Blocky for Veeam®

Highest protection against ransomware through WORM technology

GRAU DATA

Your data \ Your control _

What is Blocky?

„Your Last Line of Defense“ against ransomware

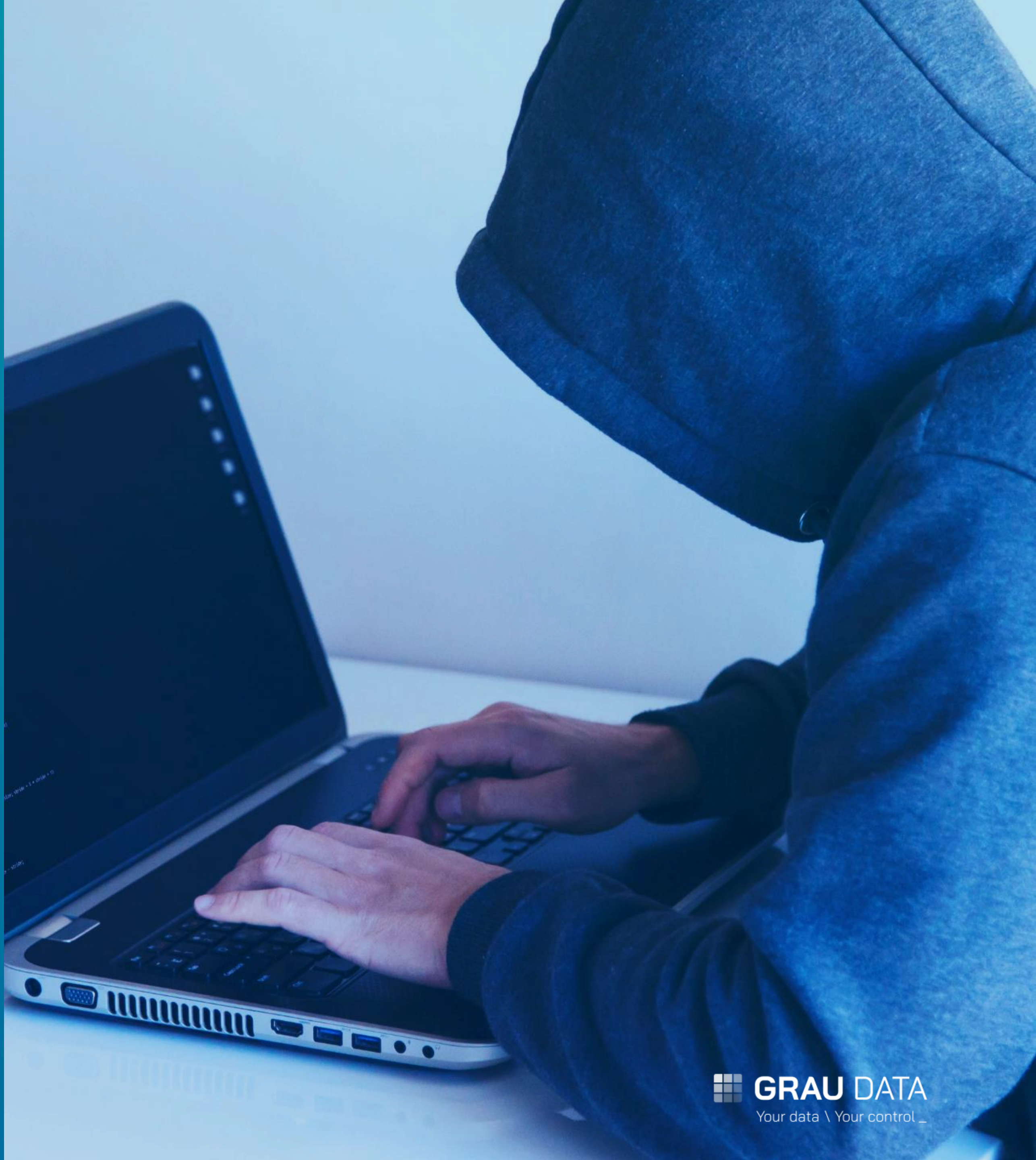
Blocky protects your Windows-based Veeam backup data against ransomware

Add Blocky to Veeam to create a **“Zero Trust”** environment

Why do you need Blocky?

Modern ransomware trojans are systematically searching to infect any high-value data, f.e. backup data.

Traditional data protection procedures such as virus scanners are ineffective against ransomware.



GRAU DATA

Your data \ Your control _

What does Blocky do?

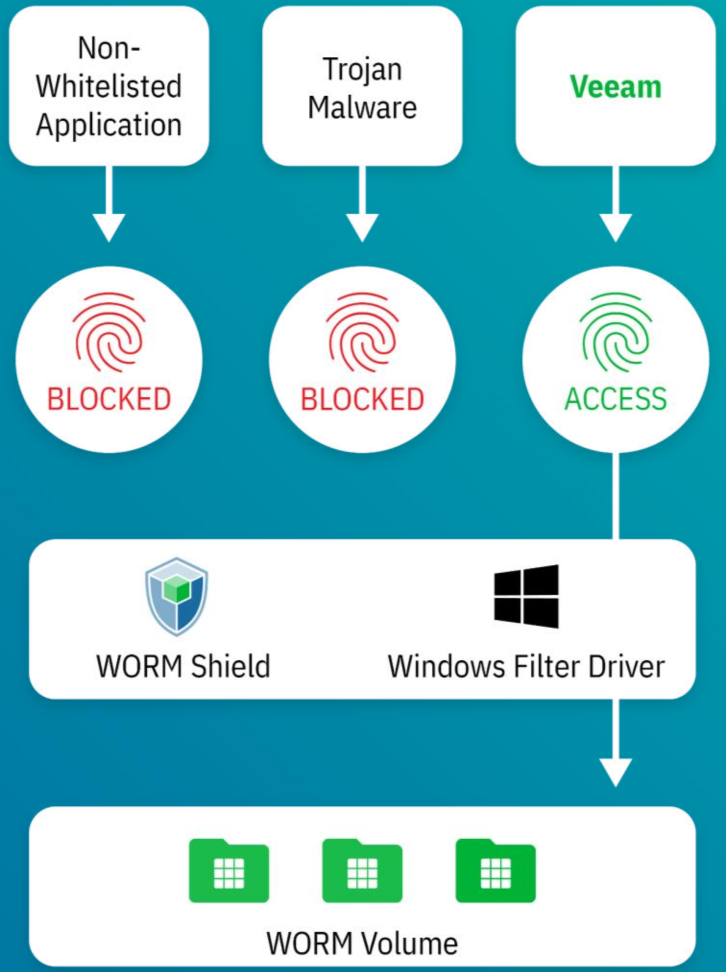
Blocky creates a **„fingerprint“** for each process accessing Veeam backup files.

Blocky prevents delete or write access if the „fingerprint“ is not explicitly matched for each process.

GRAU DATA
Your data \ Your control _

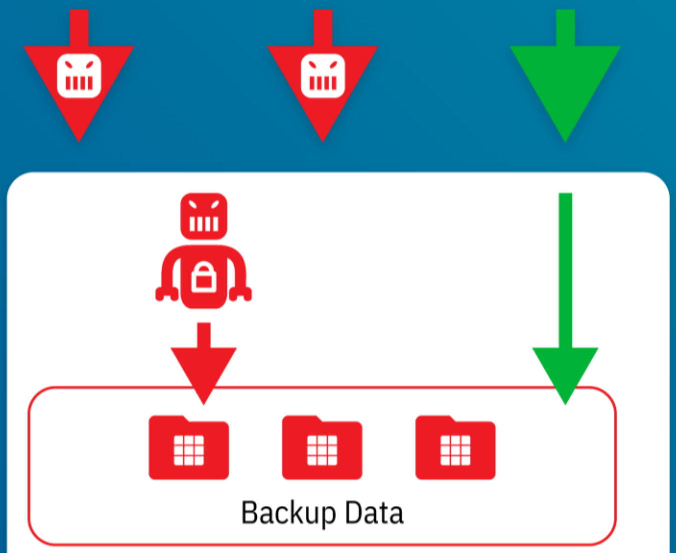
Unique process

- Only approved whitelisted applications (Veeam) have access to Veeam backup data and are allowed to write, append or delete files.
- Unauthorized access is stopped by the Blocky filter driver, preventing the destruction or encryption of backup data
- Blocky prevents damage to backup data even if a virus has entered the Windows-backup system.



Blocky for Veeam in action

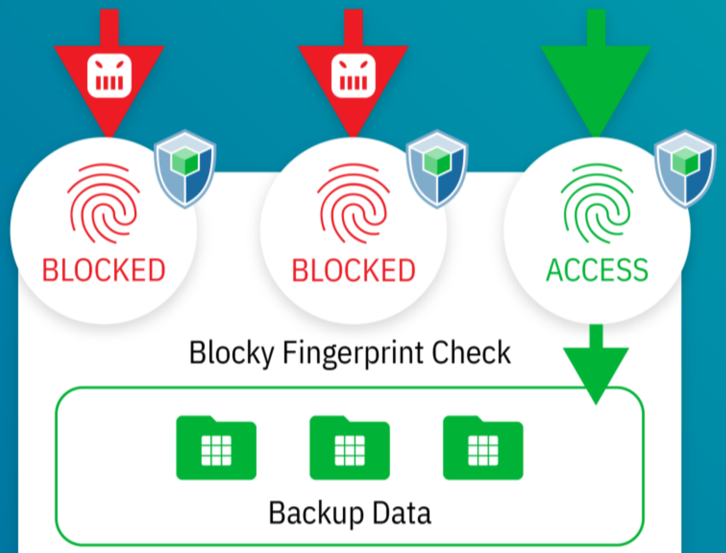
Veeam Backup Without Blocky



Ransomware can enter the backup system an modify/encrypt/delete the backup data.

The user no longer has access to their data.

Veeam Backup With Blocky



Backup data is protected by Blocky. Only the whitelist application can modify data.

Backup data is always protected and accessible even in the case of an attack.

GRAU DATA
Your data \ Your control _

Key Functions

- **Windows file systems used for backup data are transformed into a WORM file system.**
  - Blocky automatically sets the volume as WORM.
  - All accesses into the file system are then controlled via a Window's filter driver.
  - Only processes that have Whitelist permission can create and modify files within the WORM volume and unauthorized processes are blocked.

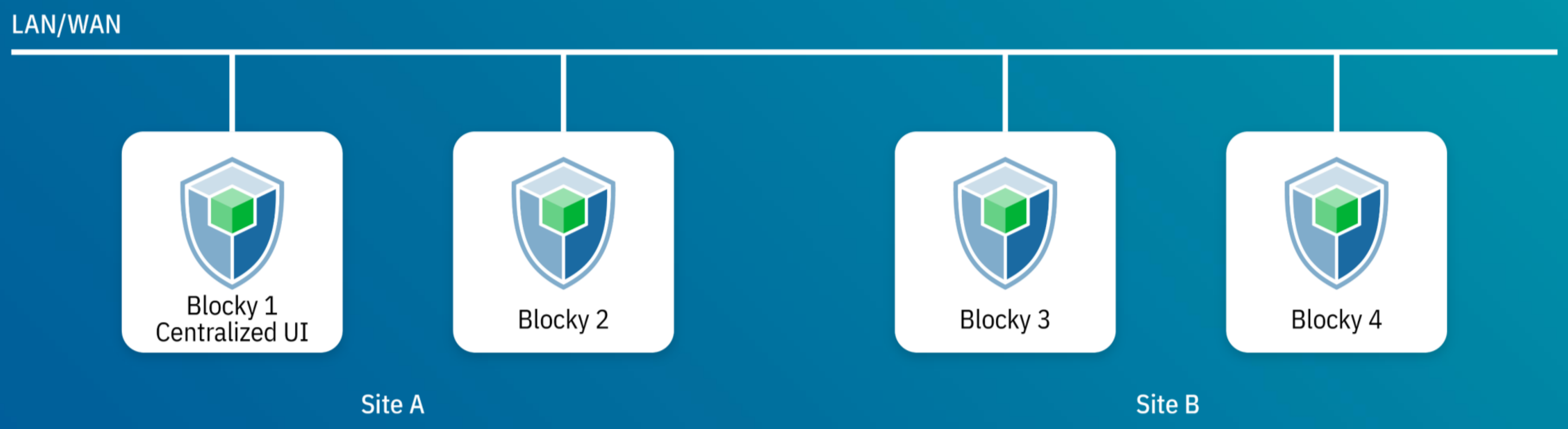
- **Processes which need permission to modify data (e.g. backup processes):**
  - must be authorized by the administrator
  - have a Blocky fingerprint.
  - fingerprint verification includes the applications DLL's

Key Functions

- **Blocky is designed to prevent hacks and work-arounds:**
  - Blocky requires a **separate password**, independent of SSO and AD, that ensures protection against unauthorized changes and manipulation of the software.
  - Blocky installations are uniquely linked to the server by incorporating the server ID which becomes part of the fingerprint, preventing unauthorized copies, clones or high jacking of the whitelist.
- **Low overhead & high performance**
  - Zero overhead while writing and reading
  - Approx. 2-3 % overhead during delete & append processes.

Scalability

- Starting with SMB customers (50 TB) up to Enterprise customers with multiple PB
- Blocky centralized management only needs to be installed on a single server to support a multi-server environment.



GRAU DATA
Your data \ Your control _

Summary

- Blocky is for Windows-based Veeam repositories on block storage
- No additional hardware or Linux repository required
- Easy installation in minutes
- Lean product design for maximum protection against ransomware
- Reseller requirements: Veeam and Windows knowledge
- GRAU DATA provides hands-on technical training for Reseller
- Attractive pricing for end-user and Veeam® partners

Kai Hambrecht

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

Didier Papion

Director GRAU DATA France
didier.papion@graudata.com
Phone: 06.07.79.41.28

GRAU DATA
Your data \ Your control _