Blocky for Veeam®

Zero-Trust Backup Protection mit Application Whitelisting:

Wie Blocky for Veeam® Backup-Repositories zuverlässig gegen moderne Ransomware schützt

Die Integrität von Backups ist entscheidend für die Widerstandsfähigkeit moderner IT-Infrastrukturen.

Aktuelle Studien zeigen, dass Ransomware heute nicht mehr nur Produktionssysteme attackiert, sondern gezielt auch Backup-Repositories. Laut dem Veeam Data Protection Trends Report 2024 wurden bei 93 % aller Ransomware-Angriffe auch Backups angegriffen, und in 75 % der Fälle wurden Backup-Daten teilweise oder vollständig kompromittiert.

Da klassische Sicherheitsmechanismen überwiegend signaturbasiert arbeiten, können sie Zero-Day-Angriffe oder legitime, aber manipulierte Systemprozesse nur eingeschränkt erkennen. „Living-off-the-Land“-Techniken nutzen vorhandene Systemtools wie PowerShell oder WMI, um ohne klassischen Schadcode zu agieren.

Application Whitelisting implementiert ein Zero-Trust-Prinzip auf Prozessebene: Nur autorisierte Anwendungen dürfen auf definierte Ressourcen schreiben; alles andere wird blockiert. Blocky for Veeam® setzt dieses Prinzip direkt im Backup-Repository um und schützt so Daten vor Verschlüsselung, Manipulation und Löschung. Die Lösung arbeitet kernelbasiert, signaturunabhängig und ohne spürbaren Performance-Overhead.

Dieses Whitepaper richtet sich an technische Ingenieure und beschreibt, wie Application Whitelisting funktioniert, warum es im Backup-Kontext besonders sinnvoll ist und wie Blocky for Veeam® sich pragmatisch in bestehende Veeam-Umgebungen integrieren lässt.

- *93 % der Organisationen: mindestens einen Ransomware-Vorfall innerhalb der letzten 12 Monate.*
- *In 75 % der Fälle: auch Backup-Daten wurden kompromittiert oder angegriffen.*
- *Klarer Trend: Angriffe richten sich nicht mehr nur auf produktive Systeme, sondern gezielt auf sämtliche Wiederherstellungs-mechanismen.*

Free Trial:
BlockyforVeeam.com

Blocky for Veeam®

Die Bedrohungslage für Backup-Systeme

Backups als primäres Angriffsziel moderner Ransomware

Ransomware hat sich von „einfacher“ Verschlüsselungssoftware zu einer hochentwickelten, mehrstufigen Angriffsmethodik entwickelt. Angriffe bestehen heute typischerweise aus:

- initialer Kompromittierung (z. B. Phishing, Schwachstellen in VPNs oder Applikationen),
- lateraler Bewegung im Netzwerk,
- Privilege-Eskalation und Credential Theft,
- gezielter Deaktivierung von Sicherheitslösungen,
- Angriff auf Backup- und Wiederherstellungsinfrastruktur,
- abschließender Verschlüsselung und Lösegeldforderung.

Für die technische Planung stellen Backups nicht mehr nur Versicherung, sondern aktives Angriffsziel dar, für dass es sich zu wappnen gilt.

Schwächen klassischer Sicherheitsmechanismen

Klassische Security-Lösungen wie Antivirus, EDR, Firewalls oder E-Mail-Gateways arbeiten primär mit:

- Signaturen (bekannte Malware-Samples),
- Heuristiken,
- Verhaltensmustern.

Diese Mechanismen sind wichtig, adressieren aber nicht alle Angriffsszenarien:

- Zero-Day-Exploits sind naturgemäß nicht signiert.
- LoTL-Angriffe verwenden legitime Tools (PowerShell, WMI, PsExec).
- Prozess-Imitation (Impersonation) kann Prozesse „so aussehen lassen“, als wären sie vertrauenswürdig.

Gerade Windows-basierte Backup-Repositories sind häufig:

- organisatorisch „hinten“ in der Priorisierung,
- mit weitreichenden Berechtigungen ausgestattet,
- weniger eng überwacht als produktive Systeme.

Die Folge:

Ein einmal erfolgreicher Angriff auf Domain- oder Backup-Server-Credentials kann zu unbemerkter Manipulation oder Verschlüsselung von Backup-Daten führen.

Blocky for Veeam®

Die Bedrohungslage für Backup-Systeme

Typische Angriffsvektoren gegen Veeam-Repositories

Für technische Ingenieure lohnt sich ein Blick auf typische Muster:

Prozess-Impersonation
Malware versucht, sich als legitimer Veeam-Prozess auszugeben, etwa durch gleiche oder ähnliche Prozessnamen.

Credential Theft & Abuse
Gestohlene Admin- oder Service-Credentials werden genutzt, um Backup-Jobs umzuleiten, zu löschen oder Repositories direkt zu verschlüsseln.

LoTL-basierte Verschlüsselung
Angreifer verwenden Bordmittel wie cipher.exe, robocopy.exe oder Skripte, um Daten auf dem Repository zu verändern, ohne „fremde“ Binärdateien einzusetzen.

Schrittweise Verschlüsselung
Anstatt auf einen Schlag alles zu verschlüsseln, werden über Tage oder Wochen inkrementell Backup-Dateien verändert, um länger unentdeckt zu bleiben.

Diese Muster eint:

Sie sind schwer über klassische Blacklisting-Ansätze zu erkennen – insbesondere, wenn legitime Tools verwendet werden.

Blocky for Veeam®

Application Whitelisting: Zero-Trust-Schutz auf Dateisystemebene

Funktionsprinzip

Application Whitelisting kehrt den üblichen Sicherheitsansatz um. Anstatt zu definieren, „was verboten ist“, wird definiert:

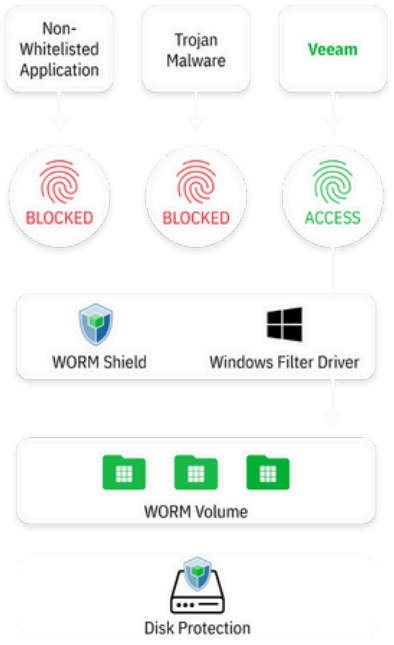
Nur klar bekannte, verifizierte Anwendungen dürfen bestimmte Aktionen ausführen. Alles andere ist grundsätzlich verboten.

Technisch heißt das:

- Jede ausführbare Datei (EXE, DLL etc.) erhält einen kryptografischen Hash (Fingerprint).
- Eine Whitelist enthält alle Fingerprints, die für bestimmte Aktionen (z. B. Schreibzugriff) zugelassen sind.
- Ein Filtermechanismus überwacht die relevanten Ressourcen (hier: Backup-Repository).
- Bei jeder Schreiboperation wird geprüft, ob der Prozess zur Whitelist gehört.
- Falls nein, wird der Zugriff blockiert – unabhängig von Berechtigungen, Herkunft oder Signaturstatus.

Das Ergebnis:

Selbst völlig neue, bislang unbekannte Malware wird gestoppt, solange sie nicht explizit freigegeben wurde.



Vorteile gegenüber klassischen Methoden

Im Backup-Kontext bietet Application Whitelisting einige besonders relevante Vorteile:

- Signaturunabhängigkeit – schützt auch vor Zero-Days.
- Prozessfokus – geschützt wird, WER schreibt, nicht WAS (Dateiinhalt).
- Schlanke Logik – es gibt wenige legitime Prozesse, die auf ein Backup-Repository schreiben müssen.
- Deterministisches Verhalten – die Regeln sind klar, wenig anfällig für Fehlinterpretation.

Einmal sauber definiert und implementiert, bietet Application Whitelisting eine klar nachvollziehbare, robuste Schutzschicht.

Blocky for Veeam®

Technische Umsetzung von Application Whitelisting im Backup-Kontext

Blocky for Veeam® implementiert Application Whitelisting direkt auf dem Windows-Backup-Repository, auf dem die Veeam-Sicherungen ablegt werden.

Architekturkomponenten

Kernelbasierter Filtertreiber

Blocky arbeitet als File-System-Filtertreiber im Windows-Kernel. Er überwacht sämtliche I/O-Operationen, die auf das konfigurierte Volume zielen, welches als Veeam-Repository dient.

Fingerprint-Datenbank

Beim Setup werden die relevanten Veeam-Prozesse identifiziert und deren Fingerprints ermittelt. Diese Fingerprints werden in einer gesicherten Konfiguration hinterlegt.

Write-Enforcement-Logik

Nur Prozesse, deren Fingerprint auf der Whitelist steht (z. B. Veeam-Backup-Services), erhalten Schreibrechte. Alle anderen Prozesse – inklusive Administrator-Tools, Skripte oder potenzieller Malware – werden blockiert.

Logging & Alerting

Jeder blockierte Zugriff wird protokolliert. Diese Informationen können:

- lokal ausgewertet,
- an SIEM-Systeme weitergeleitet,
- für forensische Analysen genutzt werden.

Kompatibilität & Performance

Blocky for Veeam® unterstützt:

- NTFS und ReFS als Dateisysteme,
- Veeam Backup & Replication in typischen Windows-Szenarien,
- Lokale Disks, iSCSI-LUNs oder FC-LUNs, die als lokales Volume im OS erscheinen.

Durch die schlanke Architektur entstehen praktisch keine Performanceeinbußen. Der Filtertreiber arbeitet effizient im Kernel und fokussiert sich ausschließlich auf die relevanten Volumes und Operationen.

Blocky for Veeam®

Implementierung in einer bestehenden Veeam-Umgebung

Voraussetzungen

- Windows-basierter Backup-Repository-Server oder Proxy
- Veeam Backup & Replication
- lokales Block-Device (RAID, JBOD, iSCSI, FC)
- administrative Rechte für die Installation des Treibers

Implementierungsschritte

1. Installation von Blocky for Veeam
   Setup auf dem entsprechenden Repository-Server.
2. Fingerprinting der Veeam-Prozesse
   Automatische oder manuelle Erfassung der relevanten Veeam-Binärdateien.
3. Konfiguration der Repository-Volumes
   Auswahl der Volumes, auf denen Schreibzugriffe kontrolliert werden sollen.
4. Test im Monitoring-Modus
   Zunächst nur Logging, um sicherzustellen, dass alle legitimen Prozesse korrekt erfasst sind.
5. Vollständige Aktivierung
   Ab diesem Punkt sind Schreibzugriffe ausschließlich für autorisierte Prozesse erlaubt.
6. Integration in Monitoring & Dokumentation
   Einbindung in Log- und SIEM-Landschaft, Aufnahme in Security- & Betriebsdokumentation.

Best Practices

- **ReFS** nutzen, wo möglich, um von höherer Performance zu profitieren.
- Repository-Server nicht unnötig in andere Aufgaben einbinden.
- Blocky-Logevents regelmäßig reviewen, um Muster zu erkennen.
- Blocky in Notfall- und Wiederherstellungsplänen berücksichtigen.

Blocky for Veeam®

Fazit

Backups sind heute ein primäres Angriffsziel. Klassische, signaturbasierte Sicherheitsmaßnahmen reichen nicht aus, um moderne Ransomware, Zero-Day-Angriffe und LoTL-Techniken zuverlässig abzuwehren – insbesondere nicht im Bereich der Backup-Repositories.

Application Whitelisting stellt auf Prozessebene sicher, dass nur verifizierte Anwendungen Schreibzugriff auf kritische Daten erhalten. Blocky for Veeam® bringt dieses Prinzip als technische, performante und einfach integrierbare Lösung in die Veeam-Backup-Welt.

Technisch bietet Blocky:

- eine klar nachvollziehbare, deterministische Schutzlogik,
- signaturunabhängigen Schutz auch bei kompromittierten Credentials,
- Integration ohne grundlegende Architekturänderungen,
- eine deutliche Erhöhung der Backup-Resilienz bei überschaubarem Betriebsaufwand.

Quellenverzeichnis

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). Lagebericht zur IT-Sicherheit in Deutschland.
6. MITRE ATT&CK Framework (2024).
7. FBI IC3 (2023). Internet Crime Report.