Blocky pour Veeam®

Protection ultime contre les ransomware* avec la technologie WORM**

* Ransomware : un rançongiciel ou logiciel rançonneur ou logiciel de rançon ou logiciel d'extorsion
** WORM (W*rite Once Read Many*) Technologie rendant non réinscriptibles les fichiers

GRAU DATA
Your data \ Your control _

Blocky c’est quoi ?

“Votre dernière ligne de défense contre les ransomware”

Blocky protège vos données Windows-Veeam de sauvegarde contre les ransomware

Ajouter Blocky à Veeam pour créer un environnement “**confiance zero**”

GRAU DATA
Your data \ Your control _

Pourquoi a-t-on besoin de Blocky?

Les Trojans ransomware modernes cherchent systématiquement à infecter toutes vos données qui ont de la valeur, comme les données de sauvegarde.

Les procédures traditionnelles de protection des données telles que les scanners de virus sont inefficaces contres les ransomware.

GRAU DATA
Your data \ Your control _

Que fait Blocky ?

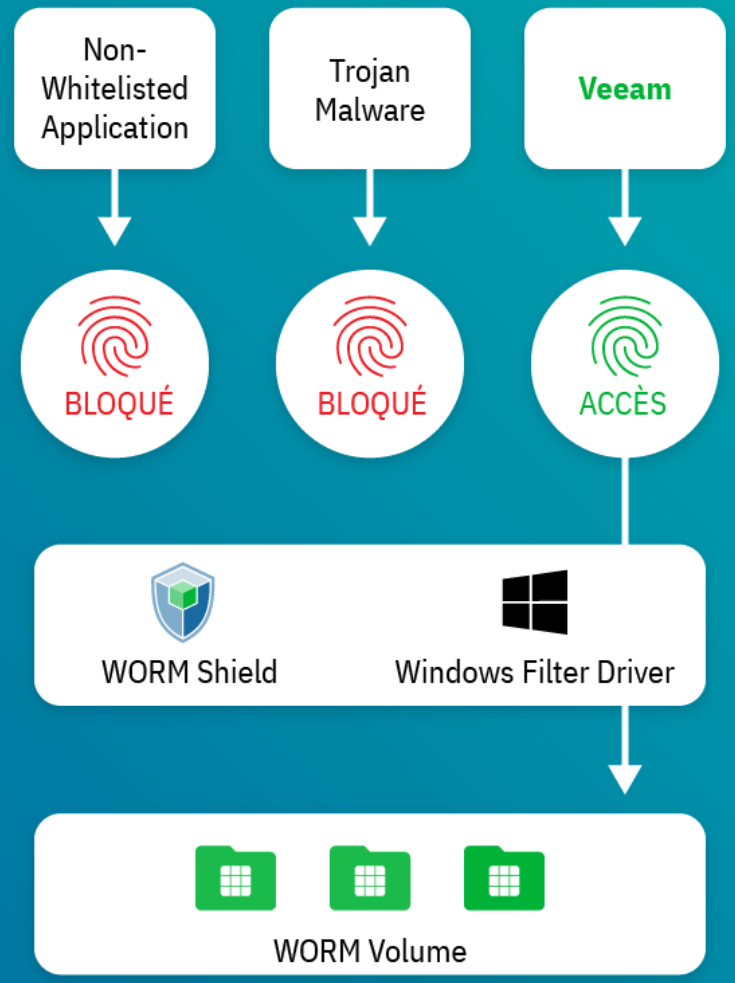
Blocky crée une empreinte digitale (“**fingerprint“)** pour chaque procédure d’accès aux fichiers de sauvegarde Veeam.

Blocky empêche l’accès pour supprimer ou écrire si l’empreinte digitale („fingerprint“) ne correspond pas explicitement pour chaque traitement.

GRAU DATA
Your data \ Your control _

Un traitement unique

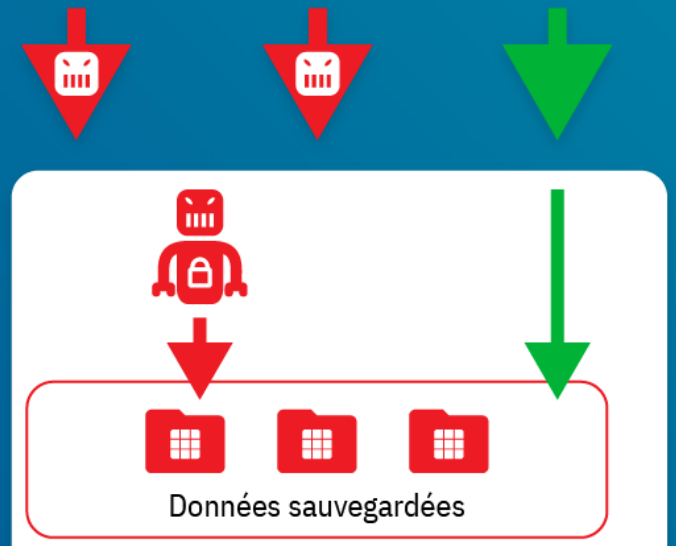
- Seules les applications approuvées “whitelisted” (Veeam) ont accès aux données de sauvegarde Veeam et sont autorisées pour écrire, ajouter ou supprimer des fichiers.
- Les accès non autorisés sont bloqués par le filtre du driver Blocky, empêchant la destruction ou l’encryptage des données de sauvegarde
- Blocky empêche d’endommager les données de sauvegarde même dans le cas où un virus a pénétré le système de sauvegarde Windows.



GRAU DATA
Your data \ Your control _

Blocky for Veeam en action

Sauvegarde Veeam sans Blocky

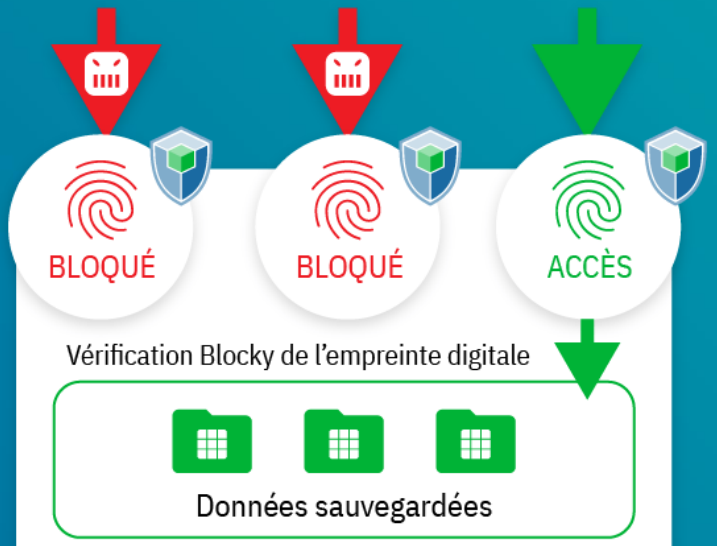


Le „ransomware“ peut entrer dans le système de sauvegarde

Et modifier/encrypter/supprimer les données de sauvegarde

L’utilisateur n’a plus accès à ses données

Sauvegarde Veeam avec Blocky



Les données de sauvegarde sont protégées par Blocky. Seule l’application « whitelisted » peut modifier les données

Les données sauvegardées sont toujours protégées et accessibles en cas d’attaque

GRAU DATA
Your data \ Your control _

Fonctionnalités-clé

- **Les systèmes de fichiers Windows utilisés pour les données de sauvegarde sont transformés en un système de fichiers WORM.**
  - Blocky rend automatiquement le volume en non-réinscriptible (WORM)
  - Tous les accès au système de fichiers sont contrôlés par un driver de filtres Windows
  - Seuls les accès ayant la permission Whitelist peuvent créer et modifier les fichiers dans le volume WORM et les accès non-autorisés sont bloqués.

- **Les accès qui nécessitent une permission pour modifier les données (par exemple les données de sauvegarde) :**
  - Doivent être autorisés par l'administrateur
  - Doivent avoir une empreinte digitale Blocky (fingerprint)
  - La vérification de l'empreinte digitale inclut les applications DLL's

Fonctionnalités-clé

- **Blocky est conçu pour empêcher les attaques et les intrusions :**
  - Blocky nécessite un **mot de passe séparé**, indépendant de SSO et AD, qui garantit la protection contre les changements et manipulations du logiciel non autorisés.
  - Les installations Blocky sont liées au serveur uniquement en incorporant le server ID qui devient une partie de l'empreinte digitale (fingerprint),empêchant des copies, des clones ou un vol de la whitelist.

- Très faible overhead & hautes performances
  - Overhead zéro pendant l'écriture et la lecture
  - Environ 2-3 % overhead pendant la suppression & l'ajout

Evolutivité

- Point d’entrée à 50 teraoctets pour les PME jusqu’à plusieurs pétaoctets pour des grands groupes
- Le système de management centralisé de Blocky nécessite une seule installation sur un seul serveur pour supporter un environnement multi-serveurs.

GRAU DATA
Your data \ Your control _

Synthèse

- Blocky est un outil pour les repositories Windows/ Veeam repositories de block storage
- Aucun hardware supplémentaire ou Linux repository est nécessaire
- Installation facile en quelques minutes
- Une conception de produit simple pour une protection maximale contre les “ransomware”
- Pré-requis pour les revendeurs : connaissances Veeam et Windows
- GRAU DATA fournit une formation clés-en-mains pour les revendeurs
- Prix attractifs pour les clients finaux et les partenaires Veeam®

Interlocuteur commercial en français

Didier Papion

Directeur GRAU DATA France
didier.papion@graudata.com
Tel : 06.07.79.41.28

Interlocuteur technique en anglais

Kai Hambrecht

Head of Service & Support
kai.hambrecht@graudata.com
Tel : +49 7171 187-317

GRAU DATA
Your data \ Your control _