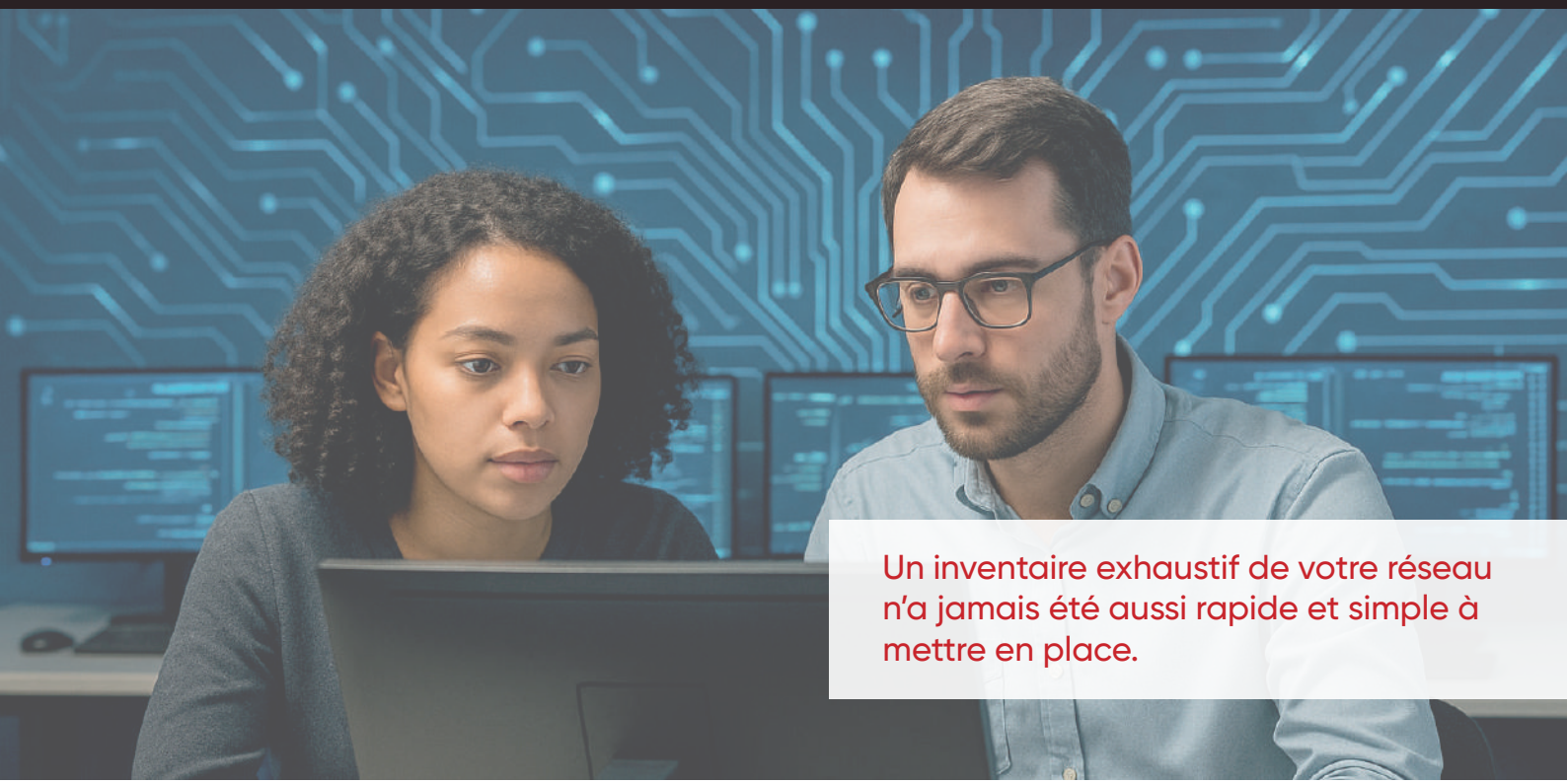
VIVALTEK | DPI SERVER



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 vulnérabilités, configurations à risque 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 DPI Server ?

Notre logiciel et son serveur spécifique sont déployés sur le site à surveiller. Il **travaille en toute discrétion**, sans être détectable. Il se connecte entre votre réseau interne et le routeur, ce qui lui permet de capter l'ensemble des flux qui y transitent.

Dans le cadre de multi-sites, il est possible d'**installer plusieurs points de capture** qui communiquent simultanément avec un **serveur central chargé d'analyser toutes les données collectées et de les restituer dans un tableau de bord dédié.**

Les équipements sont configurés en mode bridge, ce qui les rend **invisibles sur le réseau.** Ils fonctionnent comme une **boîte noire**, enregistrant localement l'activité sans procéder à **aucune externalisation des données.**

Chaque point de capture est également équipé d'une interface de gestion indépendante, accessible via une carte réseau dédiée. Cette interface permet de consulter les résultats en toute sécurité à travers un portail web.

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.

Sur quoi s'appuie DPI Server ?

Ce serveur 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[3]).

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

Grâce à l'intégration d'algorithmes d'intelligence artificielle, il **analyse en continu** les modèles de trafic habituels, repère les signaux faibles ainsi que les écarts de comportement, et **identifie des menaces** encore inconnues ou de type zero-day, sans se limiter à une base de signatures prédéfinies.

Les données collectées sont **stockées localement de manière sécurisée et inaltérable**. Chaque événement réseau détecté est enregistré et historisé, ce qui permet une traçabilité complète des incidents. Le logiciel génère également des **alertes précises et des rapports détaillés**, conformes aux exigences des audits internes ou des régulateurs.

Facile à déployer, le serveur s'**intègre sans difficulté dans votre infrastructure existante**, sans nécessiter de réarchitecture ni d'interruption de service. Il est **compatible avec les environnements multi-sites** ainsi qu'avec les architectures hybrides.

Enfin, le logiciel est conçu pour évoluer en même temps que votre réseau et s'**adapter en continu à vos besoins opérationnels et de sécurité**.

Pourquoi installer DPI Server au sein d'une entreprise ?

Cette approche offre un moyen concret de **détecter des failles souvent invisibles**, telles que l'usage de protocoles non sécurisés, la présence d'équipements obsolètes ou encore des applications non référencées par les inventaires traditionnels. Pour un DSI, cela représente une opportunité précieuse de **prévenir les incidents majeurs, d'éviter les interruptions coûteuses et de renforcer la continuité des activités**.

Le partage des résultats issus d'un inventaire en continu contribue à **responsabiliser l'ensemble des acteurs internes** et à instaurer une véritable culture de la vigilance. Mieux connaître son réseau, ses dépendances et ses vulnérabilités techniques permet également d'**assurer une bonne continuité de l'activité de l'entreprise.**

En identifiant les points faibles et les zones critiques, le DSI peut **hiérarchiser les priorités, orienter les investissements de manière stratégique et éviter les dépenses superflues sur des périmètres déjà maîtrisés.**

Notre solution s'inscrit pleinement dans les exigences des cadres réglementaires tels que le **RGPD**, la **directive NIS2** ou encore le **règlement DORA**. Elle vous offre une visibilité complète sur vos réseaux et vos données critiques. **Elle fournit une source d'informations fiables à transmettre aux autorités en cas de cyber incidents.**

L'évaluation DPI Server :

Permet d'identifier des vulnérabilités souvent invisibles, de responsabiliser les équipes et d'instaurer une culture de vigilance. Elle aide le DSI à prioriser ses actions, optimiser les investissements et répondre aux exigences réglementaires en assurant une visibilité claire sur les réseaux et données critiques.

Lexique

[1]**DPI (Deep Packet Inspection) :** 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 directe.

[3]**CVE (Common Vulnerabilities and Exposures) :** C'est un identifiant unique donné à une faille de sécurité informatique connue, pour la répertorier et la partager publiquement. Elle permet aux entreprises et aux experts de connaître, suivre et corriger plus facilement les vulnérabilités dans les logiciels et systèmes.

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