Portfolio de Tecnologías

Newtec

Observabilidad & Protección de redes IT

SUPPORTED BY

CABO NORTE S.A.

POWERED BY

Techenabler

we sell, we connect, we integrate

Newtec
Observabilidad & Protección de redes IT

Respaldo Tecnológico de Newtec

Techenabler
we sell, we connect, we integrate

EL SOCIO PERFECTO PARA TU RESPALDO TENCOLÓGICO Y SEGURIDAD WEB

Experiencia, tecnología y producción todo el tiempo garantizandote redes más seguras , inteligentes y siempre disponibles.

¿QUÉ ES TECHENABLER?

TechEnabler es una empresa brasileña, que cuenta con ingenieros con más de 25 años de experiencia en telecomunicaciones y en TI, especializada en la integración de tecnologías, con foco en observabilidad de redes, ciberseguridad y gestión de dispositivos.

Opera como MSSP (Managed Security Services Provider), diseñando, integrando y operando soluciones tecnológicas de clase mundial para operadores de telecomunicaciones y empresas.

PORQÚE TECHENABLER ES ESTRATÉGICO

EXPERIENCIA COMPROBADA
Trajectoria sólida en proyectos críticos en América Latina

OPERACIONES LAS 24 HS
Operaciones 24x7 con SOC especializado

FOCO EN LOS RESULTADOS
Soluciones que reducen costos y aumentan la eficiencia

UN MODELO FLEXIBLE, PERFECTO PARA ESCALAR

CAPEX I OPEX I Híbrido
Permitiendo escalar desde operaciones pequeñas hasta infraestructuras de gran alcance.

Pago por capacidad
Utilizado con total previsibilidad.

White - Lebel
Permite a partners como Newtec comercializar los servicios bajo su propia marca, generando nuevas fuentes de ingresos.

CAPACIDADES QUE HACEN LA DIFERENCIA

OPERACIONES 24X7
Operaciones 24x7 con monitoreo contínuo los 365 días del año.

GENERACIÓN DE VALOR
Optimización de costos, incremento de ingresos y eficiencia operativa.

MODELO MSSP
Servicios gestionados bajo las mejores tecnologías como el modelo MSSP.

SOLUCIONES PARA DIFERENTES ESCENARIOS

OPERADORAS E ISPs
continuidad y alto rendimiento

PROVEEDORES CLOUD
generación de nuevos ingresos

REDES CORPORATIVAS
escalabilidad y confiabilidad

RTI CORPORATIVA
monitoreo, aplicaciones e implementación

UNA TRAYECTORIA DE CRECIMIENTO CONTÍNUO

- **2020** — Fundación como integrador tecnológico
- **2021** — Incorporación de AIOps
- **2022** — Evolución hacia observabilidad
- **2023** — Transformación en MSSP y servicios DDoS
- **2024** — Expansión en América Latina
- **2025** — Servicios cloud y crecimiento regional

NEWTEC + TECHENABLER

EJECUCIÓN LOCAL, RESPALDO INTERNACIONAL

Newtec + TechEnabler combinan ejecución local con respaldo internacional, ofreciendo soluciones tecnológicas de clase mundial con soporte continuo.

Newtec

Observabilidad & Protección de redes IT

¿Quienes somos?

CABONORTE S.A. (Uruguay) es una empresa nacional con sede en Montevideo, constituida el 19 de noviembre de 1996, con más de 30 años de trayectoria en el sector de las telecomunicaciones. Se especializa en la instalación de redes de comunicación, despliegue de fibra óptica y mantenimiento de infraestructura de antenas, brindando soluciones y suministros a empresas multinacionales y organismos estatales bajo la modalidad de proyectos llave en mano (turn-key).

Un poco de nuestro recorrido

En 2025 ampliamos nuestro alcance estratégico incorporando una división especializada en soluciones de software, con foco en seguridad, gestión y observabilidad de infraestructuras IT, fortaleciendo nuestra propuesta de valor en entornos tecnológicos de alta criticidad. Contamos con infraestructura propia, personal técnico altamente calificado y la experiencia necesaria para ejecutar proyectos integrales de forma eficiente, acompañando a nuestros clientes en todas las etapas del proceso: desde la elaboración de la propuesta técnica y comercial hasta la implementación, puesta en marcha y recepción final de las obras y servicios.

A lo largo de estos años, hemos trabajado con las principales compañías del rubro en Uruguay, tales como Ericsson, ZTE, Nokia, Telefónica y Huawei, así como con organismos estatales como ANTEL, UTE y OSE.

En particular, destacamos nuestra participación en proyectos de gran envergadura, como la infraestructura de comunicaciones del edificio ANTEL Arena y, más recientemente, la adjudicación por parte de ANTEL para la provisión de terminales ONTmarca ZTE durante los años 2024 y 2025, destinadas a su instalación en hogares de todo el país.

Plataformas
Powered by Techenabler

Recientemente, y en línea con nuestra visión de innovación tecnológica y eficiencia operativa, ponemos a disposición de nuestros clientes un portafolio de soluciones de clase mundial orientadas a la gestión, protección y optimización de infraestructuras tecnológicas, a través de nuestra alianza estratégica como Partner Premier de Techenabler en Uruguay.

En el marco de esta alianza estratégica, mediante su nueva división NEWTEC | Observabilidad y Protección de Redes IT, Cabonorte integra y ofrece herramientas avanzadas de análisis, observabilidad, gestión y protección de redes y datos, conformando un ecosistema tecnológico robusto, escalable y adaptable a las necesidades específicas de cada organización.

Este conjunto de soluciones está diseñado para optimizar la operación, fortalecer la seguridad y garantizar la continuidad de los servicios críticos, aportando visibilidad en tiempo real y capacidad de respuesta ante entornos cada vez más dinámicos y exigentes.

kentik · new relic · corero [THE DDoS PROTECTION SPECIALISTS]

PLANISYS • CYBERSECURITY • · NEXUSGUARD® DDoS Protection Made Simple

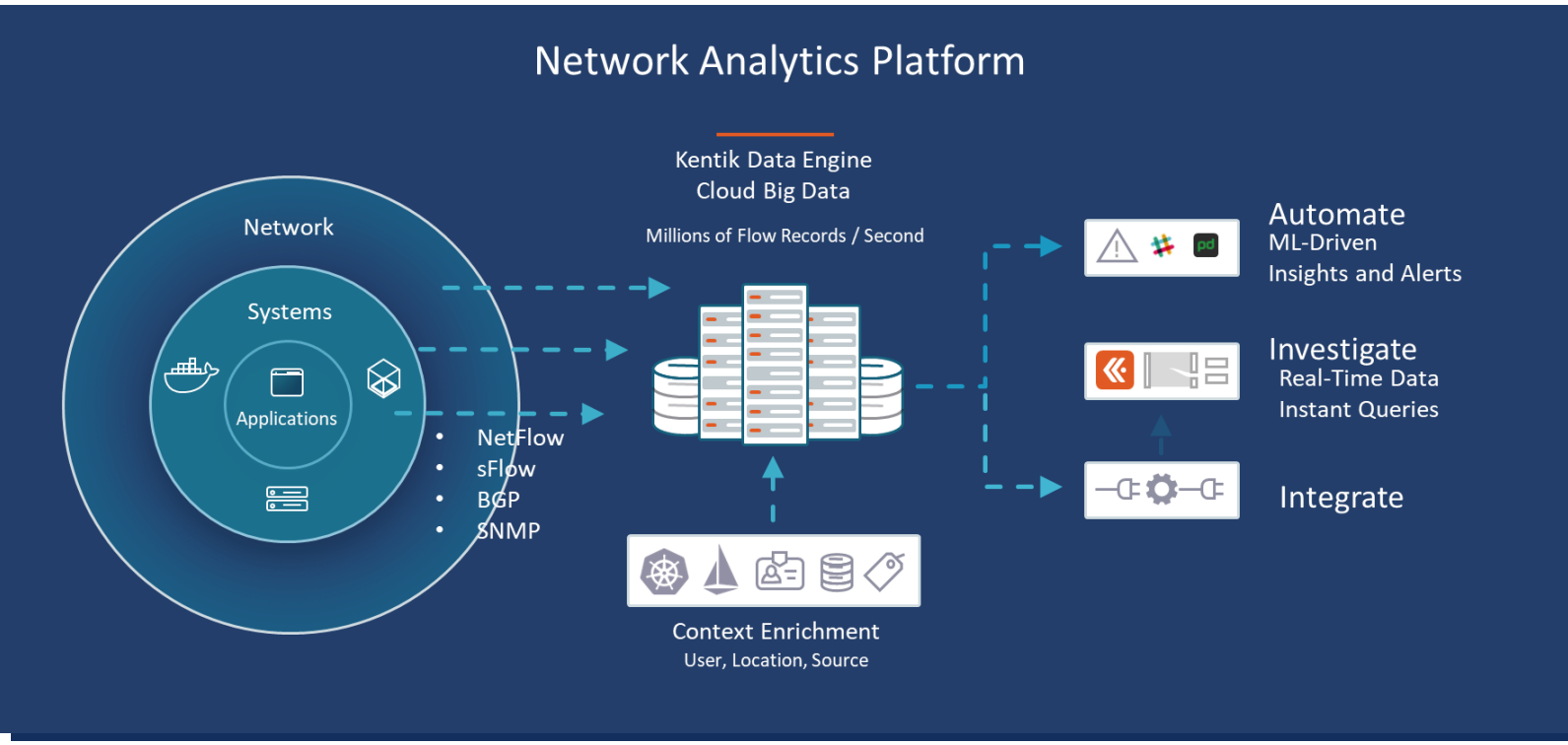
kentik

OBSERVABILIDAD DE RED UNIFICADA

¿Qué es?

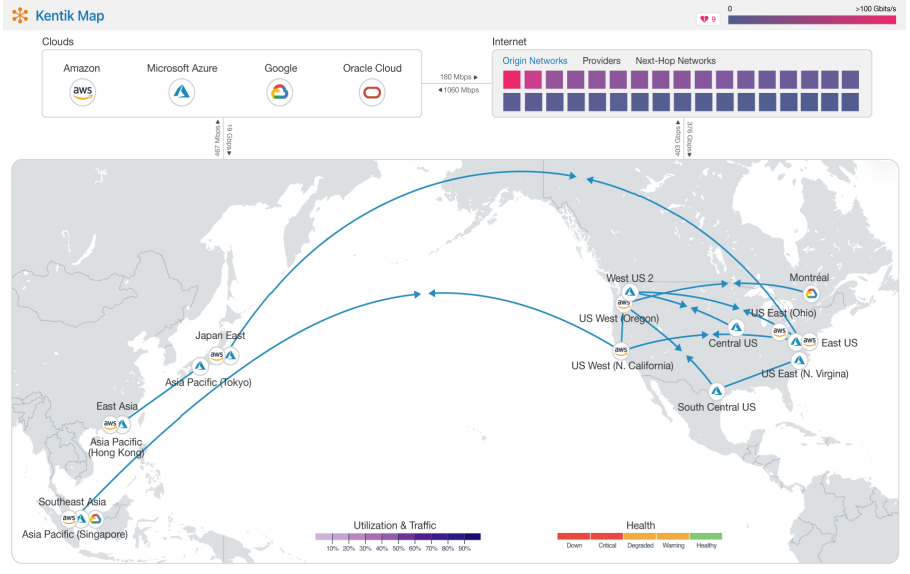
Kentik es una plataforma SaaS que ofrece múltiples servicios dentro de los cuales se destacan algunos como el monitoreo global de internet y la experiencia digital, el monitoreo de red, la optimización de la red en la nube y análisis forence digital de seguridad (DDoS) entre otros.

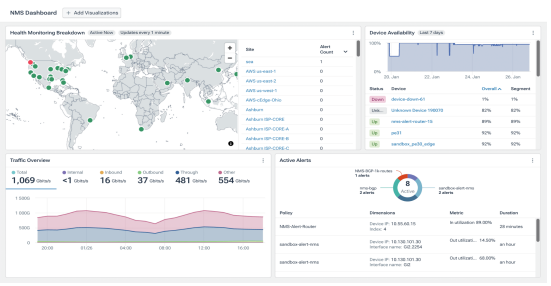
¿Cómo funciona?

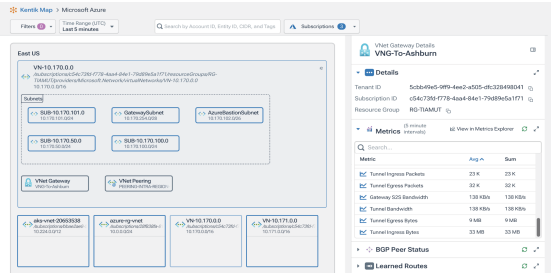


¿Qué ofrecemos?

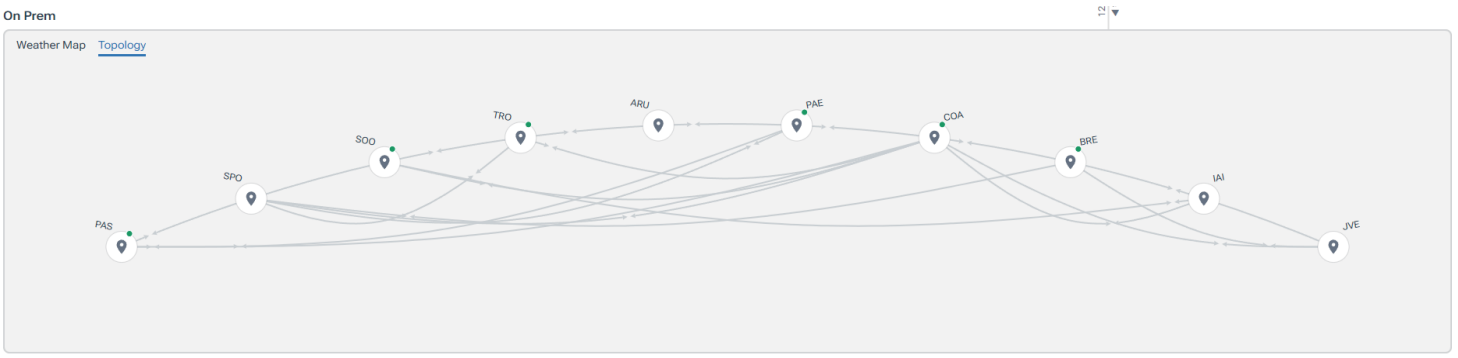
Una vista de todas las redes que te interesen



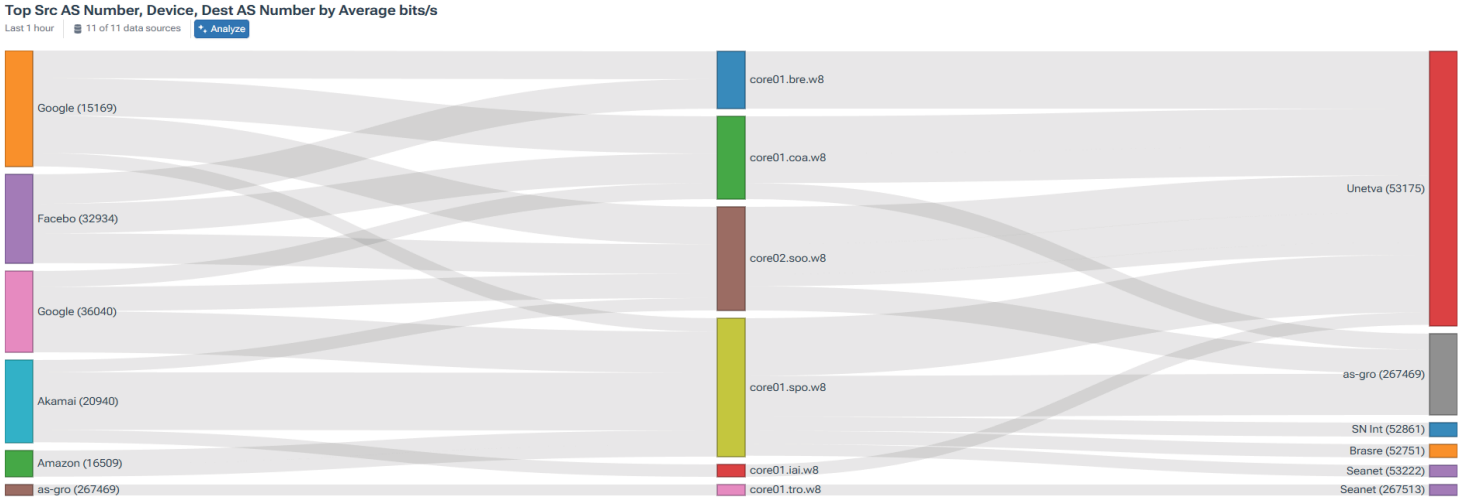




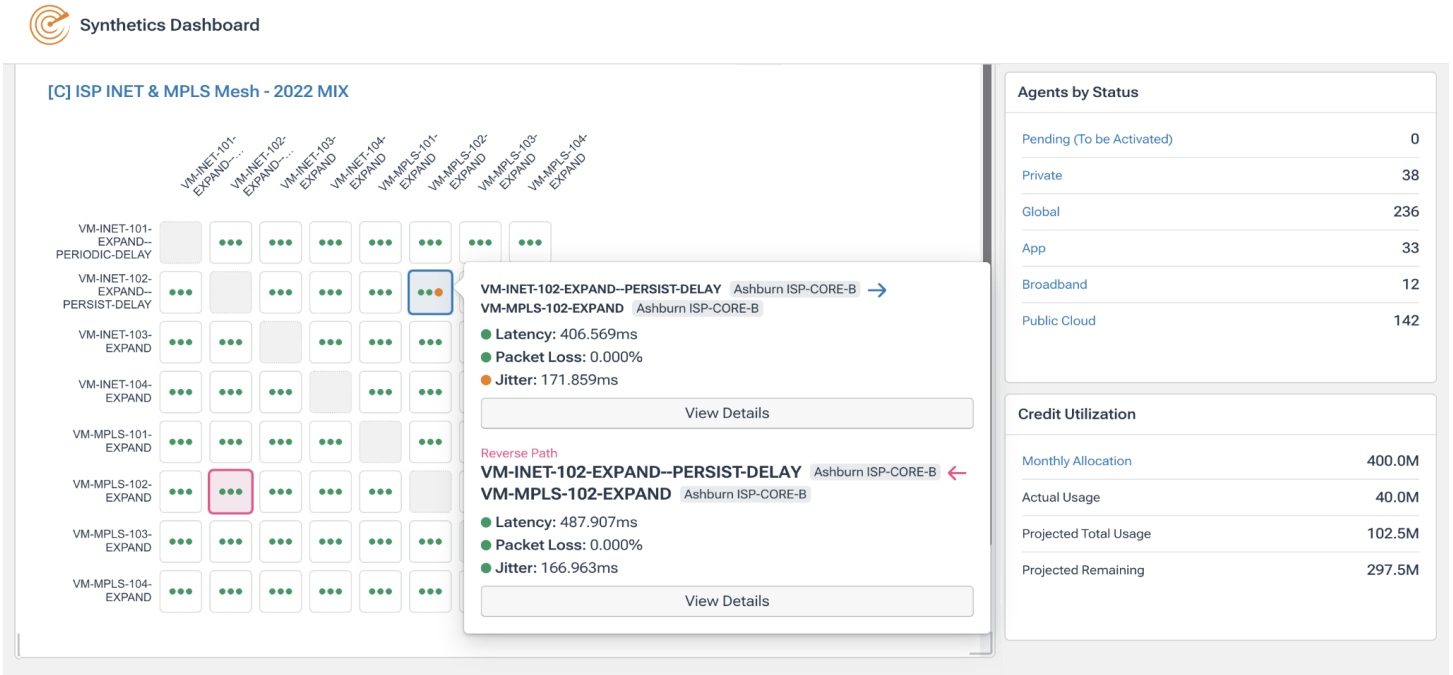
Vista integrada de red y topología



Vista integrada de tráfico y redes



Control de la experiencia digital – IA



new relic

OBSERVABILIDAD FULL STACK (UX)

¿Qué es?

Una solución integral de observabilidad Full Stack que permite monitorear y analizar en tiempo real todas las capas críticas del entorno digital, incluyendo infraestructura, web, aplicaciones y APIs. Está diseñada para optimizar el rendimiento, anticipar incidentes y garantizar una experiencia de usuario (UX) eficiente, confiable y de alta calidad.

¿Cómo funciona?

La plataforma recopila cuatro tipos fundamentales de datos:

- **Métricas** (Rendimiento, capacidad y saturación)
- **Eventos** (cambios,despliegues,incidentes)
- **Registros** (registros detallados de sistemas y aplicaciones)
- **Traces** (seguimiento de transacciones de extremo a extremo).

Lo que ofrece

Instrumentos, Aplicaciones y Servicios (APM)

El Monitoreo del Rendimiento de Aplicaciones (APM) es uno de los pilares de New Relic.

- Automáticamente instrumenta aplicaciones
- Mide el tiempo de respuesta, el rendimiento y los errores.
- Identifica cuellos de botella en código, bases de datos y dependencias.
- Crea trazas distribuidas de extremo a extremo.
- Muestra la topología real entre servicios.

Resultado: el equipo sabe dónde está el problema, por qué ocurrió y qué servicio tuvo impacto.

Monitoreo de la infraestructura y la nube

New Relic monitorea:

- Servidores físicos y virtuales
- Contenedores y Kubernetes
- Servicios en la nube (AWS, Azure, GCP)
- Entornos híbridos y multinube

Colecciona:

- CPU, memoria, disco, red
- Salud de clústeres y cargas de trabajo
- Eventos y cambios en la configuración

Resultado: la infraestructura ya no es invisible en la resolución de problemas.

Mide la experiencia real del usuario (Web y móvil)

La plataforma recoge datos reales de uso, no solo pruebas sintéticas.

Mide:

- Tiempo de carga de la página
- Latencia percibida por el usuario
- Errores en el navegador y en las aplicaciones móviles
- Rendimiento por región, dispositivo y navegador
- Viaje del usuario y embudos reales

Resultado: correlación directa entre la experiencia del cliente y el back-end.

Correlaciona todos los datos del sistema en un entorno integrado, evitando silos de información

New Relic trata los troncos como parte del flujo, no como un silo.

Te permite:

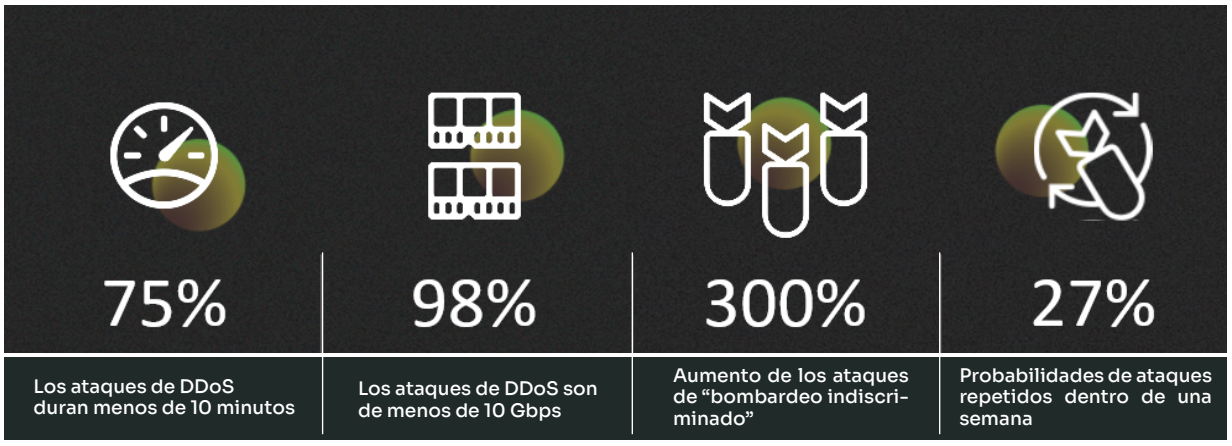
- Recopilar registros de aplicaciones, infraestructura y nube
- Registros de consulta en el contexto de: un error, una transacción o un servicio

[THE DDoS PROTECTION SPECIALISTS]

PROTECCIÓN ANTI DDOS

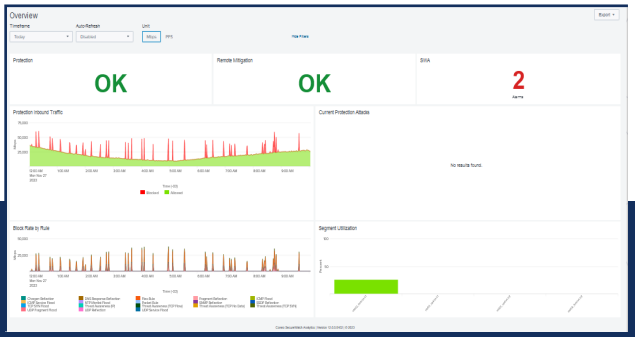
¿Qué es?

DDoS (Distributed Denial of Service) es un ciberataque que tiene como objetivo dejar de utilizar un servicio sobrecargándolo con tráfico malicioso que puede llegar a Giga o Tera Bps. Este ciberataque puede generar impactos de diferentes índoles como, pérdida significativa de ingresos, daño a la reputación de la marca, o impacto de la experiencia del cliente entre otros. Corero cumple la función de contrarrestar este ciberataque brindándote seguridad.



Lo que ofrece

La composición de soluciones usando Kentik y Corero detectan y mitigan ataques DDoS volumétricos, de protocolo y de aplicaciones en tiempo real, preservando la disponibilidad del servicio con respuesta automática y alta precisión. También destacan por su operación sencilla, visibilidad continua y despliegue flexible para diferentes entornos de red



corero

[THE DDoS PROTECTION SPECIALISTS]

PROTECCIÓN ANTI DDOS

¿Cómo funciona?

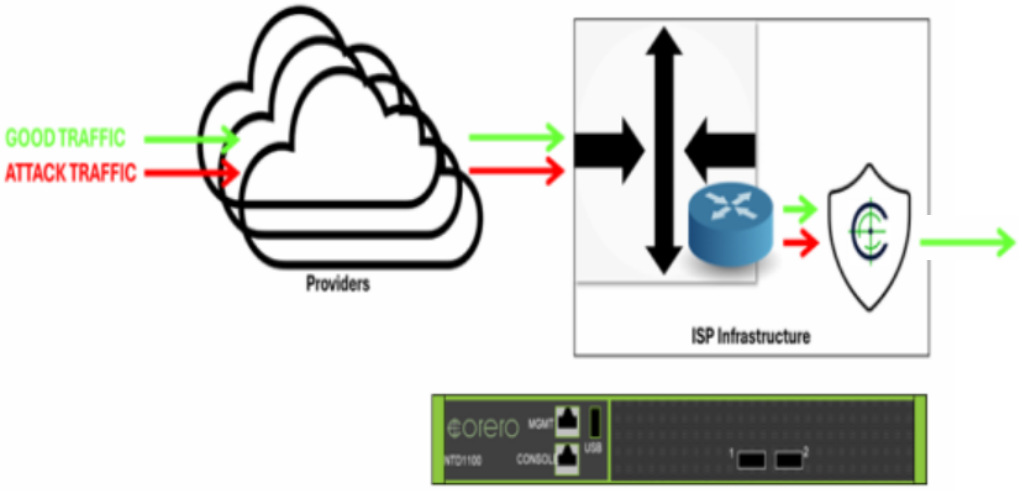
Diferencias entre un equipo instalado localmente y un servicio contratado

Equipo instalado localmente y conectado al router

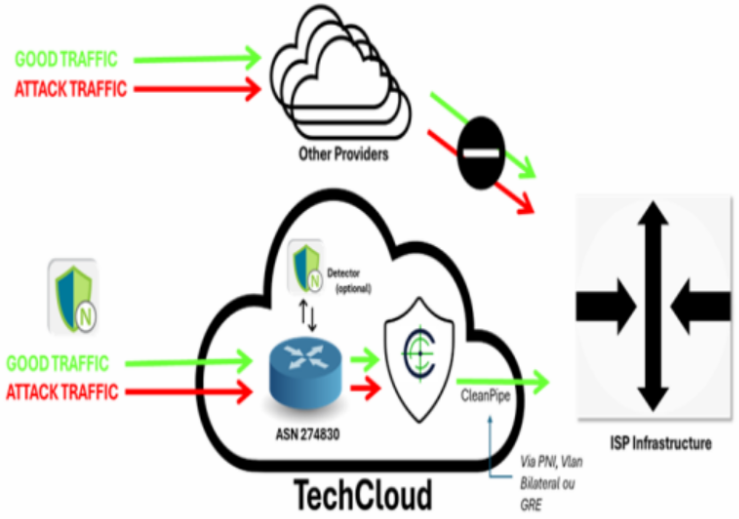
- Sin latencia añadida
- Protección en tiempo real
- No hay fugas para el cliente
- Sin anuncios BGP
- Necesita suficiente ancho de banda para manejar el ataque
- Puede causar congestión generalizada

Es un servicio contratado

- Añade latencia
- La detección y redirección tardan menos (unos segundos o minutos)
- Anuncio BGP: Cambio de conexión y cambio BGP_path
- No hacen falta puertos grandes ni
- contratos de ancho de banda elevado
- Protege toda tu infraestructura de los ataques



No se trata de ventajas o desventajas. Aquí tienes las características que mejor se adaptan a tu infraestructura. En algunos casos, se recomienda una solución combinada.



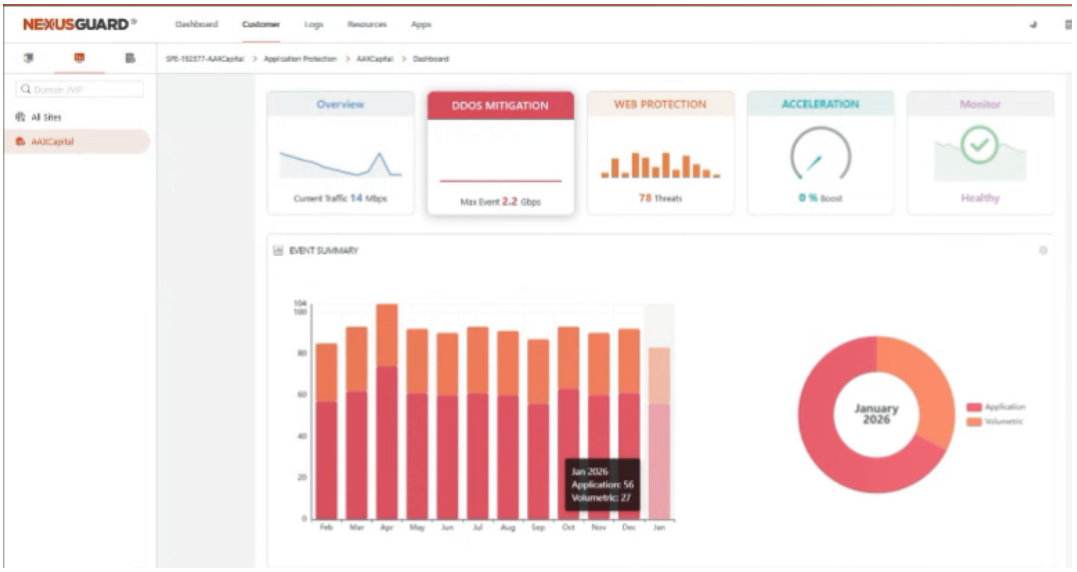
NEXUSGUARD®

PROTECCIÓN DE APLICACIONES Y WEBS

¿Qué es?

WebShield es la solución avanzada en la nube de Nexusguard, diseñada para proteger sitios web y APIs de amenazas de Capa 3 a 7 (a nivel de aplicación). Defiende contra ataques DDoS, bots maliciosos y abuso de API. No hace falta cambios en hardware local ni en infraestructura.

WAF (Firewall de Aplicaciones Web) es una solución de seguridad basada en la nube que protege sitios web, aplicaciones web y APIs de amenazas a nivel de aplicación, incluyendo las 10 principales: Vulnerabilidades de OWASP, ataques de día cero y bots maliciosos entre otros. Integrado con el servicio WebShield de Nexusguard, el WAF filtra, monitoriza y bloquea el tráfico HTTP/S malicioso antes de que llegue a tus servidores aplicación (sin afectar al rendimiento ni requerir hardware local).

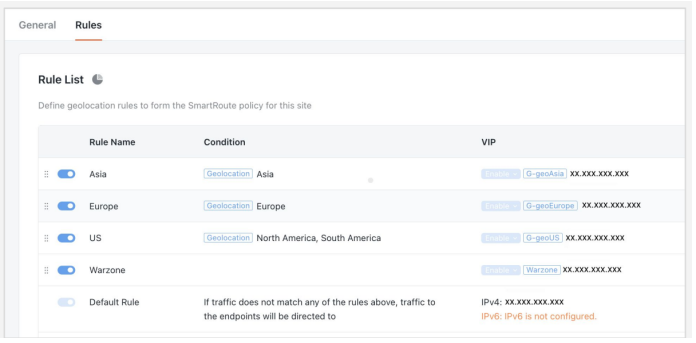


¿Cómo funciona?

WEB AND APPLICATION PROTECTION

WAF (Cortafuegos de aplicaciones web) Nexusguard es una solución de seguridad basada en la nube que protege sitios web, aplicaciones web y APIs de amenazas a nivel de aplicación, incluyendo las 10 principales Vulnerabilidades de OWASP, ataques de día cero y bots maliciosos.

Integrado con el servicio WebShield de Nexusguard, el WAF filtra, monitoriza y bloquea el tráfico HTTP/S malicioso antes de que llegue a tus servidores aplicación—sin afectar al rendimiento ni requerir hardware local.



NEXUSGUARD®

PROTECCIÓN DE APLICACIONES Y WEBS

WebShield

WAF

Lo que ofrece

Maximiza la experiencia del usuario y el rendimiento, incluso durante ataques DDoS.

- Mitiga eficazmente ataques cifrados con SSL mediante gestión segura de claves.
- Acelera la entrega de contenido de alto ancho de banda para clientes de todo el mundo, con Caché y aceleración de contenido.
- No requiere hardware ni instalación local.
- Disfruta de una visibilidad sin precedentes de tráfico de aplicaciones y amenazas en tiempo real.

PLANISYS
• CYBERSECURITY •

DNS SEGURO Y RPZ

Qué hacer si:

Mi empleado ya ha hecho clic en el enlace de PHISHING

No sé si mi red está infectada

Mis dispositivos IoT están infectados con malware

Mis empleados y clientes acceden a sitios web inapropiados

Mi red permite el acceso a destinos bloqueados por el gobierno

La cuestión no es qué...Pero, ¿dónde?

Protege tu SALIDA!

¿Qué es DNS Seguro y RPZ?

DNS SEGURO (PDNS-Protected DNS)
Es un marco compuesto por estándares y servicios que tienen como objetivo proteger el servicio de resolución de nombres frente a usos maliciosos y fallos, combinando redundancia, DNSSEC, registros bien controlados, monitoreo y filtrado de amenazas.

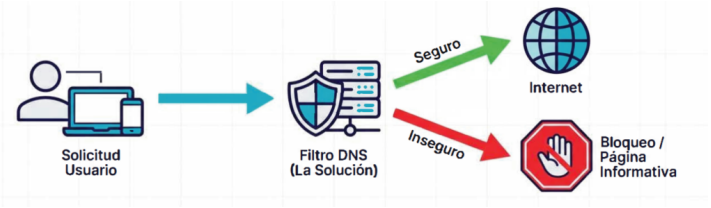
También forman parte de este concepto listas de dominios maliciosos, bloqueo de phishing/malware, prevención de exfiltración y políticas de acceso, que funcionan como una "primera línea" de defensa antes de conectar HTTP/HTTPS y RPZ.

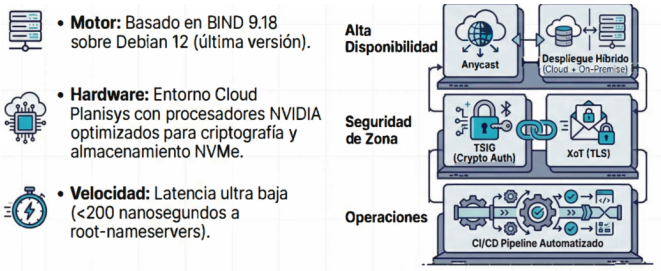
RPZ (Response Policy Zone)
RPZ es un mecanismo de cortafuegos a nivel DNS que permite al resolver modificar la respuesta DNS en función de las políticas bloqueando, redirigiendo o cambiando las respuestas a dominios presentes en listas o políticas definidas por el cliente.

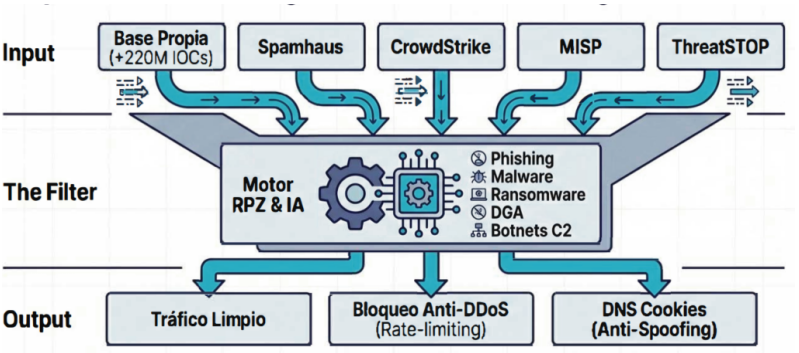
PLANISYS
• CYBERSECURITY •

DNS SEGURO Y RPZ

¿Cómo funciona?







¿Qué ofrece?

TechEnabler SMART DNS-RPZ
(Planysis –Inside)

SERVICIO DE SEGURIDAD CIBERNÉTICA EN IA
Suministro de protección para sus usuarios
y sus redes.

Para configuraciones: Solo se configuran los solucionadores DNS en el router o dispositivo. No es necesario instalar aplicaciones, agentes locales ni dispositivos.

PROTEGE:

- **USUARIOS**, desde hacer clic en enlaces en correos electrónicos peligrosos hasta virus que se ejecutan en sus dispositivos.
- **APPS**, ejecutadas en segundo plano.
- **DISPOSITIVOS IOT**, empezando por el tráfico "sucio", bloqueando destinos maliciosos.

Newtec

Observabilidad & Protección de redes IT

PROTECCIÓN AGNÓSTICA A MÚLTIPLES TECNOLOGÍAS

Newtec

Observabilidad & Protección de redes IT

Problemas solucionados

Servicio mejorado

Acelerador de caché DNS y protección proactiva basada en aprendizaje automático.

Dispositivos hackeados

Ataques desde dispositivos cliente hackeados (desde adentro hacia fuera).

IPs públicas en lista

Generan problemas de servicio y aumentan la carga de trabajo del soporte técnico, además del riesgo de perder direcciones de clientes que no tienen existencias.

Phishing

Los clientes son víctimas de phishing, ya sea haciendo clic en el correo electrónico o en sitios web "peligrosos".

Observabilidad y Experiencia Digital

Monitoreo integral de aplicaciones, servicios e infraestructura, identificando dónde ocurrió el problema y su impacto. Visibilidad completa de la infraestructura y la nube, facilitando la resolución de incidentes. Medición de la experiencia real del usuario (web y móvil) con correlación directa con el back-end.

Inteligencia y Análisis de Tráfico de Red

Análisis en tiempo real con visibilidad instantánea del tráfico de red y detección automática de anomalías y DDoS. Optimización del rendimiento mediante identificación de cuellos de botella y mejora de la calidad del servicio. Planificación de capacidad con modelos predictivos e integración sencilla con entornos híbridos, nubes y CDN.

Ciberseguridad preventiva con IA

Bloqueo de C2, Dark Web y ransomware.

Envío de SPAM

Uso por parte de los clientes al enviar SPAM, marketing por correo electrónico, facturas electrónicas, entre otros.

Restricciones de acceso

Los clientes corporativos/gubernamentales y las áreas públicas deben restringir el acceso a ciertos sitios web y tipos de contenido

Requisitos legales

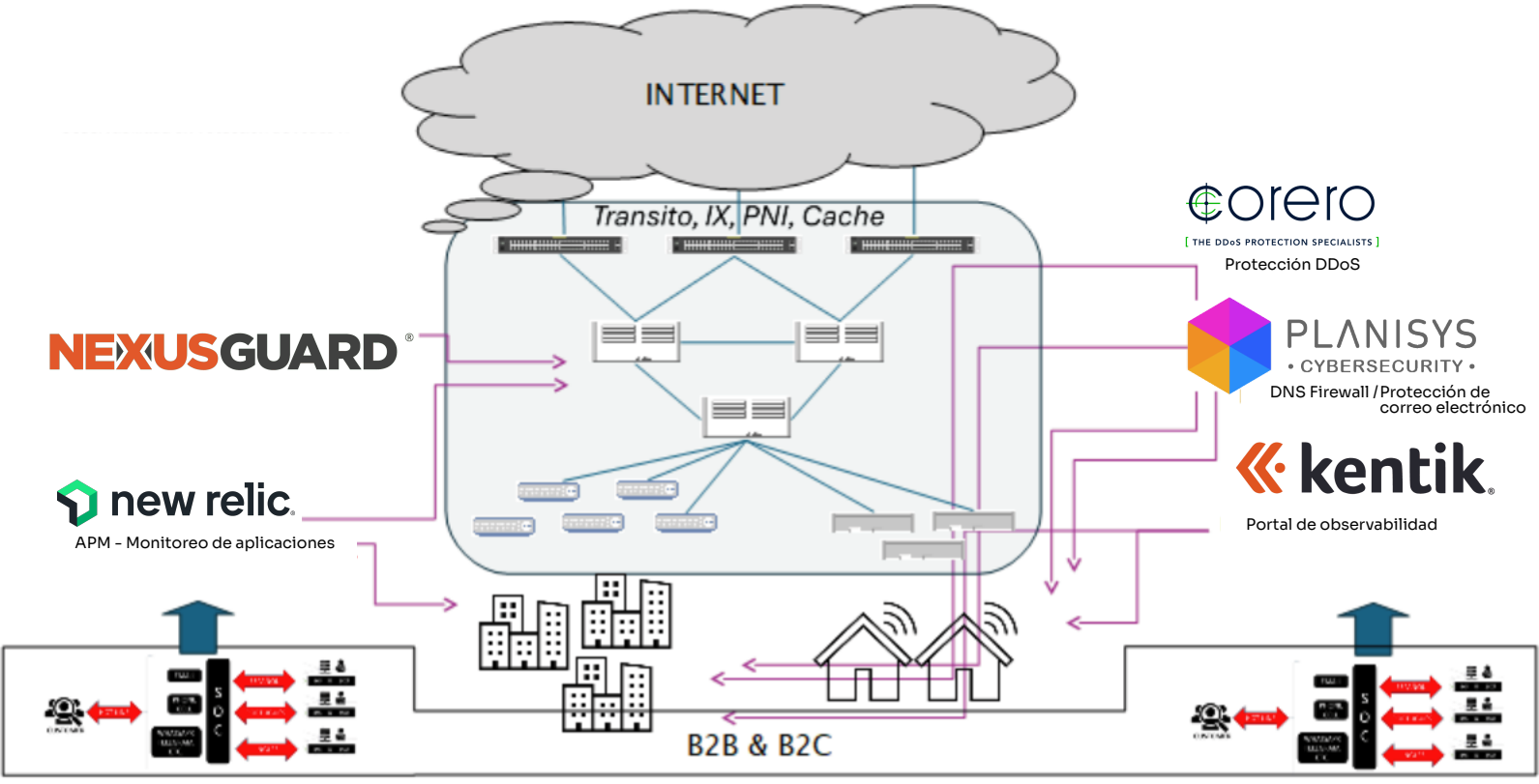
Obligación de cumplir con los requisitos legales y bloquear el acceso a sitios web prohibidos por la ley.

Protección DDoS en Tiempo Real

Mitigación instantánea de ataques DDoS con protección en línea siempre activa.
Alta precisión con baja latencia, garantizando continuidad del tráfico legítimo.
Visibilidad completa con reportes detallados e integración sencilla en entornos híbridos y multicloud.

Seguridad y Aceleración en la Nube

Mitigación efectiva de ataques cifrados (SSL) mediante gestión segura de claves. Aceleración de contenido con caché y optimización para alto rendimiento global. Visibilidad en tiempo real del tráfico y amenazas, sin necesidad de hardware ni instalación local.



POWERED BY TECHENABLER

Newtec

Observabilidad & Protección de redes IT

SUPPORTED BY

CABO NORTE S.A.

POWERED BY

Techenabler
we sell, we connect, we integrate