CPNnet Security

CATÁLOGO DE SOLUCIONES

DISTRIBUIDOR DE SOLUCIONES DE CIBERSEGURIDAD

CPNnet Security

CPNnet tiene más de 12 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

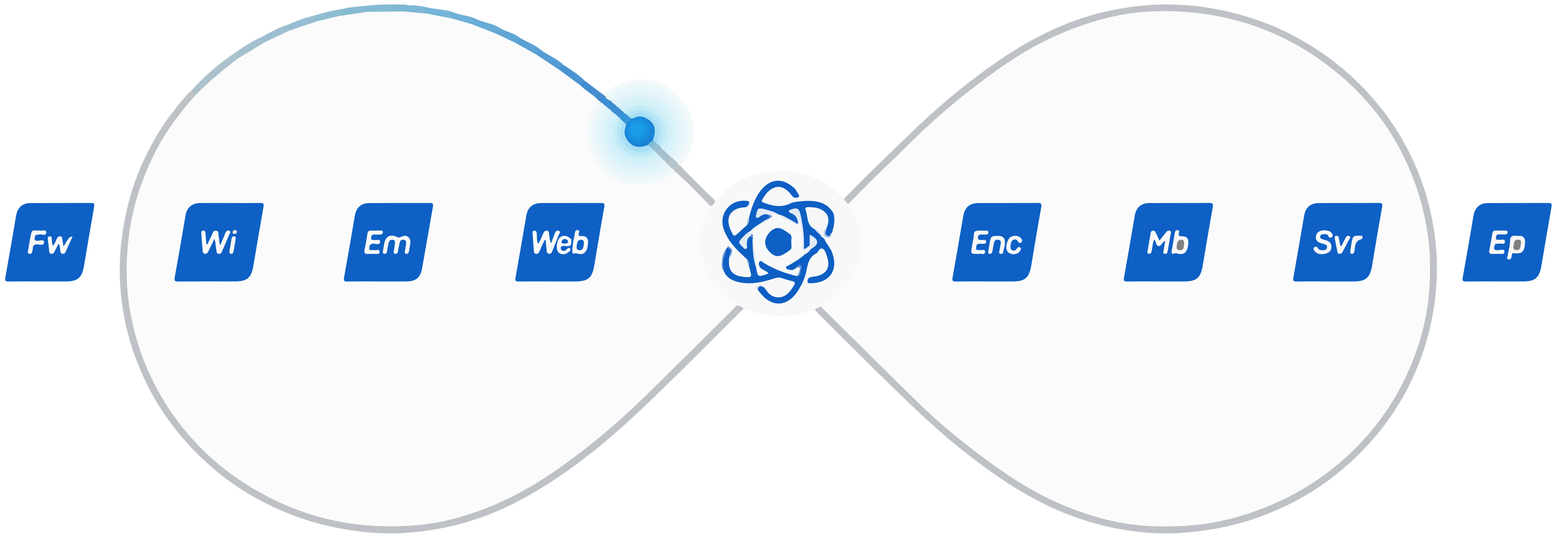
Los beneficios son variados, pueden ayudarlo a mejorar la seguridad, aprobar auditorías de cumplimiento normativo y simplificar las operaciones de TI.

SOPHOS

¿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

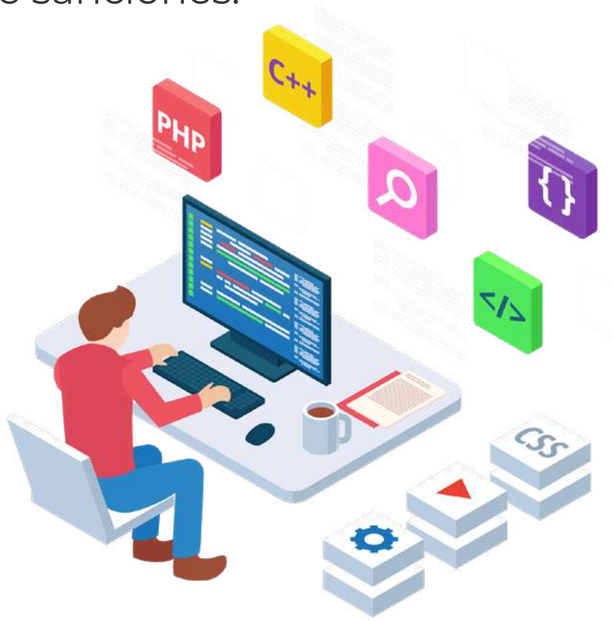
Gartner®

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.

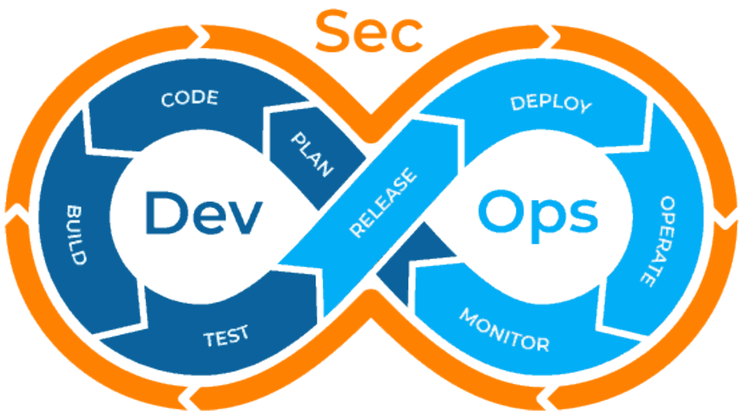
Análisis SCA - Manténgase al día con las bibliotecas de código abierto en constante evolución al automatizar la búsqueda y corrección de vulnerabilidades dentro de las bibliotecas. Automatice la búsqueda y reparación de vulnerabilidades de código abierto que afectan el cumplimiento normativo. Detecte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



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.

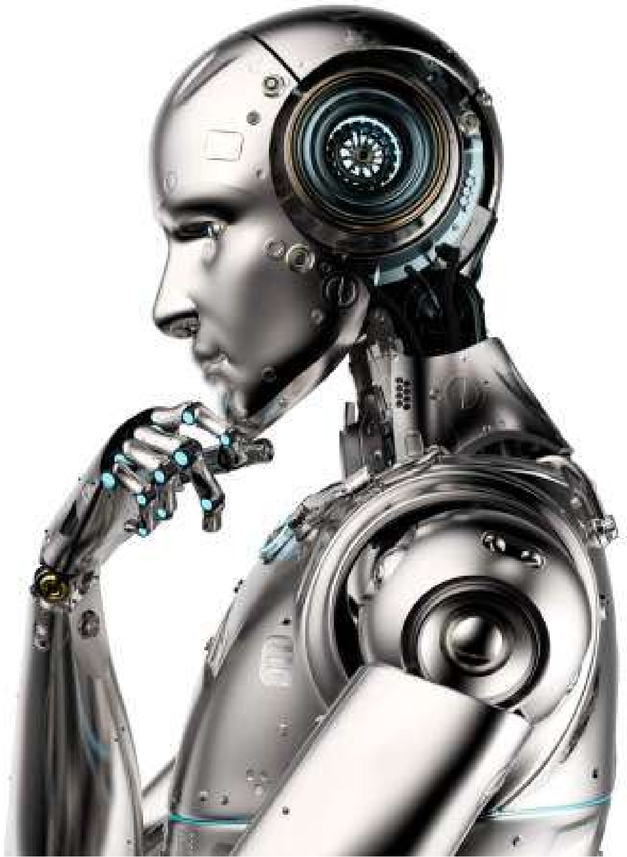
Prueba de Penetración de Sitios Web: Las aplicaciones web y todas las superficies de ataque relacionadas para obtener el control del sitio web objetivo

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



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 webvisitados 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.

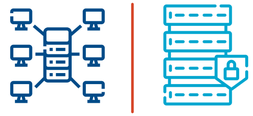
- Empoderar a los usuarios para trabajar con datos confidenciales
  Muestre notificaciones educativas a los usuarios cuando exista riesgo de infracción de la política para informarles o decidir. Aplique procesos específicos para proteger los datos más valiosos.

- 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 incidenteimportante 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

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.

SENHASEGURA - ¿QUÉ PUEDO 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.

SENHASEGURA - ¿QUÉ PUEDO HACER CON SENHASEGURA?

- **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

LastPass •••|

LASTPASS- ¿POR QUÉ LASTPASS?

Contraseñas Seguras

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.

LASTPASS- ¿POR QUÉ LASTPASS?

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.

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.

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?

Proteja su negocio con un mejor comportamiento de contraseñas.

- 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.

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.

ANDINO
NETWORKS

ANDINO NETWORK- ¿POR QUÉ ANDINO NETWORK?

Andino WEb Application Firewall

En el acelerado panorama digital actual, Andino es su solución todo en uno para afrontar los desafíos y aprovechar las oportunidades de la era digital. Al integrar perfectamente las redes de distribución de contenido (CDN) e introducir Andino Web Application Firewall (WAF), Andino garantiza que su negocio se mantenga a la vanguardia.

Imágenes & Firewall

Red de entrega de contenido (CDN)

- Optimización de imagen
- Red perimetral
- Servicios de telemetría
- Roles
- GeoDNS
- Integración SIEM
- Soporte para MSP

Firewall de aplicaciones web (WAF) de próxima generación

- Top 10 de OWASP
- Bloqueo geográfico
- Roles personalizados
- Reglas de robots
- Reglas de propiedad intelectual
- Protección Bruta Fuerte
- Integración SIEM

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.

OUTPOST24 - LICENCIAS

Netsecurity - Los sistemas sin parches y mal configurados son factores clave para los ataques cibernéticos. Sea el primero en identificar su riesgo y sepa qué vulnerabilidad reparar en sus redes, servicios en la nube y espacio aéreo inalámbrico con evaluación continua y puntuación de riesgo inteligente para la priorización de vulnerabilidades.

Escaneo de cumplimiento de PCI - Lograr y mantener el cumplimiento de PCI DSS es un proceso complejo y continuo. Outpost24 automatiza las verificaciones de sus medidas de seguridad, políticas, procedimientos, red y arquitectura de software para ayudarlo a proteger de manera proactiva las tarjetas de crédito de los clientes a través de la identificación continua de riesgos y resultados correctivos.

Pruebas de seguridad de aplicaciones dinámicas - Nuestra solución Dynamic Application Security Testing (DAST) simplifica el análisis de cientos de aplicaciones web e identifica vulnerabilidades comunes a la velocidad de DevOps, rastrea páginas web, localiza puntos finales de servicios web, entradas y salidas, para simular pruebas de penetración como ataques para descubrir vulnerabilidades de seguridad explotables y problemas de lógica comercial con resultados confiables.

OUTPOST24 -¿QUÉ PUEDO HACER CON OUTPOST24?

- Única plataforma para descubrir toda su superficie de ataque: terminales, redes, nube, aplicaciones, usuarios y datos.
- Único producto para prestar servicios gestionados MSP mensualizado.
- Los mejores productos de su clase para seguridad híbrida, multinube, seguridad de aplicaciones web, identidad y evaluación de riesgos de acceso
- Priorización de vulnerabilidades basada en riesgos impulsada por inteligencia de amenazas en tiempo real.
- De afuera hacia adentro: usa las mismas técnicas que usaría un atacante para descubrir vulnerabilidades de tiempo de ejecución explotables
- Ahorre dinero: inscribe varias aplicaciones a la vez y proporciona evaluaciones rápidas para adaptarse a cualquier ciclo de lanzamiento.
- Ahorre tiempo: reemplaza las costosas pruebas manuales que tardan demasiado en producir resultados.