Blocky for Veeam®

Your protective shield safeguarding Veeam® Backups against Ransomware attacks

Backups should be your insurance policy against Ransomware attacks, providing the ability to restore your production environment to a stable state. It comes as no surprise that sophisticated Malware is now heading straight for your backups and compromising everything there before heading for your live systems.

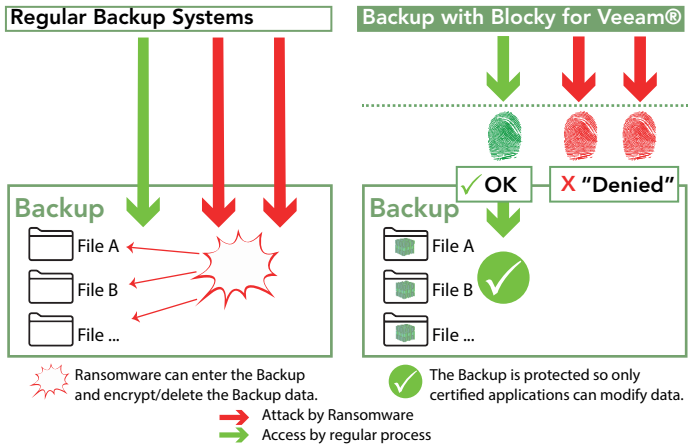
Blocky for Veeam® is especially designed to protect your Veeam backups by denying any unauthorized data access to application processes that may have breached other security measures such as firewall and anti-virus scanners.

Blocky for Veeam® - How it works

Blocky for Veeam® provides a security gateway guaranteeing effective protection for your Veeam® backups. It controls data volumes granting access only to authenticated processes - Malware is blocked out.

Blocky for Veeam® implements a kind of WORM functionality for Windows NTFS or ReFS volumes using application fingerprints to identify authorized requests.

Unauthorized processes attempting writes are blocked and alerted in real-time to the system administrator.



What does Blocky protect?

- Veeam Backup & Replication incl. V9.5 Update 4 and V10.

Where is Blocky installed?

- Blocky is installed on the Microsoft Windows Repository Server.

What storage types are supported?

- Storage can be a local disk or iSCSI/FC SAN LUNs in the case of the server being connected to a block storage SAN fabric.

What file systems are supported?

- NTFS and ReFS file systems only are supported, no NAS devices.

What technical constraints are there?

- Not supported are Microsoft Windows based: Systems Drives, Failover Clusters, De-duplication and Dynamic Data Media.

Where can I learn more about Blocky for Veeam®?

www.blockyforveeam.com

© Grau Data GmbH 2020. All rights reserved. All trademarks are the property of their respective owners.

GRAU DATA
YOUR DATA. YOUR CONTROL