CPNnet Security

CATÁLOGO DE SOLUCIONES

DISTRIBUIDOR DE SOLUCIONES DE CIBERSEGURIDAD

CPNnet Security

CPNnet tiene más de 13 años de experiencia en la representación de soluciones TI, en nuestro ADN esta el compromiso constante de generar valor para nuestros canales para el desarrollo de negocios.

Somos un grupo de profesionales dedicados 100% a la gestión de nuestros canales, dispuestos para entregar conocimientos específicos en todas nuestras marcas representadas y marketing estratégico.

- **+ 1K Clientes Finales**
- **+ 200 Canales Activos**
- **+ 500 Vendedores Certificados (últimos 3 años)**
- **+ 450 Ingenieros Certificados (últimos 3 años)**
- **+ 1M de Licencias Vendidas (últimos 3 años)**
- **+ Presencia Latam**

NUESTRO COMPROMISO COMO PARTNER

CAPACITACIONES & SOPORTE

WEBINARS

EVENTOS

ÁREAS DE PROTECCIÓN DE LA INFORMACIÓN

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.

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.

03

SEGURIDAD DE REDES

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

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

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.

06

AUDITORÍAS INFORMÁTICAS

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

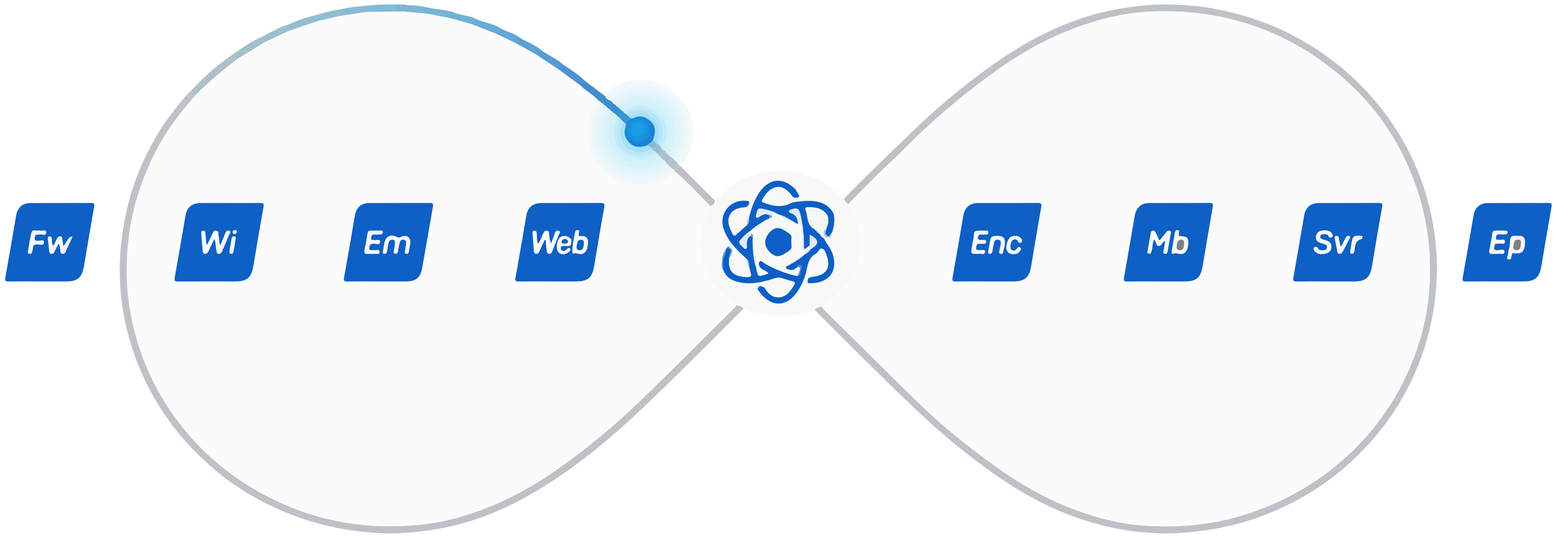
SOPHOS

DEFEAT CYBERATTACKS

¿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 ciberamenzas 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.



SOPHOS - PRODUCTOS

Una gama de soluciones eficientes y sincronizadas en un ecosistema perfecto.

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 MDR Managed Detection and Response

VERACODE

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

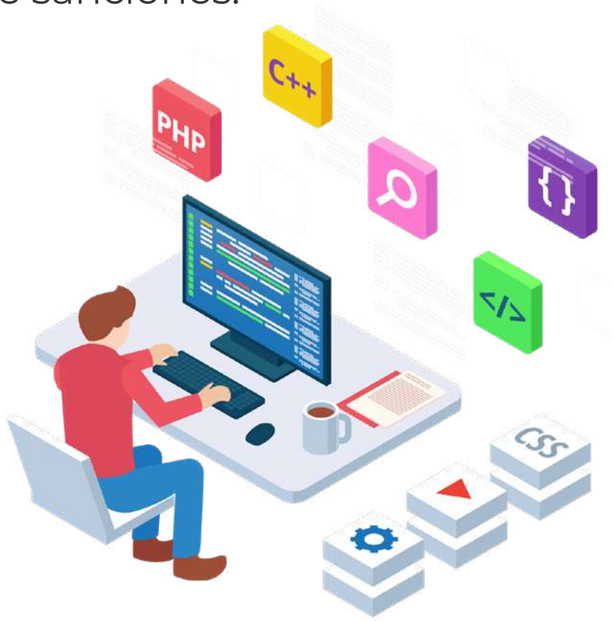
Gartner®

VERACODE - LICENCIAS

Análisis Estático - Permite a los equipos de seguridad a nivel empresarial realizar pruebas para análisis de la seguridad de la aplicación de forma estática, cultive una cultura de codificación segura con las herramientas y los conocimientos para escribir código seguro desde el principio con apoyo a los desarrolladores, administre y mida la seguridad en todas las aplicaciones para priorizar el esfuerzo y acelerar el cumplimiento. Encuentre fallas rápidamente y corríjalas más rápido con escaneos en tiempo real, orientación contextual y soporte 1 a 1.

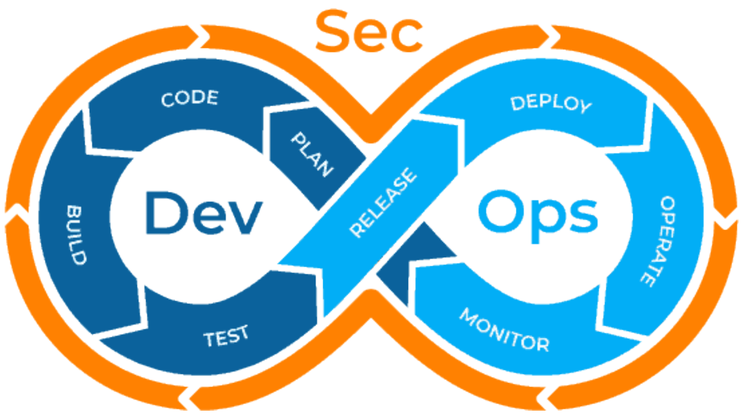
Análisis SCA - Manténgase al día con las bibliotecas de código abierto en constante evolución al automatizar la búsqueda y corrección de vulnerabilidades dentro de las bibliotecas. Automatice la búsqueda y reparación de vulnerabilidades de código abierto que afectan el cumplimiento normativo. Detecte el riesgo de la licencia, gestione el uso y evite sanciones.

Análisis Dinámico - Encuentre vulnerabilidades de tiempo de ejecución, escanee cientos de aplicaciones web y API simultáneamente. Las soluciones puntuales y las soluciones de servicios administrados simplemente no pueden mantenerse al día con la escala y el ritmo de los ciclos de desarrollo modernos.



VERACODE - ¿QUÉ PUEDE HACER CON VERACODE?

- Interfaz única para definir una vista de su política de seguridad integral
- Admite políticas comunes como OWASP Top 10 y PCI
- Informes y conocimientos para administradores y desarrolladores de políticas por igual Una plataforma que se mantiene actualizada para usted, incluidas las actualizaciones diarias de nuestra base de datos de vulnerabilidades
- Más de 16 años de datos impulsan una alta precisión y le permiten compararse con sus pares
- Elasticidad para aumentar cuando necesite potencia adicional (¿recuerda log4j?)
- Brinde seguridad a los desarrolladores con más de 40 integraciones en su IDE, CI/CD y más
- Escanee más de 100 lenguajes y marcos de forma rápida y precisa
- Trabaja en el entorno en el que trabajas
- Escaneo de alta precisión: bajas tasas de falsos positivos y falsos negativos
- Clasificación y mitigación: priorice qué fallas necesita corregir
- Coincidencia de fallas: ahorre tiempo al no tener que corregir la misma falla varias veces



safetica

SAFETICA - ¿POR QUÉ SAFETICA?

Safetica le ayuda a descubrir y clasificar datos valiosos utilizando su exclusiva Clasificación Unificada Safetica que combina el análisis del contenido del archivo, el origen del archivo y las propiedades del archivo. Ofrece visibilidad completa y monitoreo continuo, sin perder el ritmo para identificar, clasificar y rastrear datos confidenciales al instante para poder evitar la exposición de datos, con estrategias basadas en el usuario:

- Visibilidad de la actividad del correo, apps (teams, FB,WS), sitios web y dispositivos externos.
- Informes de dispositivos protegidos.
- Alertas en tiempo real.
- OCR para datos sensibles en imágenes.
- IRM para visibilidad del riesgo del usuario.
- Soporte para móvil, para apps one drive, outlook, sharepoint y teams.

SAFETICA - ¿QUÉ PUEDO HACER CON SAFETICA?

- Reconocer actividades de usuario no deseadas
  con auditoría de actividad laboral y categorías automatizadas para aplicaciones utilizadas y sitios web visitados por usuarios específicos.

- Realice un seguimiento de los cambios en el comportamiento de los usuarios
  Con una descripción detallada del comportamien-to de los usuarios en suorganización a lo largo del tiempo.

- Empoderar a los usuarios para trabajar con datos confidenciales
  Muestre notificaciones educativas a los usuarios cuando exista riesgo de infracción de la política para informarles o decidir. Aplique procesos específicos para proteger los datos más valiosos.

- Obtenga información más detallada sobre la comunicación
  Por correo electrónico con registros de todos los correos electrónicos entrantes y salientes con respecto a la privacidad del usuario

- Detectar amenazas potenciales y analizar riesgos internos
  Responda a las amenazas incluso antes de que ocurra un incidente importante gracias al descubrimiento temprano de anomalías de comportamiento y riesgos de flujo de datos en su organización

- Detectar y mitigar violaciones de cumplimiento normativo
  Obtenga información sobre los incidentes de seguridad de los datos y las violaciones del cumplimiento normativo para poder responder y mitigar sus impactos.

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.

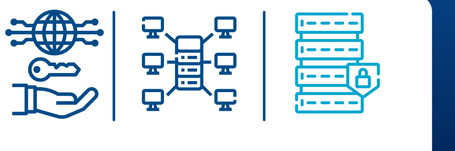
ZTNA ya no es solo para acceso remoto. La solución **ZTNA** correcta brinda acceso seguro en múltiples casos de uso, lo cual es particularmente valioso para las organizaciones híbridas que tienen empleados locales y remotos. Puede reemplazar VPN y NAC debido a su versatilidad. La adopción de **ZTNA** 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.

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.

SONICWALL®



Gestión de Seguridad

SonicWall le ayuda a crear, escalar y gestionar la seguridad en entornos de nube, híbridos y tradicionales. Desarrolla la adopción segura de la nube a tu ritmo.

Combine y combine productos de seguridad para crear o mejorar modelos de implementación híbridos y nativos de la nube que se ajusten a sus necesidades actuales y sirvan de puente hacia una realidad más virtualizada.

Aproveche las capacidades modernas de confianza cero para conectar fácil y rápidamente a usuarios remotos con recursos locales, aplicaciones alojadas en la nube, sucursales y nubes públicas, todo sin instalar hardware.

Proteja a los empleados remotos y a los trabajadores móviles con opciones de seguridad virtualizadas. Implemente seguridad fácilmente en múltiples ubicaciones, con soporte de TI mínimo, utilizando capacidades de implementación sin intervención.

SONICWALL - ¿POR QUÉ SONICWALL?

Al aprovechar las tecnologías de detección y prevención en tiempo real, SonicWall proporciona visibilidad sobre las amenazas -también sobre las encriptadas-, independientemente del tamaño del archivo. Su capacidad para escalar y potenciar la automatización y el aprendizaje automático sin necesitar tantos recursos.

Network Security	Endpoint Security	Edge Security	Managed Security Services
Firewall	Capture Client	Secure Mobile Access	MSP/MSSP
Switches & Access Points	Capture ATP	Security Service Edge (SSE)	MDR & SOCaaS
NSM & WNM (Management)	Capture Security Appliance	Cloud App Security	Capture Security Center
		Email Security	

Flexibilidad de Configuración

Proteja su organización, redes, usuarios y dispositivos según sus condiciones. Explore casos de uso del mundo real que muestran el poder y la flexibilidad de escalar la seguridad comprobada incluso en los entornos híbridos y nativos de la nube más complejos. Con SonicWall sus clientes pueden:

- Detener los ciberataques dirigidos
- Acceso remoto a la fuerza laboral
- Adopción segura de la nube
- Seguridad de red distribuida
- Seguridad de confianza cero
- Redes definidas por software

segura

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.

SEGURA - ¿QUÉ PUEDO HACER CON SEGURA?

- **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.

SEGURA - ¿QUÉ PUEDO HACER CON SEGURA?

- **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 vuelvemás 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.

- **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

algosec

ALGOSEC - ¿POR QUÉ ALGOSEC?

Infraestructura Hibrida

Los clientes hoy en día tienen Infraestructura de TI de forma hibrida con complejos entornos, lo que hace que la administración también tenga que ser gestionada por personas internas y externas a la organización cuando hay desborde, normalmente se necesitan sistemas cloud, servidores, FW, sistemas SaaS, y un sinfín de necesidades de configuración, mantenimiento, monitoreo, creación de reglas, y todo con base en cumplimiento.

ALGOSEC es una herramienta indispensable para gestionar y fortalecer la seguridad de redes complejas, optimizando recursos y garantizando cumplimiento normativo, simplificando y automatizando la gestión de tus políticas de seguridad, generando una visibilidad total de tu red y evidenciar los cambios sin riesgos. Todo esto mientras optimizas recursos y alineas la seguridad con las metas de tu negocio. ¡Con Algosec, la seguridad es eficiente y estratégica!

ALGOSEC - ¿QUÉ PUEDO HACER CON ALGOSEC?

- **Gestión eficiente de políticas de seguridad**
  Te permite administrar de forma centralizada y automatizada las políticas de seguridad en toda tu red, desde firewalls hasta entornos híbridos o en la nube. Esto reduce el riesgo de errores humanos y asegura que las reglas de seguridad estén actualizadas y alineadas con las necesidades del negocio.

- **Visibilidad completa de la red**
  Proporciona una visión integral de la red y el tráfico, permitiendo identificar riesgos, vulnerabilidades y configuraciones incorrectas que puedan comprometer la seguridad. Esto incluye la identificación de rutas inseguras o configuraciones mal optimizadas.

- **Automatización del cambio de reglas**
  Asegurando que sean evaluados y aplicados de manera consistente, evitando interrupciones y errores en el servicio

- **Reducción de tiempos de auditoría y cumplimiento**
  Las auditorías de cumplimiento son más rápidas y precisas. La herramienta facilita la generación de informes detallados para cumplir con normativas como PCI DSS, HIPAA, y SOX, ahorrando tiempo y recursos en el proceso.

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

NETWRIX -¿QUÉ PUEDO HACER CON NETWRIX?

Identifique
Comprenda qué datos necesitan protección y como de expuestos están.

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

Proteja
Minimice el riesgo de posibles incidentes de ciberseguridad.

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

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

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.


GoTo

GOTO - ¿POR QUÉ GOTO?

Tecnologías más fáciles, a su servicio, atienda, gestione y conecte a sus clientes y equipos en todos los dispositivos de la forma como más convenga para su empresa, con funciones esenciales para la asistencia de TI como el acceso remoto y los tickets conversacionales, GoTo facilita las cosas a los empleados, estén donde estén.

Estamos asistiendo a una evolución de la fuerza laboral moderna y a la revolución del lugar de trabajo. GoTo está al frente, preparado para ayudar a todos a afrontar las dificultades:

- Facilitando unas políticas laborales flexibles, híbridas y remotas
- Proporcionando soporte y asistencia bajo demanda y sin dificultades
- Ofreciendo potentes herramientas de colaboración y productos de ciberseguridad

GOTO - LICENCIAS

Rescue - Las herramientas adecuadas permiten a las empresas ofrecer asistencia remota a cualquier Mac, PC o dispositivo móvil.

Central - Implante la TI remota sin poner en riesgo a su empresa con acceso, supervisión y gestión remotos.

GoTo Resolve - Supervisión y gestión y asistencia remotas, por fin juntas. Sencillo. Seguro. Asequible. es la única solución integral de asistencia y administración de TI con asistencia y acceso nativos remotos, supervisión y gestión remotas, y gestión de tickets integrados.

GOTO - ¿QUÉ PUEDO HACER CON GOTO”

- Simplifique la experiencia del servicio de soporte con procesos que permiten a los agentes y a los usuarios finales dar y recibir asistencia sin complicaciones.

- Ahora que se trabaja desde cualquier parte, es esencial que todos, y especialmente el departamento de TI, cuenten con un acceso sencillo y seguro a archivos, programas, equipos y redes.

- Disfrute de resoluciones rápidas y sin problemas con cualquier dispositivo. La solución de problemas remota y avanzada le permite ayudar de forma sencilla a sus clientes

- Mantenga conectado a todo el mundo y proteja cada dispositivo sin renunciar a nada. Proteja a su plantilla remota con una TI proactiva.

- Guíe a los clientes hacia unos mejores resultados con una tecnología cobrowsing segura e independiente, o resuelva los problemas con videoasistencia basada en el navegador.

STELLAR CYBER®

OPEN XDR DE STELLAR CYBER

Stellar Cyber es una plataforma de detección y respuesta extendida con Open XDR, que te proporciona una visibilidad completa de toda tu red incluyendo IT y OT , permitiéndote detectar y responder a amenazas en tiempo real. Con su enfoque centrado en la automatización y la inteligencia artificial, la solución reduce drásticamente el tiempo de detección y respuesta, optimizando los recursos del equipo de seguridad y minimizando riesgos.

La completamente integrada plataforma de Stellar Cyber ofrece:

STELLAR CYBER - ¿QUÉ PUEDO HACER CON STELLAR CYBER?

- **Plataforma XDR (Extended Detection and Response)**
  Correlaciona datos de múltiples fuentes de seguridad (red, endpoint, aplicaciones, nube, etc.).
  Proporciona un análisis unificado para detectar y responder a amenazas avanzadas.
- **NDR (Network Detection and Response)**
  Monitoreo de tráfico de red para identificar actividades sospechosas o anómalas.
  Detección de amenazas basadas en comportamiento en el tráfico de la red.
- **SOAR (Security Orchestration, Automation, and Response)**
  Orquestación y automatización de flujos de trabajo de seguridad.
  Respuestas automáticas o semiautomáticas a incidentes y amenazas.
- **UEBA (User and Entity Behavior Analytics)**
  Detección de comportamientos anómalos de usuarios y entidades dentro de la red.
  Uso de inteligencia artificial para identificar comportamientos fuera de lo normal.

aikido

AIKIDO - ¿POR QUÉ AIKIDO?

En un entorno donde la velocidad del desarrollo puede convertirse en la puerta de entrada a vulnerabilidades críticas, asegurar el código desde su creación es una necesidad estratégica.

Con AIKIDO, la seguridad se integra de forma continua en todo el ciclo Dev SecOps, analizando el código fuente mediante SAST, revisando módulos y dependencias de terceros para evitar riesgos heredados, y garantizando la calidad y consistencia del código antes de su despliegue. Su capacidad de autorremediación inteligente permite corregir vulnerabilidades automáticamente, reduciendo el tiempo de exposición y esfuerzo del equipo técnico. Además, AIKIDO amplía la protección hacia los entornos de contenedores y pipelines CI/CD, asegurando que cada etapa —desde el desarrollo hasta la producción— mantenga altos estándares de seguridad. Así, las organizaciones logran aplicaciones más seguras, eficientes y resilientes, sin comprometer la agilidad que exige la innovación moderna.

AIKIDO es una solución de ciberseguridad diseñada especialmente para equipos de desarrollo y MSPs que buscan ofrecer protección integral y automatizada frente a amenazas digitales sin complicar su operación. Al incorporar AIKIDO en su ciclo de desarrollo, obtienen una solución de rápida implementación, bajo costo operativo y gran valor agregado desde los desarrolladores, con un modelo SaaS flexible y escalable, detecta y remedia vulnerabilidades antes de que se conviertan en incidentes, ofrece una plataforma centrada en seguridad desde el código hasta la nube.

AIKIDO -¿QUÉ PUEDO HACER CON AIKIDO?

- **Escanear vulnerabilidades en código, dependencias y contenedores**
  Detecta amenazas en el código fuente, bibliotecas y contenedores antes del despliegue.

- **Identificar configuraciones inseguras en la nube y CI/CD**
  Supervisa la postura de seguridad en pipelines y entornos cloud.

- **Centralizar la gestión de riesgos en un solo panel**
  Consolida alertas y métricas en un dashboard fácil de usar para priorizar remediaciones.

- **Revisión de la Calidad del código**
  Revisar malas prácticas que puedan afectar el rendimiento y la mantenibilidad del software.

- **Automatizar la corrección de vulnerabilidades**
  Sugiere parches y acciones correctivas inteligentes para mantener la seguridad al día.

- **Cumplir con normativas y buenas prácticas de seguridad**
  Facilita la alineación con estándares como ISO 27001, SOC 2 y OWASP Top 10.

FARONICS™

FARONICS - ¿POR QUÉ FARONICS?

Faronics te ofrece con su licencia Deep Freeze una forma de volver los endpoints a su configuración inicial, garantizando máxima seguridad y eficiencia operativa. Con su tecnología patentada, puedes restaurar automáticamente los sistemas al reiniciarlos, eliminando malware y configuraciones no deseadas. Además, facilita la gestión centralizada de actualizaciones y políticas de seguridad, reduciendo la carga sobre el equipo de TI. Esto se traduce en menos tiempo de inactividad, mejor rendimiento de los dispositivos y mayor protección frente a amenazas, todo mientras mantienes tus sistemas operativos estables y seguros. ¡Con Faronics, controlas y proteges tus activos digitales sin esfuerzo!

FARONICS - ¿QUÉ PUEDO HACER CON FARONICS?

- **Gestión eficiente de políticas de seguridad**
  Revierta los cambios de configuración
  Revierta los cambios de configuración con un simple reinicio al tiempo que permite a los usuarios guardar su trabajo.
- **Protección contra estafas de phishing**
  Revierta los cambios maliciosos al reiniciar y proteja los equipos de estafas de phishing.
- **Cumplimiento de licencias**
  Solo se conserva el software autorizado y se elimina el software no autorizado con el fin de garantizar el cumplimiento de las licencias.
- **Funciones de gestión**
  Realice acciones como Reiniciar, Apagar o Reactivar a petición o de forma programada. También puede bloquear el teclado y ratón de forma remota con el fin de evitar cambios no autorizados.
- **Elimine la protección restrictiva**
  Proporcione a los usuarios acceso sin restricciones y evite el bloqueo restrictivo de los equipos para mantener la seguridad.

IRONCHIP

IRONCHIP - ¿POR QUÉ IRONCHIP?

Nuestra plataforma de gestión centralizada cuenta con todas las herramientas e integraciones necesarias para garantizar la gestión de usuarios y la protección del acceso a tus servicios más críticos. gestión de privilegios basada en roles - Establece diferentes privilegios de usuario para prevenir el acceso no autorizado al resto del sistema y el mal uso de la información, mitigando la presencia de usuarios maliciosos. Restringe el acceso desde lugares no autorizados. Supervisión de accesos en tiempo real. Verifica la actividad de los usuarios, visualiza el acceso en una línea de tiempo, obtén informes y descárgalos para un control completo.

IRONCHIP - ¿QUÉ PUEDES HACER CON IRONCHIP?

- **Autenticación basada en ubicación**
  Verificación de identidad mediante la ubicación única del usuario, utilizando su entorno geográfico como una capa adicional de seguridad.
  Elimina la necesidad de contraseñas tradicionales, mejorando la seguridad con un enfoque geocéntrico.

- **Control de acceso granulado**
  Define reglas estrictas sobre quién, cuándo y desde dónde puede acceder a sistemas y datos sensibles, permitiendo una gestión más granular de permisos de acceso.

- **Integración con sistemas de autenticación multifactor (MFA)**
  Añade una capa de autenticación adicional basada en la ubicación geográfica junto a otros métodos de MFA como biometría o tokens.

HACKNOID

HACKNOID - ¿POR QUÉ HACKNOID?

En un entorno donde los ciberataques evolucionan a diario, comprender la verdadera madurez de la ciberseguridad corporativa es esencial para proteger los activos críticos. Hacknoid permite a las organizaciones auditar y monitorear de forma continua su postura de seguridad, identificando vulnerabilidades, brechas y configuraciones débiles antes de que sean explotadas. A través de sus capacidades de Cyber Risk Scoring y Continuous Security Validation, la plataforma proporciona una visión clara y cuantificable del nivel de exposición, facilitando decisiones estratégicas basadas en evidencia. Hacknoid convierte los datos de seguridad en conocimiento útil, ayudando a optimizar inversiones, priorizar acciones y cumplir con normativas internacionales. Con esta herramienta, las empresas logran elevar su resiliencia digital y mantener la confianza de sus clientes y aliados.

Hacknoid no solo identifica las brechas, sino que permite medir el impacto real del riesgo y optimizar la defensa. Gracias a su motor de análisis automatizado, los equipos de seguridad pueden comprender dónde concentrar sus esfuerzos, qué controles son realmente efectivos y qué áreas necesitan reforzarse. Su enfoque proactivo ayuda a reducir la superficie de ataque, mejorar la respuesta ante incidentes y fortalecer la postura general de ciberseguridad. En pocas palabras, Hacknoid ofrece la claridad necesaria para transformar la gestión del riesgo en una estrategia continua de mejora y protección.

HACKNOID - ¿QUÉ PUEDO HACER CON HACKNOID?

- **Auditar continuamente la postura de seguridad**
  Evalúa vulnerabilidades, configuraciones y cumplimiento de forma automatizada en toda la red.

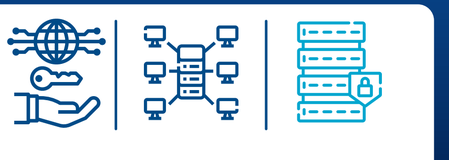
- **Cuantificar el riesgo cibernético**
  Asigna puntajes de riesgo claros que facilitan priorizar acciones y justificar inversiones.

- **Validar controles y políticas de seguridad**
  Verifica si las medidas implementadas realmente protegen frente a amenazas reales.

- **Detectar brechas y reducir la superficie de ataque**
  Identifica puntos débiles antes de que puedan ser explotados.

- **Mejorar la madurez y resiliencia cibernética**
  Permite evolucionar de la reacción a la prevención, fortaleciendo la confianza digital.

cymulate



CYMULATE - ¿POR QUÉ CYMULATE?

Con Cymulate puedes realizar una auditoría continua del valor real de tus inversiones en ciberseguridad, en un entorno donde las amenazas evolucionan más rápido que las estrategias defensivas, auditar las inversiones en ciberseguridad se ha convertido en una prioridad crítica. Muchas organizaciones invierten en herramientas costosas sin saber si realmente están cumpliendo su propósito. Cymulate permite validar de manera continua la efectividad real de las defensas existentes, simulando ataques en todos los vectores posibles —desde correo y red hasta endpoint y nube— para medir la resiliencia y capacidad de respuesta.

Gracias a su enfoque de Breach and Attack Simulation (BAS), Cymulate traduce resultados técnicos en métricas comprensibles para la dirección, facilitando la optimización del presupuesto, la priorización de mejoras y la reducción del riesgo operativo. Con Cymulate, las empresas pueden demostrar con evidencia el retorno de sus inversiones en seguridad, alineando cada acción con la protección efectiva del negocio.

CYMULATE - ¿QUÉ PUEDO HACER CON CYMULATE?

- **Simular ataques reales en todos los vectores**
  Prueba la efectividad de tus defensas frente a amenazas reales sin afectar la operación.
- **Identificar brechas de seguridad y configuraciones débiles**
  Detecta puntos vulnerables en email, red, endpoints, aplicaciones y nube.

- **Validar controles y políticas de seguridad**
  Verifica si las medidas implementadas realmente protegen frente a amenazas reales.

- **Detectar brechas y reducir la superficie de ataque**
  Identifica puntos débiles antes de que puedan ser explotados.

- **Mejorar la madurez y resiliencia cibernética**
  Permite evolucionar de la reacción a la prevención, fortaleciendo la confianza digital.

TERAMIND

TERAMIND - ¿POR QUÉ TERAMIND?

En un contexto donde la movilidad, el trabajo remoto y la nube amplían la superficie de ataque, las organizaciones necesitan una solución capaz de ofrecer visibilidad total y control centralizado sobre sus dispositivos, usuarios y aplicaciones. Teramine permite monitorear, detectar y responder de forma proactiva ante comportamientos anómalos, previniendo brechas antes de que comprometan la operación. Su enfoque integral combina seguridad, productividad y cumplimiento normativo, ayudando a las empresas a mantener su entorno digital bajo control. Con Teramine, los equipos de TI pueden gesti nar riesgos, controlar accesos, proteger datos sensibles y optimizar recursos tecnológicos, todo desde una plataforma unificada, fácil de administrar y adaptable a cualquier entorno corporativo.

Teramine va más allá de la simple supervisión: ofrece una visión inteligente de la actividad del usuario, las aplicaciones y los datos corporativos. Gracias a sus capacidades de análisis en tiempo real y su motor de detección conductual, la plataforma permite anticipar amenazas internas, controlar el uso de recursos y garantizar la productividad sin sacrificar seguridad. Con Teramine, las organizaciones pueden proteger la información crítica, detectar comportamientos sospechosos y cumplir con políticas de ciberseguridad y privacidad de forma continua y automatizada.

TERAMIND - ¿QUÉ PUEDO HACER CON TERAMIND?

- **Monitorear la actividad del usuario y el uso de aplicaciones**
  Ofrece visibilidad total sobre las acciones que impactan la seguridad o productividad.

- **Proteger datos sensibles y prevenir fugas de información (DLP)**
  Detecta y bloquea la transferencia no autorizada de datos corporativos.

- **Controlar el cumplimiento de políticas de seguridad**
  Asegura que cada dispositivo y usuario opere bajo los estándares definidos por la empresa.

- **Optimizar la productividad y recursos tecnológicos**
  Identifica cuellos de botella, software ineficiente y patrones de uso para mejorar rendimiento.

- **Detectar comportamientos anómalos y prevenir amenazas internas**
  Usa análisis conductual para anticipar riesgos y proteger la operación.

LastPass •••|

LASTPASS - ¿POR QUÉ LASTPASS?

Mejore y proteja el acceso a su negocio, para todos sus usuarios, sin importar dónde se encuentren, ayude a que el departamento de TI trabaje de manera productiva. La consola de administración de LastPass proporciona una vigilancia completa al equipo de TI. Podrá gestionar todas las tareas diarias desde la consola de administración, como, por ejemplo: supervisar la gestión de contraseñas de los empleados, actualizar políticas de seguridad, crear y eliminar usuarios, instalar métodos de autenticación cuando se incorpora o se da de baja a un empleado, la autenticación multifactor (MFA) es una segunda forma de autenticación que verifica la identidad de un usuario antes de concederles acceso y además realizar informes de seguridad para los administradores y las auditorias.

El mejor cifrado de su clase

Su contraseña maestra y las contraseñas almacenadas se mantienen en secreto, incluso para LastPass. Su bóveda está cifrada y descifrada solo a nivel de dispositivo.

Certificaciones globales

LastPass cuenta con certificaciones de terceros, incluidas ISO 27001, SOC2 Tipo II, SOC3, BSI C5, TRUSTe y más, para igualar el cumplimiento de su empresa.

Protégete contra la dark web

Las violaciones de seguridad ocurren todo el tiempo. LastPass protege sus datos privados y le notifica cuando se ven comprometidos.

LASTPASS - ¿QUÉ PUEDO HACER CON LASTPASS?

Facilite a los usuarios acceder y compartir de forma segura aplicaciones no protegidas por SSO e información confidencial.
Escale la adopción con automatización y supervise proactivamente el estado de las contraseñas en toda la empresa.

- **Reduzca aún más el uso de contraseñas con opciones de inicio de sesión sin contraseña.**
- **Elimine la reutilización de contraseñas con el generador de contraseñas integrado.**
- **Autocompletar contraseñas e información con un solo clic, en cualquier dispositivo.**
- **Evalúe su comportamiento de seguridad y controle las violaciones de datos.**
- **Minimice la necesidad de escribir contraseñas para disfrutar de una experiencia sin contraseñas.**

vicarius

VICARIUS - ¿POR QUÉ VICARIUS?

En la carrera contra las ciberamenazas, el tiempo entre la detección y la corrección de vulnerabilidades marca la diferencia entre la seguridad y la exposición. Vicarius ofrece una plataforma de gestión de vulnerabilidades y parchado automatizado (vulnerability remediation) diseñada para prevenir ataques antes de que ocurran, reduciendo drásticamente el riesgo operativo.

A diferencia de soluciones centradas en auditoría como Hacknoid, Vicarius actúa directamente sobre las vulnerabilidades detectadas, aplicando parches o mitigaciones incluso cuando los proveedores aún no los han publicado. Su motor de inteligencia prioriza amenazas según criticidad y contexto, permitiendo a los equipos de TI remediar más rápido, sin depender de procesos manuales o tiempos prolongados de parcheo.

Con Vicarius, las organizaciones no solo identifican los riesgos, sino que los neutralizan de manera inmediata, fortaleciendo su resiliencia y manteniendo una operación continua y segura.

VICARIUS - ¿QUÉ PUEDO HACER CON VICARIUS?

Con Vicarius, las empresas obtienen una plataforma todo en uno para identificar, priorizar y remediar vulnerabilidades en sistemas, aplicaciones y endpoints. Su enfoque unificado combina análisis inteligente de amenazas, priorización basada en riesgo y ejecución automatizada de parches. Además, Vicarius ofrece visibilidad completa del entorno, alertando sobre software obsoleto, configuraciones inseguras y activos desactualizados, para mantener la infraestructura siempre protegida y alineada con las mejores prácticas de ciberseguridad.

- **Automatizar la gestión de parches y vulnerabilidades**
  Aplica actualizaciones críticas de manera proactiva, reduciendo tiempos y esfuerzo.
- **Priorizar amenazas según criticidad y contexto**
  Analiza el riesgo real de cada vulnerabilidad para enfocar la corrección donde más importa.
- **Proteger aplicaciones sin parches disponibles**
  Implementa virtual patching para evitar exploits antes de la actualización oficial.
- **Centralizar la visibilidad del estado de seguridad**
  Consolida métricas, alertas y reportes de cumplimiento en un solo panel de control.
- **Reducir la exposición y fortalecer la resiliencia operativa**
  Minimiza el tiempo de vulnerabilidad y asegura la continuidad del negocio con acciones automatizadas.

RIDGE
SECURITY

RIDGE- ¿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 cualquier persona responsable de garantizar la seguridad del software y 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

RIDGE- ¿QUÉ PUEDE HACER CON RIDGE BOT?

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.

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