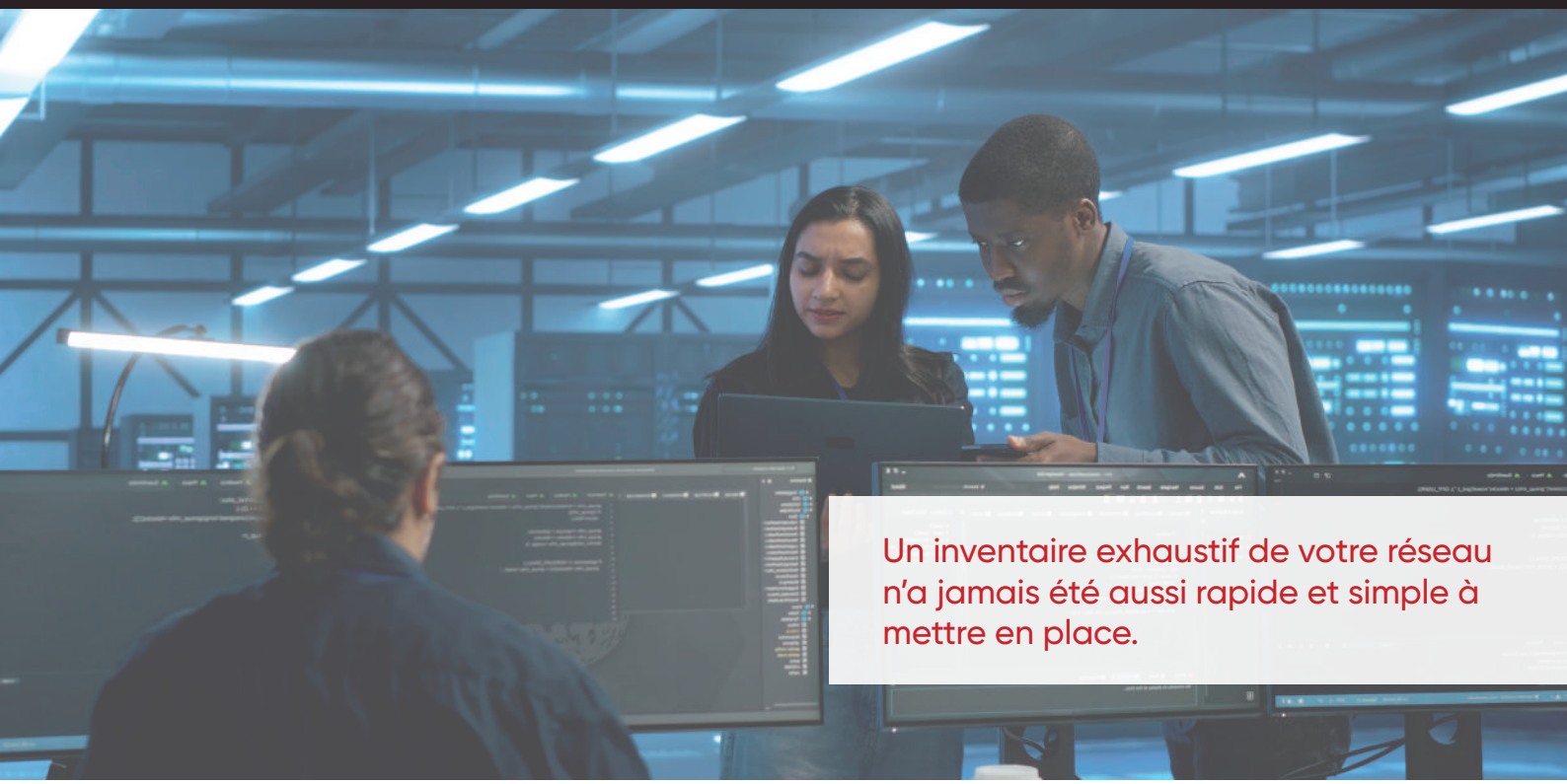
VIVALTEK | DPI NETWORK INVENTORY



Un inventaire exhaustif de votre réseau n'a jamais été aussi rapide et simple à mettre en place.

INTRODUCTION

Savez-vous réellement ce qui circule sur votre réseau ? **Identifier les services oubliés, les ports ouverts, les périphériques connectés et les failles invisibles** sont des tâches difficiles à réaliser pour un service informatique.

Identifier de façon exhaustive ces vulnérabilités réseau vous permet de mettre des actions en place afin d'**éviter des interruptions coûteuses, de protéger vos données et de préserver la confiance de vos partenaires** avant qu'un attaquant ne puisse s'en servir contre vous.

OBJECTIFS

Scanner et inventorier l'intégralité du réseau interne en identifiant équipements, services exposés et failles potentielles grâce à la technologie DPI[1].

- **Diagnostic rapide avec tableaux de bord complets**
- **Détecter les configurations à risque, vulnérabilités et menaces actives**
- **Préserver la confiance de vos partenaires**
- **Protéger les données, renforcer votre sécurité**

LES CHIFFRES CLÉS*

76 %

des attaques exploitent des assets réseau inconnus ou mal gérés, montrant l'urgence de connaître exactement ce qui circule en interne

97 %

des entreprises ont détecté au moins une activité réseau suspecte lors d'analyses DPI (ex : accès non autorisés, proxys, Tor...).

83 %

des organisations ont rapporté au moins un incident interne au cours de l'année écoulée. Ces incidents incluent à la fois des attaques malveillantes et des erreurs internes.

**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 le module DPI Network Inventory ?

Notre module travaille en toute discrétion, sans être détectable, déployée directement sur le site à évaluer, en étant interconnectée entre deux équipements du réseau (par exemple, entre un switch et un pare-feu).

Elle fonctionne en mode miroir : elle **capture l'intégralité des trames réseau sans altérer ni ralentir le trafic**. Cette approche est totalement transparente pour les utilisateurs, sans impact sur leur activité.

L'équipement intègre une interface de gestion indépendante, permettant un accès à **un portail web pour consulter les résultats de l'analyse.**

Une fois en place, notre solution utilise ses capacités de Deep Packet Inspection (DPI) pour **analyser en profondeur les paquets réseau.**

Elle fournit ensuite un **inventaire exhaustif des équipements connectés** (adresses IP et MAC, systèmes d'exploitation, applications détectées) et répertorie les communications internes.

Sur quoi s'appuie le module DPI Network Inventory ?

Ce module s'appuie sur les **capacités avancées de la technologie Deep Packet Inspection (DPI)**. Cette technologie permet une analyse fine du trafic en temps réel, quelque soit la taille du réseau (IP illimitées), en identifiant automatiquement :

- Les périphériques connectés (PC, téléphonie, IoT[2], équipements réseau),
- Les flux de communication (IP, Bluetooth, RF)
- Les protocoles utilisés (RDP, SSH, Telnet, etc.),
- Les ports ouverts,
- Les logiciels ainsi que leurs versions exposées,
- Ainsi que les signatures connues de vulnérabilités (CVE).

Grâce à cette inspection en profondeur, le module fournit une **vision précise et actualisée de l'état du réseau**, essentielle pour détecter les risques et maîtriser son exposition.

Pourquoi effectuer une évaluation via ce module DPI Network Inventory ?

Il s'agit d'un moyen concret de **révéler des failles souvent invisibles**, telles que l'usage de protocoles non sécurisés, la présence d'équipements obsolètes ou d'applications non détectées par les inventaires classiques.

Pour un DSI, cela permet d'**anticiper les incidents majeurs, d'éviter des interruptions coûteuses et de renforcer la continuité des activités**.

Partager les résultats d'un inventaire contribue à **responsabiliser les équipes internes** et à instaurer une véritable culture de la vigilance.

Une **meilleure connaissance du réseau**, de ses dépendances et de ses vulnérabilités techniques est notamment essentielle en cas de crise.

En **identifiant les points faibles et les zones critiques**, le DSI peut prioriser ses actions, orienter les investissements de manière pertinente et éviter des dépenses superflues sur des environnements déjà maîtrisés.

L'évaluation avec le module DPI Network Inventory

Elle permet de détecter des failles réseau souvent invisibles et de mieux anticiper les incidents critiques. Ce module favorise la responsabilisation des équipes, renforce la connaissance des environnements techniques et aide le DSI à cibler ses actions et investissements avec pertinence.

Sur quelle fréquence effectuer l'analyse, l'inventaire réseau et la détection du trafic ?

L'analyse réseau physique sur site permet une **inspection technique avancée du trafic réseau interne**, directement depuis vos locaux. Grâce à notre module, cette évaluation offre une **visibilité approfondie** sur les flux réels échangés dans votre système d'information.

Ce module nécessite une intervention physique sur site. **Sa mise en œuvre implique plusieurs étapes :** un déplacement sur site, une installation sur un point de capture stratégique, puis un retour de l'équipement une fois l'analyse terminée.

Ce type de prestation est à réaliser ponctuellement, notamment dans le cadre d'un audit complet de sécurité interne, lors d'un changement d'infrastructure tel qu'une refonte réseau, une segmentation ou un déménagement, ou encore en cas de suspicion d'intrusion ou de comportement anormal.

Sans installation sur les postes, cet audit **détecte les vulnérabilités, les configurations à risque et les menaces actives**, en offrant un diagnostic rapide et des tableaux de bord complets vous permettant d'agir précisément afin de renforcer votre sécurité.

Ce module convient aussi bien aux PME qu'aux grandes entreprises, en passant par les acteurs Publics et de la Santé, pour contrôler et maîtriser l'activité sur le réseau.

Lexique

[1]**DPI :** Technologie qui permet d'analyser en détail le contenu des paquets réseau (pas seulement l'en-tête), afin de détecter les types de trafic, les applications utilisées, les protocoles, et même les menaces potentielles comme les malwares ou les tentatives d'intrusion.

[2]**IoT (Internet des Objets) :** Désigne tous les objets connectés à Internet capables de collecter, transmettre ou recevoir des données, sans intervention humaine direct.

IA : L'intelligence artificielle (IA) désigne un ensemble de techniques qui permettent à des machines d'imiter certaines capacités humaines, comme comprendre, apprendre, raisonner ou générer du contenu.

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