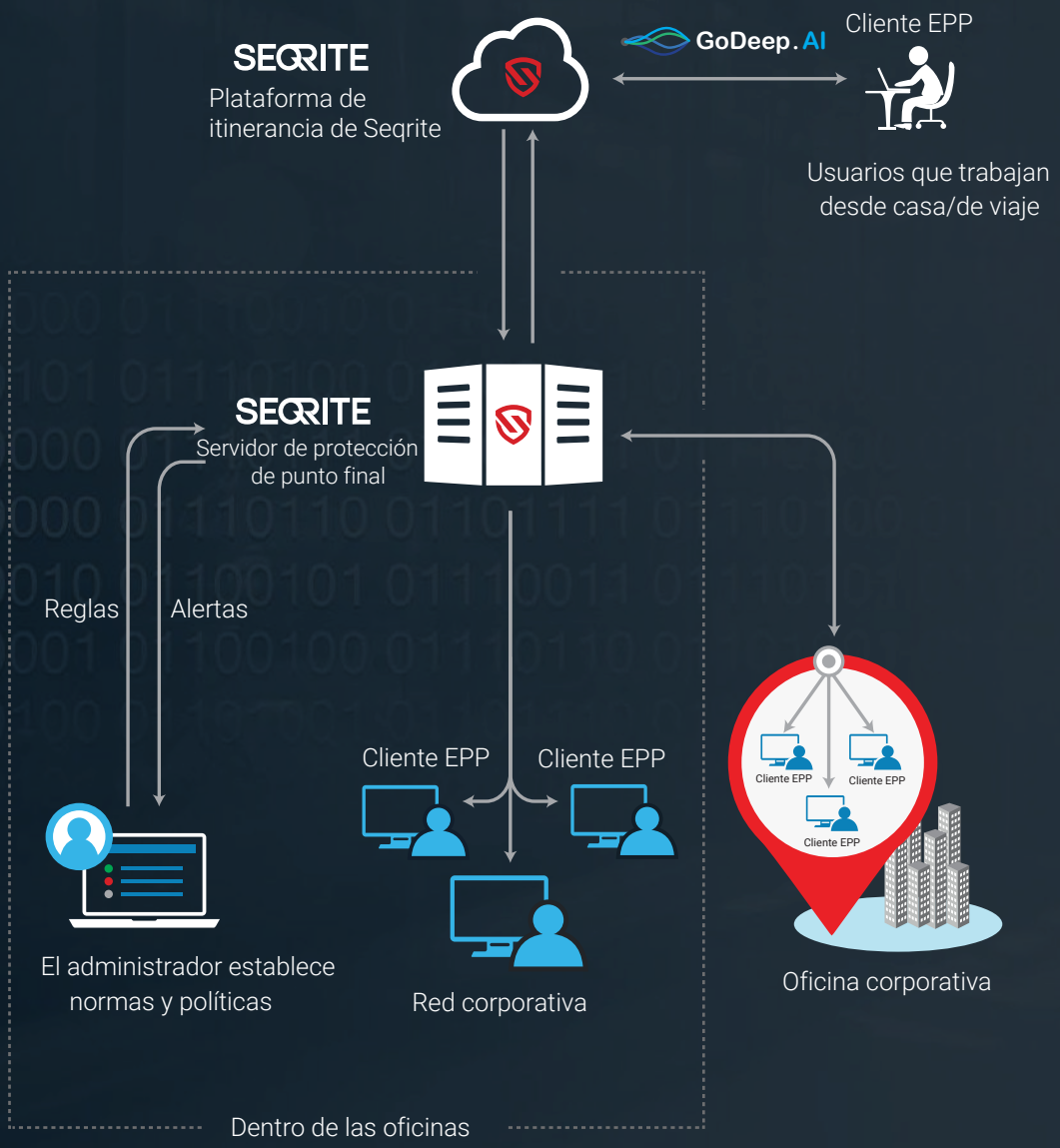
¡Una solución unificada para detener las amenazas en seco!

La Protección de punto final de Seqrite es una plataforma sencilla y completa que integra tecnologías innovadoras como Anti Ransomware, y Behavioural para proteger su red de las amenazas avanzadas de hoy en día.Sistema de detección para proteger su red de las amenazas avanzadas de hoy en día.

Ofrece una amplia gama de funciones de vanguardia, como control avanzado de dispositivos, DLP, análisis de vulnerabilidades, gestión de parches, filtrado web, gestión de activos, búsqueda de archivos empresariales, etc., para garantizar una protección completa de los activos digitales de las empresas.

Una plataforma **Soluciona múltiples problemas**

Protección de punto final de Seqrite



¿Por qué elegir la **Protección de punto final de Seqrite?**

1 Protección y control integrales de punto final

Una plataforma sencilla pero potente que impone el control sobre los datos, las aplicaciones y el acceso web mediante un completo conjunto de funciones, entre las que se incluyen el control avanzado de dispositivos, DLP, la gestión de activos, el control de aplicaciones y mucho más.

2 Protección multicapa

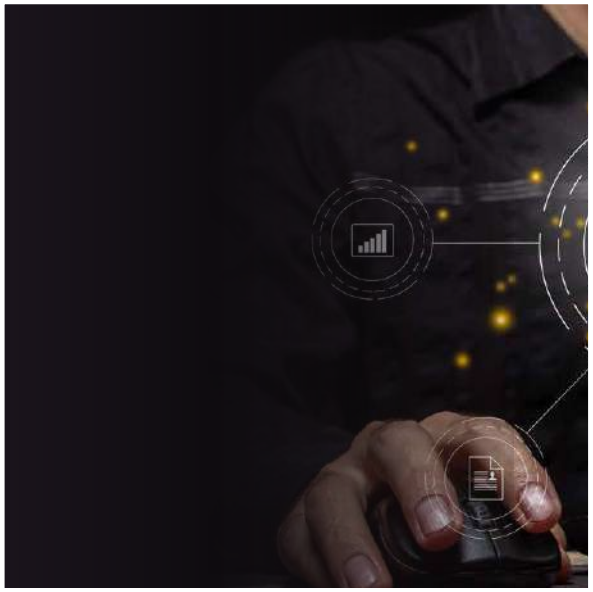
Certificado por varias certificaciones del sector, integra tecnologías innovadoras como Análisis avanzado de ADN, detección de comportamientos, búsqueda de archivos de empresa y anti-ransomware para proteger su sistema contra malware y amenazas avanzadas a diferentes niveles.

3 Explore y parchee las vulnerabilidades de las aplicaciones

Ayuda a detectar las vulnerabilidades de las aplicaciones y del sistema operativo y las corrige instalando los parches que faltan. La actualización periódica de las aplicaciones hace que la red sea menos vulnerable a los ataques de malware.

4 Gestión y control centralizados

Dispone de una interfaz fácil de usar para supervisar, configurar y gestionar varios sistemas de la red con informes detallados y un panel gráfico.



Descripción de funciones

Protección básica

Antivirus
Ofrece protección contra malware certificada por las principales certificaciones del sector.

Anti-Ransomware
Protección contra ataques de ransomware y copia de seguridad automática de los tipos de archivos seleccionados.

Sandboxing de archivos
Se integra con Sandbox en la nube de Seqrite para analizar archivos sospechosos en busca de malwares. No hay razón para comprar y utilizar hardware o software para el análisis de malware.

Control de dispositivos y DLP

Control de dispositivos avanzado
Aplique políticas relativas al uso de dispositivos de almacenamiento, dispositivos móviles y portátiles, dispositivos inalámbricos, interfaces de red conectadas a puntos finales.

Prevención de pérdida de datos
Evita la pérdida de datos mediante la supervisión de los datos confidenciales y definidos por el usuario que se comparten a través de unidades extraíbles, la red o diversas aplicaciones.

Protección Web

Protección de navegación
Bloquea los sitios maliciosos

Protección contra phishing
Bloquea los sitios de phishing.

Filtrado web
Bloquea sitios según sus categorías.

Acceso programado a Internet
Programe el acceso a Internet en función de la hora.

Controlador de acceso a Google y YouTube
Bloquea el acceso personal y permite el acceso corporativo a Google en función de los dominios de cuenta elegidos por el administrador. Bloquea los vídeos de YouTube en función de la categoría de contenido, el nombre del editor, etc.

Protección de red

IDS/IPS
Detecta las actividades maliciosas en la red que aprovechan las vulnerabilidades de las aplicaciones y bloquea los intentos de intrusión.

Cortafuegos
Supervisa el tráfico de red entrante y saliente basándose en reglas.

Prevención de ataques de escaneo de puertos
Alertas sobre ataques de escaneo de puertos.

Prevención de ataques DDOS
Alertas sobre ataques DDOS.

Supervisión y control

Exploración de vulnerabilidades
Proporciona una vista resumida de vulnerabilidades según su gravedad

Gestión de parches
Solución de gestión de parches centralizada para parchear vulnerabilidades de aplicaciones de Microsoft y ajenas a Microsoft.

Monitor de actividad de archivos
Supervisa los archivos confidenciales de la empresa y notifica a los administradores cuando dichos archivos se copian, renombran o eliminan.

Gestión y control

Administración centralizada
Consola basada en web con panel gráfico, gestión de grupos y políticas, notificación por correo electrónico y SMS, fácil implantación.

Plataforma de itinerancia
Gestione a los clientes aunque se desplacen fuera de la red corporativa.

Migración sin problemas de las instalaciones a la nube
Simplifica la transición de Protección de punto final v8.3 y v7.6 a las funciones avanzadas de la Nube de protección de punto final mediante una ruta de actualización optimizada.

Alta disponibilidad (HA)
La alta disponibilidad garantiza el acceso ininterrumpido de los usuarios a los servicios, aplicaciones y datos, incluso durante fallos de hardware y software, minimizando así el tiempo de inactividad del sistema.

Descripción de funciones

Gestión y control

Cifrado BitLocker Gestión de la seguridad de los datos

Permite la gestión centralizada de las políticas de cifrado, claves y opciones de recuperación de BitLocker, lo que garantiza una sólida seguridad de los datos y el cumplimiento de los requisitos normativos.

Gestión multisede

Permite el control centralizado de ubicaciones geográficamente dispersas, garantizando la seguridad y la eficacia.

Detección y respuesta de punto final (EDR)

Consulta rápida a puntos finales

Obtiene los puntos finales en tiempo real para recopilar información de fuentes de datos predefinidas en los puntos finales.

Búsqueda automatizada de IoC

Se integra con el servidor MISP para la alimentación de amenazas. Estos archivos hash del MISP se buscarán regularmente (diariamente/semanalmente), y los resultados se incluirán en los informes.

Bloqueo de IoC en tiempo real

Envíe Hashes de archivos para una investigación continua de contenido malicioso y bloqueo en tiempo real.

Gestión de aplicaciones y activos

Lista segura de control de aplicaciones

Restringe el acceso a las aplicaciones basándose en la metodología de Confianza Cero. Permite definir los permisos de las aplicaciones en función del Sistema Operativo, incluyendo las aplicaciones por defecto del SO y Seqrite. Ofrece un modo 'Solo supervisión' para registrar el acceso a las aplicaciones para su visualización administrativa sin bloquearlo.

Gestión de activos

Proporciona una visibilidad total del hardware y el software que se ejecuta en los terminales y también ayuda a realizar un seguimiento de los cambios de software y hardware que se producen en los puntos finales.

Protección avanzada

Búsqueda de archivos de empresa (EFS)

EFS es una forma eficaz de encontrar archivos que coincidan con hashes maliciosos a través de sus puntos finales. Basándose en los hashes proporcionados por un usuario, EFS detecta ataques ocultos y ayuda a cazarlos antes de que dañen el sistema.

Comparación de productos

Características	Pymes	Empresas	Total	Enterprise Suite	EDR
Antivirus	✓	✓	✓	✓	✓
Anti-Ransomware	✓	✓	✓	✓	✓
Protección del correo electrónico	✓	✓	✓	✓	✓
Protección IDS/ IPS	✓	✓	✓	✓	✓
Protección de cortafuegos	✓	✓	✓	✓	✓
Protección contra phishing	✓	✓	✓	✓	✓
Protección de navegación	✓	✓	✓	✓	✓
Exploración de vulnerabilidades	✓	✓	✓	✓	✓
Plataforma de itinerancia	✓	✓	✓	✓	✓
Gestión multisede	✓	✓	✓	✓	✓
Gestión de activos		✓	✓	✓	✓
Protección contra el spam		✓	✓	✓	✓
Filtrado web		✓	✓	✓	✓
Control de dispositivos avanzado		✓	✓	✓	✓
Integración SIEM		✓	✓	✓	✓
Control de aplicaciones– Lista de bloqueos			✓	✓	✓
control de aplicaciones - Lista segura			✓	✓	✓
Tuneup			✓	✓	✓
Monitor de actividad de archivos			✓	✓	✓
Gestión de parches			✓	✓	✓
Controlador de acceso a YouTube				✓	✓
Controlador de acceso a Google				✓	✓
Gestión del cifrado de discos				✓	✓
Consulta rápida a puntos finales					✓
Búsqueda automatizada de IoC					✓
Bloqueo de IoC en tiempo real					✓
Búsqueda de archivos de empresa (EFS)					✓
Prevención de pérdida de datos		Complemento	Complemento	✓	✓
Sandboxing de archivos		Complemento	Complemento	Complemento	Complemento

Nota: *Solo disponible para 7.x.

Certifications

Protección de punto final de Seqrite certificado como ‘Protección autorizada de puntos finales corporativos’ para Windows por ‘AV-Test’

¿Preparado para una prueba?

Haga clic aquí

O escanee

Acerca de Seqrite

Seqrite es un proveedor líder de soluciones de ciberseguridad empresarial. Con un enfoque en la simplificación de la ciberseguridad, Seqrite ofrece soluciones y servicios integrales a través de nuestra pila tecnológica patentada, impulsada por IA/ML para proteger a las empresas contra las últimas amenazas mediante la protección de dispositivos, aplicaciones, redes, nube, datos e idnetidad. Seqrite es el brazo empresarial de la marca mundial de ciberseguridad Quick Heal Technologies Limited, la única empresa de productos y soluciones de ciberseguridad que cotiza en bolsa en la India.

En la actualidad, más de 30 000 empresas de más de 76 países confían sus necesidades de ciberseguridad a Seqrite.

SEQRITE | sp source point

Contacto de Sourcepoint:
Teléfono: 966 902 700 | ventas@sourcepoint.pe | sourcepoint.pe