



Blocky for Veeam®

Zero-Trust-Backup-Security als Wettbewerbsvorteil:

Wie Blocky for Veeam® Margen stärkt,
Risiken reduziert und Portfolios differenziert

Der Markt für Managed Backup- und Wiederherstellungsdienste ist stark umkämpft. Viele Anbieter setzen auf ähnliche Technologien, insbesondere auf Veeam, und unterscheiden sich für die Kunden nur noch über Preis, Vertragsgestaltung und Zusatzservices. Parallel dazu hat die Zunahme von Ransomware-Angriffen dazu geführt, dass Kund*innen heute nicht mehr nur „Backup“ kaufen, sondern **Resilienz und garantierte Wiederherstellbarkeit**.

Für Managed Service Provider (MSPs), Systemhäuser und Reseller bedeutet das:

- Backup-Sicherheit ist ein zentrales Kaufkriterium geworden.
- Rein lizenzbasierte Backup-Angebote geraten unter Margendruck.
- Sicherheits- und Compliance-Aspekte entscheiden zunehmend über Auftragsvergabe und Vertragsverlängerung.

Blocky for Veeam® bietet hier einen klaren Hebel: Die Lösung implementiert Application Whitelisting direkt auf dem Backup-Repository und verhindert jede unautorisierte Schreiboperation – einschließlich Zero-Day-Angriffe, Insider-Bedrohungen und manipulativer Tools.

Für Produktmanager eröffnet das **neue, hochmarginige Servicekomponenten**, die das **Portfolio differenzieren**, **Risiken senken** und **Kunden stärker binden**.

Laut Veeam (2024) berichten 93 % der Unternehmen von Ransomware-Vorfällen, bei denen in 75 % der Fälle auch Backups betroffen waren. Die durchschnittlichen Kosten eines Angriffs liegen bei über 1,8 Mio. USD (Sophos 2024) – ohne Lösegeldzahlungen.

Free Trial:
BlockyforVeeam.com



Blocky for Veeam®

Markttrends:

Warum Backup-Sicherheit kaufentscheidend wurde

Vom „Backup-Produkt“ zur „Resilience-Lösung“

Früher war Datensicherung eine interne IT-Aufgabe. Heute ist sie ein geschäftskritischer Faktor:

- Ransomware-Angriffe führen zu Betriebsunterbrechungen, Vertragsstrafen und Reputationsverlust.
- Regulatorische Anforderungen (z. B. NIS2, DORA, branchenspezifische Vorgaben) verlangen nachvollziehbare Strategien zur Sicherstellung der Wiederherstellbarkeit.
- Kunden fragen gezielt nach: „Wie stellen Sie sicher, dass unsere Backups nicht manipuliert werden?“



Für Serviceanbieter heißt das:

Wer keine überzeugende Backup-Security-Story hat, verliert Projekte oder muss massiv über den Preis konkurrieren.

Produktmanager stehen vor mehreren strukturellen Herausforderungen:

- **Margendruck:** Standard-Backup-Dienste sind austauschbar. Preise werden gedrückt, Margen sinken.
- **Steigende SLA-Anforderungen:** Kunden erwarten garantierte RTO/RPO-Zeiten und schriftlich fixierte Wiederherstellbarkeit.
- **Höhere operative Risiken:** Ransomware, die Backups zerstört, führt zu aufwändigen Kriseneinsätzen, erhöhtem Support und potenziellen Vertragsstrafen.
- **Fehlende Differenzierung:** Wenn alle dasselbe Produkt mit ähnlicher Konfiguration anbieten, bleibt nur der Preis als Unterscheidungsmerkmal.



Blocky for Veeam®

Blocky for Veeam® als Portfolio-Baustein

Blocky for Veeam® bietet eine spezialisierte Application-Whitelisting-Implementierung für Veeam Backup & Replication. Die Lösung arbeitet **direkt auf dem Windows-Backup-Repository** und schützt die Volumes, auf denen die Veeam-Sicherungen gespeichert werden.

Reduktion operativer Risiken

Weniger zerstörte Backups bedeuten:

- geringere Restore-Aufwände,
- weniger Krisenprojekte,
- niedrigere interne Supportkosten,
- geringere Wahrscheinlichkeit von SLA-Verletzungen.



Hochmarginiges Zusatzprodukt

Security-Funktionen werden im Markt tendenziell höher bewertet als reine Infrastrukturleistungen.



Differenzierung

Klare Abgrenzung möglich:

- “Wir bieten nicht nur Veeam – wir bieten Veeam mit Zero-Trust-Backup-Schutz.“
- “Unsere Backups sind gegen Zero-Day- und LoTL-Angriffe geschützt”

Einfacher Go-to-Market

Blocky for Veeam®:

- nutzt **bestehende Windows-Repository-Server**,
- erfordert **keine zusätzliche Hardware oder Linux-Infrastruktur**,
- lässt sich **in wenigen Minuten installieren** und konfigurieren,
- kann in **Standard-Templates** für Kundenumgebungen integriert werden.
- kann auch in **vorgelagerten On-Prem-Umgebungen** des Kunden eingesetzt werden

Das verkürzt:

- Time-to-Market für neue Angebote,
- Implementierungszeiten pro Kunde,
- Schulungsaufwand für Technikteams.

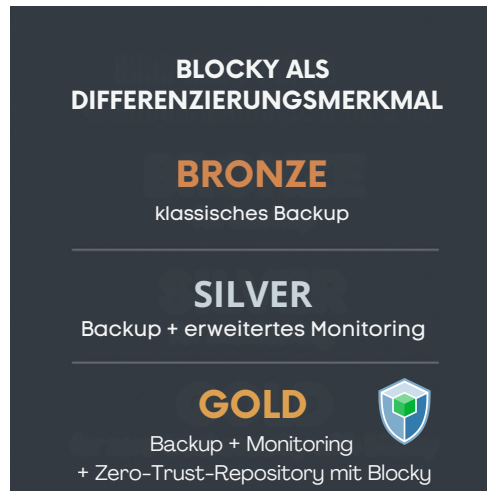


Blocky for Veeam®

Strategische Einsatzszenarien im Portfolio

Premium-Tiers („Gold / Secure / Resilient Backup“)

Blocky eignet sich ideal als Differenzierungsmerkmal zwischen Standard- und Premium-Serviceebenen:



Wichtig in kritischen Branchen

In regulierten Sektoren ist manipulationssichere Datensicherung essentiell.

Blocky unterstützt hier die Argumentation gegenüber:

- Banken und Versicherungen,
- Gesundheitsdienstleistern,
- Energieversorgern,
- Industrie & KRITIS-Betreibern.

Bestandteil von DRaaS & Business-Continuity-Angeboten

Disaster-Recovery-as-a-Service (DRaaS) basiert auf der Annahme, dass:

- die bereitgestellten Backups vollständig,
- manipulationsfrei
- und im Ernstfall nutzbar sind.

Blocky erhöht die Glaubwürdigkeit dieser Zusagen wesentlich.



Blocky for Veeam®

Wirtschaftlicher Nutzen im Überblick

UMSATZ

Höhere Preise für Security-Tiers, zusätzliche Services wie Security-Audits oder Compliance-Berichte und neue, sicherheitsorientierte Kundensegmente steigern den Umsatz erheblich.



KOSTEN

Weniger und effizientere Restore-Projekte reduzieren Notfall- und Overtime-Kosten der Technikteams und minimieren das Risiko von Vertragsstrafen durch verfehlte RTO-/RPO-Ziele.

KUNDEN

Mehr Vertrauen und höhere Loyalität sorgen für langfristige Verträge und stabile Kundenbeziehungen.





Backup-Sicherheit ist heute ein kaufentscheidender Faktor und ein wesentlicher Bestandteil moderner Service-Portfolios.

Unternehmen erwarten nachvollziehbare, robuste Maßnahmen, die sicherstellen, dass selbst bei erfolgreichen Angriffen eine Wiederherstellung möglich bleibt.

Blocky for Veeam® bietet hierfür einen klar greifbaren, technisch fundierten und wirtschaftlich attraktiven Ansatz:

- **Zero-Trust-Backup-Sicherheit** durch Application Whitelisting auf Repository-Ebene,
- **einfache Integration** in bestehende Veeam-Umgebungen,
- **neue Möglichkeiten** zur Differenzierung, Marge und Kundenbindung.

Für das Portfolio ist Blocky kein „Nice-to-have“, sondern ein strategisches Element, mit dem Sie Ihr Angebot vom Markt abheben und gleichzeitig Ihre eigene Risiko- und Kostenbasis optimieren können.

Quellenverzeichnis

1. Veeam Software (2024) Data Protection Trends Report.
2. ENISA (2023) Cybersecurity Threat Landscape Report.
3. Sophos (2024) State of Ransomware Report.
4. Verizon (2023) Data Breach Investigations Report.
5. FBI IC3 (2023) Internet Crime Complaint Center – Annual Report.
6. MITRE (2024) ATT&CK Framework – Enterprise Techniques