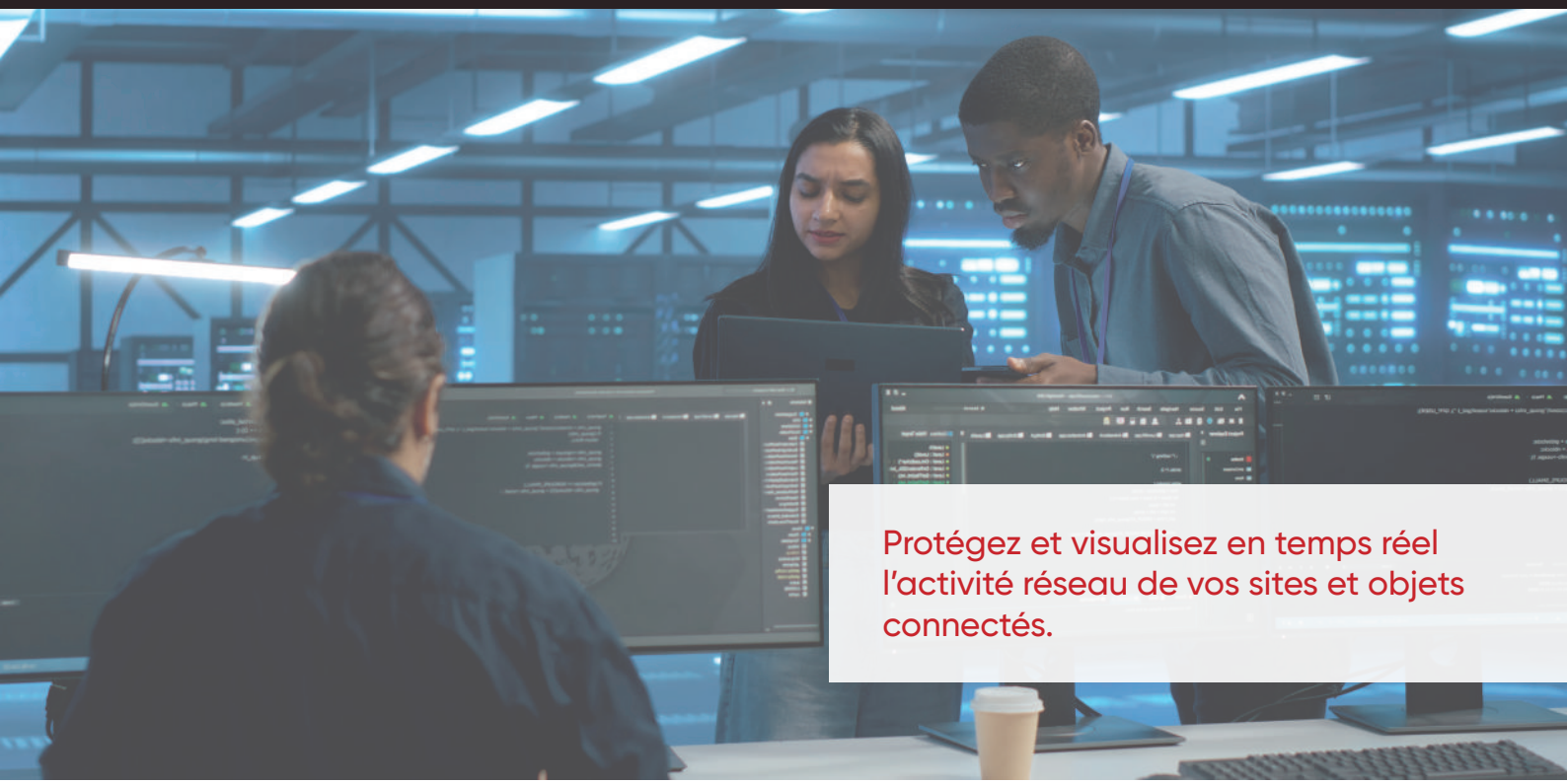
VIVALTEK | NETWORK SERVER



Protégez et visualisez en temps réel l'activité réseau de vos sites et objets connectés.

INTRODUCTION

Network Server convient aussi bien aux PME qu'aux grandes entreprises, en passant par les acteurs Publics et de la Santé. Il **apporte le niveau de sécurité d'un SOC[1] avancé**, sans la complexité ni les coûts d'un service managé. Une **protection haut de gamme**, accessible, pérenne et immédiatement opérationnelle.

Anticipez et neutralisez les cyberattaques avant qu'elles ne vous affectent. Grâce à son **moteur d'Intelligence Artificielle[2]**, Network Server analyse les flux en temps réel et réagit automatiquement en quelques secondes.

OBJECTIFS

Surveiller, anticiper et bloquer les cybermenaces en temps réel grâce à une combinaison puissante d'Intelligence Artificielle, de technologies avancées de filtrage et d'analyse réseau.

- **Suveiller, anticiper et bloquer les cybermenaces**
- **Analyser le réseau**
- **Détecter les cybermanaces en temps réel**
- **Protéger vos données**

LES CHIFFRES CLÉS*

4 386

événements de sécurité traités par L'ANSSI en 2024, soit une hausse de 15 % par rapport à 2023.

5 414

attaques à grande échelle ont été confirmées en 2024, soit une hausse de 11 % par rapport à 2023.

130

milliards de dollars en 2024, c'est le prix qu'a couté la cybersécurité en France contre 94 milliards l'année précédente.

**Toutes les sources sont disponibles sur notre site internet, dans la fiche produit correspondante.*

CONTACTEZ NOTRE EXPERT 02 52 61 46 75 | contact@vivaltek.com

Comment fonctionne Network Server ?

Network Server fonctionne comme une **véritable tour de contrôle de cybersécurité** embarquée. Installée au cœur de votre réseau ou sur un site distant, elle **sécurise immédiatement l'ensemble des flux entrants et sortants.**

Grâce à une carte réseau en mode passif (bridge) et à des technologies avancées comme le Deep Packet Inspection (DPI), elle **analyse en profondeur** chaque paquet sans impacter l'activité. Le serveur **détecte ainsi menaces, comportements anormaux, failles ou erreurs de configuration,** tout en établissant un inventaire des équipements, services, ports et protocoles présents.

L'Intelligence Artificielle intégrée **croise en continu les données collectées avec des bases de menaces mises à jour toutes les 2 minutes.** Elle peut ainsi anticiper les attaques via un module prédictif, et bloquer automatiquement toute tentative d'intrusion ou d'exploitation grâce à son module défensif.

Surveiller, anticiper et bloquer les cybermenaces en temps réel grâce à une combinaison puissante d'Intelligence Artificielle, de technologies avancées de filtrage et d'analyse réseau.

Network Server est une solution de cybersécurité de nouvelle génération, conçue comme un **véritable Centre de Sécurité des Opérations (SOC)** automatisé et accessible aux structures de toutes tailles.

Sur quoi s'appuie Network Server ?

Network Server repose sur une architecture modulaire capable de **protéger l'ensemble de votre environnement numérique** : réseaux internes, sites distants, télétravailleurs, objets connectés (IoT) et données sensibles. Son **approche à 360° répertorie en continu** les vulnérabilités et offre une protection dynamique contre les menaces émergentes.

Network Server **détecte les signaux faibles pour anticiper les attaques**, tandis que son moteur défensif déclenche des alertes et bloque automatiquement les **comportements malveillants**, y compris les attaques inconnues (zero-day). L'Intelligence Artificielle intégrée réagit en temps réel face aux tentatives de ransomware, de phishing ou d'intrusion.

Fonctionnalités de sécurité avancées :

- **Pare-feu nouvelle génération (NGFW) :** filtrage précis des flux et blocage intelligent des connexions suspectes.
- **Deep Packet Inspection (DPI) :** détection des comportements anormaux et des fuites de données.
- **IDS/IPS intégrés :** détection et prévention des intrusions avec réponse en temps réel.
- **VPN IPsec / SSL :** sécurisation des connexions inter-sites et télétravail via chiffrement AES-256.
- **Filtrage web et DNS :** contrôle de la navigation et blocage des sites malveillants selon des profils personnalisés.

Toutes les actions sont journalisées avec des logs complets exportables, compatibles avec les **outils SIEM**[3] et répondent aux les **exigences réglementaires (ISO 27001, NIS2, RGPD)**. Une interface web intuitive et une API ouverte facilitent la gestion centralisée, même sans équipe cybersécurité dédiée.

Pourquoi installer Network Server dans une entreprise ?

Contrairement aux solutions traditionnelles du marché comme DarkTrace (IA centralisée), Sophos (solution logicielle à déployer) ou Stormshield (matériel orienté pare-feu), Network Server propose une **approche 360°, autonome, souveraine et on premise**, pensée pour les entreprises qui veulent **sécuriser rapidement et efficacement leur réseau**, sans mobiliser des ressources humaines expertes et financières significatives et sans dépendre de services cloud externalisés.

1. **Une solution autonome et instantanée : Aucune installation logicielle et mise en fonctionnement rapide**. **Inspection réseau passive en bridge** sans modifier l'architecture existante. **Détection et blocage automatisés** des menaces grâce à l'IA embarquée (pas d'analyse déportée ni besoin de cloud).

2. **Une solution souveraine et conforme :** Conçue et hébergée en **France**, respectant les exigences **RGPD, NIS2 et DORA**. Sans transfert de données vers des clouds étrangers ou à risque. Convient aussi bien aux PME qu'aux grandes entreprises, en passant par les acteurs Publics et de la Santé.

3. **Une vision complète et unifiée de la cybersécurité :** Pare-feu NGFW. IDS/IPS. VPN sécurisé. Filtrage DNS/web. Module prédictif + défensif IA. Console de supervision + journalisation complète.

4. **Une solution proactive et évolutive :** Mises à jour automatiques **toutes les 2 minutes**. Détection proactive des **zero-days, ransomwares, cryptolockers** et comportements réseau anormaux. Adaptée à des environnements **multi-sites, télétravail ou OT (industriel/IoT)**.

Solution de cybersécurité autonome, souveraine et sans installation, elle s'intègre rapidement en passif sans modifier l'infrastructure existante, tout en bloquant les menaces grâce à une IA embarquée.

Conçue et hébergée en France, conforme RGPD, NIS2 et DORA, **elle s'adresse aux entreprises de toutes tailles**, y compris les secteurs publics et de la santé.

Lexique

[1]**SOC (Security Operations Center) :** Centre de sécurité qui surveille en temps réel l'ensemble des systèmes informatiques d'une organisation, afin de détecter, analyser et réagir rapidement aux cybermenaces.

[2]**IA : :** L'Intelligence Artificielle désigne un ensemble de techniques qui permettent à des machines d'imiter certaines capacités humaines, comme comprendre, apprendre, raisonner ou générer du contenu.

[3]**SIEM (Security Information and Event Management):** Outil qui centralise, analyse et corrèle en temps réel les journaux et événements de sécurité d'un système informatique, afin de détecter les incidents et alerter rapidement en cas de menace.

Consultez notre lexique complet à l'adresse suivante : https://vivaltek.com/lexique-complet

VIVALTEK
2, Impasse Johannes Gutenberg, Z.A Les Acacias III 85430 La Boissière des Landes
02 52 61 46 75 | contact@vivaltek.com