



## **Blocky for Veeam®**

Blocky Disc Protection & WORM  
Funktionalität – Die ultimative  
Sicherheit für das Windows VBR



**GRAU DATA**

Your data \ Your control \_

# Was ist Blocky?

Blocky schützt Windows basierte Backup Daten auf der letzten möglichen Verteidigungslinie.

**„Your Last Line of Defense“ against ransomware**

Blocky ermöglicht eine “Zero Trust” Sicherheit für Ihr Veeam Backup.



# Warum benötigen Sie Blocky?

Schützen Sie Ihre wertvollen Veeam Backupdaten vor Cyberangriffen, Manipulation und versehentlichem Löschen.

Diese Features bieten einen leistungsstarken Schutzmechanismus für Ihre physischen Datenträger unter Windows und sichern Ihre Backup Daten zuverlässig ab.



# Wie funktioniert Blocky?

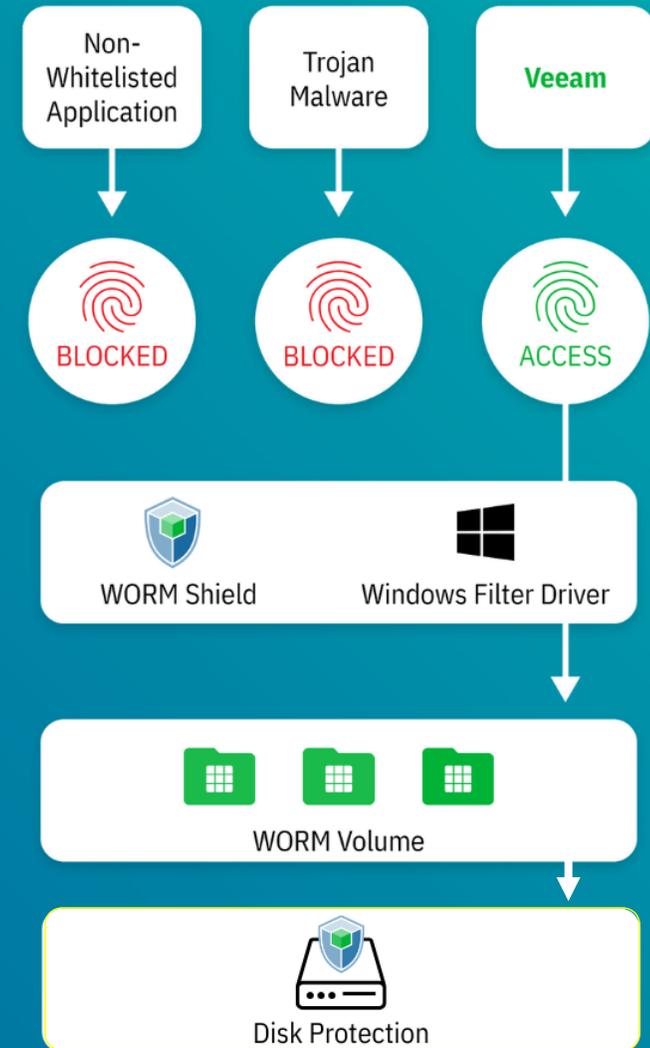
Blocky nimmt von jedem Prozess einen „**Fingerabdruck**“ und verhindert schreibende Zugriffe, wenn der „Fingerabdruck“ nicht explizit für diesen Vorgang freigegeben ist.

Nur die Backup Applikation Veeam wird mit ihrem Fingerabdruck „**White gelistet**“ und kann dadurch Daten löschen oder ändern.



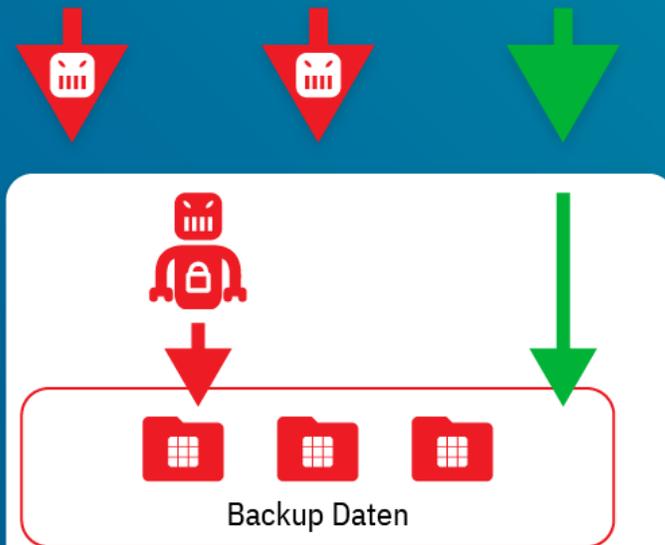
# Unique **process**

- **Echtzeitschutz** – Verhindert unerwünschte Änderungen und schützt vor Cyberangriffen.
- **Unveränderlicher Modus** – Sperrt Ihre Disc-Inhalte gegen jegliche unautorisierte Modifikationen.
- **Benutzerfreundlich** – Einfache Installation und intuitive Bedienung für maximale Kontrolle.



# Blocky for Veeam in Aktion

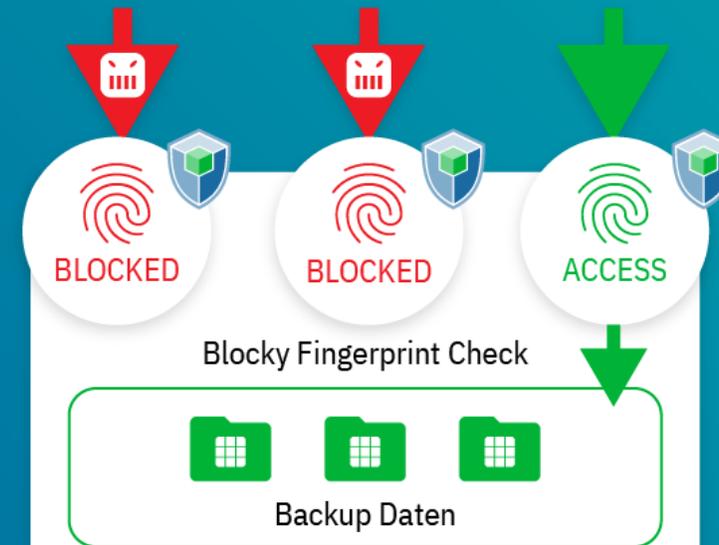
## Veeam Backup ohne Blocky



Ransomware kann in das Backup-System eindringen und die Backup Daten löschen oder verschlüsseln.

Der User hat keine Möglichkeit mehr auf die geänderten Dateien zuzugreifen.

## Veeam Backup mit Blocky



Backup Schutz über eine Methode mit Fingerabdruck. Nur die zugelassene Anwendung kann Daten ändern.

Die Veeam Backup Daten werden selbst im Falle eines erfolgreichen Angriff auf das System immer geschützt sein.

# Zentrale Funktionen

- **Das Windows Filesystem wird für die Datenablage als Ganzes zum WORM Filesystem**
  - Blocky setzt das/die Volumes automatisch zum WORM Volume.
  - Wenn bereits existierende Files gelöscht oder verändert werden sollen, blockiert der Windows Filter-Treiber diese Zugriffe.
  - Prozesse, denen das Verändern von Daten erlaubt werden soll, z. B. Veeam Backup-Prozesse, müssen vom Administrator über „Fingerabdrücke“ freigegeben werden.
- **Alle Prozesse, denen das Verändern der Daten erlaubt werden soll:**
  - Müssen vom Administrator freigegeben werden.
  - Brauchen einen Blocky Fingerabdruck.
  - Der Fingerprint beinhaltet zur zusätzlichen Sicherheit die DLL's

# Zentrale Funktionen

- **Blocky verhindert “Hacks” und Umgehungsversuche:**
  - Es ist für die Bedienung und Konfiguration ein separates Passwort nötig, unabhängig von SSO oder Active Directory.
  - Die Blocky Software ist über eine eindeutige ID mit dem Veeam Repository Server verknüpft. Die Server ID ist Teil des Fingerprints, so kann verhindert werden, dass unautorisierte Kopien, Clones oder Kapern der Blocky Whitelist erfolgen kann.
- **Geringer Overhead & Hohe Performance im laufenden Betrieb**
  - Beim Schreiben & Lesen beträgt der Overhead “Null”.
  - Beim Löschen und Verändern von Daten beträgt der Overhead ca. 2-3 %.

# Skalierbarkeit

- Blocky beginnt bei 25 TB Kapazität (KMU) und skaliert bis zu mehreren PB für Enterprise Kunden
- Die Centralized Management UI muss nur auf einem von mehreren Blocky Servern installiert werden.



# Highlights

- Blocky schützt Windows-basierte Veeam Backups-Repositories für Block-Storage
- Keine zusätzliche Hardware oder Linux System notwendig
- Einfache Installation in wenigen Minuten
- Schlankes Produkt mit höchstem Schutz gegen Ransomware
- GRAU DATA liefert technisches Training für Blocky Reseller (Einzige Voraussetzung: Veeam und Windows Kenntnisse)
- Attraktiver Preis für Endkunden und Veeam® Partner



# Jochen Strubel

Channel Manager  
Jochen.Strubel@graudata.com  
Tel: +49 7171 187-123

# Kai Hambrecht

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



**GRAU DATA**

Your data \ Your control \_