



EL PARTNER QUE NECESITAS



01

SEGURIDAD DE APLICACIONES

La seguridad de las aplicaciones ayuda a identificar, corregir y prevenir vulnerabilidades de seguridad en cualquier tipo de software de aplicaciones.

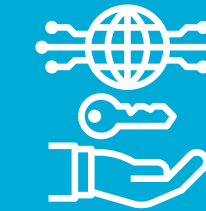


Veracode
Outpost 24

02

SEGURIDAD DE ACCESO

A medida que el número y la complejidad de las amenazas cibernéticas continúan creciendo, la administración de cuentas privilegiadas eficaz y ágil se ha convertido en la clave para organizaciones de todos los tamaños.

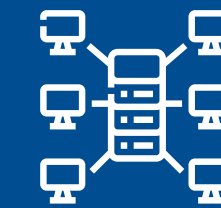


Thycotic

03

SEGURIDAD DE REDES

Mantener el intercambio de información libre de riesgo y proteger los recursos informáticos de las empresas.



Sophos
Infovista
Outpost 24

04

SEGURIDAD DE DATOS

La seguridad de datos está relacionada con las políticas y medidas que se deben tener en una empresa para asegurar que sus datos y los de sus clientes no se vean expuestos al mal uso de estos



Sophos
Infovista
Trap X

05

GESTIÓN DE VULNERABILIDADES

La gestión de vulnerabilidades es un proceso continuo, que permite reducir y corregir este riesgo es función de los departamentos de TI.



Veracode
Outpost 24

06

AUDITORÍAS INFORMÁTICAS

Los beneficios son variados, pueden ayudarlo a mejorar la seguridad, aprobar auditorías de cumplimiento normativo y simplificar las operaciones de TI.



Netwrix

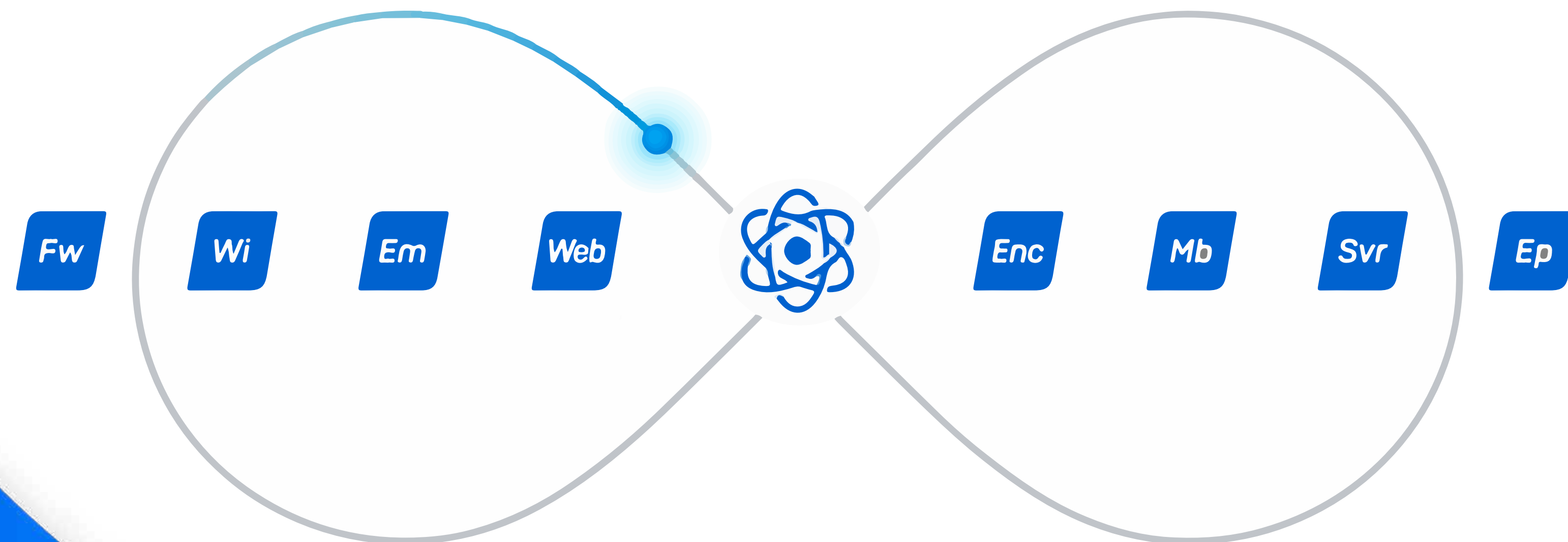


SOPHOS

¿Por qué Sophos?

La mejor ciberseguridad.
Perfectamente integrada. Fácil. Efectiva.

Las soluciones de Sophos, nativas de la nube y con IA mejorada, permiten proteger de las ciberamenazas a todas las estaciones de trabajo de la red, portátiles, escritorios virtuales, servidores, redes, internet, datos, correo electrónico y los dispositivos móviles, sin importar el tamaño de su empresa.



Productos principales

La mejor ciberseguridad.
Perfectamente integrada, Fácil y Efectiva.

Soluciones de administración en la nube para todas sus tecnologías next-gen de Sophos: endpoints, servidores, dispositivos móviles, firewalls, ZTNA, correo electrónico y muchísimo más. Gracias a su consola de administración unificada, la información que se comparte en tiempo real entre productos y la respuesta automatizada a incidentes, haciendo que la ciberseguridad sea más fácil y efectiva.



**Sophos Endpoint
Intercept X**



**Sophos Firewall
XG**



**Sophos MTR
Managed Threat
Response**

VERACODE

¿Por qué Veracode?

Descubre las vulnerabilidades de tus aplicaciones.

Veracode ofrece las soluciones y servicios de seguridad de aplicaciones que requiere el mundo impulsado por software de hoy. La plataforma unificada de Veracode evalúa y mejora la seguridad de las aplicaciones desde el inicio hasta la producción para que las empresas puedan innovar con confianza con la web y las aplicaciones móviles que crean, compran y ensamblan, así como los componentes que integran en sus entornos.

**Líderes en Gartner por 8 años
consecutivos en Seguridad de las
Aplicaciones**

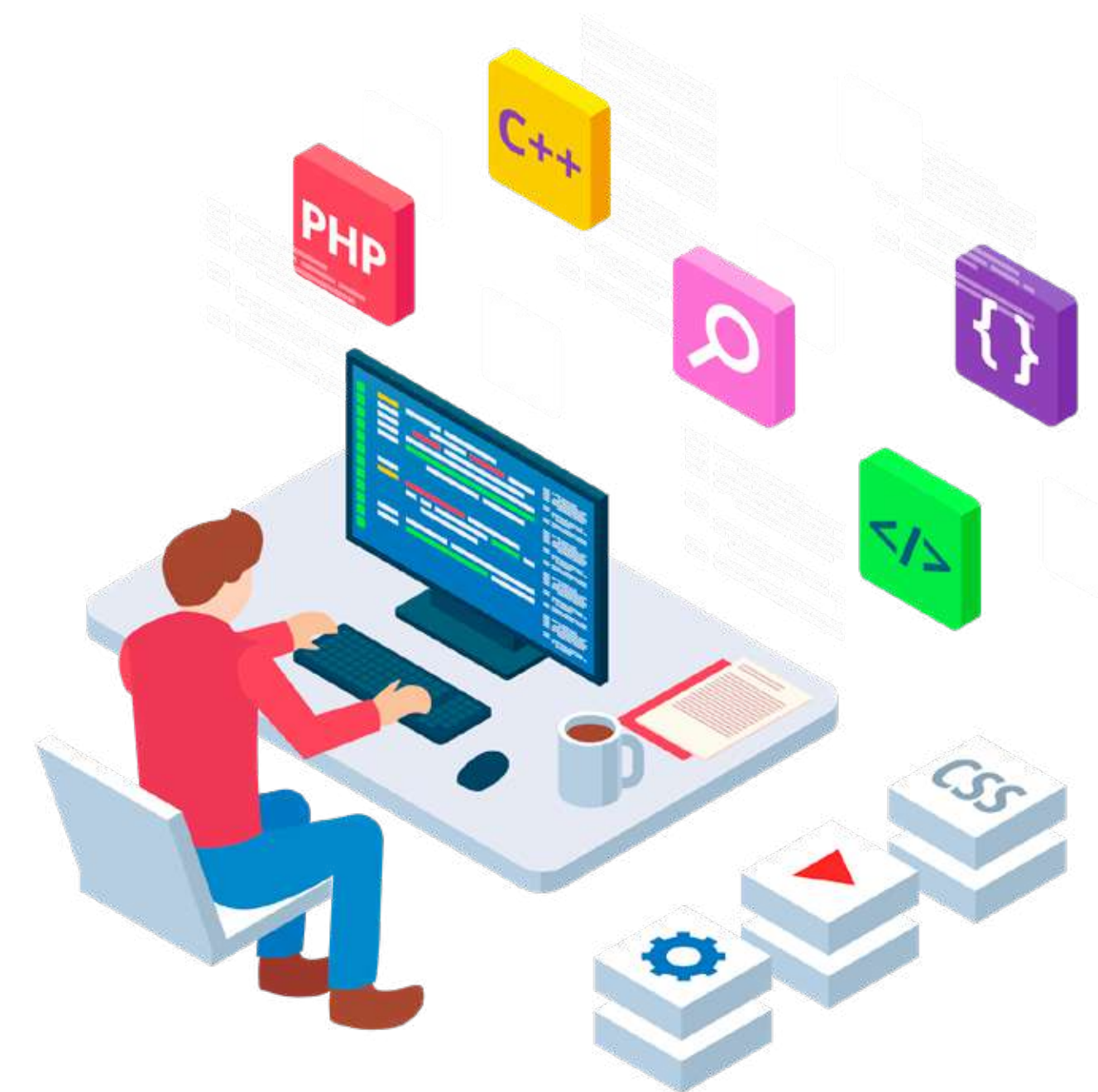
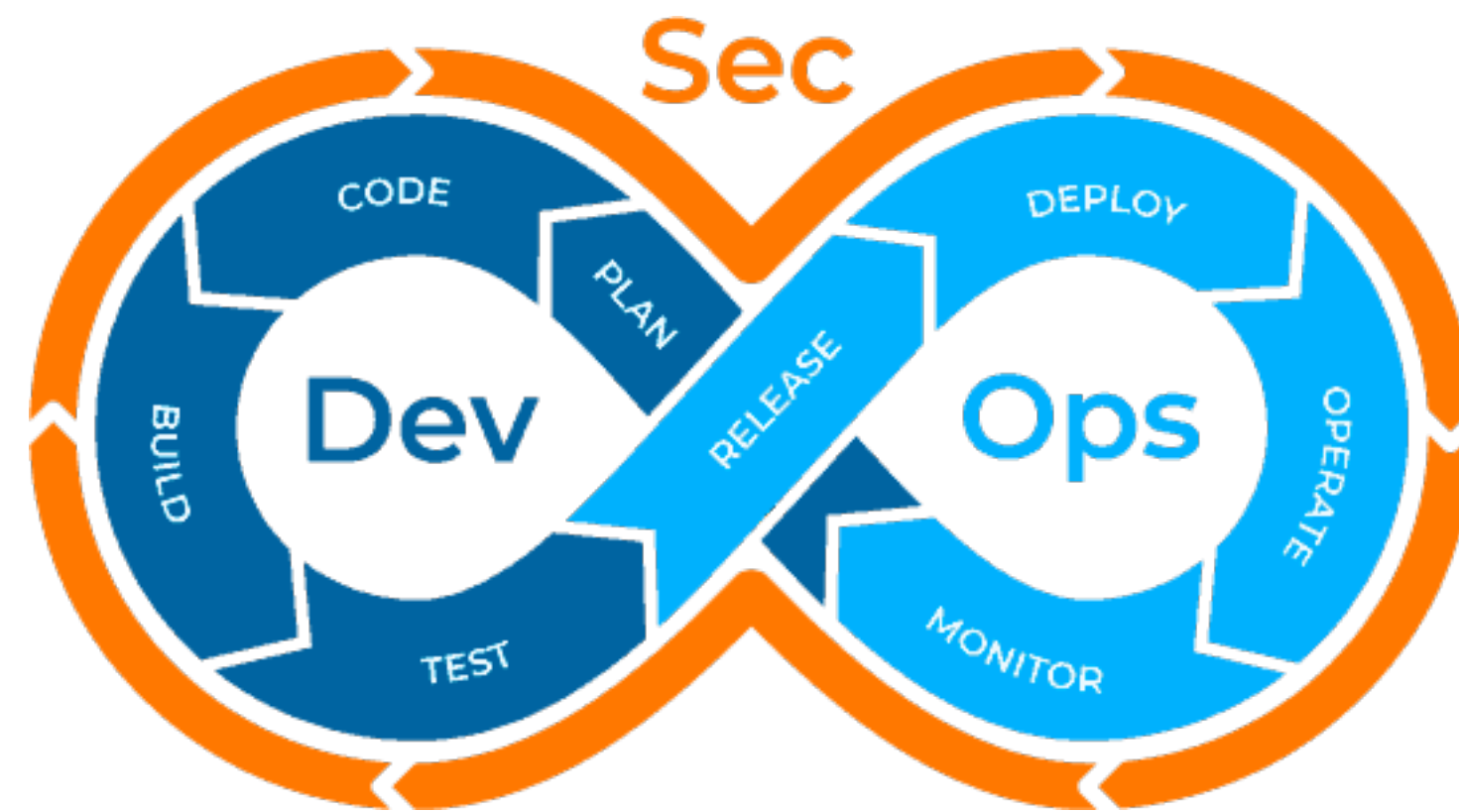
Gartner®



Análisis Estático de Aplicaciones

Análisis estático

Permite a los equipos de seguridad a nivel empresarial realizar pruebas para análisis de la seguridad de la aplicación de forma estática y con ejemplos de remediación, combinado, además con el análisis de los módulos open source dan resultados con los más altos estándares de seguridad.





¿Por qué Ridge?

La revolución del Pentesting es hoy.

Ridge Security permite a las empresas y a los equipos de aplicaciones web, DevOps, ISVs, gobiernos, sanidad, educación -o a cualquier persona responsable de garantizar la seguridad del software- probar sus sistemas de forma asequible y eficiente.

RidgeBot

Ayuda a los encargados de las pruebas de seguridad a superar las limitaciones de conocimientos y experiencia y siempre por formas a un nivel superior consistente. El cambio de las pruebas manuales y de trabajo intensivo a la automatización asistida por máquinas alivia la grave escasez actual de profesionales de la seguridad. Permite a los expertos en seguridad humana dejar de lado el trabajo diario intensivo y dedicar más energía a la investigación de nuevas amenazas y nuevas tecnologías.

- Mejorar la cobertura y la seguridad
- Reducir el costo de la validación de seguridad
- Proteger continuamente el entorno informático
- Producir resultados factibles interesados



¿Qué puede hacer RidgeBot?

Prueba de Penetración: Completa Basándose en la inteligencia de amenazas y en la base de conocimientos de exploits

Ransomware: Ayuda a los clientes a validar rápidamente si sus entornos son vulnerables.

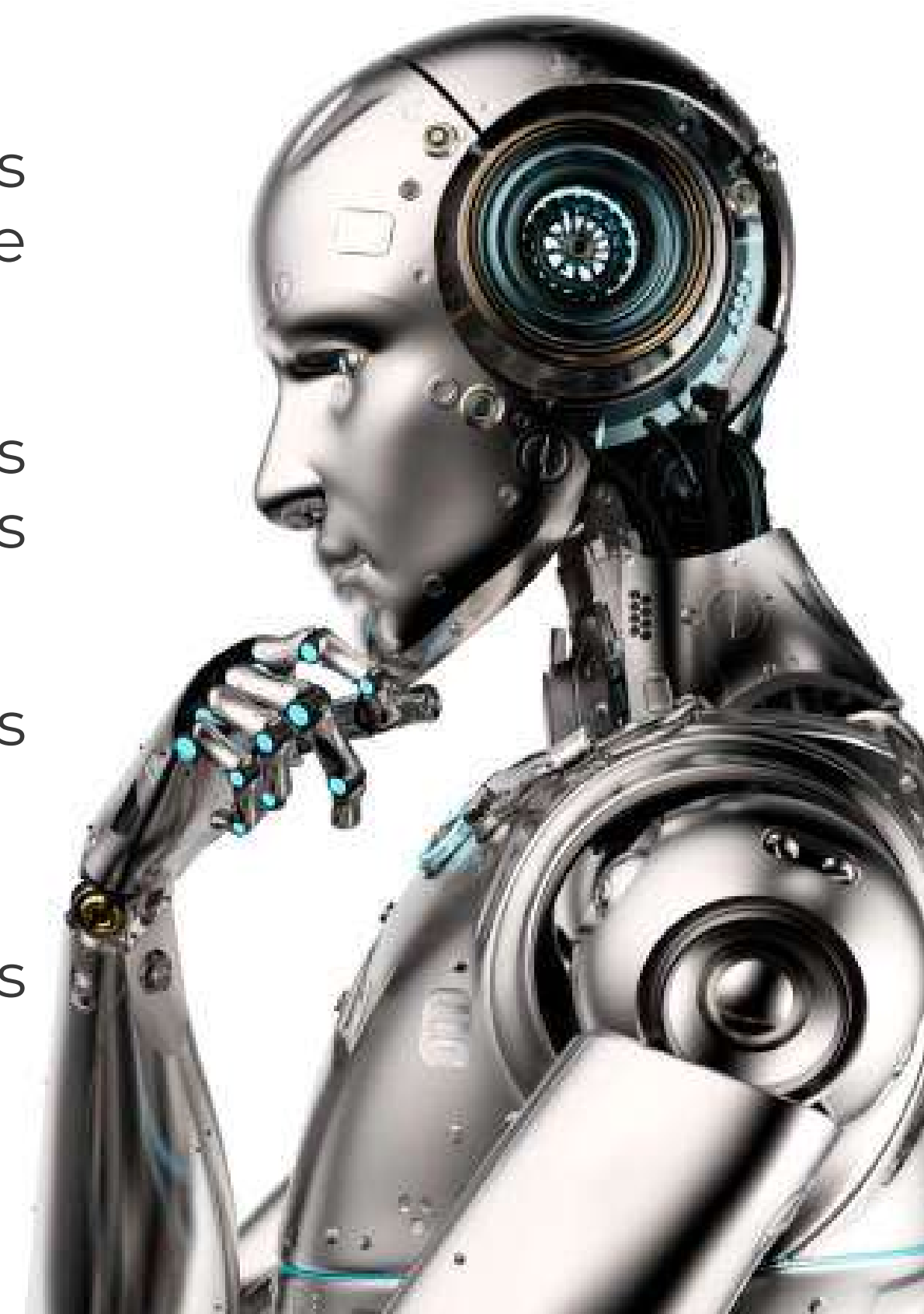
Prueba de Penetración de Sitios Web: Las aplicaciones web y todas las superficies de ataque relacionadas para obtener el control del sitio web objetivo

Prueba de Penetración Interna del Host : Utiliza técnicas avanzadas como la escalada de privilegios, el movimiento lateral, la penetración de dominios y otra.

Explotación de contraseñas débiles: Lanza ataques directos o iterativos basados e información sensible recogida a través de credenciales débiles o vulnerabilidades.

Marco de terceros: Lanza ataques de escalada de privilegios e iterativos basados en vulnerabilidades conocidas d

Perfiles de activos: Esta prueba perfila los activos y desentierra todas las superficies de ataque basadas en nombres



netwrix

¿Por qué Netwrix?

Auditoria de Cambios en Tiempo Real

Netwrix proporciona una plataforma unificada para monitorear lo que está sucediendo tanto en los almacenes de datos como en los sistemas de backbone. Esta visibilidad permite a nuestros clientes comprender dónde se encuentran los datos confidenciales, cuáles son los riesgos a su alrededor y qué actividad está amenazando su seguridad.



Auditoría de Cambios



Gestión Documental



Informes Centralizados



¿Por qué Netwrix?



Identifique

Comprenda qué datos necesitan protección y como de expuestos están.



Recupere

Facilite la recuperación de los datos clave y aprenda de incidentes pasados.



Responda

Tome decisiones de respuesta a incidentes más rápidas y mejor informadas.



Detecte

Detecte la actividad que pone en riesgo la seguridad de sus datos.



Proteja

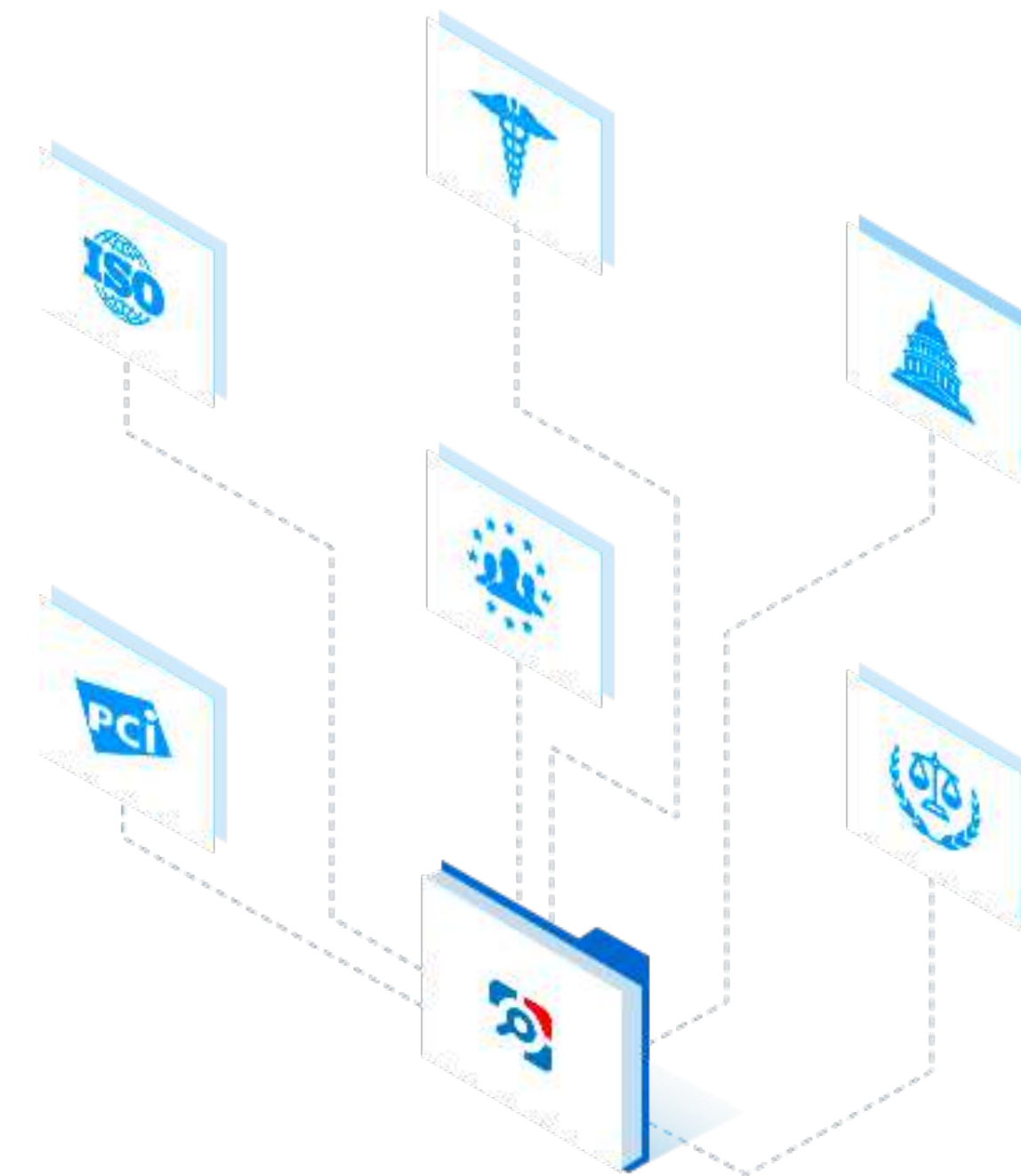
Minimice el riesgo de posibles incidentes de ciberseguridad.



Cumpla

Establezca controles de seguridad y demuestre el cumplimiento normativo.

Las soluciones de Netwrix soportan un amplio rango de plataformas y aplicaciones para dar visibilidad sobre lo que está pasando tanto en los sistemas de almacenamiento de datos como en los sistemas informáticos troncales.





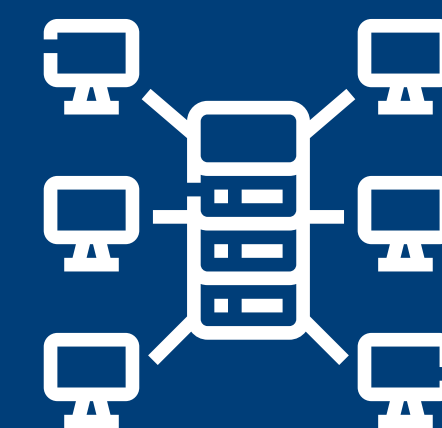
¿Por qué Viewtinet?

Monitoreo y Optimización de Redes

Viewtinet se apoya en la última tecnología para ofrecer a tu empresa una solución para entender y optimizar todo tu ecosistema de TI. Con Viewtinet podrá ver todo lo que sucede en cada dispositivo (datos de registro), en la red (datos de cable) y también optimizar el rendimiento de la red. Para simplificar las cosas, todas estas funciones se ejecutan en el mismo front-end (Viewtisight).

Viewtilog

Realiza el procesamiento, análisis y recolección de logs de cualquier activo, dispositivo, servidor, aplicación o sistema de una empresa. Integra todo tipo de expedientes, registros y bitácoras, también puede sacar todas las métricas y registros de los dispositivos del tipo IoT, como también puede integrar todos los datos de los sistemas OT, puede beneficiarse de tener análisis avanzados, con alta tasa de retención, geolocalización y detección de anomalías.



Monitoreo y Optimización de Redes

Viewtimon

Proporciona todos los conocimientos del tráfico IP, visibilidad y comprensión completa sobre todo lo que sucede en su red en conexiones, paquetes, rendimiento, volumen, IP origen y destino, puerto origen y destino. Ofrece de forma predeterminada un amplio conjunto de métricas de calidad de la experiencia, como: tiempo de viaje, latencia de extremo a extremo, tiempo de sesión HTTP (TTL), hora de configuración de HTTP, VoIP (MOS, Jitter, escalera SIP, etc.). Ofrece la última tecnología DPI para el reconocimiento de aplicaciones, con un conjunto de firmas robustas y actualizadas.

Viewtifi

Gestión y control de tráfico, aplicar políticas de control de aplicaciones en tiempo real, administrar por ejemplo cuando se debe actualizar un software, administrar el tráfico que puede pasar y optimización de tráfico, Permite generar las reglas de clasificación de acuerdo a muchas variables diferentes: protocolo, puerto, rango de puertos, IP, rango de IP, VLAN entre otras. Con la capacidad para definir muchos tipos diferentes de reglas, estas reglas se pueden aplicar para tráfico entrante, tráfico saliente, o lo mismo para ambos sentidos. La optimización TCP de Viewtifi mejora la velocidad más del 100%, especialmente cuando hay entornos inalámbricos.

Monitoreo y Optimización de Redes

Viewtisight

Consola única para todo el ecosistema Viewtinet que viene incluida con todos sus licenciamientos, Abarca todas las capas involucradas en la adquisición de datos (smart data broker), almacenamiento (base de datos de alto rendimiento) y Business Intelligence.

Proporcionará todos los informes a través de una interfaz gráfica de usuario fácil de usar.

Todo lo que puedo hacer con Viewtinet

Gracias a su arquitectura, hay varios casos de uso en los que Viewtinet puede ayudar a su organización.

Monitorización de red : Viewtinet puede ingerir y analizar SNMP, NetFlow, WMI, ICMP, etc. Dispone de una potente consola de alarmas. También puede conectarse con API a cualquier servicio en la nube. Todo esto, sumado a las capacidades de sondeo de red, lo convierte en la herramienta más completa para el monitoreo, análisis y solución de problemas del rendimiento de la red.

Traffic Sniffer : para beneficiarse de las capturas forenses, Viewtimon sniffer captura el tráfico 24x7, con una alta tasa de retención.

Todo lo que puedo hacer con Viewtinet

Traffic Shaping : asegura el rendimiento de las aplicaciones críticas y limita las no deseadas. Mejore la QoE : acelere los flujos de TCP aumentando significativamente el rendimiento de la red.

Análisis de VoIP : juntando la sonda, con decenas de KQIs, con el Call Detail Record, Viewtinet proporciona una visibilidad de 360º de las llamadas tanto a nivel de registro como a nivel de red.

Vista de panel único y análisis avanzado : integre con Syslog, API o cualquier otro mecanismo todos los diferentes datos de su red y benefíciense del análisis avanzado. Mejora el tablero de Meraki, los informes de Pulse Secure, etc.

SOC/NOC : gracias a su arquitectura multiusuario, Viewtinet se utiliza en varios MSP para proporcionar un portal en vivo a los clientes finales con paneles en vivo potentes e interactivos.

Mejora del trabajo desde casa : integre datos de servidores de correo, llamadas, videollamadas, VPN, etc. para proporcionar todos los análisis relacionados con el trabajo desde casa. Mejore la QoE de sus empleados.

Análisis inteligente de IoT : Viewtinet también puede integrar todo tipo de registros y métricas desde cualquier dispositivo IoT.



¿Por qué Outpost24?

Gestión de riesgos de vulnerabilidad completa

La Suite de Outpost24 lo ayuda a automatizar sin esfuerzo la identificación de vulnerabilidades en la infraestructura de red, puede realizar una gestión basada en riesgos para una reparación rápida y monitorear continuamente su exposición de nuevos riesgos.

En la capa de la aplicación encuentre y repare las vulnerabilidades de software continuamente con escaneo automatizado y Pentesting para orquestar la seguridad integral de DevOps, ejecute pruebas en cualquier etapa del ciclo de desarrollo para identificar lagunas que pueden dar involuntariamente a los atacantes acceso a datos confidenciales y funcionalidad.



Todo lo que puede hacer Outpost24



CLOUD SECURITY

Servidores, puntos finales, dispositivos, switches, aplicaciones, nubes y contenedores. Lo cubrimos todo desde el cumplimiento hasta la reducción de riesgos

CLOUDSEC INSPECT

API-instalada en la infraestructura Cloud para escaneo de vulnerabilidades en:

- AWS
- Azure
- Google Cloud (coming soon)
- Docker
- Kubernetes.



NETWORK SECURITY

Se necesita un hacker para atrapar a un hacker. Incorporamos años de experiencia de Ethical Hacking en nuestros productos para obtener los mejores resultados.

OUTSCAN

Cloud-based, evaluación de infraestructura y cumplimiento para redes externas y sucursales.

HIAB (HACKER IN A BOX)

Appliance-based, evaluación automatizada de vulnerabilidades de la infraestructura y de cumplimiento para redes internas.

FARSIGHT

Proporciona inteligencia de amenazas en profundidad sobre la importancia del riesgo.

NEW PWN PULSE

Evaluación de seguridad para redes inalámbricas WIFI y Bluetooth.



APPLICATION SECURITY

Nuestras herramientas funcionan las 24 horas para automatizar escaneos y organizar controles de seguridad para protegerlo de forma continua

SWAT

Penetration testing híbrido con soporte de remediación x 1 año revisiones automatizadas.

SNAPSHOT

Penetration testing híbrido con soporte de remediación x 30 días, bajo demanda.

ASSURE

Penetration testing híbrido con soporte de remediación x 3 días por aplicación.

SCALE

Herramienta Automatizada para análisis DAST.

GoTo

A thick, bright yellow brushstroke underline that starts under the 'G' and extends to the right, ending under the 'o'.

¿Por qué Goto?

Comunicación Avanzada y Segura

El control es tranquilidad por eso gracias a Goto tienes la posibilidad de mantener los ordenadores y los usuarios activos y en funcionamiento, permitiendo continuar la productividad desde cualquier lugar, además de automatizar las soluciones a los problemas rutinario.



Implemente de forma remota y automatice tareas de TI rutinarias
Proteja su empresa con Administración y seguridad de puntos de acceso para empresas



Rescue es un herramienta de asistencia técnica remota que ofrece a las organizaciones la posibilidad de prestar servicios a clientes internos y externos que usan distintos dispositivos y sistemas operativos.



Si tenemos en cuenta que las contraseñas provocan el 81% de las vulnerabilidades, deben convertirse en su prioridad de seguridad fundamental.



¿Por qué Goto?

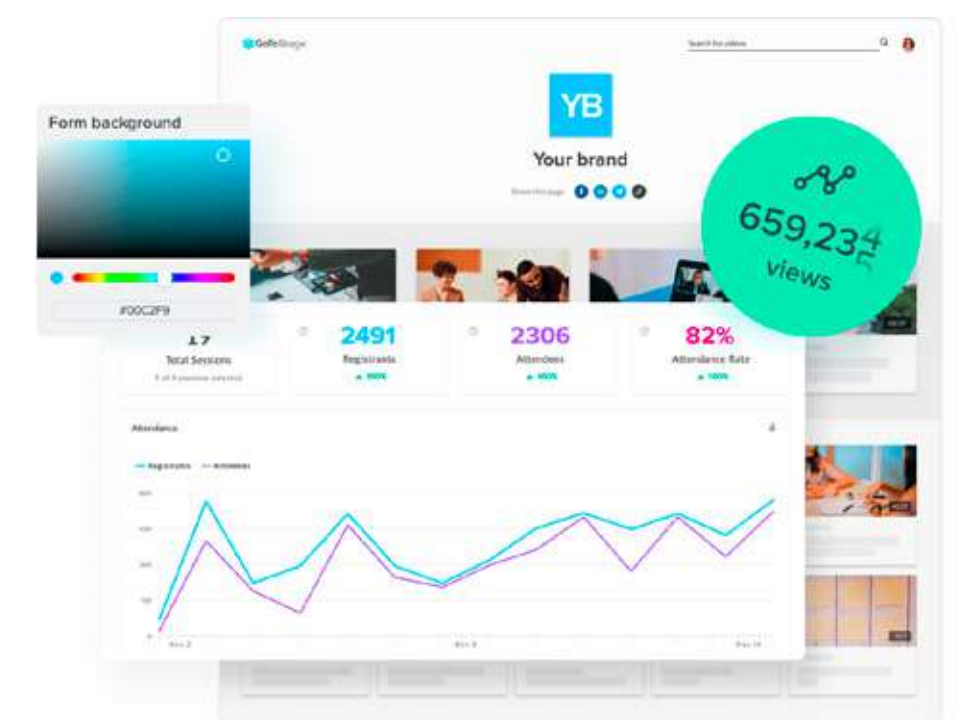
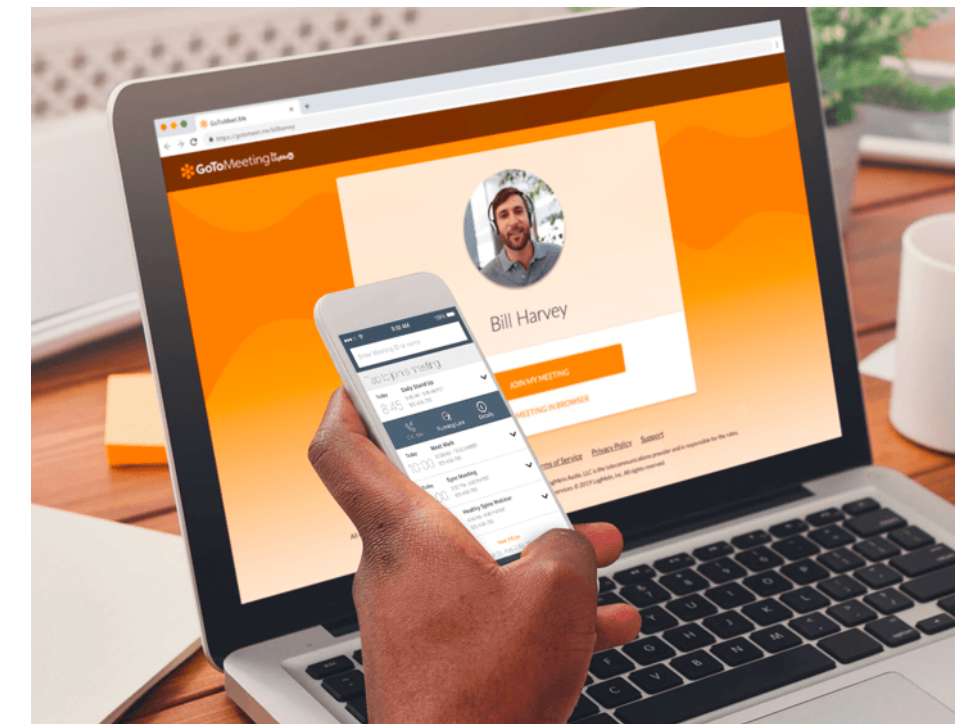
Reuniones online simples profesionales

GoToMeeting está diseñado para realizar reuniones más profesionales y demostraciones de ventas confiables, todo lo que un cliente potencial o cliente necesita para unirse a su reunión es un navegador web, sin necesidad de descargas. Puede organizar una gran videoconferencia o una conferencia rápida con un proveedor desde cualquier lugar.

- o Integración con Outlook
- o Grabación de las reuniones
- o Delege la presentación a otros asistentes
- o Genere un informe de asistencia
- o Múltiples plataformas, como Windows, iOS, Android

GoToWebinar hace que puedas capacitar a prospectos, empleados, socios y clientes de una forma fácil y eficiente que cualquier otro seminario web. Es muy fácil crear eventos interactivos donde todos pueden participar y que parezca que estas en persona.

- o Podrá crear una invitación y enviarla por correo electrónico con el enlace, desde la plataforma.
- o Página de registro de invitados.
- o Utilice levantamiento de manos, encuestas, preguntas.
- o Video compartido para atraer y monitorear a la audiencia Conexión desde múltiples plataformas, como Windows, iOS, Android
- o Mostrar el logotipo de la empresa.
- o Seminarios web en vivo simulados: Crear eventos pregrabados que tienen todo el impacto de un webinar en vivo





¿Por qué Senhasegura ?

Gartner Challenger Top 10 en PAM

Gartner nos ha reconocido como un Challenger, entre las 10 mejores tecnologías PAM globales, en su informe Cuadrante mágico 2021 para la gestión de acceso privilegiado.

Garantizar la seguridad digital de su empresa no tiene por qué ser una preocupación cuando aplica la solución adecuada.

Nuestros productos sirven para asegurar el buen funcionamiento del sistema crítico de su empresa. Descubra qué solución se adapta mejor a cada necesidad y cómo funciona en la práctica.

Senhasegura es una solución PAM que ayuda a centralizar el acceso privilegiado de equipos internos y de terceros. La arquitectura del sistema todo en uno ofrece alta disponibilidad en nuestra infraestructura multisitio.



¿Qué puede hacer con Senhasegura?



Plataforma de pila completa plug-and-play con configuración más rápida y mantenimiento simple.

Con cada componente del producto conectado, su organización obtendrá un retorno de la inversión más rápido sin costos de infraestructura adicionales. En solo 7 minutos *, podemos configurar y entregar una arquitectura de hardware y software de alta disponibilidad.



Sin costos ocultos por licencias adicionales, como sistemas operativos o licencias de bases de datos

Esto permite a la organización planificar un volumen de inversión más preciso mientras implementa la solución PAM en su entorno crítico.



Complementos de integración completamente abiertos

Senhasegura tiene características de integración reconocidas por Gartner a partir de conectores abiertos, lo que permite una nueva integración en menos de 4 horas.



Diseñado para PAM

Diseñado exclusivamente para PAM, creamos PAM Crypto Appliance de senhasegura, hardware que ofrece funciones de seguridad avanzadas para agregar aún más protección y rendimiento a su implementación. Al utilizar nuestros dispositivos criptográficos PAM, se puede simplificar el proceso de implementación y permitir el cumplimiento de los requisitos de seguridad física.

El dispositivo criptográfico PAM de senhasegura fue diseñado para escenarios de configuración activo-activo y activo-pasivo, independientemente del número de miembros del clúster. Esto permite que los miembros se agreguen al clúster de forma continua y rápida, lo que se traduce en una mejor escalabilidad.



Funciones de Cloud Identity and Governance Administration (IGA) y capacidades de descubrimiento de DevOps

Senhasegura le permite incluir Cloud Identity and Governance directamente en la solución PAM, lo que simplifica y reduce los costos para los clientes que no tienen una solución de Cloud Identity and Governance Administration. Además, las características de MT4: senhasegura incluyen escanear y descubrir secretos de DevOps a través de integraciones con herramientas CI / CD, lo que mejora la visibilidad de los riesgos y la toma de decisiones para la implementación de DevSecOps.



Interfaz de usuario intuitiva

La capacitación en implementación y soporte se vuelve más rápida y sencilla, de modo que los usuarios pueden utilizar todas las funciones de la solución, desde la más simple hasta la más compleja, sin problemas.

appgate

¿Por qué Appgate?

Acceso Remoto Seguro

Cambiar la estrategia hacia “acceso seguro” en lugar de “acceso remoto” Un motor de políticas unificado reduce la complejidad de las organizaciones híbridas actuales. Permite que un usuario tenga la misma experiencia sin importar si está en la oficina o trabajando de forma remota. Ese motor también puede eliminar la confianza implícita para todos los dispositivos, incluidos los dispositivos IoT.

ZTNA ya no es solo para acceso remoto. La solución ZTNA correcta brinda acceso seguro en múltiples casos de uso, lo cual es particularmente valioso para las organizaciones híbridas que tienen empleados locales y remotos. Puede reemplazar VPN y NAC debido a su versatilidad. La adopción de ZTNA está aumentando, al ofrecer una automatización robusta y diversas opciones de implementación, la arquitectura Zero Trust de Appgate SDP fortalece su postura de seguridad al tiempo que alivia la carga de los equipos de TI ocupados.



¿Por qué Appgate?

Acceso Remoto Seguro

Con el enfoque hacia el cliente externo **Appgate** tiene una solución para aumentar las medidas de autenticación débiles, como la contraseña, las organizaciones sin querer han creado fricciones para sus clientes. La autenticación basada en riesgos ofrece un enfoque inteligente y basado en datos para autenticar a los usuarios sin fricción.

Para poder monitorear las transacciones y el fraude en línea que está en constante evolución para eludir las estrategias establecidas para detectarlo. Si bien las reglas son efectivas para encontrar esquemas de fraude conocidos, el análisis de comportamiento y el aprendizaje automático brindan una mayor visibilidad para detectar actividades sospechosas y prevenir el fraude en tiempo real.

Todo lo que puede hacer con Appgate

Appgate SDP es un nuevo enfoque de la seguridad.

Protege la red con un perímetro definido por software, un modelo de seguridad de red que crea dinámicamente conexiones de red uno a uno entre el usuario y los recursos a los que accede.

- Diseñado en torno a la identidad del usuario y del dispositivo, no a la dirección IP.
- Hace cumplir el “modelo de confianza cero” aplicando el principio del mínimo privilegio a la red.
- Ofrece una experiencia fluida con acceso simultáneo.

RBA – Risk-Based Authentication: La autenticación basada en riesgos brinda protección a nivel de usuario al adaptarse a comportamientos conocidos y usar el contexto para autenticar usuarios y aprobar transacciones.

- Califique el riesgo de cualquier transacción dada, en cualquier canal, en tiempo real y en comparación con el comportamiento normal del usuario.
- Cree reglas personalizadas para impulsar la acción en función de su tolerancia al riesgo.
- Implemente los métodos de autenticación que mejor funcionen para su organización.



EL PARTNER QUE NECESITAS