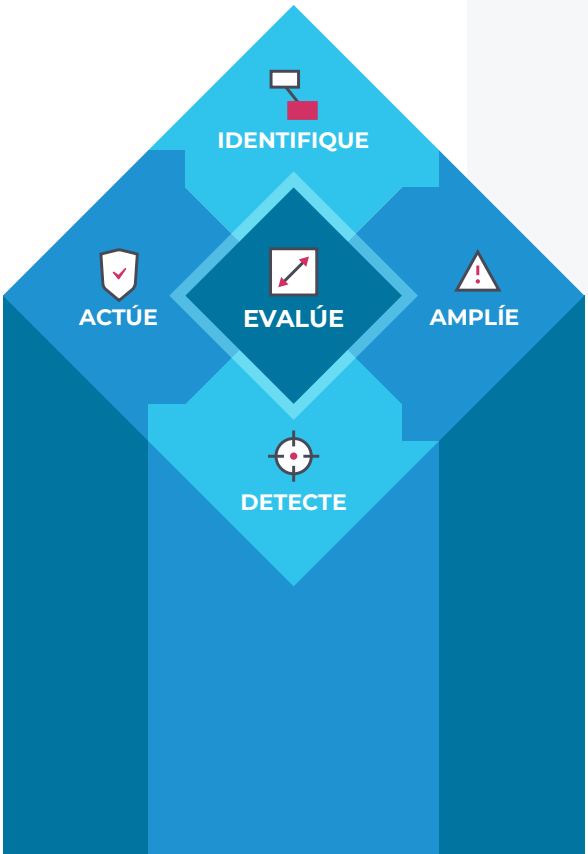
HOJA DE DATOS

Guardian

Seguridad y visibilidad de TO e IoT robustas para la industria

Nozomi Networks **Guardian**™ le otorga visibilidad para todos sus recursos de TO, IoT, TI, perimetrales y de nube, lo que le permite agilizar la seguridad y la transformación digital.

Guardian reduce los riesgos de TO para los sitios de mayores dimensiones destinados a la infraestructura crítica, energía, fabricación, minería, transporte y automatización de edificios, entre otros sitios de TO en todo el mundo.



Vea

Todos los comportamientos y recursos de TO e IoT en sus redes para obtener información única

Detecte

Amenazas, vulnerabilidades, riesgos y anomalías cibernéticos para una respuesta más rápida

Unifique

La seguridad, la visibilidad y la monitorización de todos sus recursos para una mayor resiliencia

Identifique

Detección de recursos y visualización de la red

Rastree automáticamente los recursos de TO e IoT

Inventario actualizado de recursos

Mejora la resiliencia cibernética y ahorra tiempo con el inventariado automático de recursos

Identifica todos los recursos en los que hay comunicaciones

Brinda información exhaustiva sobre los nodos, incluidos el nombre, tipo, número de serie, versión de firmware y componentes

Presenta información sobre riesgos, que incluye alertas de seguridad y confiabilidad, parches faltantes y vulnerabilidades

COMPLEMENTO

Smart Polling

Amplía la detección pasiva de recursos que se encuentra integrada en Guardian mediante el sondeo activo de bajo volumen. Consulte el sitio: **nozominetworks.com/smart-polling**

SUSCRIPCIÓN

Asset Intelligence

Acelera el proceso de aprendizaje en relación con los recursos y mantiene actualizados los datos de los comportamientos y los perfiles de los recursos. Consulte el sitio: **nozominetworks.com/asset-intelligence**

Conozca al instante sus propias redes

Menores riesgos mediante la visualización de la red

Brinda información instantánea de la red de TO e IoT y de sus patrones de actividad

Presenta datos claves, como el rendimiento del tráfico, las conexiones por TCP y los protocolos

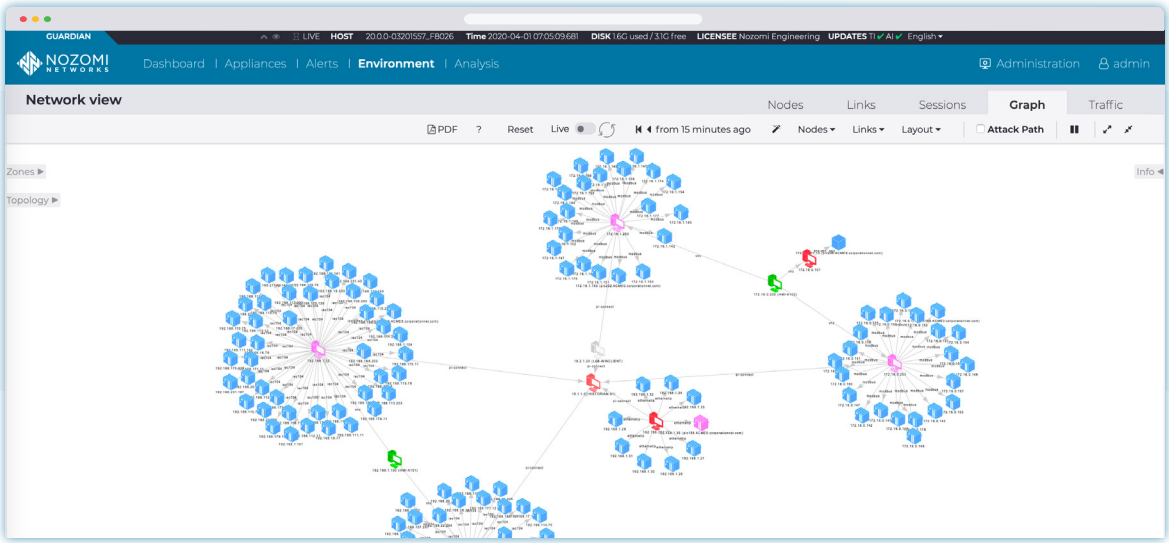
Permite conocer mejor las operaciones «normales»

Paneles e informes intuitivos

Explore las vistas de macros y consulte la información detallada acerca de los dispositivos terminales y las conexiones

Filtre por subredes, tipos, roles, zonas y topologías

Agrupe los recursos visualmente, en listas y en vistas detalladas de recursos individuales



Parte del **gráfico interactivo de visualización de red.**

Evalúe

Evaluación de vulnerabilidades y monitorización de riesgos

Identifique rápidamente los riesgos de vulnerabilidades

Evaluación automática de vulnerabilidades

Identifica los dispositivos de proveedores que son vulnerables

Utiliza la base de datos nacional de vulnerabilidades (National Vulnerability Database, NVD) del Gobierno de Estados Unidos para la asignación de nombres, descripciones y puntuaciones de acuerdo con los estándares correspondientes

Determinación de prioridades y reparación eficientes

Acelera la capacidad de respuesta mediante paneles de vulnerabilidades, análisis detallados e informes

Responde preguntas como las siguientes:

- «¿Mis recursos están ejecutando firmware vulnerable?»
- «¿Los recursos del proveedor X son vulnerables?»

Monitorice continuamente sus redes y sistemas de automatización

Monitorización continua

Monitoriza de forma continua todos los protocolos admitidos: TO, IoT y TI

Elimina los puntos ciegos de seguridad críticos derivados de una monitorización limitada o de protocolos inadecuados

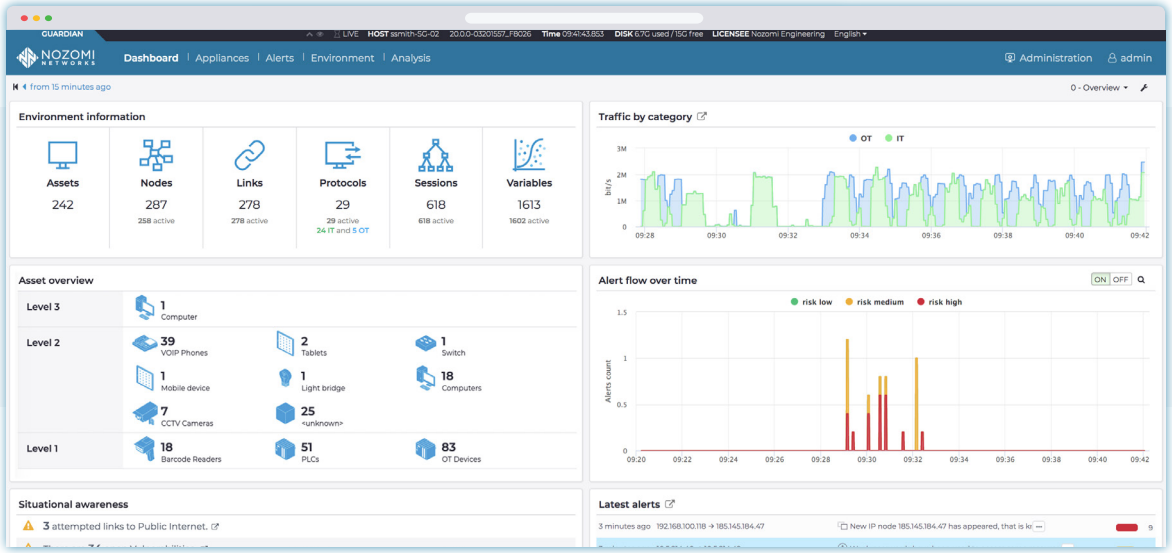
Monitoriza los recursos de todos los proveedores y todas las comunicaciones de red

Fácil acceso a los datos de TO

Resume la información sobre riesgos de TO e IoT para establecer rangos personalizados de fechas y horas

Destaca los indicadores de problemas de confiabilidad, como los valores de procesos inusuales

Inspecciona cualquier aspecto de la red o del rendimiento del sistema de control, lo que reduce la cantidad de datos recolectados y las tareas de las hojas de cálculo



Parte del **panel personalizable de Guardian**.

Detecte

Detección avanzada de anomalías y amenazas

Detecte e interrumpa al instante las amenazas y los comportamientos anómalos

Detección de amenazas con las últimas actualizaciones

Identifica amenazas relacionadas con la ciberseguridad y la confiabilidad de los procesos

Detecta amenazas avanzadas y riesgos cibernéticos tanto en las etapas iniciales como en las tardías

Bloquea ataques cuando se integra con productos de seguridad para dispositivos terminales y firewalls compatibles

La mejor detección de amenazas de TO e IoT

Combina la detección de anomalías basada en el comportamiento con la detección de amenazas basada en firmas para una monitorización exhaustiva de los riesgos

Proporciona información detallada de amenazas, como las reglas YARA, reglas de paquetes, indicadores de tipo STIX, definiciones de amenazas, una base de conocimientos de amenazas y firmas de vulnerabilidades

Monitorice de manera efectiva los entornos mixtos

SUSCRIPCIÓN

Threat Intelligence

Garantiza una detección de amenazas y una identificación de vulnerabilidades actualizadas mediante indicadores creados y seleccionados por Nozomi Networks Labs

Ofrece información continua sobre amenazas y vulnerabilidades de TO, IoT y TI

SUSCRIPCIÓN

Asset Intelligence

Impulsa una detección de anomalías precisa y de avanzada para TO e IoT que filtra las alertas sobre comportamientos benignos, lo que acelera la respuesta ante incidentes

Proporciona de manera continua datos de comportamiento y perfiles de recursos de TO e IoT

Detección de anomalías de avanzada para TO e IoT

Identificación rápida de recursos

Garantiza un inventario de recursos preciso

Alertas precisas de anomalías

Aceleran la respuesta ante incidentes

Asset Intelligence para redes dinámicas

Mantiene un inventario y una detección precisos

Actúe

Herramientas forenses y paneles que ahorran tiempo

Mejore considerablemente la gestión de riesgos de TO e IoT

Los paneles y los informes personalizables resaltan los riesgos

Se concentra en las preocupaciones más relevantes mediante el resumen de riesgos y amenazas

Los informes integrados son personalizables. Puede seleccionar entre widgets predefinidos para agregar exactamente la información que necesita

Las alertas detalladas brindan información clave

Genera alertas detalladas y precisas

Identifica riesgos de seguridad y confiabilidad

Agrupa las alertas por incidentes, proporcionándole al personal de seguridad y de operaciones una vista simple, clara y consolidada de lo que está sucediendo en la red

Reduzca en gran medida las tareas de resolución de problemas y de análisis forense

Rápida respuesta ante incidentes

Combina la detección de anomalías de avanzada para TO e IoT de Guardian con el servicio **Asset Intelligence™** para obtener alertas específicas y procesables

Comprende el comportamiento normal de los recursos cuyo comportamiento cambia con frecuencia, lo que elimina las alertas de anomalías benignas

Mejora el tiempo de respuesta y la productividad mediante alertas precisas que son fáciles de priorizar

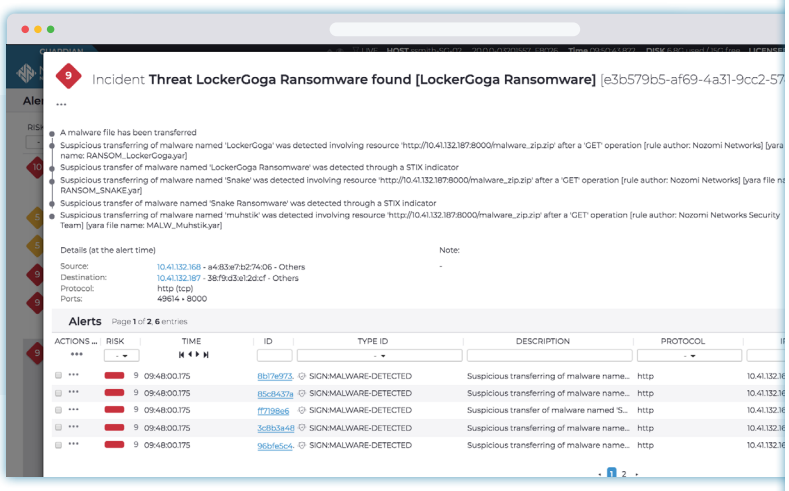
Análisis forense rápido

Centra los esfuerzos con Smart Incidents™, que:

- Correlaciona y consolida las alertas
- Proporciona un contexto operativo y de seguridad
- Suministra capturas automáticas de paquetes

Decodifica incidentes con Time Machine™ antes y después de las instantáneas del sistema

Proporciona respuestas rápidas con una poderosa herramienta de consultas *ad hoc*



Smart Incident muestra las alertas relacionadas y el contexto de seguridad.

Los informes resumen las alertas para un sitio en particular.

Ampliable

Seguridad unificada para cientos de miles de recursos

Fácilmente ampliable con un rendimiento óptimo

Rendimiento local y global de excelencia

Procesa datos para hasta 500,000 recursos en tiempo real

Genera visualizaciones de red, paneles e informes rápidamente

Acelera la detección de amenazas y la capacidad de respuesta mediante el procesamiento local de la información de amenazas y recursos

Monitorización consolidada de todas las instalaciones

Agrupa datos provenientes de múltiples sitios cuando se utiliza junto con **Vantage**™

Permite una gestión centralizada de los riesgos de seguridad para todos los sitios

Proporciona visibilidad de todos los entornos de TO e IoT

Se integra fácilmente con los entornos de los centros de operaciones de seguridad (SOC) y de TI

Infraestructura de seguridad integrada

Simplifica los procesos de seguridad de TI y TO

Facilita la armonización de los datos de seguridad para lograr una respuesta coherente

Incluye integraciones predefinidas para los sistemas de gestión de identidades, recursos y tickets, y para los sistemas SIEM

nozominetworks.com/integrations

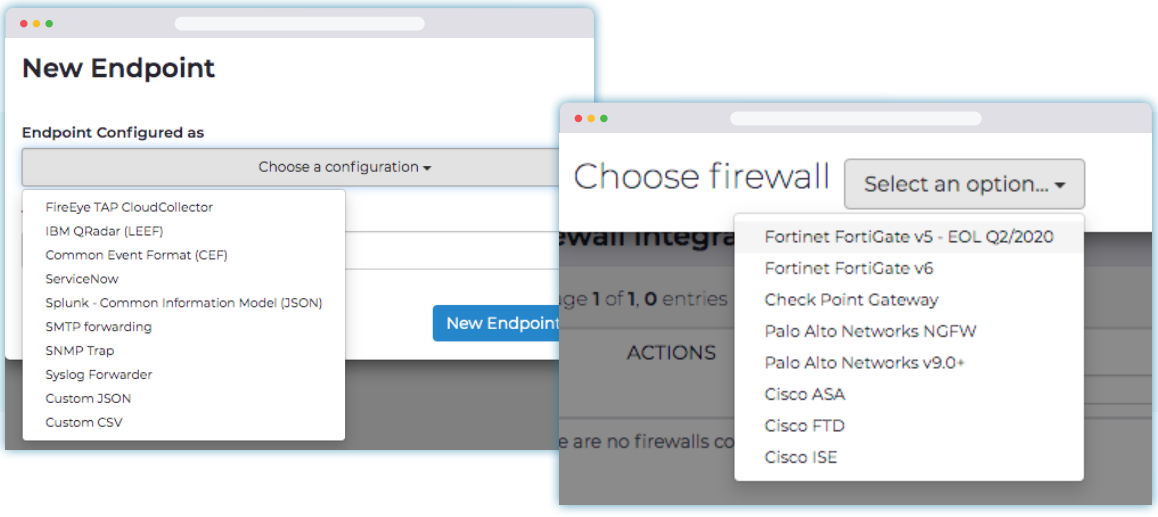
Amplio soporte de protocolos

Admite cientos de protocolos de TO, IoT y TI

Utiliza los conocimientos avanzados que tiene Nozomi Networks sobre los protocolos de TO para realizar análisis precisos

Incluye servicios de ingeniería on-demand y un kit de desarrollo de software (SDK) para protocolos a fin de admitir los nuevos protocolos

nozominetworks.com/techspecs

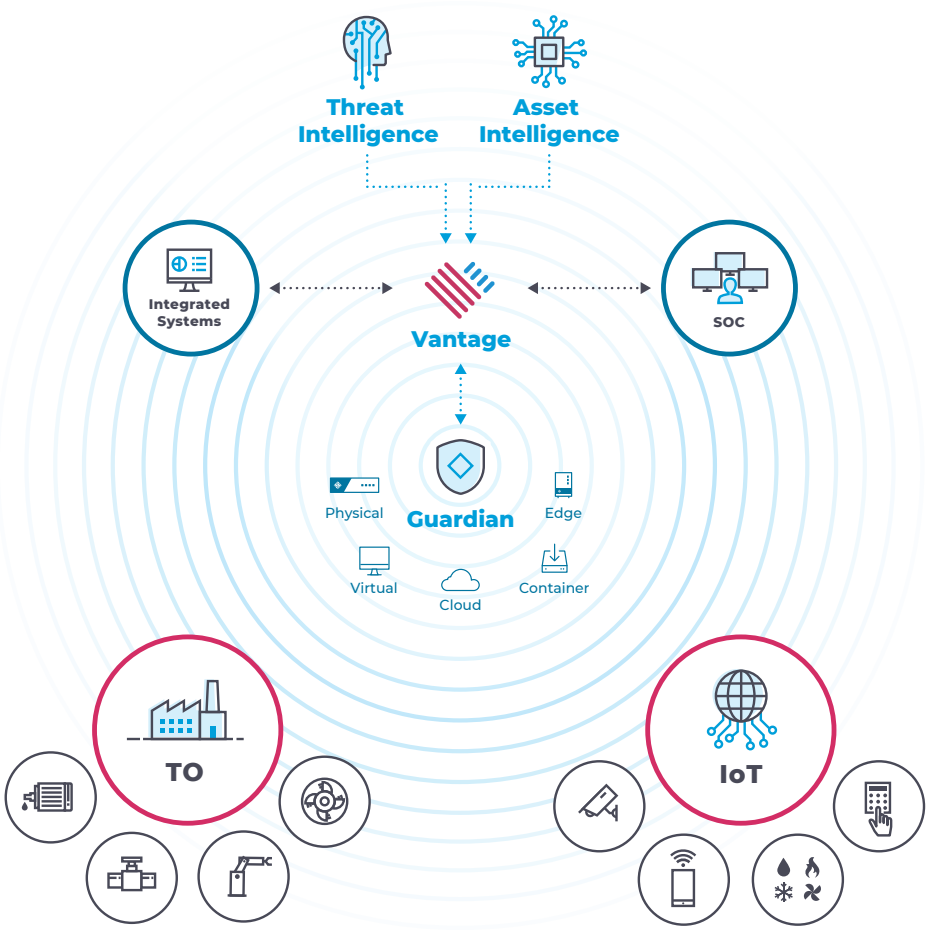


Las integraciones predefinidas ayudan a simplificar los procesos de seguridad.

Seguridad y visibilidad de TO e IoT

Resiliencia operativa y cibernética robustas para la industria

La plataforma del SaaS ampliable de Vantage protege los recursos de TO, IoT, TI, perimetrales y de nube, sea cual sea su número y en cualquier lugar.



Respuesta más rápida a incidentes

Por primera vez, usted puede ver todos los recursos de su red y conocer su comportamiento.

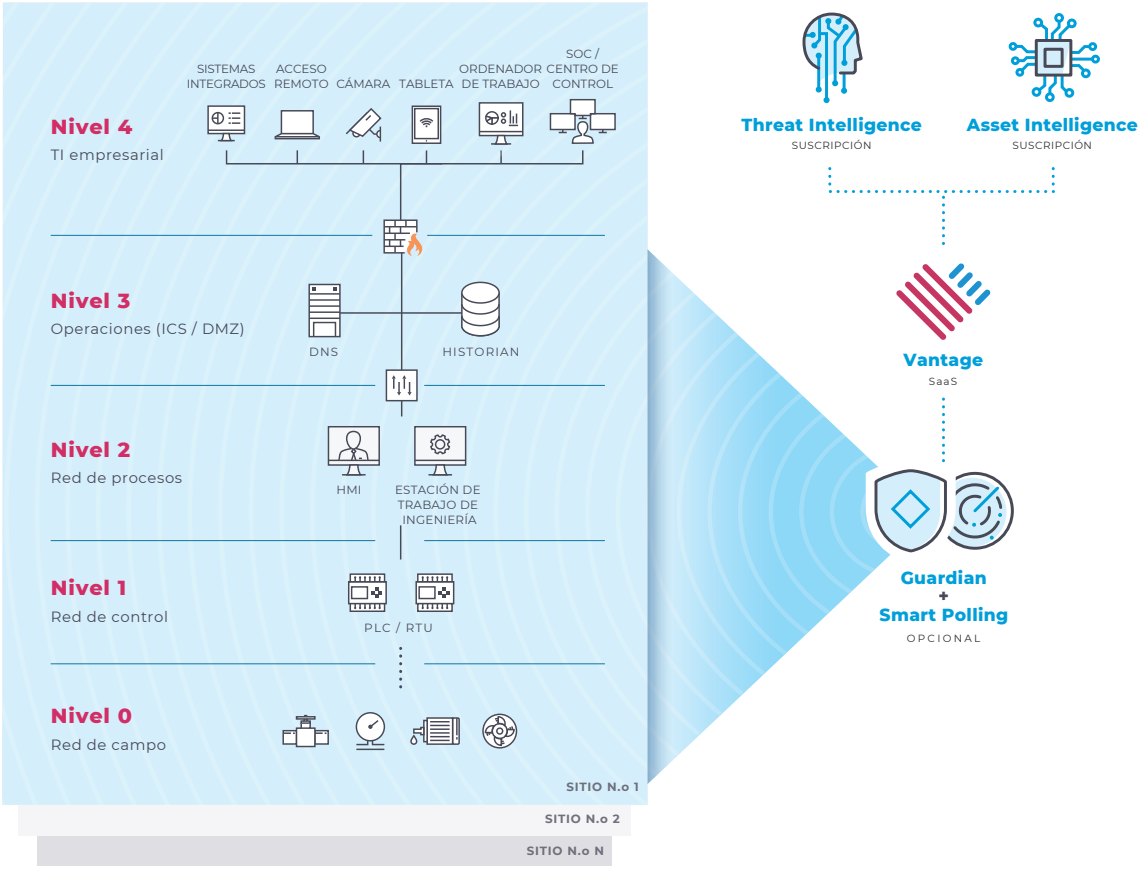
Nuestra tecnología detecta de forma rápida y precisa toda la actividad maliciosa y anómala.

Usted dispone del conocimiento que necesita para comprender las amenazas y responder antes de que se produzca el robo de datos o la interrupción de las operaciones.

Muestra de arquitectura de implementación

Ejemplo del modelo Purdue

Puede adaptar la solución de Nozomi Networks para satisfacer sus necesidades aprovechando su arquitectura flexible, su amplio rango de dispositivos y las integraciones con otros sistemas.



Socios de clase mundial

Nozomi Networks se integra totalmente con los servicios de TI y TO y con las empresas tecnológicas de su confianza. Esto incluye:

- **Alianzas estratégicas** con proveedores de seguridad administrada y TI empresarial
- **Integraciones tecnológicas** con las principales soluciones de TI y TO
- **Red global** de socios integradores de sistemas (SI), revendedores de valor agregado (VAR) y de distribución

Visite **nozominetworks.com/partners** para obtener más información.

Optimice Guardian para una mayor visibilidad y detección de amenazas

SUSCRIPCIÓN

Threat Intelligence

Disminuye los riesgos al reducir el tiempo promedio de detección (MTTD), lo que a su vez minimiza los efectos

Ofrece actualizaciones periódicas para detectar amenazas emergentes y nuevas vulnerabilidades

Consta de reglas, firmas y actualizaciones de vulnerabilidades creadas y seleccionadas por Nozomi Networks Labs, un equipo de investigadores especializados en seguridad

Encontrará todos los detalles en:
nozominetworks.com/threat-intelligence

SUSCRIPCIÓN

Asset Intelligence

Reduce los riesgos al disminuir el tiempo promedio de respuesta (MTTR) ante las anomalías operativas

Ofrece actualizaciones periódicas para lograr una detección más rápida y más precisa de las anomalías

Actualiza la tecnología de detección de anomalías de Guardian mediante datos de comportamiento y perfiles de dispositivos basados en el análisis de millones de recursos que se utilizan en diferentes sitios alrededor del mundo.

Encontrará todos los detalles en:
nozominetworks.com/asset-intelligence

COMPLEMENTO DE GUARDIAN

Smart Polling

Incorpora el sondeo activo de bajo volumen a la detección pasiva de recursos de Guardian

Identifica recursos que no se comunican y dispositivos no autorizados

Proporciona una evaluación de vulnerabilidades precisa para una respuesta rápida y eficiente

Encontrará todos los detalles en:
nozominetworks.com/smart-polling

COMPLEMENTO DE GUARDIAN

Remote Collectors

Complementa los datos de Guardian a través de sensores de bajos recursos para ubicaciones distribuidas

Recopila datos y los envía a Guardian para realizar otros análisis

Reduce los costes de implementación para instalaciones en áreas silvestres, plataformas off-shore y otras ubicaciones remotas

Encontrará todos los detalles en:
nozominetworks.com/techspecs

Sensores Guardian

para grandes empresas

Serie NSG-HS

Sensores de montaje en bastidor para lograr visibilidad, ciberseguridad y supervisión de TO/IoT en tiempo real.

- **De 300,000 a 500,000 nodos**
- **Rendimiento máx. de 6 Gbps**

Serie NSG-H

Sensores de montaje en bastidor para lograr visibilidad, ciberseguridad y supervisión de TO/IoT en tiempo real.

- **De 100,000 a 200,000 nodos**
- **Rendimiento máx. de 3 Gbps**

	NSG-HS 3500	NSG-HS 3000	NSG-H 2500	NSG-H 2000
Cant. máx. de nodos protegidos	500,000	300,000	200,000	100,000
Cant. max. de elementos de red protegidos[1]	2,000,000	1,500,000	1,200,000	1,000,000
Cant. máx. de dispositivos de IoT inteligentes protegidos[2]	3,000,000	1,800,000	1,200,000	600,000
Rendimiento máx.[3]	6 Gbps		3 Gbps	
Cant. máx. de Remote Collectors[4]	50		50	
Puertos de supervisión	Modular hasta 16+1		Modular hasta 8+1	
Puertos de administración	1x1000Base-T		1x1000Base-T	
Ranuras de expansión	4 ranuras disponibles: 4x1000BaseT | 4xSFP | 4xSFP+		2 ranuras disponibles: 4x1000BaseT | 4xSFP | 4xSFP+	
Almacenamiento	512 GB		512 GB	
Factor de forma	Unidad con 1 bastidor		Unidad con 1 bastidor	
Consumo de energía máximo	750 W		750 W	
Fuente de alimentación	100-240V AC - 50/60Hz, 36-72V DC, Dual		100-240V AC - 50/60Hz, 36-72V DC, Dual	
Rango de temperatura	0 / +40° C		0 / +40° C	
Alto x ancho x largo (mm/in)	44 x 438 x 600 / 1.73 x 17.24 x 23.60		44 x 438 x 600 / 1.73 x 17.24 x 23.60	
Peso	18 Kg		17 Kg	
Certificaciones	CE, FCC, UL		CE, FCC, UL	

[1] Elementos de red: la suma de nodos, enlaces, variables. [2] Dispositivos inteligentes de IoT: el concepto de "dispositivo inteligente de IoT" cubre los dispositivos que se comunican en un forma intermitente y resulta en un bajo rendimiento. [3] Todos los valores de rendimiento son "hasta" y varían según el tráfico analizado. [4] Ver colector remoto especificaciones técnicas para obtener más detalles. Para obtener especificaciones técnicas completas y actualizadas, visite: **nozominetworks.com/techspecs**, o contáctenos.

Sensores Guardian

para medianas empresas

Série NSG-M

Sensores de montaje en bastidor para lograr visibilidad, ciberseguridad y supervisión de TO/IoT en tiempo real.

- **De 10,000 a 40,000 nodos**
- **Rendimiento máx. de 1 Gbps**

Série NSG-L

Sensores de montaje en bastidor para lograr visibilidad, ciberseguridad y supervisión de TO/IoT en tiempo real.

- **De 1,000 a 5,000 nodos**
- **Rendimiento máx. de 250 a 500 Mbps**

	NSG-M 1000	NSG-M 750	NSG-L 250	NSG-L 100
Cant. máx. de nodos protegidos	40,000	10,000	5,000	1,000
Cant. max. de elementos de red protegidos[1]	600,000	200,000	90,000	20,000
Cant. máx. de dispositivos de IoT inteligentes protegidos[2]	200,000	50,000	20,000	5,000
Rendimiento máx.[3]	1 Gbps		500 Mbps	250 Mbps
Cant. máx. de Remote Collectors[4]	50		20	
Puertos de supervisión	7x1000BASE-T + 4xSFP		5x1000BASE-T	
Puertos de administración	1x1000Base-T		1x1000Base-T	
Ranuras de expansión	1 ranura disponible: 4x1000Base-T | 4xSFP | 4xSFP+		1 ranura disponible: 4x1000Base-T | 4xSFP	
Almacenamiento	256 GB		64 GB	
Factor de forma	Unidad con 1 bastidor		Unidad con 1 bastidor	
Consumo de energía máximo	360W		250W	
Fuente de alimentación	100-240V AC - 50/60 Hz, única		100-240V AC - 50/60 Hz, única	
Rango de temperatura	0 / +45° C		0 / +45° C	
Alto x ancho x largo (mm/in)	44 x 429 x 438 / 1.73 x 16.89 x 17.24		44 x 438 x 300 / 1.7 x 17.2 x 11.8	
Peso	14 Kg		8 Kg	
Certificaciones	CE, FCC, UL		CE, FCC, UL	

[1] Elementos de red: la suma de nodos, enlaces, variables. [2] Dispositivos inteligentes de IoT: el concepto de "dispositivo inteligente de IoT" cubre los dispositivos que se comunican en un forma intermitente y resulta en un bajo rendimiento. [3] Todos los valores de rendimiento son "hasta" y varían según el tráfico analizado. [4] Ver colector remoto especificaciones técnicas para obtener más detalles. Para obtener especificaciones técnicas completas y actualizadas, visite: **nozominetworks.com/techspecs**, o contáctenos.

Sensores Guardian

para requisitos especializados

Serie reforzada

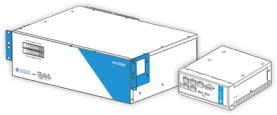
Sensores reforzados para lograr visibilidad, ciberseguridad y supervisión de TO/IoT en tiempo real.

- **De 500 a 5,000 nodos**
- **Rendimiento máx. de 100 a 250 Mbps**

Portátil

Sensor portátil para lograr visibilidad, ciberseguridad y supervisión de TO/IoT en tiempo real.

- **2,500 nodos**
- **Rendimiento máx. de 200 Mbps**



	NG-500R	NSG-R 50	Portable P550
Cant. máx. de nodos protegidos	5,000	500	2,500
Cant. max. de elementos de red protegidos[1]	80,000	10,000	50,000
Cant. máx. de dispositivos de IoT inteligentes protegidos[2]	30,000	2,500	12,500
Rendimiento máx.[3]	800 Mbps	100 Mbps	200 Mbps
Cant. máx. de Remote Collectors[4]	30	10	No disponible
Puertos de supervisión	3x1000BASE-T	4x1000BASE-T	5x1000BASE-T
Puertos de administración	1x1000Base-T		1x1000Base-T
Ranuras de expansión	2	No disponible	No disponible
Almacenamiento	256 GB (partición de datos redundantes)	64 GB	256 GB
Factor de forma	Unidad con 3 bastidores	DIN	Escritorio con kit de montaje en pared
Consumo de energía máximo	115W	60W	38W
Fuente de alimentación	100-240V AC, 100-240V DC, Dual	100-240V AC, 12-36V DC, Única (PSU externo)	90-240V AC, 12-30V DC, Única
Rango de temperatura	-40° C / +70° C (Max 40° C with SFP NIC)	-40 / +75° C	0 / +60° C
Alto x ancho x largo (mm/in)	131.8x438x300.1 5.18x17.2x11.8	80 x 130 x 146 3.15 x 5.11 x 5.74	70 x 180 x 240 2.75 x 7.08 x 9.44
Peso	8.5 Kg / 18.74 Lb	3 Kg	2.5 Kg
Certificaciones	CE, FCC, UL		FCC

[1] Elementos de red: la suma de nodos, enlaces, variables. [2] Dispositivos inteligentes de IoT: el concepto de "dispositivo inteligente de IoT" cubre los dispositivos que se comunican en un forma intermitente y resulta en un bajo rendimiento. [3] Todos los valores de rendimiento son "hasta" y varían según el tráfico analizado. [4] Ver colector remoto especificaciones técnicas para obtener más detalles. Para obtener especificaciones técnicas completas y actualizadas, visite: **nozominetworks.com/techspecs**, o contáctenos.

Sensores Guardian

para sitios remotos

Remote Collector

Sensores de bajos recursos que recopilan datos de recursos y redes en ubicaciones remotas y los envían a Guardian para realizar otros análisis.

- **Rendimiento de hasta 15 Mbps**

	NRC-5
Rendimiento máx.	Hasta 15 Mbps
Soporte para Remote Collectors	No disponible
Puertos de supervisión	2x1000Base-T, 1xSFP
Puertos de administración	1x1000Base-T
Ranuras de expansión	No disponible
Almacenamiento	8 GB
Factor de forma	DIN que se puede montar
Consumo de energía máximo	12W
Fuente de alimentación	100-240VAC, 12-36V CC, Única
Rango de temperatura	-40 / +70° C
Generación de calor	55.44 BTU/hr
Alto x ancho x largo (mm/in)	41.5 x 170 x 138 / 2.71 x 6.67 x 5.00
Peso	1.2 Kg
Cumplimiento	RoHS
Certificaciones	CE, FCC, UL

	Recolector de datos virtual para sitios remotos
Rendimiento máx.	15 Mbps
Opciones de implementación	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+

Para obtener todas las especificaciones técnicas actuales, visite: **nozominetworks.com/techspecs**, o póngase en contacto con nosotros.

Sensores Guardian

para entornos virtuales y contenedores

Serie virtual

Sensores virtuales para lograr visibilidad, ciberseguridad y supervisión de TO/IoT en tiempo real.

- **De 1,000 a 40,000 nodos**
- **Rendimiento máx. de 1 Gbps**

	V1000	V750	V250	V100
Cant. máx. de nodos protegidos	40,000	10,000	5,000	1,000
Cant. max. de elementos de red protegidos[1]	400,000	200,000	100,000	20,000
Cant. máx. de dispositivos de IoT inteligentes protegidos[2]	200,000	100,000	25,000	5,000
Rendimiento máx.[3]	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Escenarios	Empresarial	Grande	Mediano	Pequeño
Opciones de implementación	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+			
Cant. máx. de Remote Collectors[4]	50	50	20	20

[1] Elementos de red: la suma de nodos, enlaces, variables. [2] Dispositivos inteligentes de IoT: el concepto de "dispositivo inteligente de IoT" cubre los dispositivos que se comunican en un forma intermitente y resulta en un bajo rendimiento. [3] Todos los valores de rendimiento son "hasta" y varían según el tráfico analizado. [4] Ver colector remoto especificaciones técnicas para obtener más detalles. Para obtener especificaciones técnicas completas y actualizadas, visite: **nozominetworks.com/techspecs**, o contáctenos.

Edición para contenedor

Sensor de contenedor integrado para conmutadores, enrutadores y otras infraestructuras de seguridad. Opción de implementación rápida y flexible que aprovecha sus dispositivos existentes.

- **Disponible para Guardian solo con el módulo adicional Smart Polling**

	Contenedor
Ofertas integradas	Gatewatcher, Siemens RUGGEDCOM
Complementos	Módulo Smart Polling: *incluido* | | Suscripciones a Threat Intelligence y Asset Intelligence: *se pueden agregar*
Soporte para Remote Collectors	No disponible

Para obtener todas las especificaciones técnicas actuales, visite: **nozominetworks.com/techspecs**, o póngase en contacto con nosotros.

Varias opciones de implementación y soporte

A continuación se incluyen diversas opciones de implementación y asistencia de apoyo:

- **Nozomi Networks Global Strategic Alliance Partners**
- **Nozomi Networks SI/VARs**
- **Nozomi Networks Professional Services**
- **Nozomi Networks Global Customer Support**

Productos y Servicios

SAAS

Vantage

Vantage acelera la respuesta de seguridad con detección de amenazas inigualable y visibilidad en todo su OT, IoT y redes de TI. Su plataforma SaaS ampliable le permite proteger varios recursos, en cualquier lugar. Puede responder con mayor rapidez y eficacia a las amenazas cibernéticas, garantizando una resiliencia operativa.

Requiere sensores Guardian

PERÍMETRO O NUBE PÚBLICA

Guardian

Guardian proporciona una seguridad y una visibilidad de TO e IoT robustas para la industria. Combina detección de recursos, visualización de redes, evaluación de vulnerabilidades, control de riesgos y detección de amenazas en una sola aplicación. Guardian comparte datos tanto con Vantage como con CMC.

PERÍMETRO O NUBE PÚBLICA

Central Management Console

Central Management Console (CMC) consolida el control de riesgos y la visibilidad de TO e IoT en todos sus sitios distribuidos, tanto en el perímetro como en la nube pública. Se integra con su infraestructura de seguridad de TI para lograr flujos de trabajo optimizados y respuestas más rápidas ante amenazas y anomalías.

SUSCRIPCIÓN

Asset Intelligence

El servicio Asset Intelligence ofrece actualizaciones de perfil regulares para lograr una detección más rápida y más precisa de las anomalías. Lo ayuda a enfocar los esfuerzos y reducir el tiempo promedio de respuesta (MTTR). .

SUSCRIPCIÓN

Threat Intelligence

El servicio Threat Intelligence ofrece inteligencia continua para amenazas y vulnerabilidades de TO e IoT. Le ayuda a estar al tanto de las amenazas emergentes y de las nuevas vulnerabilidades y a reducir su tiempo promedio de detección (MTTD).

COMPLEMENTO DE GUARDIAN

Smart Polling

Smart Polling agrega sondeo activo de bajo volumen a la detección pasiva de recursos de Guardian, mejorando el rastreo de recursos, la evaluación de vulnerabilidades y la monitorización de seguridad.

COMPLEMENTO DE GUARDIAN

Remote Collectors

Los recolectores de datos para sitios remotos son sensores de bajos recursos que capturan datos desde las ubicaciones distribuidas y los envían a Guardian para su análisis. Mejoran la visibilidad y reducen los costes de implementación.

NOZOMI NETWORKS

Nozomi Networks

La solución líder para la seguridad y la visibilidad de la tecnología operativa y del internet de las cosas

Nozomi Networks acelera la transformación digital protegiendo la infraestructura crítica así como a las organizaciones industriales y gubernamentales de las ciber-amenazas. Nuestra solución proporciona una visibilidad excepcional de la red y de los activos, capacidad de detección de amenazas e información detallada sobre los entornos OT e IoT. Los clientes confían en nosotros para minimizar el riesgo y la complejidad al tiempo que maximizan la resiliencia operativa.

DS-G-A4-ES-018

nozominetworks.com