WhiteN®

STATION DE NEUTRALISATION
DES MENACES USB

# Maîtrisez les contenus importés dans votre SI via supports amovibles

- Filtrage des contenus et vérification d'innocuité
- Vérification de formats et détection de charges actives cachées
- Blocage des périphériques non reconnu
- Cloisonnement fort des environnements d'analyse

*Security by design certifiée*
SOLUTION BASEE SUR NOTRE HYPERVISEUR DE SECURITE
CERTIFIE EAL 5+ & LABELLISE FRANCE CYBERSECURITY

www.bertin-it.com

bertin IT

CNIM

# WhiteN®

## STATION DE NEUTRALISATION DES MENACES USB

*« Même lorsqu'ils sont isolés d'Internet, les systèmes d'information sensibles et les infrastructures critiques demeurent exposés au risque d'injection de contenus malveillants parle biais de supports amovibles non maîtrisés (clés USB, téléphones portables, chargeurs de batterie, etc.).*

**WhiteN®** combine plusieurs barrières pour assurer la défense en profondeur des SI sensibles et des infrastructures critiques contre les menaces issues de tout type de supports amovibles (clés USB, téléphones portables, chargeurs de batterie, etc.).

### FILTRAGE DES CONTENUS

Certains types de fichiers sont explicitement autorisés ou interdits (p.ex. exclusion des .avi, ...) selon la politique de sécurité en vigueur dans l'entreprise.

### VERIFICATION D'INNOCUITE

**WhiteN®** vérifie la présence de virus et autres malwares sur tout type de supports au moyen de deux antivirus leaders sur le marché.

### VERIFICATION DE FORMAT

Les fichiers changés (p.ex. modification malicieuse d'un .txt en .pdf), les contenus exécutables ou les charges actives cachées sont détectés et neutralisés.

### LABELLISATION

Cette fonctionnalité permet à l'utilisateur d'apposer sur des fichiers (p.ex. mise à jour SCADA...) un sceau garantissant l'intégrité et l'authenticité des données. La vérification de ce label est effectuée lors du traitement.

## *Security by design certifiée*

### CLOISONNEMENT DES SYSTEMES HOTES

D'une architecture basée sur **PolyXene®**, socle logiciel de très haute sécurité certifié EAL 5+ et labellisé France Cybersecurity, **WhiteN®** est doté de mécanismes de cloisonnement fort des environnements virtualisés. Ainsi, **le SI n'est jamais exposé au support non maîtrisé.**

Non seulement, toute attaque est confinée au sas de neutralisation sans risque de compromission du SI, mais la fuite d'informations est également empêchée.

### FILTRAGE DES PERIPHERIQUES (option)

**WhiteN®** assure le filtrage par classe et par liste blanche des périphériques : tout appareil non explicitement autorisé par la politique de sécurité est bloqué. Ceci protège contre les attaques de type **BadUSB** et limite l'utilisation d'appareils personnels sur le lieu de travail.

### MISE EN QUARANTAINE (option)

Les fichiers refusés peuvent être conservés pour une investigation a posteriori en vue d'identifier les éléments ayant motivé le blocage.

## Simplicité de déploiement et d'utilisation

Déployé en **standalone** ou **connecté au SI**, **WhiteN®** est très peu intrusif et facilement paramétrable. Après branchement, une interface guide l'administrateur pour régler la politique de sécurité et configurer le dispositif selon ses besoins.

Présenté sous la forme d'une **station de travail tout-en-un** accessible à l'ensemble des collaborateurs, **WhiteN®** est d'utilisation tout aussi simple :

1. connexion du support
2. sélection des fichiers à importer dans le SI
3. récupération de contenus sains et approuvés, via un support amovible maîtrisé (p.ex. clé corporate) ou par courrier électronique (mode connecté au SI).

Un rapport rassemblant les informations relatives aux traitements effectués sur les fichiers est remis à l'utilisateur. Un journal d'évènements est également établi au format SYSLOG et exporté vers un serveur de journalisation.

[© 2017, Bertin IT. Tous droits réservés.]

Suivez Bertin IT
www.bertin-it.com

Bertin IT, société du groupe CNIM
10 bis avenue Ampère, 78180 Montigny-le-Bretonneux
E. security@bertin-it.com T. +33(0)1 39 30 60 00