



FICHE PRODUIT

Guardian

Sécurité et visibilité renforcées pour les systèmes industriels et de l'IoT

Nozomi Networks **Guardian™** améliore la visibilité sur vos ressources industrielles, informatiques, de l'IoT, à la périphérie et dans le Cloud, pour accélérer la sécurité et la transformation digitale.

Guardian réduit les risques pour les systèmes industriels des plus grandes infrastructures critiques dans les secteurs de l'énergie, de la fabrication, de l'extraction minière, du transport, de l'automatisation de bâtiments et d'autres sites dans le monde entier.

Voir

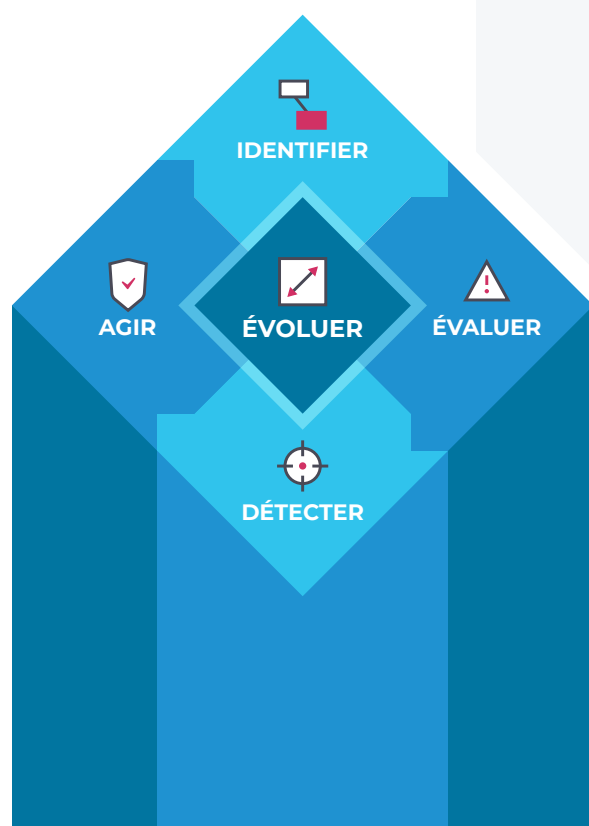
Toutes les ressources et tous les comportements des systèmes industriels et de l'IoT sur vos réseaux pour une connaissance sans pareille

Détecter

Les cybermenaces, les vulnérabilités, les risques et les anomalies pour un traitement plus rapide

Unifier

La sécurité, la visibilité et la supervision de l'ensemble de vos ressources pour une meilleure résilience



Identification

Découverte des ressources et visualisation du réseau

Suivez automatiquement vos ressources industrielles et de l'IoT

Inventaire actualisé des ressources

Améliore la cyber-résilience et le gain de temps grâce à l'inventaire automatisé des ressources

Identifie toutes les ressources communicantes

Fournit des informations complètes sur les nœuds, notamment le nom, le type, le numéro de série, la version du micrologiciel et les composants, ainsi que sur les risques, notamment les alertes de sécurité et de fiabilité, les correctifs manquants et les vulnérabilités

Réduction des risques grâce à la visualisation du réseau

Fournit une compréhension instantanée de votre réseau industriel/IoT et de ses schémas d'activité

Présente des données clés telles que le débit du trafic, les connexions TCP et les protocoles

Améliore votre compréhension des activités « normales »

MODULE COMPLÉMENTAIRE

Smart Polling

Étend la découverte passive des ressources intégrée à Guardian par un sondage des ressources à faible bande passante.

nozominetworks.com/smart-polling

ABONNEMENT

Asset Intelligence

Accélère le processus d'apprentissage des ressources, et gère des profils et des données sur les comportement des ressources.

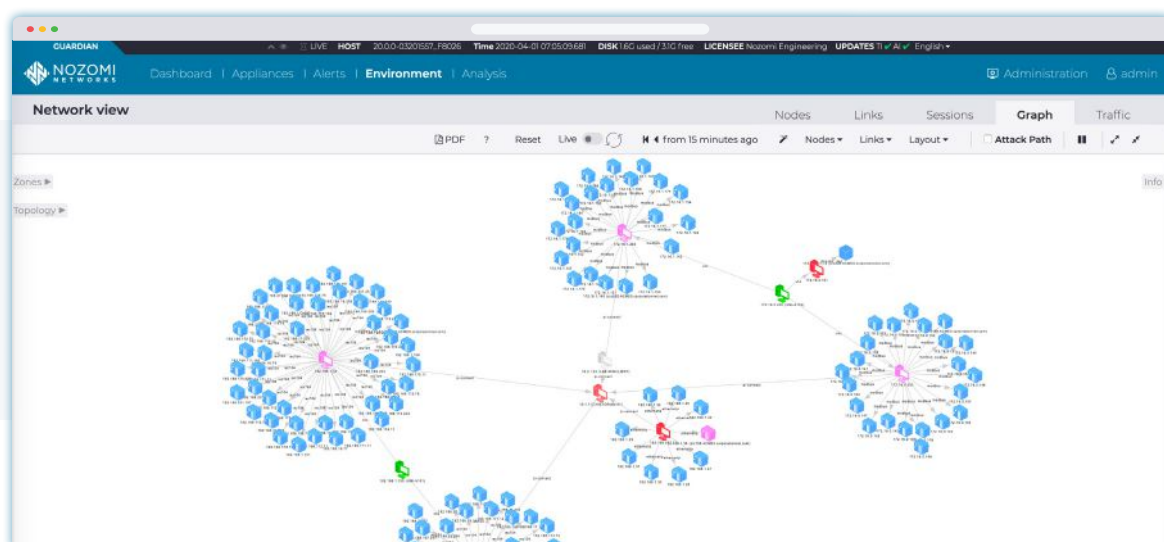
nozominetworks.com/asset-intelligence

Tableaux de bord et rapports intuitifs

Présente des vues globales ainsi que des informations détaillées sur les ressources et les connexions

Filtre par sous-réseaux, types, rôles, zones et topologies

Regroupe les ressources visuellement, dans des listes et des vues détaillées de chaque ressource



Portion du graphique interactif de visualisation du réseau.



Évaluation

Évaluation des vulnérabilités et surveillance des risques

Identifiez rapidement les risques de vulnérabilité

Évaluation automatique des vulnérabilités

Identifie les appareils des fournisseurs qui sont vulnérables

Utilise la base de données des vulnérabilités maintenue par le gouvernement américain (NVD) pour la dénomination, la description et la notation standardisées

Hiérarchisation et remédiation efficaces

Accélère le traitement grâce à des tableaux de bord et des rapports détaillés sur les vulnérabilités

Les questions suivantes sont notamment adressées :

- « Mes ressources utilisent-elles un micrologiciel vulnérable ? »
- « Les ressources du fournisseur X sont-elles vulnérables ? »

Surveillez en permanence vos réseaux et vos systèmes d'automatisation

Surveillance continue

Surveillance continue de tous les protocoles pris en charge : industriels, informatiques et IoT

Pas d'angles morts critiques dans la protection causés par une surveillance limitée ou une prise en charge inadéquate des protocoles

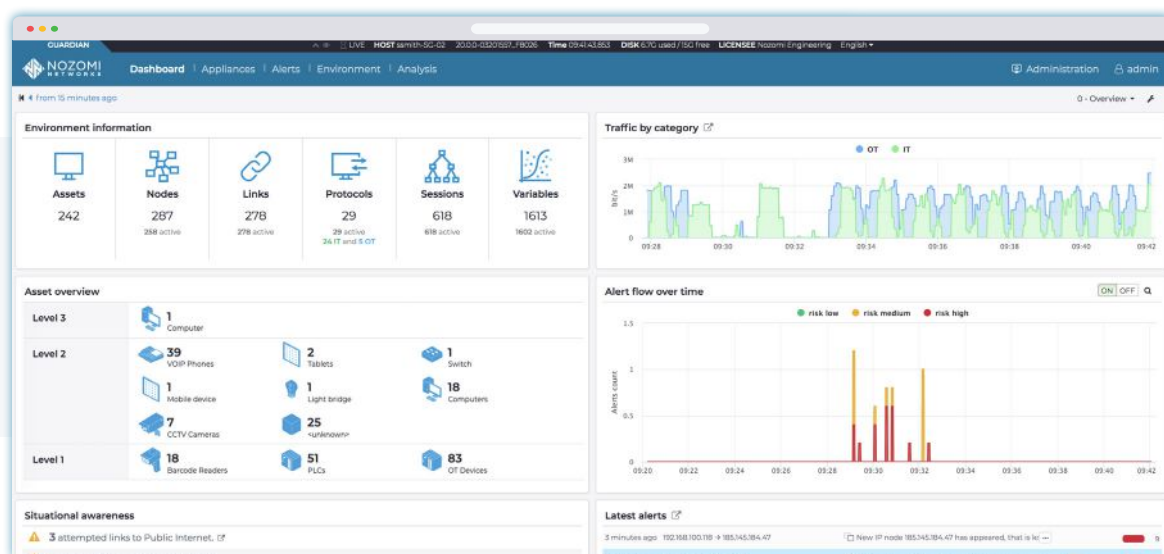
Surveillance des ressources de tous les fournisseurs et de toutes les communications réseau

Accès facile aux données sur les systèmes industriels

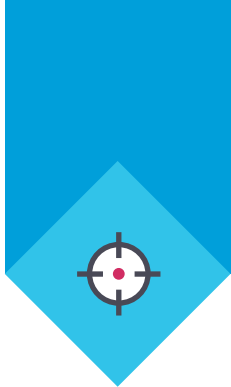
Résume les informations sur les risques pour les systèmes industriels et l'IoT, sur des plages de dates et d'heures personnalisables

Met en évidence des indicateurs de problèmes de fiabilité, tels que des valeurs de processus inhabituelles

Interroge n'importe quel aspect des performances de votre réseau ou de votre système de contrôle, en réduisant la collecte de données et le travail dans un tableur



Portion du **tableau de bord personnalisable** de Guardian.



Détection

Détection avancée des anomalies et des menaces

Déterminez et stoppez rapidement les menaces et les comportements anormaux

Détection des menaces à la minute près

Identifie les menaces pour la cybersécurité et la fiabilité des processus

Détecte les menaces avancées et les cyber-risques à un stade précoce et avancé

Bloque les attaques lorsque la solution est intégrée à des pare-feu et des produits compatibles de sécurité des terminaux

Détection des menaces ciblant les systèmes industriels et de l'IoT

Combine la détection des anomalies en fonction des comportements et la détection des menaces s'appuyant sur des signatures pour une surveillance complète des risques

Fournit des informations détaillées sur les menaces sous forme de règles Yara, de règles de paquets, d'indicateurs STIX, de définitions des menaces, d'une base de connaissances sur les menaces et de signatures de vulnérabilités

Contrôlez efficacement les environnements mixtes

ABONNEMENT Threat Intelligence

Détecte les menaces et identifie les vulnérabilités à l'aide d'indicateurs créés et classés par Nozomi Networks Labs

Fournit des renseignements en continu sur les menaces et les vulnérabilités des systèmes industriels, informatiques et de l'IoT

ABONNEMENT Asset Intelligence

Détecte les anomalies avec une efficacité inégalée pour les systèmes industriels et de l'IoT, et un filtrage des alertes relatives à des comportements anodins, accélérant ainsi le traitement des incidents

Données en continu sur le profil et le comportement des ressources industrielles et de l'IoT

Détection extrêmement fiable des anomalies sur les équipements OT et IoT



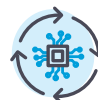
Identification rapide des ressources

Garantit un inventaire précis des ressources



Alertes fiables sur les anomalies

Accélère le traitement des incidents



Informations sur les ressources dans les réseaux dynamiques

Fiabilité de l'inventaire et des détections

Action

Tableaux de bord et outils d'analyse pour gagner du temps

Améliorez considérablement la gestion des risques sur les systèmes industriels et de l'IoT

Les tableaux de bord et les rapports personnalisables soulignent les risques

Concentre l'attention sur les préoccupations clés en résumant les risques et les menaces

Rapports intégrés personnalisables Vous pouvez choisir parmi des widgets prédéfinis pour ajouter précisément les informations dont vous avez besoin

Des alertes détaillées fournissent des informations clés

Génère des alertes détaillées et précises

Identifie les risques pour la sécurité et la fiabilité

Regroupe les alertes en incidents, offrant ainsi au personnel chargé de la sécurité et de l'exploitation une visibilité simple, claire et consolidée sur les activités de leur réseau

Réduisez considérablement les efforts de dépannage et d'investigation

Traitement accéléré des incidents

Combine la détection révolutionnaire par Guardian des anomalies des systèmes industriels et de l'IoT avec le service **Asset Intelligence™** pour des alertes ciblées et exploitables

Comprend le comportement normal des ressources dont le comportement change fréquemment, en éliminant les alertes relatives à des anomalies anodines

Réduit le délai de traitement et améliore la productivité grâce à des alertes fiables et faciles à hiérarchiser

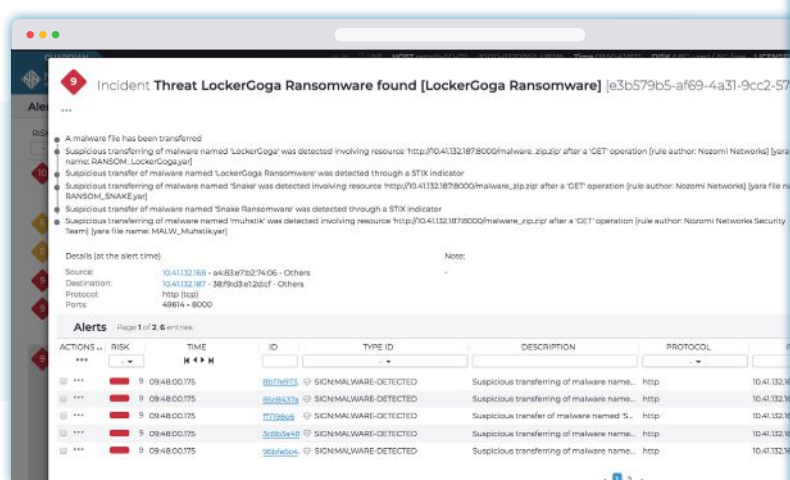
Analyses rapides

Concentre les efforts avec Smart Incidents™ qui :

- Corrèle et consolide les alertes
- Fournit un contexte opérationnel et de sécurité
- Capture automatiquement les paquets

Décode les incidents avec Time Machine™ avant et après les instantanés système

Fournit des réponses rapidement grâce à un puissant outil d'interrogation ad hoc



Smart Incident présentant les alertes associées et le contexte de sécurité.



Rapport résumant les alertes pour un site.

Évolutivité

Sécurité unifiée pour des centaines de milliers de ressources

S'adapte facilement pour des performances optimales

Des performances locales et mondiales exceptionnelles

Capable de traiter les données de 500 000 ressources en temps réel

Génère rapidement des visualisations, des tableaux de bord et des rapports sur le réseau

Accélère la détection et la remédiation des menaces grâce au traitement local des renseignements sur les menaces et les ressources

Surveillance consolidée de toutes les installations

Agrège les données de plusieurs sites lorsque la solution est utilisée avec **Vantage™**

Permet une gestion centralisée des risques pour la sécurité de tous les sites

Offre une visibilité sur tous les environnements industriels/IoT

Intégration facile avec les environnements SOC/informatiques

Infrastructure de sécurité intégrée

Optimise les processus de sécurité informatiques/industriels

Facilite l'harmonisation des données de sécurité pour un traitement cohérent

Comprend des intégrations prédéfinies avec des systèmes de gestion des ressources, des tickets et des identités, et des SIEM

nozominetworks.com/integrations

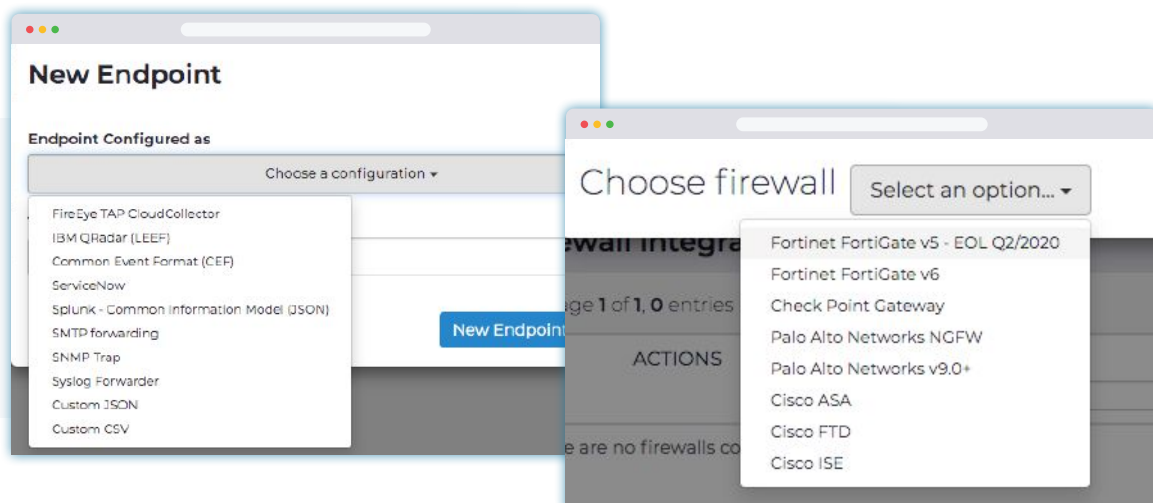
Prise en charge étendue des protocoles

Prend en charge des centaines de protocoles industriels, informatiques et de l'IoT

Utilise l'expertise approfondie de Nozomi Networks en matière de protocoles industriels pour une analyse fiable

Comprend un kit de développement de protocole et des services d'ingénierie à la demande pour la prise en charge de nouveaux protocoles

nozominetworks.com/techspecs

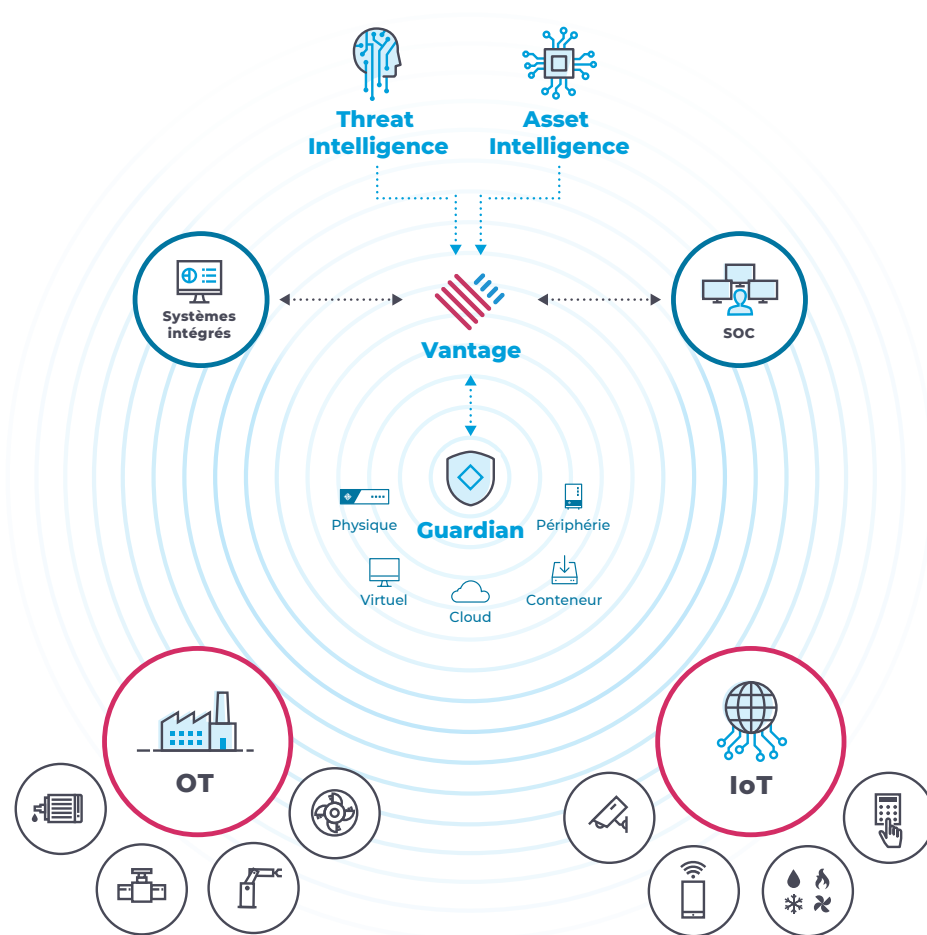


Les **intégrations prédéfinies** permettent d'optimiser facilement les processus de sécurité.

Sécurité et visibilité sur les ressources industrielles et de l'IoT

Cyber-résilience et résilience opérationnelle renforcées

Vous pouvez protéger une grande variété d'environnements mixtes grâce à la découverte rapide des ressources, la visualisation du réseau et l'accélération de la sécurité.



Traitez les incidents plus rapidement

Vous pouvez voir tous les ressources de votre réseau et connaître leur comportement.

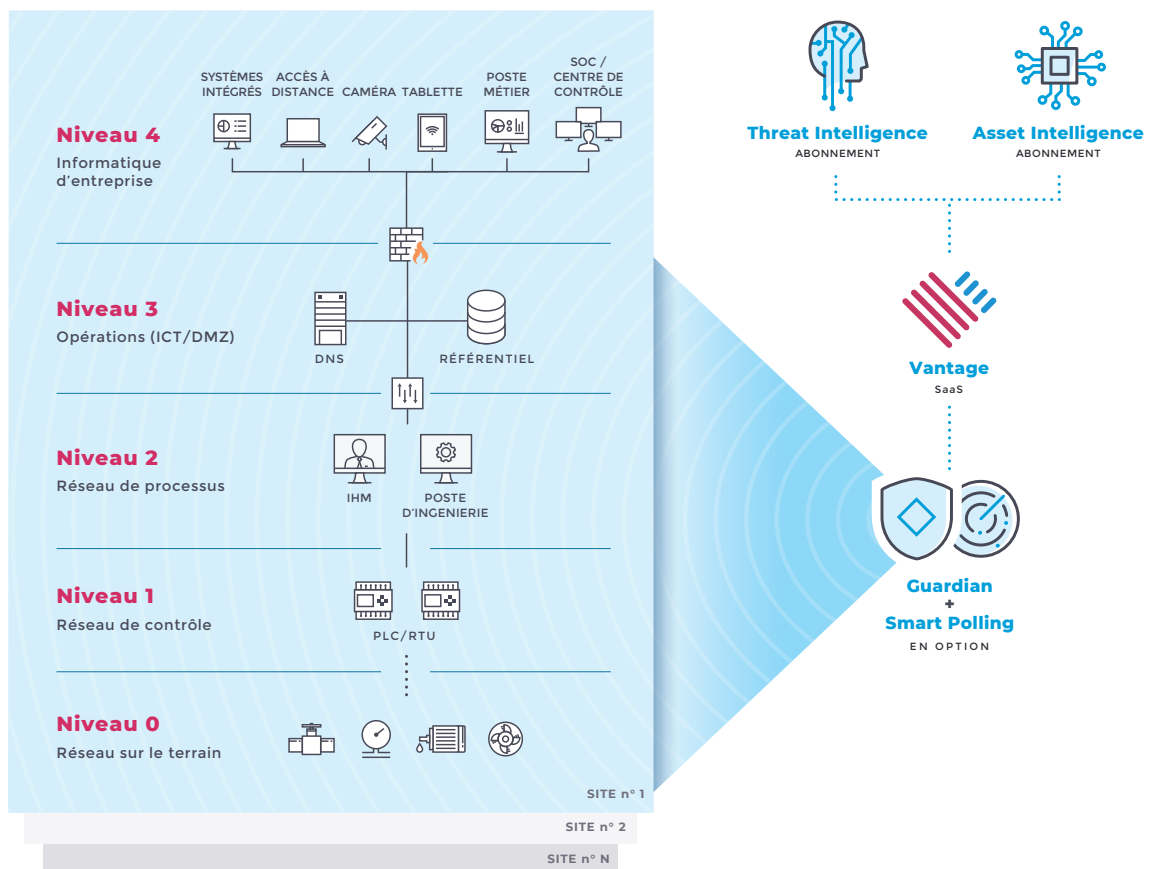
Notre technologie détecte rapidement et de manière fiable les activités malveillantes et anormales.

Vous disposez des informations dont vous avez besoin pour comprendre les menaces et les traiter avant qu'un vol de données ou des perturbations ne se produisent.

Exemple d'architecture de déploiement

Exemple de modèle Purdue

Vous pouvez adapter la solution Nozomi Networks à vos besoins en utilisant son architecture flexible, sa gamme étendue de capteurs, et ses intégrations avec d'autres systèmes.



Partenaires de haut niveau

Nozomi Networks s'associe étroitement avec les entreprises de technologie et les prestataires de services informatiques/industriels auxquels vous faites confiance :

- **Alliances stratégiques** avec des prestataires d'informatique d'entreprise et de sécurité managée
- **Intégrations technologiques** avec les principales solutions informatiques/industrielles
- **Réseau mondial** de partenaires SI, VAR et de distribution

Consultez nozominetworks.com/partners pour plus d'informations.

Améliore Guardian pour une meilleure **visibilité** et une meilleure **détection** **des menaces**



ABONNEMENT

Threat Intelligence

Réduit le délai moyen de détection (MTTD) pour minimiser l'impact des risques

Fournit des mises à jour régulières pour détecter les menaces émergentes et les nouvelles vulnérabilités

Il s'agit de règles, de signatures et de correctifs de vulnérabilités créés et gérés par Nozomi Networks Labs, une équipe de chercheurs experts en sécurité

Tous les détails sont disponibles sur :

nozominetworks.com/threat-intelligence



ABONNEMENT

Asset Intelligence

Réduit le délai moyen de traitement (MTTR) des anomalies opérationnelles pour minimiser les risques

Fournit des mises à jour régulières des profils pour une détection plus rapide et plus fiable des anomalies

Actualise la technologie de détection des anomalies de Guardian avec des profils d'appareils et des données sur les comportements basés sur l'analyse de millions de ressources utilisées sur des sites du monde entier

Tous les détails sont disponibles sur :

nozominetworks.com/asset-intelligence



OPTION POUR GUARDIAN

Smart Polling

Ajout d'un sondage actif à faible bande passante à la fonctionnalité de Guardian de découverte passive des ressources

Identifie les ressources non communicantes et les appareils malveillants

Fournit une évaluation précise des vulnérabilités pour un traitement rapide et efficace

Tous les détails sont disponibles sur :

nozominetworks.com/smart-polling



OPTION POUR GUARDIAN

Remote Collectors

Complète les données de Guardian par des capteurs à faibles ressources pour les sites distribués

Collecte les données et les envoie à Guardian pour une analyse plus approfondie

Réduit les coûts de déploiement pour les sites isolés ou off-shore

Tous les détails sont disponibles sur :

nozominetworks.com/techspecs

Capteurs Guardian

pour les **grandes entreprises**

Gamme NSG-HS

Capteurs en rack pour la visibilité, la cybersécurité et la surveillance en temps réel des systèmes industriels/de l'IoT.

◆ 300 000 à 500 000 nœuds

◆ 6 Gbps de débit max.



Gamme NSG-H

Capteurs en rack pour la visibilité, la cybersécurité et la surveillance en temps réel des systèmes industriels/de l'IoT.

◆ 100 000 à 200 000 nœuds

◆ 3 Gbps de débit max.



	NSG-HS 3500	NSG-HS 3000	NSG-H 2500	NSG-H 2000
Nœuds protégés max.	500 000	300 000	200 000	100 000
Éléments réseau protégés max. ¹	2 000 000	1 500 000	1 200 000	1 000 000
Appareils IoT intelligents protégés max. ²	3 000 000	1 800 000	1 200 000	600 000
Débit max. ³	6 Gbps		3 Gbps	
Remote Collectors max. ⁴	50		50	
Ports de surveillance	Modulaires jusqu'à 16+1		Modulaires jusqu'à 8+1	
Ports d'administration	1x1000Base-T		1x1000Base-T	
Emplacements d'extension	4 emplacements disponibles : 4x1000BaseT 4xSFP 4xSFP+		2 emplacements disponibles : 4x1000BaseT 4xSFP 4xSFP+	
Stockage	512 Go		512 Go	
Format	1U		1U	
Consommation max.	750 W		750 W	
Alimentation électrique	100-240 VAC - 50/60 Hz, 36-72 VDC, double		100-240 VAC - 50/60 Hz, 36-72 VDC, double	
Plage de températures	0 / +40 °C		0 / +40 °C	
H x l x L (mm/po)	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	
Poids	18 Kg		17 Kg	
Certifications	CE, FCC, UL		CE, FCC, UL	

¹ Éléments réseau : La somme des nœuds, des liens, des variables. ² Appareils IoT intelligents : Le concept d'« appareil IoT intelligent » couvre les appareils communiquant de manière intermittente à faible débit. ³ Toutes les valeurs de performance sont « jusqu'à » et varient en fonction du trafic analysé.

⁴ Voir les spécifications techniques des Remote Collectors pour plus de détails. Pour les spécifications techniques complètes et actuelles, consultez nozominetworks.com/techspecs ou contactez-nous.

Capteurs Guardian

pour les entreprises de taille moyenne

Gamme NSG- M

Capteurs en rack pour la visibilité, la cybersécurité et la surveillance en temps réel des systèmes industriels/de l'IoT.

- ◆ 10 000 à 40 000 nœuds
- ◆ 1 Gbps de débit max.



Gamme NSG-L

Capteurs en rack pour la visibilité, la cybersécurité et la surveillance en temps réel des systèmes industriels/de l'IoT.

- ◆ 1 000 à 5 000 nœuds
- ◆ 250 à 500 Mbps de débit max.



	NSG-M 1000	NSG-M 750	NSG-L 250	NSG-L 100
Nœuds protégés max.	40 000	10 000	5 000	1 000
Éléments réseau protégés max. ¹	600 000	200 000	90 000	20 000
Appareils IoT intelligents protégés max. ²	200 000	50 000	20 000	5 000
Débit max. ³	1 Gbps		500 Mbps	250 Mbps
Remote Collectors max. ⁴	50		20	
Ports de surveillance	7x1000BASE-T + 4xSFP		5x1000BASE-T	
Ports d'administration	1x1000Base-T		1x1000Base-T	
Emplacements d'extension	1 emplacement disponible : 4x1000Base-T 4xSFP 4xSFP*		1 emplacement disponible : 4x1000Base-T 4xSFP	
Stockage	256 Go		64 Go	
Format	1U		1U	
Consommation max.	360 W		250 W	
Alimentation électrique	100-240 VAC - 50/60 Hz, simple		100-240 VAC - 50/60 Hz, simple	
Plage de température	0 / +45 °C		0 / +45 °C	
H x l x L (mm/po)	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	
Poids	14 Kg		8 Kg	
Certifications	CE, FCC, UL		CE, FCC, UL	

¹ Éléments réseau : La somme des nœuds, des liens, des variables. ² Appareils IoT intelligents : Le concept d'« appareil IoT intelligent » couvre les appareils communiquant de manière intermittente à faible débit. ³ Toutes les valeurs de performance sont « jusqu'à » et varient en fonction du trafic analysé.

⁴ Voir les spécifications techniques des Remote Collectors pour plus de détails. Pour les spécifications techniques complètes et actuelles, consultez nozominetworks.com/techspecs ou contactez-nous.

Capteurs Guardian

pour les **besoins spécialisés**

Gamme durcie

Capteurs durcis pour la visibilité, la cybersécurité et la surveillance en temps réel des systèmes industriels/de l'IoT.

- ◆ 500 à 5 000 nœuds
- ◆ 100 à 250 Mbps de débit max.



Portable

Capteur portable pour la visibilité, la cybersécurité et la surveillance en temps réel des systèmes industriels/de l'IoT.

- ◆ 2 500 nœuds
- ◆ 200 Mbps de débit max.



	NG-500R	NSG-R 50	P550
Nœuds protégés max.	5 000	500	2 500
Éléments réseau protégés max. ¹	80 000	10 000	50 000
Appareils IoT intelligents protégés max. ²	30 000	2 500	12 500
Débit max. ³	800 Mbps	100 Mbps	200 Mbps
Remote Collectors max. ⁴	30	10	Non disponible
Ports de surveillance	3x1000BASE-T	4x1000BASE-T	5x1000BASE-T
Ports d'administration	1x1000Base-T		1x1000Base-T
Emplacements d'extension	2	Non disponible	Non disponible
Stockage	256 Go (partition de données redondante)	64 Go	256 Go
Format	3U	Montage DIN	Desktop avec kit de montage mural
Consommation max.	115 W	60 W	38 W
Alimentation électrique	100-240 VAC, 100-240 VDC, double	100-240 VAC, 12-36 VDC, simple (PSU externe)	90-240 VAC, 12-30 VDC, simple (PSU externe)
Plage de températures	-40 °C / +70 °C (40 °C max. avec interface SFP)	-40 °C / +75 °C	0 °C / +60 °C
H x l x L (mm/po)	131,8 x 438 x 300,1 5,18 x 17,2 x 11,8	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
Poids	8,5 Kg / 18,74 lb	3 Kg	2,5 Kg
Certifications	CE, FCC, UL		FCC

¹ Éléments réseau : La somme des nœuds, des liens, des variables. ² Appareils IoT intelligents : Le concept d'« appareil IoT intelligent » couvre les appareils communiquant de manière intermittente à faible débit. ³ Toutes les valeurs de performance sont « jusqu'à » et varient en fonction du trafic analysé.

⁴ Voir les spécifications techniques des Remote Collectors pour plus de détails. Pour les spécifications techniques complètes et actuelles, consultez nozominetworks.com/techspecs ou contactez-nous.

Capteurs Guardian

pour les **sites distants**

Remote Collectors

Capteurs à faibles ressources qui collectent des données sur les ressources et les réseaux dans des endroits éloignés, et les envoient à Guardian pour une analyse plus approfondie.

◆ Jusqu'à 15 Mbps de débit



	NRC-5
Débit max.	Jusqu'à 15 Mbps
Prise en charge des Remote Collectors	Non disponible
Ports de surveillance	2x1000Base-T, 1xSFP
Ports d'administration	1x1000Base-T
Emplacements d'extension	Non disponibles
Stockage	8 Go
Format	Montage DIN
Consommation max.	12 W
Alimentation électrique	100-240VAC, 12-36 VDC, simple (PSU externe)
Plage de températures	-40 °C / +45 °C
Production de chaleur	55,44 BTU/hr
H x l x L (mm/po)	78 x 146 x 127 / 3,07 x 6,67 x 5,00
Poids	1,2 Kg
Conformité	RoHS
Certifications	CE, FCC, UL
	Remote Collector virtuel
Débit max.	15 Mbps
Options de déploiement	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+

Pour les spécifications techniques complètes et actuelles, consultez nozominetworks.com/techspecs ou contactez-nous.

Capteurs Guardian

pour les **environnements virtuels** et les **conteneurs**

Gamme virtuelle

Capteurs virtuels pour la visibilité, la cybersécurité et la surveillance en temps réel des systèmes industriels/de l'IoT.

◆ 1 000 à 40 000 nœuds

◆ 1 Gbps de débit max.

	V1000	V750	V250	V100
Nœuds protégés max.	40 000	10 000	5 000	1 000
Éléments réseau protégés max. ¹	400 000	200 000	100 000	20 000
Appareils IoT intelligents protégés max. ²	200 000	100 000	25 000	5 000
Débit max. ³	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Déploiement	Entreprise	Grand	Moyen	Petit
Options de déploiement	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+			
Remote Collectors max. ⁴	50	50	20	20

¹ Éléments réseau : La somme des nœuds, des liens, des variables. ² Appareils IoT intelligents : Le concept d'« appareil IoT intelligent » couvre les appareils communiquant de manière intermittente à faible débit. ³ Les performances dépendent de la configuration matérielle et de l'allocation des ressources.

⁴ Voir les spécifications techniques des Remote Collectors pour plus de détails. Pour les spécifications techniques complètes et actuelles, consultez nozominetworks.com/techspecs ou contactez-nous.

Édition conteneur

Capteur embarqué en conteneur pour les commutateurs, les routeurs et autres infrastructures de sécurité. Option de déploiement rapide et flexible qui tire parti de vos appareils existants.

◆ Disponible uniquement pour Guardian avec le module complémentaire Smart Polling

	Conteneur
Offres embarquées	Gatewatcher, Siemens RUGGEDCOM
Modules complémentaires	Module Smart Polling : <i>inclus</i> Abonnements Threat Intelligence et Asset Intelligence : <i>peuvent être ajoutés</i>
Prise en charge des Remote Collectors	Non disponible

Pour les spécifications techniques complètes et actuelles, consultez nozominetworks.com/techspecs ou contactez-nous.

multiples options de déploiement et d'assistance

Voici plusieurs options pour le déploiement et l'assistance technique :

- **Partenaires de l'alliance stratégique mondiale** Nozomi Networks
- **SI/VARs** Nozomi Networks
- **Services professionnels** Nozomi Networks
- **Support client mondial** Nozomi Networks

Produits et services



SAAS

Vantage

Vantage accélère les interventions de sécurité grâce à une détection des menaces et une visibilité sans pareil sur vos réseaux industriels, informatiques, et l'IoT. Sa plateforme SaaS évolutive protège un nombre illimité de ressources en tout lieu. Vous pouvez réagir plus rapidement et plus efficacement aux cybermenaces, ce qui garantit la résilience opérationnelle.

Requiert les capteurs Guardian.



PÉRIPHÉRIE OU CLOUD PUBLIC

Guardian

Guardian fournit une sécurité et une visibilité robuste sur les systèmes industriels et de l'IoT. Il combine la découverte des ressources, la visualisation du réseau, l'évaluation des vulnérabilités, la surveillance des risques et la détection des menaces en une seule application. Guardian partage ses données avec Vantage et la CMC.



PÉRIPHÉRIE OU CLOUD PUBLIC

Console d'administration centrale

La console d'administration centrale (CMC) consolide la visibilité et la surveillance des risques sur les systèmes industriels et de l'IoT de vos sites distribués, à la périphérie ou dans le Cloud public. Elle s'intègre à votre infrastructure de sécurité informatique pour optimiser les workflows, et traiter les menaces et les anomalies plus rapidement.



ABONNEMENT

Asset Intelligence

Le service Asset Intelligence fournit des mises à jour régulières des profils pour une détection plus rapide et plus fiable des anomalies. Il vous aide à concentrer vos efforts et réduire le délai moyen de traitement (MTTR).



ABONNEMENT

Threat Intelligence

Le service Threat Intelligence fournit des renseignements en continu sur les menaces et les vulnérabilités des systèmes industriels et de l'IoT. Il vous aide à devancer les menaces émergentes et les nouvelles vulnérabilités, et réduire le délai moyen de détection (MTTD).



OPTION POUR GUARDIAN

Smart Polling

Smart Polling ajoute une interrogation active de faible volume à la découverte passive des ressources de Guardian, améliorant ainsi le suivi des ressources, l'évaluation des vulnérabilités et la supervision de la sécurité.



OPTION POUR GUARDIAN

Remote Collectors

Les Remote Collectors sont des capteurs nécessitant peu de ressources, qui collectent des données de vos sites distribués et les envoient à Guardian pour analyse. Ils améliorent la visibilité tout en réduisant les coûts de déploiement.



Nozomi Networks

La solution leader de sécurité et de visibilité OT et IoT

Nozomi Networks accélère la transformation digitale en protégeant les infrastructures critiques, les entreprises industrielles et les gouvernements du monde entier contre les cybermenaces. Notre solution offre une visibilité exceptionnelle sur le réseau et les ressources, une détection des menaces et des informations pour les environnements industriels et l'IoT. Les clients comptent sur nous pour minimiser les risques et la complexité tout en maximisant la résilience.