Blocky for Veeam®

Zero-Trust Backup Protection with Application Whitelisting:

How Blocky for Veeam® backup repositories reliably protect against modern ransomware

The integrity of backups is critical to the resilience of modern IT infrastructures.

Recent studies show that ransomware no longer attacks only production systems, but also specifically targets backup repositories. According to the Veeam Data Protection Trends Report 2024, backups were attacked in 93% of all ransomware incidents, and in 75% of cases backup data was partially or fully compromised.

Because traditional security mechanisms are largely signature-based, they can detect zero-day attacks or legitimate but manipulated system processes only to a limited extent. "Living-off-the-Land" techniques use existing system tools such as PowerShell or WMI to operate without conventional malware code.

Application Whitelisting implements a zero-trust principle at process level: Only authorized applications may write to defined resources; everything else is blocked. Blocky for Veeam® applies this principle directly within the backup repository and protects data from encryption, manipulation and deletion. The solution is kernel-based, signature-independent and has no noticeable performance overhead.

This whitepaper is intended for technical engineers and describes how application whitelisting works, why it is particularly useful in the backup context and how Blocky for Veeam® can be pragmatically integrated into existing Veeam environments.

- ***93% of organizations:***
  at least one ransomware incident within the last 12 months.
- ***In 75% of cases:***
  backup data was also compromised or attacked.
- ***Clear trend:***
  attacks no longer target only production systems, but also specifically target all recovery mechanisms.

Free Trial:
BlockyforVeeam.com

Blocky for Veeam®

The threat landscape for backup systems

Backups as a primary target of modern ransomware

Ransomware has evolved from "simple" encryption software into a highly developed, multi-stage attack methodology. Today, attacks typically consist of:

- initial compromise (e.g. phishing, vulnerabilities in VPNs or applications),
- lateral movement in the network,
- privilege escalation and credential theft,
- targeted disabling of security solutions,
- attack on backup and recovery infrastructure,
- final encryption and ransom demand.

For technical planning, backups are no longer just insurance; they are an active attack target that organizations must prepare for.

Weaknesses of traditional security mechanisms

Traditional security solutions such as antivirus, EDR, firewalls or email gateways primarily work with:

- signatures (known malware samples),
- heuristics,
- behavioral patterns.

These mechanisms are important, but they do not address every attack scenario:

- Zero-day exploits are, by definition, not signed.
- LoTL attacks use legitimate tools (PowerShell, WMI, PsExec).
- Process impersonation can make processes "look" as if they were trustworthy.

Windows-based backup repositories in particular are often:

- placed low in organizational priorities,
- equipped with extensive permissions,
- monitored less closely than production systems.

The result:

One successful attack on domain or backup server credentials can lead to unnoticed manipulation or encryption of backup data.

Blocky for Veeam®

The threat landscape for backup systems

Typical attack vectors against Veeam repositories

For technical engineers, it is worth looking at typical patterns:

Process impersonation
Malware attempts to present itself as a legitimate Veeam process, for example by using identical or similar process names.

Credential theft & abuse
Stolen admin or service credentials are used to redirect or delete backup jobs, or to encrypt repositories directly.

LoTL-based encryption
Attackers use built-in tools such as cipher.exe, robocopy.exe or scripts to modify data on the repository without deploying "foreign" binaries.

Gradual encryption
Instead of encrypting everything at once, backup files are modified incrementally over days or weeks to remain undetected for longer.

These patterns have one thing in common:

They are difficult to detect with traditional blacklisting approaches - especially when legitimate tools are used.

Blocky for Veeam®

Application Whitelisting: Zero-Trust Protection at File System Level

Functional principle

Application whitelisting reverses the usual security approach. Instead of defining "what is forbidden", it defines:

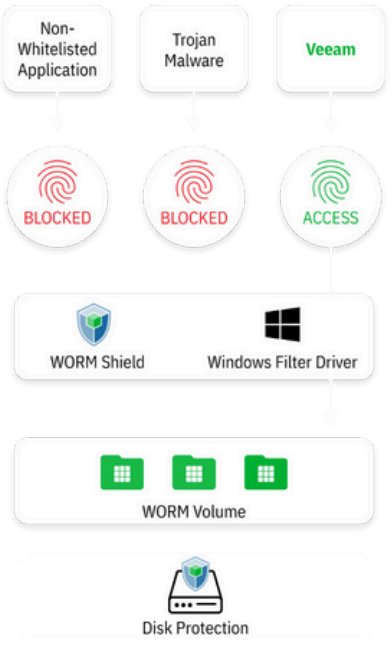
Only clearly known, verified applications may perform specific actions. Everything else is prohibited by default.

Technically, this means:

- Every executable file (EXE, DLL, etc.) receives a cryptographic hash (fingerprint).
- A whitelist contains all fingerprints that are approved for specific actions (e.g. write access).
- A filter mechanism monitors the relevant resources (here: backup repository).
- For every write operation, it checks whether the process belongs to the whitelist.
- If not, access is blocked - regardless of permissions, origin or signature status.

The result:

Even completely new, previously unknown malware is stopped as long as it has not been explicitly approved.



Advantages over traditional methods

In the backup context, application whitelisting offers several particularly relevant advantages:

- Signature independence - also protects against zero-days.
- Process focus - protection is based on WHO writes, not WHAT is written (file content).
- Lean logic - only a small number of legitimate processes need to write to a backup repository.
- Deterministic behavior - the rules are clear and less prone to misinterpretation.

Once cleanly defined and implemented, application whitelisting provides a clear, traceable and robust layer of protection.

Blocky for Veeam®

Technical implementation of application whitelisting in the backup context

Blocky for Veeam® implements application whitelisting directly on the Windows backup repository where Veeam backups are stored.

Architecture components

Kernel-based filter driver

Blocky operates as a file system filter driver in the Windows kernel. It monitors all I/O operations targeting the configured volume used as the Veeam repository.

Fingerprint database

During setup, the relevant Veeam processes are identified and their fingerprints are calculated. These fingerprints are stored in a secured configuration.

Write enforcement logic

Only processes whose fingerprint is on the whitelist (e.g. Veeam backup services) receive write permissions. All other processes - including administrator tools, scripts or potential malware - are blocked.

Logging & alerting

Every blocked access attempt is logged. This information can be:

- evaluated locally,
- forwarded to SIEM systems,
- used for forensic analyses.

Compatibility & performance

Blocky for Veeam® supports:

- NTFS and ReFS file systems,
- Veeam Backup & Replication in typical Windows scenarios,
- local disks, iSCSI LUNs or FC LUNs that appear as a local volume in the OS.

Thanks to the lean architecture, there is practically no performance impact. The filter driver operates efficiently in the kernel and focuses exclusively on the relevant volumes and operations.

Blocky for Veeam®

Implementation in an existing Veeam environment

Prerequisites

- Windows-based backup repository server or proxy
- Veeam Backup & Replication
- local block device (RAID, JBOD, iSCSI, FC)
- administrative rights to install the driver

Implementation steps

1. Installation of Blocky for Veeam
   Setup on the relevant repository server.
2. Fingerprinting of the Veeam processes
   Automatic or manual capture of the relevant Veeam binaries.
3. Configuration of repository volumes
   Selection of the volumes on which write access is to be controlled.
4. Test in monitoring mode
   Logging only at first to ensure that all legitimate processes are captured correctly.
5. Full activation
   From this point on, write access is permitted exclusively for authorized processes.
6. Integration into monitoring & documentation
   Integration into the log and SIEM landscape, inclusion in security and operations documentation.

Best practices

- Use ReFS where possible to benefit from higher performance.
- Do not assign unnecessary additional tasks to the repository server.
- Review Blocky log events regularly to identify patterns.
- Include Blocky in emergency and recovery plans.

Blocky for Veeam®

Conclusion

Backups are now a primary attack target. Traditional, signature-based security measures are not sufficient to reliably defend against modern ransomware, zero-day attacks and LoTL techniques - especially in the area of backup repositories.

Application whitelisting
ensures at process level that only verified applications receive write access to critical data. Blocky for Veeam® brings this principle to the Veeam backup world as a technical, performant and easy-to-integrate solution.

Technically, Blocky provides:

- a clearly traceable, deterministic protection logic,
- signature-independent protection even with compromised credentials,
- integration without fundamental architectural changes,
- a significant increase in backup resilience with manageable operational effort.

Sources
1. Veeam Software (2024). Data Protection Trends Report.
2. ENISA (2023). Cybersecurity Threat Landscape Report.
3. Verizon (2023). Data Breach Investigations Report.
4. Sophos (2024). State of Ransomware Report.
5. BSI (2023). Report on IT Security in Germany.
6. MITRE ATT&CK Framework (2024).
7. FBI IC3 (2023). Internet Crime Report.