



Catálogo de Ciberseguridad

Conoce el portafolio, las alianzas tecnológicas y la cobertura regional de CPNnet en ciberseguridad para Latinoamérica.



PROTECCIÓN

GESTIÓN DE RIESGO

OPERACIONES DE SEGURIDAD



PORTAFOLIO

Portafolio de Ciberseguridad CPNnet

En **CPNnet** organizamos nuestro portafolio en tres dominios, **Protección, Gestión de Riesgo y Operaciones de Seguridad**, para abordar la ciberseguridad desde los riesgos reales del negocio, identificando brechas y relacionándolas con las capacidades necesarias para proteger activos críticos, reducir la exposición y fortalecer la detección y respuesta frente a las amenazas.

01

Protection Layer

Soluciones orientadas a prevenir incidentes y proteger identidades, accesos, redes, endpoints, infraestructura híbrida y aplicaciones.

02

Risk Management Layer

Soluciones para identificar exposición, priorizar riesgos, proteger datos sensibles, validar controles y reducir brechas de cumplimiento.

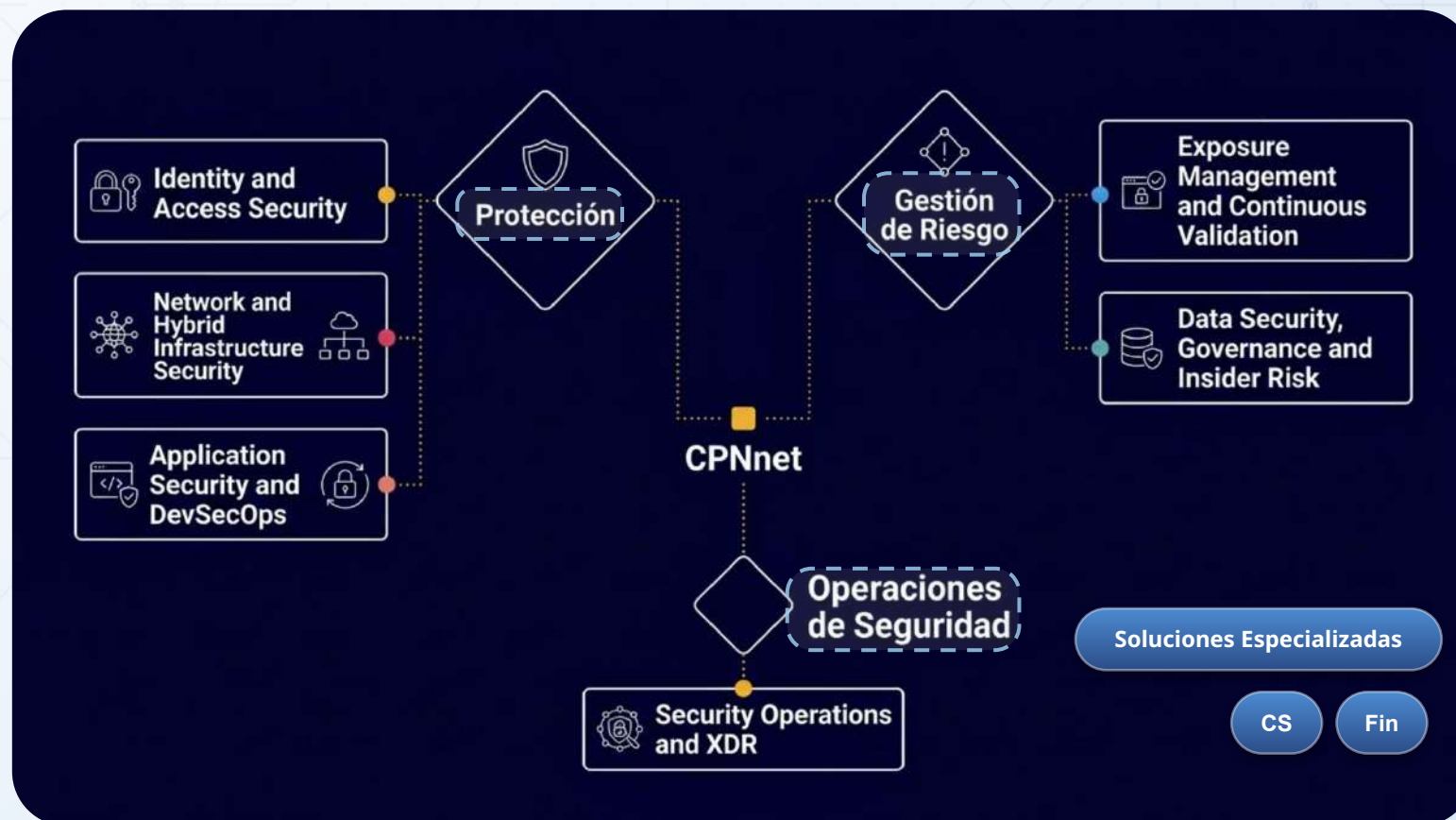
03

Security Operations Layer

Plataformas para detectar, correlacionar, responder y operar la seguridad de forma continua en modelos SOC, MDR, XDR y MSSP.

Arquitectura CPNnet – 3 Dominios / 6 Categorías

El portafolio de CPNnet está organizado en **tres dominios estratégicos y seis categorías de solución**, permitiendo abordar de forma integral las principales necesidades de ciberseguridad de cada organización y relacionarlas con las capacidades necesarias para **proteger, reducir riesgos y fortalecer las operaciones de seguridad**.



◀ DOMINIO 01

Protección

Soluciones orientadas a prevenir incidentes y proteger identidades, accesos, redes, endpoints e infraestructura.

Identity & Access Security

Segura

OneSpan

Network & Hybrid Infrastructure Security

Sophos Network

SonicWall

Faronics

Application Security & DevSecOps

Aikido Security

Haz clic en una marca para ver su ficha ›



Segura

Plataforma de seguridad de identidades privilegiadas diseñada para controlar, limitar y auditar los accesos más críticos de una organización.

POSICIONAMIENTO PRÁCTICO

Controlar, limitar y auditar los accesos privilegiados de personas, terceros, endpoints y máquinas desde una plataforma unificada.

VISIÓN GENERAL

Segura permite descubrir y proteger cuentas privilegiadas, resguardar credenciales, aplicar accesos Just-in-Time, supervisar sesiones, controlar proveedores y terceros, y extender la protección hacia secretos, endpoints y ambientes híbridos. Su valor principal es reducir el riesgo asociado al abuso de privilegios y entregar trazabilidad sobre quién accede, a qué recurso, durante cuánto tiempo y qué acciones realiza. Es especialmente relevante en organizaciones con administradores, proveedores externos, cuentas de servicio, DevOps, cloud, OT o exigencias de auditoría.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

Se vende por módulos y alcance. Levantar: usuarios/administradores privilegiados, cuentas privilegiadas y de servicio, servidores/dispositivos, cantidad de terceros y módulos requeridos (PAM, Domum, EPM, DSM, CIEM, etc.). **Entrada recomendada:** PAM Assessment o revisión de accesos de terceros.

¿Qué problemas resuelve?

- **Cuentas privilegiadas compartidas o sin trazabilidad:** Centraliza credenciales privilegiadas, controla su uso y registra sesiones para saber quién accedió, cuándo y qué hizo.
- **Contraseñas administrativas que no se rotan:** Gestiona credenciales en bóveda y automatiza su rotación, reduciendo la exposición de contraseñas conocidas por varias personas.
- **Proveedores con acceso amplio o permanente:** Domum permite entregar acceso remoto controlado, basado en roles y con grabación de sesiones, evitando depender de accesos VPN demasiado amplios.
- **Usuarios con privilegios locales innecesarios:** Endpoint Privilege Manager permite retirar derechos de administrador local y elevar privilegios solo cuando la tarea lo requiere.
- **Secretos, cuentas de servicio y permisos cloud difíciles de gobernar:** Extiende el control a secretos DevOps, identidades de máquina y permisos cloud, reduciendo privilegios excesivos y credenciales expuestas.

¿Por qué elegir Segura?

- **Cobertura de privilegio más allá del PAM tradicional:** Además de administradores, cubre terceros, endpoints, secretos DevOps, identidades de máquina y permisos cloud.
- **Acceso de terceros sin entregar conectividad amplia a la red:** Domum permite controlar el acceso al recurso y la sesión.
- **Sesiones privilegiadas auditables:** La grabación y trazabilidad permiten investigar y demostrar qué ocurrió durante una operación administrativa.
- **Mínimo privilegio en endpoint integrado:** Complementa PAM de servidores con control de privilegios locales en estaciones de trabajo.
- **Plataforma unificada de Identity Security:** Reduce la necesidad de abordar cada problema de privilegio con una herramienta aislada y facilita una estrategia progresiva.



OneSpan

Protege la identidad digital y la integridad de operaciones de alto valor mediante autenticación fuerte, autenticación móvil, mecanismos passwordless, firma de transacciones y seguridad para aplicaciones móviles.

POSICIONAMIENTO PRÁCTICO

Proteger identidades, aplicaciones móviles y transacciones digitales con autenticación de alta seguridad y prevención de fraude.

VISIÓN GENERAL

Su propuesta es especialmente relevante cuando no basta con comprobar quién inicia sesión, sino que también es necesario asegurar qué operación está autorizando y desde qué contexto se realiza. Se utiliza principalmente en banca, fintech, servicios financieros, canales digitales, aplicaciones móviles y procesos donde fraude, suplantación o manipulación de transacciones representan un riesgo crítico.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

El dimensionamiento depende del caso de uso: usuarios/identidades, autenticaciones, transacciones, aplicaciones móviles o volumen de firmas. **Entrada recomendada:** workshop de caso de uso. No vender "OneSpan" de forma genérica; identificar si el problema principal es autenticación, fraude/transacción, seguridad móvil o acuerdos digitales.

¿Qué problemas resuelve?

- **Robo o compromiso de credenciales:** Refuerza la autenticación con métodos de alta seguridad y opciones passwordless/passkeys, reduciendo dependencia de contraseñas.
- **Fraude en transacciones digitales:** Permite vincular la aprobación a los datos de la transacción mediante mecanismos de firma y autenticación contextual.
- **Aplicaciones móviles expuestas a manipulación:** Añade capacidades de protección de aplicaciones y dispositivos para dificultar manipulación, malware y abuso del canal móvil.
- **Experiencias de autenticación fragmentadas:** DigipassONE unifica modernización de autenticación, seguridad transaccional, credenciales digitales y analítica en una plataforma.
- **Procesos de firma y acuerdos digitales con demasiada fricción:** OneSpan Digital Agreements integra eSignature, verificación de identidad y flujos digitales seguros.

¿Por qué elegir OneSpan?

- **Foco en autenticación de alto aseguramiento:** Escenarios donde la identidad y la transacción requieren mayor nivel de confianza que un MFA básico.
- **Seguridad de identidad y transacción en una misma estrategia:** No se limita a iniciar sesión; también protege el momento en que el usuario aprueba una operación sensible.
- **Modernización progresiva:** DigipassONE permite avanzar desde métodos existentes hacia passwordless/passkeys sin plantear un reemplazo abrupto.
- **Capacidad para casos regulados y de alto riesgo:** Encaja especialmente bien en banca, fintech, gobierno y procesos donde la autenticidad de la operación es crítica.
- **Cobertura del ciclo digital del usuario:** Protege acceso, dispositivo/app, operación y firma, reduciendo puntos aislados de control.



Sophos Network Security

Portafolio integrado de seguridad de red que reúne firewall, switching, wireless, SD-WAN, SD-RED, ZTNA y capacidades de detección de red administradas desde Sophos Central.

POSICIONAMIENTO PRÁCTICO

Proteger y administrar de forma integrada el perímetro, las sucursales, la LAN, el Wi-Fi y el acceso remoto mediante Sophos Firewall, SD-WAN/SD-RED, Switch, Wireless, ZTNA y NDR, gestionados desde Sophos Central.

VISIÓN GENERAL

Permite proteger el perímetro, conectar sucursales, dar acceso seguro a usuarios remotos y coordinar la respuesta entre red y endpoint. Su principal fortaleza comercial es la integración del ecosistema Sophos, que simplifica la administración y permite automatizar acciones frente a amenazas activas. Es especialmente adecuada para organizaciones distribuidas que quieren consolidar seguridad de red, acceso y administración en una misma arquitectura.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

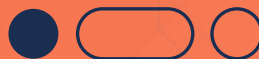
Para Sophos Firewall: throughput con servicios habilitados, velocidad de enlaces WAN, usuarios/conexiones, VPN, interfaces, HA y crecimiento esperado. **Entrada recomendada:** renovación de firewall, apertura de nuevas sucursales, consolidación de redes distribuidas o reemplazo de VPN por ZTNA.

¿Qué problemas resuelve?

- **Seguridad de red fragmentada en múltiples consolas:** Sophos integra firewall, switches, puntos de acceso, conectividad de sucursales y acceso Zero Trust dentro de un mismo ecosistema administrado desde Sophos Central, reduciendo la dispersión operacional.
- **Ataques avanzados y tráfico cifrado atraviesan el perímetro:** Sophos Firewall XGS combina IPS, control de aplicaciones y web, inspección TLS, protección frente a amenazas de día cero y otras capas de seguridad.
- **Sucursales difíciles de conectar y administrar:** SD-WAN y los dispositivos SD-RED permiten extender conectividad segura con despliegue zero-touch y administración centralizada.
- **El acceso remoto depende de VPN amplias y poco granulares:** Sophos ZTNA permite entregar acceso por aplicación y recurso.
- **La red y los endpoints reaccionan de forma aislada:** Synchronized Security y Active Threat Response comparten estado y telemetría para aislar dispositivos comprometidos y limitar movimiento lateral.

¿Por qué elegir Sophos Network?

- **Portafolio de red integrado:** Sophos cubre firewall, SD-WAN, sucursales, switching, wireless, ZTNA y NDR bajo un mismo ecosistema.
- **Integración real entre endpoint y red:** Security Heartbeat y Synchronized Security permiten que Sophos Endpoint y Sophos Firewall compartan estado y automaticen acciones de aislamiento.
- **Firewall preparado para MDR/XDR:** Sophos Firewall aporta telemetría a XDR/MDR y soporta Active Threat Response.
- **Arquitectura Xstream e inspección TLS:** Diseñada para acelerar inspección y protección, permitiendo inspeccionar tráfico cifrado sin renunciar a funciones de seguridad.
- **Flexibilidad de despliegue:** Disponible como appliance XGS, software, virtual y cloud, complementándose con Switch, Wireless y SD-RED.



SonicWall

Portafolio de seguridad de red orientado a proteger oficinas, sucursales, usuarios remotos y ambientes híbridos mediante firewalls de nueva generación, SD-WAN, acceso seguro y administración centralizada.

POSICIONAMIENTO PRÁCTICO

Proteger redes, sucursales y accesos híbridos mediante firewalls, SD-WAN, gestión centralizada y servicios de seguridad.

VISIÓN GENERAL

Ayuda a controlar tráfico, aplicaciones, amenazas y conectividad entre sedes, manteniendo políticas consistentes a medida que la infraestructura crece. Es especialmente relevante para organizaciones con múltiples ubicaciones, renovación de firewall, trabajo híbrido o necesidad de proteger conectividad distribuida con una propuesta amplia y reconocida en seguridad de red.



Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

Para NGFW: throughput con servicios habilitados, usuarios/conexiones simultáneas, interfaces, VPN, HA, sedes y crecimiento. Para Cloud Secure Edge: licenciamiento por usuario y función/tier. **Entrada recomendada:** sizing de firewall o revisión de arquitectura de sucursales.

¿Qué problemas resuelve?

- **Firewalls antiguos o insuficientes para el tráfico actual:** Las nuevas familias NGFW y servicios de seguridad permiten actualizar capacidad, inspección y protección del perímetro.
- **Sucursales con configuraciones y seguridad inconsistentes:** La gestión centralizada facilita aplicar políticas, visibilidad y reporting de forma común entre múltiples sitios.
- **Acceso remoto demasiado amplio:** Cloud Secure Edge permite abordar acceso privado/ZTNA y seguridad de Internet por usuario según el caso.
- **Necesidad de conectar sedes sin separar red y seguridad:** Secure SD-WAN combina conectividad, routing y seguridad para sedes distribuidas.
- **Falta de segmentación y control del tráfico interno:** NGFW y políticas de segmentación ayudan a limitar movimientos laterales y separar zonas de confianza.

¿Por qué elegir SonicWall?

- **Portafolio amplio para sucursal, datacenter y virtual:** Permite seleccionar plataforma según capacidad y ubicación sin cambiar de ecosistema.
- **Seguridad y conectividad en la misma propuesta:** Combina NGFW, SD-WAN, VPN y routing, reduciendo soluciones separadas para la sucursal.
- **Opciones de servicio gestionado:** MPSS añade gestión de firewall y monitoreo, útil para clientes que no quieren operar todo internamente.
- **Ruta hacia Zero Trust / SASE:** Cloud Secure Edge permite ampliar la conversación más allá del firewall físico hacia acceso por usuario.
- **Fuerte encaje en canal y MSP:** La arquitectura de administración y servicios facilita operar múltiples clientes y sedes desde una estrategia común.



Faronics

Orientado a mantener endpoints estables, disponibles y fáciles de administrar, especialmente en ambientes con equipos compartidos, públicos o de alta rotación mediante tecnología Deep Freeze.

POSICIONAMIENTO PRÁCTICO

Mantener equipos compartidos o críticos en un estado operativo conocido y reducir tareas repetitivas de soporte y administración.

VISIÓN GENERAL

Su tecnología Deep Freeze permite restaurar un equipo a un estado conocido mediante reinicio, mientras que Deep Freeze Cloud agrega administración, despliegue, patching, personalización y otras funciones de endpoint management. Su valor se hace evidente en colegios, universidades, laboratorios, kioscos, call centers, retail y organizaciones donde reducir tickets y recuperar rápidamente estaciones de trabajo tiene un impacto operacional directo.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

Principalmente por cantidad de dispositivos/workstations y producto/edición requerida. Levantar número de PCs, ubicación/remotos, SO, necesidad cloud u on-premise y capacidades adicionales.

Entrada recomendada: piloto controlado en 10-20 equipos de alto soporte.

¿Qué problemas resuelve?

- **Equipos compartidos que quedan mal configurados:** Deep Freeze devuelve el equipo a un estado definido al reiniciar, eliminando cambios no deseados.
- **Usuarios que instalan software o modifican configuraciones:** El enfoque reboot-to-restore evita que cambios persistentes degraden el equipo.
- **Alta carga de soporte en laboratorios, kioscos o salas:** Restaurar automáticamente reduce tickets causados por configuraciones dañadas o software no autorizado.
- **Endpoints remotos difíciles de administrar:** Faronics Cloud/Deploy permite administrar, desplegar software y actualizar equipos locales o remotos.
- **Necesidad de mantener equipos disponibles y consistentes:** Políticas de restauración y administración ayudan a mantener un baseline estable entre múltiples dispositivos.

¿Por qué elegir Faronics?

- **Reboot-to-restore como propuesta central:** En lugar de depender solo de reparar el equipo después del incidente, restaura automáticamente un estado conocido.
- **Especialización en equipos compartidos y públicos:** Tiene un encaje muy claro en laboratorios, educación, kioscos, POS y estaciones de atención.
- **Reducción directa de tickets de configuración:** El beneficio es fácil de medir: menos tiempo dedicado a corregir cambios hechos por usuarios.
- **Administración remota complementaria:** No se limita a "congelar" el equipo; puede complementarse con despliegue, actualización y acceso remoto.
- **Mantiene homogeneidad en grandes grupos de PCs:** Ayuda a que cientos de estaciones vuelvan al mismo baseline tras cada reinicio.



Aikido Security

Plataforma unificada de seguridad de aplicaciones que protege código, cloud y runtime desde un mismo entorno con capacidades de priorización y corrección asistida por IA.

POSICIONAMIENTO PRÁCTICO

Unificar seguridad de aplicaciones desde código y dependencias hasta cloud y runtime, con foco en reducir ruido y facilitar la corrección por los desarrolladores.

VISIÓN GENERAL

Integra análisis de código y dependencias, detección de secretos, infraestructura como código, seguridad de contenedores y cloud, pruebas ofensivas y protección en ejecución. Su propuesta destaca por acercar la seguridad al flujo de trabajo del desarrollador y reducir la fragmentación de herramientas. Es especialmente útil para empresas que desarrollan software, SaaS, APIs o aplicaciones cloud-native y necesitan incorporar seguridad sin frenar DevOps.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

La plataforma se dimensiona principalmente por número de desarrolladores cubiertos y plan. Para enterprise y módulos avanzados el precio es personalizado. **Entrada recomendada:** demo conectando uno o pocos repositorios de prueba.

¿Qué problemas resuelve?

- **Vulnerabilidades detectadas demasiado tarde:** Integra escaneo de código, dependencias, secretos e infraestructura dentro del flujo de desarrollo para encontrar riesgos antes de producción.
- **Demasiadas herramientas AppSec separadas:** Consolida SAST, SCA, secrets, IaC, cloud, contenedores, DAST/ASM y otras capacidades en una plataforma modular.
- **Muchos falsos positivos y hallazgos irrelevantes:** Utiliza análisis de alcanzabilidad, auto-triage y reducción de ruido para priorizar problemas realmente aplicables al entorno.
- **Correcciones que dependen totalmente del desarrollador:** AutoFix y pull requests preparados reducen el esfuerzo para pasar del hallazgo a la corrección.
- **Secretos y configuraciones expuestas en el SDLC:** Detecta secretos, errores de IaC, configuraciones cloud y componentes vulnerables a lo largo del ciclo de desarrollo.

¿Por qué elegir Aikido Security?

- **Plataforma unificada de Code-to-Runtime:** Reduce la necesidad de operar múltiples scanners aislados para cada etapa del SDLC.
- **Experiencia centrada en desarrolladores:** Integra resultados y correcciones en herramientas y flujos que el equipo ya utiliza.
- **Reducción de ruido como parte del diseño:** Reachability y auto-triage ayudan a concentrarse en problemas explotables o relevantes.
- **Corrección integrada, no solo detección:** AutoFix y pull requests facilitan convertir hallazgos en cambios de código concretos.
- **Cobertura modular y escalable:** El cliente puede comenzar con Code/AppSec y ampliar a cloud, runtime, pentest u otros módulos.

◀ DOMINIO 02

Gestión de Riesgo

Soluciones para identificar exposición, priorizar riesgos, proteger datos sensibles y validar controles.

Exposure Management & Continuous Validation

Vicarius

Cymulate

Action1

VectorIQ

Data Security, Governance & Insider Risk

Kriptos

Safetica

Haz clic en una marca para ver su ficha >

Vicarius

Plataforma de gestión de exposición orientada a la remediación: no se limita a identificar vulnerabilidades, sino que busca cerrar el ciclo mediante priorización, patching, scripting y protección sin parche.

POSICIONAMIENTO PRÁCTICO

Convertir vulnerabilidades en acciones de remediación mediante patching, scripting y protección sin parche, priorizando el riesgo.

VISIÓN GENERAL

Ayuda a reducir el backlog y la ventana de exposición cuando los equipos saben qué problemas tienen pero no logran corregirlos con suficiente rapidez. Su principal diferenciación es combinar varias rutas de remediación dentro de un mismo flujo. Es especialmente relevante para endpoints y servidores distribuidos, aplicaciones de terceros, sistemas legacy y ambientes donde un parche no siempre existe o puede aplicarse inmediatamente.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

El foco comercial suele ser cantidad de endpoints/servidores administrados y alcance de módulos. Levantar: número de endpoints y servidores, SO, aplicaciones críticas/terceros y backlog de vulnerabilidades. **Entrada recomendada:** assessment de remediación o prueba sobre un grupo representativo de equipos.

¿Qué problemas resuelve?

- **Backlog de vulnerabilidades que no deja de crecer:** Prioriza hallazgos y los conecta con acciones de remediación para que TI y Seguridad trabajen sobre el mismo flujo.
- **Parches pendientes en sistemas y aplicaciones:** Automatiza patch management y facilita el despliegue de correcciones en endpoints.
- **Vulnerabilidades sin parche disponible:** Patchless Protection puede bloquear rutas de explotación mientras se espera una corrección oficial aplicable.
- **Correcciones manuales que consumen demasiado tiempo:** El motor de scripting permite automatizar fixes y tareas que no se resuelven con un parche estándar.
- **Falta de validación de que el riesgo realmente desapareció:** La capa de inteligencia y el ciclo de remediación permiten volver a evaluar el riesgo después de actuar.

¿Por qué elegir Vicarius?

- **Remediation-first:** La propuesta no termina en identificar el problema; está diseñada para cerrar la brecha mediante acciones concretas.
- **Tres caminos de corrección:** Combina patching, scripting y patchless protection en lugar de depender de un solo mecanismo.
- **Cobertura cuando no hay parche:** Patchless Protection ofrece una alternativa temporal para vulnerabilidades compatibles sin tocar la aplicación.
- **Une IT y Security en un mismo flujo:** Relaciona el hallazgo técnico con la acción que debe ejecutar operaciones.
- **Adecuada para clientes que ya tienen scanner:** Puede complementar herramientas de detección existentes centrándose en priorización y remediación.

Cymulate

Plataforma de Exposure Validation que permite comprobar continuamente si los controles de seguridad realmente previenen, detectan y responden frente a técnicas de ataque actuales.

POSICIONAMIENTO PRÁCTICO

Comprobar de forma continua si los controles de seguridad realmente previenen y detectan las técnicas de ataque relevantes para el entorno.

VISIÓN GENERAL

Utiliza Breach and Attack Simulation y otras capacidades de validación para identificar brechas, demostrar explotabilidad, priorizar exposiciones y optimizar controles existentes. Su valor está en entregar evidencia práctica sobre la efectividad de inversiones como EDR/XDR, firewall, correo, SIEM/SOAR, DLP y cloud. Es especialmente útil para organizaciones que necesitan pasar de evaluaciones puntuales a una validación continua y medible de su postura.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

El dimensionamiento depende de módulos, alcance de validación y tamaño/activos del entorno. Levantar qué controles se quieren validar, número aproximado de activos/segmentos y casos de uso requeridos. **Entrada recomendada:** baseline de validación o assessment de efectividad de controles.

¿Qué problemas resuelve?

- **Controles instalados pero nunca probados:** Ejecuta validaciones controladas para medir si las defensas previenen, detectan y responden como se espera.
- **Pentest anual que se queda desactualizado:** Automatiza validaciones repetibles para revisar cambios en amenazas, configuraciones y controles durante todo el año.
- **Demasiadas vulnerabilidades sin contexto de explotabilidad:** Relaciona exposición con validación para ayudar a priorizar hallazgos que realmente pueden afectar el entorno.
- **SIEM/EDR/XDR con reglas que no se han probado:** Detection Engineering permite probar y ajustar capacidades de detección frente a técnicas específicas.
- **Cambios de seguridad sin evidencia de mejora:** Permite repetir pruebas después de ajustes o remediaciones para comprobar el efecto real.

¿Por qué elegir Cymulate?

- **Validación continua frente a pruebas puntuales:** Permite medir postura durante el año, no solo en la fecha de un pentest.
- **Prueba controles existentes en condiciones controladas:** No se limita a revisar configuración; genera evidencia de cómo responderían las defensas.
- **Conecta ofensiva y defensiva:** Puede ser usado por SOC, purple team, vulnerability management y líderes de seguridad.
- **Prioriza con evidencia:** Ayuda a enfocar esfuerzos en exposiciones validadas y no únicamente en scores técnicos.
- **Complementa inversiones existentes:** Su valor aumenta cuando el cliente ya tiene varias herramientas y necesita comprobar que funcionan juntas.

Action1

Plataforma cloud de Autonomous Endpoint Management enfocada en automatizar patching, remediación de vulnerabilidades y administración de endpoints distribuidos.

POSICIONAMIENTO PRÁCTICO

Automatizar patch management y remediación de vulnerabilidades en endpoints y servidores distribuidos, incluyendo software de terceros.

VISIÓN GENERAL

Permite mantener Windows, macOS, Linux y aplicaciones de terceros actualizados sin depender de VPN y con visibilidad continua del estado de parchado. Su principal fortaleza es simplificar un problema operacional muy concreto: reducir el tiempo y trabajo manual necesarios para mantener los equipos actualizados. Es especialmente adecuada para organizaciones con workforce remoto, múltiples sedes, alta carga de patching o necesidad de demostrar cumplimiento continuo.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

Se dimensiona principalmente por número de endpoints/servidores administrados. Levantar cantidad de estaciones, servidores, SO, ubicaciones/remotos y principales aplicaciones de terceros. **Entrada recomendada:** assessment de patch compliance o piloto.

¿Qué problemas resuelve?

- **Parches atrasados en Windows, macOS y aplicaciones:** Detecta actualizaciones faltantes y automatiza el despliegue en sistemas y software soportado.
- **Equipos remotos fuera de la VPN:** Gestiona patching de endpoints distribuidos sin depender de que estén conectados a la red corporativa.
- **Software de terceros que queda fuera de WSUS/Intune:** Incluye third-party patching para ampliar cobertura más allá del sistema operativo.
- **Dificultad para demostrar cumplimiento de parches:** Entrega visibilidad y reporting de patch compliance en tiempo real.
- **Procesos manuales de actualización que consumen recursos:** Automatiza detección, priorización y remediación reduciendo tareas repetitivas.

¿Por qué elegir Action1?

- **Patching como foco principal y simple:** Es fácil de posicionar cuando el problema concreto es mantener sistemas y aplicaciones actualizados.
- **Cobertura de terceros integrada:** Evita depender de procesos separados para gran parte del software instalado.
- **No requiere VPN para equipos remotos:** El modelo cloud facilita administrar dispositivos fuera de la oficina.
- **Vulnerability + remediation en el mismo flujo:** Relaciona hallazgo con parche disponible, reduciendo trabajo entre herramientas.
- **Entrada comercial rápida:** El valor puede demostrarse midiendo patch compliance y automatizando un grupo de equipos.

VectoralQ

Plataforma modular que aplica inteligencia artificial a distintos dominios de ciberseguridad, incluyendo gestión de riesgo y exposición, DevSecOps, offensive security, insider risk y análisis conductual.

POSICIONAMIENTO PRÁCTICO

Plataforma modular de agentes de IA con capacidades de rating/ASM, DevSecOps, offensive security, insider risk y respuesta conductual; en este catálogo se ancla principalmente en gestión de exposición.

VISIÓN GENERAL

Debido a la amplitud de sus módulos, su mejor posicionamiento comercial es partir por un caso de uso específico en vez de presentar toda la plataforma de una vez. Dentro de la arquitectura CPNnet se utiliza principalmente para ampliar capacidades de gestión de exposición y riesgo, pudiendo abrir oportunidades adicionales en aplicaciones, validación ofensiva y comportamiento. Es relevante para clientes que buscan automatización e inteligencia aplicada a procesos de seguridad especializados.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

El canal debe identificar primero el módulo/caso de uso y levantar activos, usuarios, aplicaciones o alcance según corresponda. CPNnet debe validar el modelo con el fabricante antes de cotizar. **Entrada recomendada:** elegir un módulo concreto, especialmente SecureRatingIQ/ASM u Offensive Security.

¿Qué problemas resuelve?

- **Visibilidad incompleta de superficie de ataque:** SecureRatingIQ combina security rating y attack surface management para identificar activos y puntuar riesgo.
- **Evaluaciones ofensivas demasiado manuales:** Offensive Security Suite automatiza actividades de pentesting, red teaming y simulación de adversarios.
- **Vulnerabilidades en código y pipelines:** DevSecOps Engine incorpora SAST/DAST/SCA y reparación automatizada dentro de CI/CD.
- **Riesgo interno difícil de detectar:** El módulo de Personnel Intelligence aplica análisis conductual y UEBA al factor humano.
- **Señales de red y comportamiento sin respuesta coordinada:** XSR/XNC analizan anomalías, tráfico y dispositivos para apoyar decisiones y acciones automatizadas.

¿Por qué elegir VectoralIQ?

- **Arquitectura modular de agentes especializados:** Permite abordar varios dominios con módulos coordinados en lugar de una única función aislada.
- **SecureRatingIQ comunica riesgo con scoring:** Facilita traducir hallazgos de ASM a una calificación entendible por negocio.
- **Automatización ofensiva dentro del mismo ecosistema:** Reduce separación entre descubrimiento de exposición y pruebas ofensivas.
- **Módulo DevSecOps con remediación:** Extiende la plataforma desde superficie externa hacia código y CI/CD.
- **Posibilidad de expansión por módulos:** Permite comenzar por un caso de uso y ampliar a otros sin presentar toda la plataforma desde el inicio.

Kriptos

Ayuda a descubrir, clasificar y gobernar información sensible para que la organización sepa qué datos posee, dónde están almacenados y quién puede acceder a ellos mediante automatización e IA.

POSICIONAMIENTO PRÁCTICO

Descubrir, clasificar y gobernar datos no estructurados para saber qué información sensible existe, dónde está y quién puede acceder a ella.

VISIÓN GENERAL

Su principal valor es generar visibilidad antes de aplicar controles de DLP o gobierno, evitando proteger datos que la empresa ni siquiera ha identificado. Es especialmente relevante en ambientes Microsoft 365, Google Workspace, repositorios compartidos, datos personales, propiedad intelectual y adopción de herramientas de IA.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

El dimensionamiento depende de fuentes de datos, usuarios/entornos y volumen documental. El canal debe levantar cantidad de usuarios/endpoints, servidores y repositorios cloud a revisar. **Entrada recomendada:** Data Discovery Assessment. La pregunta inicial: "¿Saben exactamente dónde está toda la información sensible de la empresa y quién puede verla?".

¿Qué problemas resuelve?

- **La empresa no sabe dónde está toda su información sensible:** Escanea e inventaría documentos en endpoints, servidores y almacenamiento cloud para identificar datos críticos.
- **Clasificación manual o basada en palabras clave:** Utiliza múltiples modelos de IA para clasificar contenido con contexto y aplicar etiquetas.
- **Permisos excesivos y sobreexposición en M365/Google:** Access Governance muestra quién tiene acceso a qué y detecta oversharing o permisos riesgosos.
- **Dificultad para preparar evidencia de cumplimiento:** Data Compliance y dashboards ayudan a organizar visibilidad, clasificación y riesgo para auditoría.
- **Uso de datos sensibles en herramientas de IA sin gobierno:** AI Governance ayuda a preparar y controlar el uso de información corporativa en escenarios de adopción de IA.

¿Por qué elegir Kriptos?

- **Especialización en datos no estructurados:** Ataca directamente documentos y archivos distribuidos, un área donde muchas empresas tienen poca visibilidad.
- **Clasificación contextual con múltiples modelos de IA:** Busca ir más allá de listas de palabras o expresiones estáticas.
- **Clasificación conectada con gobierno de acceso:** No se limita a etiquetar; muestra quién puede acceder y dónde existe oversharing.
- **Interoperabilidad con etiquetas existentes:** Puede usar etiquetado de Microsoft Purview y Google Workspace para integrarse con controles ya desplegados.
- **Extensión natural hacia AI Governance:** Permite convertir la clasificación de datos en una base para controlar adopción de IA corporativa.

Safetica

Solución de Data Loss Prevention e Insider Risk orientada a controlar cómo los usuarios utilizan y mueven información sensible a través de endpoints, correo, web, dispositivos removibles y servicios cloud.

POSICIONAMIENTO PRÁCTICO

Prevenir pérdida de datos y gestionar riesgo interno combinando contexto de datos, identidad y comportamiento del usuario.

VISIÓN GENERAL

Combina políticas de protección de datos con contexto de usuario y comportamiento para reducir fugas accidentales o intencionales. Su propuesta es especialmente adecuada para organizaciones que necesitan implementar DLP con una operación manejable y obtener visibilidad sobre actividades de riesgo interno. Sus casos habituales incluyen colaboradores salientes, propiedad intelectual, datos personales, contratistas y uso no autorizado de canales o aplicaciones.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

Normalmente se dimensiona por usuarios/endpoints y por edición/módulos. El canal debe levantar cantidad de usuarios, endpoints, plataformas cloud, canales a controlar y tipo de información sensible. **Entrada recomendada:** DLP/Insider Risk Assessment.

¿Qué problemas resuelve?

- **Datos sensibles que salen por canales no autorizados:** Clasifica, monitorea y controla información en dispositivos y nube para prevenir transferencias riesgosas.
- **Empleados que copian información antes de salir de la empresa:** Analiza comportamiento y señales de riesgo para detectar actividad inusual relacionada con datos.
- **USB, correo, web y cloud difíciles de controlar de forma consistente:** Aplica políticas DLP sobre múltiples canales y contextos de uso.
- **Demasiadas alertas DLP sin contexto:** Combina datos, identidad y comportamiento para distinguir actividad normal de acciones realmente riesgosas.
- **Información en Microsoft 365 y plataformas cloud:** Extiende protección a cloud y file-sharing para seguir el dato fuera del endpoint tradicional.

¿Por qué elegir Safetica?

- **DLP + Insider Risk en una misma propuesta:** No mira solo el archivo o solo al usuario: combina ambas dimensiones.
- **Contexto conductual:** Busca entender intención y patrón de comportamiento para mejorar la calidad de las alertas.
- **Foco en productividad:** La propuesta busca bloquear acciones riesgosas sin interrumpir innecesariamente el trabajo normal.
- **Atractiva para mid-market:** Puede ser una alternativa práctica para organizaciones que necesitan DLP sin construir un programa excesivamente complejo.
- **Complementa clasificación externa:** Puede aprovechar contexto de herramientas como Kriptos para aplicar políticas más precisas sobre información sensible.

◀ DOMINIO 03

Operaciones de Seguridad

Plataformas para detectar, correlacionar, responder y operar la seguridad de forma continua.

Security Operations & XDR

Sophos XDR/MDR

Sophos Taegis

Seceon

Haz clic en una marca para ver su ficha ›

Sophos XDR / MDR

Permiten ampliar la protección de endpoint hacia una capacidad integral de detección, investigación y respuesta, con XDR para equipos internos y MDR con monitoreo y respuesta gestionada 24/7 por especialistas.

POSICIONAMIENTO PRÁCTICO

Proteger endpoints y ampliar detección e investigación con XDR; o delegar monitoreo, threat hunting y respuesta 24/7 mediante MDR.

VISIÓN GENERAL

La integración con el ecosistema Sophos y fuentes de terceros permite correlacionar señales y acelerar la contención. Es especialmente relevante para organizaciones que tienen demasiadas alertas, poca cobertura 24/7, equipos reducidos o necesidad de mejorar su capacidad de respuesta sin construir un SOC completo.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

Se licencia principalmente por usuario y por servidor. El canal debe levantar usuarios, servidores, SO, modalidad XDR o MDR, fuentes de terceros y necesidad de retención. **Entrada recomendada:** revisión de madurez de detección/respuesta. Para MDR, el gatillante es falta de 24/7, poco personal o demasiadas alertas.

¿Qué problemas resuelve?

- **Ataques que evaden controles preventivos:** XDR correlaciona señales y permite investigar actividad que no fue bloqueada inicialmente.
- **Datos aislados entre endpoint, firewall, email, identidad y cloud:** Sophos integra telemetría propia y de terceros para dar más contexto a la investigación.
- **Demasiadas alertas para el equipo interno:** XDR ayuda a priorizar e investigar; MDR traslada la operación 24/7 a analistas especializados.
- **Falta de cobertura fuera de horario:** MDR entrega threat hunting, detección e incident response 24/7.
- **Empresa sin capacidad para construir un SOC completo:** MDR permite obtener capacidad operativa y especialistas sin crear toda la estructura internamente.

¿Por qué elegir Sophos XDR / MDR?

- **Prevención de endpoint + XDR + MDR dentro del mismo ecosistema:** Reduce fricción entre tecnología y servicio gestionado.
- **MDR no depende exclusivamente de telemetría Sophos:** Puede integrar productos de terceros para enriquecer la detección.
- **Modelo simple por usuario y servidor para XDR/MDR:** Facilita dimensionamiento frente a propuestas basadas principalmente en ingestión de logs.
- **Escalabilidad de XDR a MDR:** Una organización puede operar XDR internamente o pasar a un servicio gestionado según recursos.
- **Ecosistema coordinado de endpoint, firewall, email y otras capas:** Permite construir una propuesta integrada y abrir cross-selling dentro y fuera de Sophos.



Sophos Taegis

Plataforma abierta de operaciones de seguridad que integra capacidades de XDR, MDR y Next-Gen SIEM para correlacionar telemetría de múltiples fabricantes y convertirla en incidentes investigables y accionables.

POSICIONAMIENTO PRÁCTICO

Plataforma SecOps abierta con XDR, MDR, Next-Gen SIEM, NDR y VDR para integrar telemetría multivendor y operar seguridad a escala.

VISIÓN GENERAL

Está pensada para organizaciones con entornos complejos que quieren modernizar el SOC, consolidar herramientas o evolucionar desde un SIEM tradicional hacia una operación más integrada. Su valor diferencial está en combinar plataforma y servicios de seguridad gestionada sin obligar a reemplazar necesariamente las inversiones existentes. Es especialmente fuerte en ambientes multivendor, SOC propios, empresas grandes y escenarios con alta necesidad de integración.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

Taegis se dimensiona según solución (XDR/MDR/SIEM/NDR/VDR), endpoints/usuarios y servidores, fuentes de datos, volumen/retención de logs y módulos requeridos. **Entrada recomendada:** workshop de arquitectura SecOps. Es especialmente fuerte cuando el cliente tiene SIEM legacy, muchas herramientas o SOC propio.

¿Qué problemas resuelve?

- **SOC con demasiadas herramientas y datos aislados:** Taegis integra telemetría y logs de cientos de integraciones para centralizar visibilidad y contexto.
- **SIEM tradicional costoso o difícil de operar:** Next-Gen SIEM combina ingesta, retención, búsqueda y analítica dentro de la plataforma SecOps.
- **Investigaciones lentas por falta de correlación:** Analítica, IA y automatización ayudan a reducir ruido y acelerar investigación.
- **Organización que necesita XDR abierto:** Taegis XDR integra tecnologías de distintos proveedores sin exigir reemplazar todo el stack.
- **Falta de analistas especializados:** Taegis MDR puede operar de forma gestionada o colaborativa con el equipo interno.

¿Por qué elegir Sophos Taegis?

- **Arquitectura abierta y multivendor:** Se posiciona para clientes con stack heterogéneo que no quieren reemplazar inversiones existentes.
- **XDR + SIEM en una misma plataforma:** Reduce la separación entre detección, búsqueda, retención y reporting.
- **Sophos Endpoint incluido en XDR/MDR Taegis:** Integra de forma nativa protección de endpoint dentro de la plataforma.
- **MDR operado hasta resolución:** El servicio combina plataforma abierta con analistas especializados.
- **NDR/VDR como extensiones naturales:** Permite crecer hacia red y vulnerabilidades manteniendo contexto central.



Seceon

Plataforma de operaciones de seguridad orientada a AI-SIEM, XDR y automatización, con especial foco en reducir la complejidad operativa y facilitar modelos de SOC y servicios administrados.

POSICIONAMIENTO PRÁCTICO

Plataforma all-in-one orientada a SIEM/XDR y SOC autónomo, con fuerte foco en MSP/MSSP, automatización y licenciamiento por activos.

VISIÓN GENERAL

Centraliza telemetría de endpoints, red, identidades, cloud y otras fuentes para correlacionar eventos y automatizar acciones. Su propuesta es atractiva para organizaciones y MSP/MSSP que buscan consolidación, operación multi-tenant y costos más predecibles. Es especialmente útil cuando existe un equipo de seguridad pequeño, muchas fuentes de eventos o necesidad de construir servicios SOC escalables.

Problemas que resuelve Diferencias Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

El fabricante posiciona licenciamiento basado en activos. El canal debe levantar número/tipo de activos, endpoints, servidores, dispositivos de red, cloud, fuentes principales y si el modelo será enterprise o MSP/MSSP. **Entrada recomendada:** POV de 30 días o discovery de arquitectura SOC.

¿Qué problemas resuelve?

- **SIEM con alto costo y demasiadas herramientas adicionales:** La plataforma OTM busca consolidar analítica, detección, respuesta y gestión en una sola propuesta.
- **Demasiadas alertas para un SOC pequeño:** Correlación, IA/ML y automatización reducen ruido y ayudan a priorizar incidentes reales.
- **MSSP que necesita multi-tenant y operación escalable:** Seceon está diseñado para MSP/MSSP con administración multi-tenant y servicios 24/7.
- **Telemetría distribuida en logs, red, identidad, endpoint y cloud:** Integra datos de múltiples fuentes para obtener visibilidad unificada.
- **Necesidad de previsibilidad comercial frente a crecimiento de logs:** El fabricante posiciona licenciamiento basado en activos para evitar variación anual por crecimiento de datos.

¿Por qué elegir Seceon?

- **Diseño explícito para MSP/MSSP:** La plataforma y el programa comercial están pensados para servicios multi-tenant.
- **All-in-one SecOps:** Busca reducir herramientas redundantes mediante SIEM, XDR, postura, compliance y respuesta integrada.
- **Licenciamiento basado en activos:** Puede resultar atractivo para clientes preocupados por costos variables de ingestión.
- **Automatización nativa:** Incluye playbooks, correlación y respuesta como parte central de la propuesta.
- **Foco en eficiencia del SOC:** La propuesta comercial prioriza reducción de alertas y trabajo operativo.

◀ Soluciones Especializadas

Soluciones Especializadas

Además de nuestras marcas estratégicas, **CPNnet** cuenta con un portafolio de Soluciones Especializadas que permite cubrir necesidades específicas y robustecer la arquitectura de seguridad de cada cliente.

Marcas de cross-selling

Stellar Cyber

Veracode

Ridge Security

Appgate

GoTo

LastPass

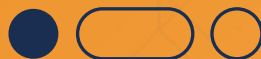
AlgoSec

Hacknoid

Ironchip

Teramind

Haz clic en una marca para ver su ficha >



Stellar Cyber

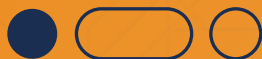
Plataforma de operaciones de seguridad abierta que integra AI-SIEM, NDR, ITDR, UEBA y Open XDR para correlacionar señales de múltiples herramientas y entregar incidentes priorizados.

POSICIONAMIENTO PRÁCTICO

Plataforma SecOps abierta que unifica AI-SIEM, NDR/OT, ITDR, UEBA y Open XDR para correlacionar señales de múltiples herramientas.

VISIÓN GENERAL

Su fortaleza está en complementar entornos multivendor y aportar visibilidad de red y otras fuentes sin obligar a reemplazar necesariamente el EDR existente. Dentro de la arquitectura actual de CPNnet se posiciona como un cross-selling estratégico para casos de SOC, NDR, OT y consolidación de telemetría. Es especialmente relevante para empresas grandes y proveedores de servicios que necesitan una plataforma abierta, multi-tenant y orientada a automatizar investigación.



Problemas que resuelve

Diferencias

Dimensionamiento

DIMENSIONAMIENTO Y PUERTA DE ENTRADA

El dimensionamiento depende de fuentes y volumen de telemetría, activos/usuarios y módulos. El canal debe levantar EPS/GB por día si aplica, cantidad de fuentes, retención requerida, NDR/OT, tenants y EDR existente.

Entrada recomendada: workshop de arquitectura SOC/NDR o POC con fuentes representativas.

¿Qué problemas resuelve?

- **SOC con herramientas aisladas:** Open XDR integra datos de distintas fuentes y los correlaciona en una plataforma común.
- **Falta de visibilidad de red y movimiento lateral:** NDR/OT aporta telemetría profunda de red y detección de comportamiento lateral.
- **SIEM tradicional con alto esfuerzo de investigación:** AI-driven SIEM y case management ayudan a organizar señales en incidentes accionables.
- **Riesgo de identidad no correlacionado con red/endpoint:** ITDR y UEBA añaden comportamiento de usuario e identidad al contexto del SOC.
- **MSSP que necesita arquitectura multi-tenant:** La plataforma ofrece capacidades multi-tier, multi-tenant y multi-site para servicios gestionados.

¿Por qué elegir Stellar Cyber?

- **Open XDR como filosofía de integración:** Está diseñada para conservar herramientas existentes y unificar su telemetría.
- **NDR/OT integrado en la misma plataforma:** Evita separar análisis de red del resto de la investigación.
- **SIEM + XDR + ITDR + UEBA:** Consolida varias capacidades de SecOps bajo un único flujo.
- **Bring Your Own EDR:** Permite mantener EDR existente y usar Stellar como capa de correlación/operación.
- **MITRE ATT&CK Coverage Analyzer:** Aporta una forma adicional de medir cobertura de detección y brechas de control.

Veracode

Application Risk Management

Plataforma de gestión de riesgo de aplicaciones orientada a identificar, priorizar y reducir vulnerabilidades durante todo el ciclo de desarrollo. Integra SAST, DAST, SCA y gestión de riesgo. Especialmente adecuada para organizaciones con múltiples aplicaciones, grandes equipos de desarrollo y programas formales de AppSec o DevSecOps que necesitan estandarizar la seguridad a escala.

¿Qué problemas resuelve?

- **Vulnerabilidades en código interno** Los errores de programación pueden introducir vulnerabilidades que llegan hasta producción. Veracode analiza el código durante el desarrollo para detectarlas antes.
- **Riesgos en componentes open source** Las aplicaciones modernas dependen de librerías que pueden contener vulnerabilidades o riesgos de licencia. Veracode identifica estas dependencias y prioriza su tratamiento.
- **APIs y aplicaciones vulnerables en ejecución** Las pruebas dinámicas evalúan aplicaciones y APIs en funcionamiento para identificar comportamientos potencialmente explotables.
- **Demasiados hallazgos sin priorización** Veracode centraliza el riesgo de aplicaciones y prioriza las acciones de remediación cuando los equipos reciben resultados de distintas herramientas.
- **Seguridad que retrasa el desarrollo** Cuando la revisión ocurre al final del proyecto, corregir es más costoso. Veracode se integra al flujo de desarrollo para detectar problemas antes y reducir retrabajo.

¿Qué capacidades entrega Veracode?

SAST

Analiza el código fuente para identificar vulnerabilidades durante el desarrollo, antes de llegar a producción.

DAST

Prueba aplicaciones web y APIs en ejecución, aportando visión complementaria sobre riesgos en funcionamiento.

SCA

Identifica vulnerabilidades y riesgos en dependencias y componentes open source. Controla la cadena de suministro de software.

Application Risk Management / ASPM

Centraliza hallazgos y contexto para entregar una visión consolidada del riesgo y mejorar la priorización.

Remediación asistida

Entrega apoyo para acelerar la corrección de vulnerabilidades y reducir la carga manual del desarrollador.

Cobertura cloud-native

Extiende el análisis a contenedores, infraestructura como código, secretos y otros elementos de entornos modernos.

Ridge Security

RidgeBot

Plataforma automatizada de seguridad ofensiva que permite descubrir, intentar explotar de forma controlada y validar vulnerabilidades para determinar cuáles representan un riesgo real. Automatiza actividades del penetration testing y permite realizar pruebas con mayor frecuencia sobre redes, sistemas, aplicaciones y APIs. Especialmente relevante para organizaciones que necesitan pasar de "tenemos vulnerabilidades" a "sabemos cuáles realmente pueden explotarse".

¿Qué problemas resuelve?

- **Pentesting demasiado esporádico** Las evaluaciones una o dos veces al año entregan una fotografía puntual. RidgeBot permite repetir pruebas con mayor frecuencia para reducir periodos sin validación.
- **Vulnerabilidades que nunca se validan** Los scanners generan muchos hallazgos potenciales. RidgeBot intenta explotarlos de forma controlada para demostrar cuáles representan una exposición real.
- **Falta de especialistas en seguridad ofensiva** Las pruebas manuales requieren perfiles especializados y consumen tiempo. RidgeBot automatiza reconocimiento, análisis y validación ofensiva.
- **Dificultad para identificar rutas de ataque** Una vulnerabilidad aislada no siempre muestra cómo podría avanzar un atacante. RidgeBot evidencia cadenas de ataque y escenarios de movimiento lateral.
- **APIs y aplicaciones sin validación ofensiva** Las APIs amplían la superficie de ataque. RidgeBot permite incorporar pruebas ofensivas específicas sobre estos activos.

Principales capacidades

Automated Pen Testing

Automatiza reconocimiento, análisis y explotación controlada de vulnerabilidades.

Validación real

Comprueba si un hallazgo puede explotarse en el ambiente concreto del cliente.

Pruebas recurrentes

Permite repetir validaciones con mayor frecuencia hacia un modelo continuo.

Cadenas de ataque

Documenta pasos y rutas utilizados para facilitar comprensión del riesgo.

API y apps web

Evalúa APIs y aplicaciones frente a escenarios ofensivos y vulnerabilidades de referencia.

Adversary Emulation

Simula técnicas de adversarios para observar la capacidad de los controles defensivos.

Appgate

Zero Trust Network Access

Appgate ZTNA controla el acceso a aplicaciones y recursos basándose en identidad, dispositivo y contexto, sustituyendo el modelo tradicional de acceso amplio a la red por conexiones específicas hacia los recursos autorizados. Aplica principios Zero Trust para reducir exposición y limitar movimientos innecesarios dentro de la infraestructura. Especialmente relevante para trabajo remoto, acceso de terceros, infraestructura híbrida y organizaciones que buscan reducir su dependencia de VPN tradicionales.

¿Qué problemas resuelve?

- **VPN con acceso excesivo** Permite otorgar acceso específico a los recursos que cada identidad realmente necesita.
- **Usuarios remotos y distribuidos** Aplica políticas de acceso consistentes independientemente de la ubicación.
- **Acceso de proveedores y terceros** Limita el acceso a aplicaciones y recursos autorizados, evitando conectividad excesiva.
- **Infraestructura híbrida** Permite aplicar políticas sobre recursos distribuidos en distintos ambientes.
- **Exposición innecesaria** Reduce la exposición mediante un modelo de acceso oculto y controlado.

Principales capacidades

Políticas basadas en identidad

El acceso se determina por identidad, dispositivo y contexto, no solo por ubicación de red.

Acceso de mínimo privilegio

Entrega conexión únicamente hacia aplicaciones o recursos autorizados.

Direct Routing

Conexiones directas hacia recursos autorizados, sin desviar todo el tráfico por un punto central.

Infraestructura oculta

Los recursos permanecen invisibles hasta que el usuario y su contexto son validados.

Políticas adaptativas

Utiliza señales de contexto para ajustar dinámicamente las decisiones de acceso.

Acceso para usuarios y workloads

El modelo se extiende más allá de usuarios humanos hacia dispositivos y cargas de trabajo.

GoTo / LogMeIn Resolve

Administración y Soporte TI

Plataforma integrada de administración y soporte de TI que combina soporte remoto, Remote Monitoring & Management, automatización, helpdesk, administración de activos y gestión de endpoints. Orientada a equipos TI y MSP que administran usuarios y dispositivos distribuidos y buscan reducir la cantidad de herramientas necesarias. Especialmente útil en ambientes híbridos, fuerzas de trabajo remotas y organizaciones con alto volumen de soporte.

¿Qué problemas resuelve?

- **Soporte remoto lento o fragmentado** Centraliza funciones de asistencia y control remoto independientemente de dónde esté el usuario.
- **Falta de visibilidad sobre endpoints** RMM permite monitorear equipos distribuidos y conocer su estado.
- **Tareas operativas manuales** Permite ejecutar instalaciones, actualizaciones y automatizaciones de manera remota.
- **Helpdesk y administración separados** Integra soporte, ticketing, RMM y activos en una sola consola.
- **Fuerza laboral distribuida** Centraliza administración de Windows, macOS y dispositivos móviles.

Principales capacidades

Remote Support

Visualiza, diagnostica y controla remotamente los dispositivos que requieren asistencia.

RMM

Supervisa endpoints, genera alertas y ejecuta tareas administrativas sobre equipos distribuidos.

Remote Execution y automatización

Instala software y despliega acciones en múltiples equipos sin intervenir uno por uno.

Helpdesk y ticketing

Integra la gestión de solicitudes e incidentes con las capacidades de soporte y administración.

Asset Management

Centraliza información de los dispositivos administrados para mejorar inventario y operación.

MDM y administración de apps

Permite administrar dispositivos móviles y desplegar o configurar aplicaciones según la edición.

LastPass Business

Gestión de Contraseñas Empresariales

LastPass Business permite centralizar, proteger y administrar las contraseñas utilizadas por empleados y equipos empresariales. Proporciona bóvedas cifradas, generación y autocompletado de contraseñas, uso compartido controlado, políticas administrativas e integraciones con directorios. Especialmente útil cuando las organizaciones todavía dependen ampliamente de contraseñas y necesitan reducir malas prácticas como reutilización, almacenamiento inseguro o uso compartido informal.

¿Qué problemas resuelve?

- **Contraseñas débiles o reutilizadas** Los usuarios tienden a reutilizar credenciales porque deben recordar muchas. LastPass permite generar y almacenar credenciales diferentes y robustas.
- **Contraseñas en planillas o documentos** Estas prácticas dificultan aplicar políticas corporativas. LastPass centraliza las credenciales en bóvedas empresariales cifradas.
- **Contraseñas compartidas entre empleados** Equipos que necesitan una misma cuenta pueden terminar enviando la contraseña directamente. LastPass permite compartir accesos de forma controlada.
- **Poca visibilidad de TI** Sin herramienta corporativa, TI no sabe si los usuarios emplean credenciales inseguras. LastPass incorpora administración y políticas centralizadas.
- **Procesos manuales de alta y baja** Las integraciones con directorios ayudan a simplificar el ciclo de vida de usuarios y retirar accesos eficientemente.

Principales capacidades

Bóveda cifrada

Repositorio empresarial para crear, almacenar y utilizar credenciales de forma controlada.

Generador y autocompletado

Permite usar contraseñas complejas sin obligar al usuario a memorizarlas.

Uso compartido controlado

Comparte credenciales entre equipos mediante carpetas y permisos administrativos.

Administración centralizada

TI administra usuarios, grupos y políticas desde una consola central.

Integraciones con directorios

Facilita altas, bajas y ciclo de vida mediante conexión con proveedores de identidad.

MFA, SSO y más

La oferta empresarial puede complementarse con autenticación multifactor, SSO y otras funciones de identidad.

AlgoSec

Gestión de Seguridad de Red

Plataforma de gestión de seguridad de red centrada en las aplicaciones, diseñada para administrar conectividad y políticas a través de ambientes on-premise, cloud y redes híbridas. Permite descubrir dependencias de aplicaciones, visualizar flujos, analizar riesgos, automatizar cambios de políticas y mantener evidencia de cumplimiento. Especialmente adecuada para organizaciones con múltiples firewalls, tecnologías de red, ambientes multi-cloud y procesos frecuentes de cambios de conectividad.

¿Qué problemas resuelve?

- **Reglas de firewall demasiado complejas** Años de cambios producen reglas redundantes y riesgos. AlgoSec entrega visibilidad y contexto sobre esas políticas.
- **Cambios de red lentos y manuales** Solicitudes para abrir puertos pueden tardar días. AlgoSec automatiza el flujo de cambios y su análisis de riesgo.
- **Sin relación entre reglas y aplicaciones** AlgoSec ayuda a mapear qué servicio de negocio depende de cada regla.
- **Riesgo de indisponibilidad por cambios** Permite analizar impacto antes de implementar modificaciones.
- **Auditorías difíciles de mantener** Ayuda a mantener monitoreo, evidencia y reportes de cumplimiento.

Principales capacidades

Visibilidad application-centric

Relaciona aplicaciones de negocio con sus reglas y flujos de red para dar contexto a la conectividad.

Descubrimiento y mapeo

Identifica dependencias y flujos para crear una visión actualizada de la conectividad requerida.

Security Policy Management

Analiza políticas de firewall para identificar riesgos, reglas innecesarias y oportunidades de optimización.

Automatización de cambios

Automatiza desde la solicitud y análisis de riesgo hasta la implementación y validación del cambio.

Cobertura híbrida y multivendor

Gestiona políticas a través de data center, cloud, SDN y distintos fabricantes.

Riesgo y cumplimiento continuo

Evalúa políticas frente a requerimientos regulatorios y genera evidencia para auditoría.

Hacknoid

Gestión Continua de Vulnerabilidades

Plataforma de gestión continua de vulnerabilidades que descubre activos, mantiene un inventario actualizado, analiza de forma recurrente la superficie tecnológica y prioriza los hallazgos para ayudar a los equipos a concentrarse en los riesgos más importantes. Funciona con arquitectura sin agentes y puede desplegarse en ambientes on-premise, cloud o híbridos. Especialmente adecuada para organizaciones que buscan visibilidad continua de activos y vulnerabilidades con una operación simplificada.

¿Qué problemas resuelve?

- **Activos que TI no sabe que existen** Hacknoid descubre automáticamente dispositivos, cloud, IoT y otros componentes fuera de inventarios manuales.
- **Evaluaciones demasiado espaciadas** Un análisis puntual pierde vigencia rápidamente. Hacknoid mantiene monitoreo y análisis recurrente.
- **Demasiados hallazgos sin priorización** Combina señales de riesgo y criticidad del activo para apoyar la priorización.
- **Herramientas demasiado complejas** Hacknoid pone énfasis en una operación centralizada y simplificada para equipos pequeños.
- **Dificultad para demostrar evolución** Genera reportes y estadísticas para seguir la evolución del tratamiento del backlog.

Principales capacidades

Evaluación continua

Automatiza el monitoreo y análisis recurrente de la infraestructura.

Descubrimiento automático de activos

Mantiene inventario de dispositivos y sistemas presentes en el ambiente.

Arquitectura sin agentes

Reduce la necesidad de instalar software adicional en cada equipo para el descubrimiento y análisis.

Priorización contextual

Combina fuentes y métricas de vulnerabilidad con criticidad del activo para entregar prioridades accionables.

Dashboard centralizado

Consolida activos, vulnerabilidades, criticidad y evolución en una vista simplificada.

Reportes y seguimiento

Genera reportes de alertas, categorización, estado y evolución para operación y auditoría.

Ironchip

Identidad y Autenticación Contextual

Plataforma de identidad y autenticación orientada a reducir la dependencia de contraseñas y reforzar la verificación del usuario mediante factores contextuales, incluyendo señales de localización. Incorpora autenticación passwordless, protección anti-phishing, distintos métodos de autenticación e Identity Threat Detection & Response. Especialmente relevante para organizaciones que buscan modernizar MFA, proteger acceso remoto o de proveedores y reducir riesgos asociados al robo de credenciales.

¿Qué problemas resuelve?

- **Dependencia excesiva de contraseñas** Ironchip permite implementar modelos passwordless y reducir la superficie asociada a credenciales tradicionales.
- **Phishing y robo de credenciales** Incorpora controles contextuales y mecanismos de autenticación reforzada.
- **MFA con demasiada fricción** Ofrece distintos métodos para adaptar la experiencia al escenario del usuario.
- **Accesos sospechosos que parecen legítimos** Utiliza contexto y comportamiento para detectar señales anómalas.
- **Acceso de proveedores y terceros** Permite reforzar estos accesos con políticas de identidad sin incrementar innecesariamente el riesgo.

Principales capacidades

Autenticación passwordless

Permite eliminar o reducir el uso de contraseñas tradicionales en determinados escenarios.

Inteligencia de localización

Utiliza contexto de ubicación como señal adicional para determinar la legitimidad del acceso.

Protección anti-phishing

Reduce el riesgo de que el usuario entregue sus credenciales a un servicio fraudulento.

ITDR

Supervisa actividad de identidad y ayuda a detectar patrones de acceso sospechosos.

Múltiples métodos de autenticación

Combina distintos factores y mecanismos según el nivel de riesgo y el caso de uso.

Integración de identidad y SSO

Se integra con aplicaciones y servicios corporativos para centralizar políticas y simplificar el acceso.

Teramind

Insider Risk y Prevención de Pérdida de Datos

Plataforma centrada en el comportamiento del usuario para gestionar insider risk, prevenir pérdida de información y entregar visibilidad detallada sobre cómo empleados, contratistas y terceros utilizan sistemas y datos corporativos. Combina User Activity Monitoring, DLP, analítica de comportamiento, reglas automáticas y evidencia forense de las sesiones. Especialmente útil cuando el riesgo proviene de actividades realizadas de manera accidental, negligente o maliciosa por personas que ya tienen acceso autorizado.

¿Qué problemas resuelve?

- **Fuga intencional de información** Un usuario autorizado puede copiar o transferir información que legítimamente puede visualizar. Teramind relaciona actividad con políticas de DLP y comportamiento.
- **Pérdidas de datos por errores** Las reglas permiten detectar o bloquear actividades no permitidas realizadas por equivocación.
- **Falta de visibilidad sobre usuarios con acceso sensible** Teramind permite registrar y analizar las acciones de perfiles con acceso a información crítica.
- **Dificultad para investigar incidentes internos** Incorpora actividad contextual y grabación de sesiones más allá de los logs.
- **Comportamientos anómalos difíciles de identificar** La analítica de comportamiento ayuda a detectar descargas masivas, cambios de conducta o accesos inusuales.

Principales capacidades

User Activity Monitoring

Visibilidad detallada sobre aplicaciones, sitios, archivos y otras actividades realizadas por los usuarios.

Data Loss Prevention — DLP

Políticas para detectar y controlar el movimiento de información sensible a través de distintos canales.

UEBA

Analiza comportamientos para identificar anomalías que puedan indicar riesgo interno o compromiso de una identidad.

Reglas y acciones automáticas

Genera alertas, bloquea actividades o ejecuta respuestas cuando se detectan condiciones de riesgo.

Grabación y análisis de sesiones

Conserva evidencia contextual de la actividad realizada para facilitar investigación y análisis forense.

Protección basada en contexto

Combina información del usuario, actividad y políticas para distinguir entre uso permitido, error y comportamiento malicioso.

Mapa de Marcas y Cross-Selling

DOMINIO	CATEGORÍA	MARCAS DE PRIMER ORDEN	CROSS-SELLING
Protección	Identity & Access Security	Segura OneSpan	Sophos XDR/MDR
Protección	Network & Hybrid Infrastructure Security	Sophos Network SonicWall Faronics	Segura Cymulate
Protección	Application Security & DevSecOps	Aikido Security	Segura OneSpan Cymulate
Gestión de Riesgo	Exposure Management & Continuous Validation	Vicarius Cymulate Action1 VectoraIQ	Aikido Security
Gestión de Riesgo	Data Security, Governance & Insider Risk	Kriptos Safetica	Segura Sophos XDR/MDR
Operaciones de Seguridad	Security Operations & XDR	Sophos XDR/MDR Taegis Seceon	Vicarius Segura Stellar Cyber Action1



SOCIO ESTRATÉGICO

CPNnet como Socio Estratégico para su Ciberseguridad

CPNnet no es solo un distribuidor: es un socio estratégico en ciberseguridad que acompaña a cada organización desde la identificación de sus principales riesgos y necesidades, hasta la selección, implementación y evolución de las soluciones que mejor se ajustan a su entorno.

01

Conocimiento Técnico

Soporte especializado para cada marca del portafolio.

02

Generación de Demanda

Herramientas y recursos para abrir oportunidades con clientes finales.

03

Presencia Regional

Operaciones en Colombia, Perú y toda Latinoamérica.

Juntos Construimos el Futuro de la Ciberseguridad en Latinoamérica

CPNnet lleva más de 18 años acompañando a canales, integradores y fabricantes con un portafolio especializado, conocimiento profundo y compromiso permanente con el éxito de sus partners.

¿Listo para fortalecer su estrategia de ciberseguridad?
Conozca cómo las soluciones de CPNnet pueden ayudar a proteger sus activos, reducir la exposición y mejorar su capacidad de respuesta frente a las amenazas.



[◀ Volver](#)