Blocky for Veeam®

Zero-Trust Backup Security as a Competitive Advantage:

How Blocky for Veeam® Strengthens Margins, Reduces Risks and Differentiates Portfolios

The market for managed backup and recovery services is highly competitive. Many providers rely on similar technologies, especially Veeam, and from the customer's perspective are often differentiated only by price, contract design and add-on services. At the same time, the rise in ransomware attacks has led customers to buy not just "backup" anymore, but resilience and guaranteed recoverability.

For managed service providers (MSPs), system integrators and resellers this means:

- Backup security has become a key buying criterion.
- Purely license-based backup offerings are under margin pressure.
- Security and compliance aspects increasingly determine contract awards and renewals.

Blocky for Veeam® provides a clear lever here: The solution implements application whitelisting directly on the backup repository and prevents every unauthorized write operation - including zero-day attacks, insider threats and manipulative tools.

For product managers, this opens up new, high-margin service components that differentiate the portfolio, reduce risks and strengthen customer retention.

According to Veeam (2024), 93% of companies report ransomware incidents in which backups were affected in 75% of cases. The average cost of an attack is more than USD 1.8 million (Sophos 2024) - excluding ransom payments.

Free Trial:
BlockyforVeeam.com

Blocky for Veeam®

Market trends:
Why backup security became a buying decision

From "Backup Product" to "Resilience Solution"

In the past, data backup was an internal IT task. Today it is a business-critical factor:

- Ransomware attacks lead to operational disruptions, contractual penalties and reputational damage.
- Regulatory requirements (e.g. NIS2, DORA, industry-specific rules) demand traceable strategies to ensure recoverability.
- Customers ask specifically: "How do you ensure that our backups cannot be manipulated?"

For service providers, this means:

Without a convincing backup security story, you lose projects or have to compete massively on price.

Product managers face several structural challenges:

- Margin pressure: Standard backup services are interchangeable. Prices are pushed down, margins shrink.
- Rising SLA requirements: Customers expect guaranteed RTO/RPO times and contractually fixed recoverability.
- Higher operational risks: Ransomware that destroys backups leads to costly crisis operations, more support and potential contractual penalties.
- Lack of differentiation: When everyone offers the same product with similar configuration, price remains the only differentiator.

Blocky for Veeam®

Blocky for Veeam® as a Portfolio Component

Blocky for Veeam® provides a specialized application whitelisting implementation for Veeam Backup & Replication. The solution runs directly on the Windows backup repository and protects the volumes on which Veeam backups are stored.

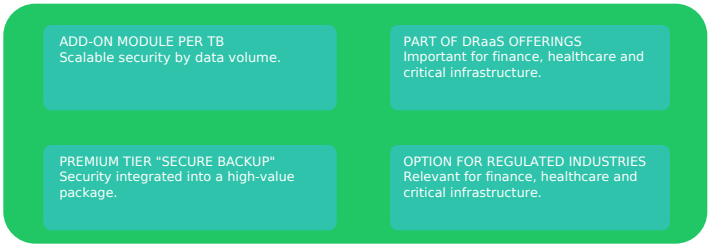
Reduction of operational risks

Fewer destroyed backups mean:

- lower restore efforts,
- fewer crisis projects,
- lower internal support costs,
- reduced likelihood of SLA violations.

High-margin add-on product

Security functions tend to be valued higher in the market than pure infrastructure services.



Differentiation

Clear positioning is possible:

- "We offer not just Veeam - we offer Veeam with zero-trust backup protection."
- "Our backups are protected against zero-day and LoTL attacks."

Simple go-to-market

Blocky for Veeam®:

- uses existing Windows repository servers,
- requires no additional hardware or Linux infrastructure,
- can be installed and configured in minutes,
- can be integrated into standard templates for customer environments,
- can also be deployed in upstream on-premises customer environments.

This shortens:

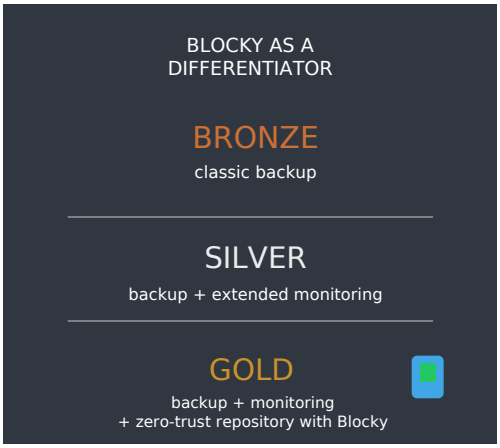
- time-to-market for new offerings,
- implementation time per customer,
- training effort for technical teams.

Blocky for Veeam®

Strategic Deployment Scenarios in the Portfolio

Premium tiers ("Gold / Secure / Resilient Backup")

Blocky is ideally suited as a differentiator between standard and premium service levels:



Important in critical industries

In regulated sectors, tamper-proof data backup is essential.

Blocky supports the argumentation with:

- banks and insurance companies,
- healthcare providers,
- energy suppliers,
- industrial companies and critical infrastructure operators.

Part of DRaaS & business continuity offerings

Disaster-Recovery-as-a-Service (DRaaS) is based on the assumption that:

- the provided backups are complete,
- free from manipulation,
- and usable in an emergency.

Blocky significantly increases the credibility of these commitments.

Blocky for Veeam®

Business Value at a Glance

REVENUE

Higher prices for security tiers, additional services such as security audits or compliance reports and new, security-oriented customer segments significantly increase revenue.

COSTS

Fewer and more efficient restore projects reduce emergency and overtime costs for technical teams and minimize the risk of contractual penalties due to missed RTO/RPO targets.

CUSTOMERS

More trust and higher loyalty lead to long-term contracts and stable customer relationships.

Blocky for Veeam®

Conclusion

Backup security is now a buying-decision factor and an essential component of modern service portfolios.

Companies expect transparent, robust measures that ensure recovery remains possible even after successful attacks.

Blocky for Veeam® offers a clear, technically sound and economically attractive approach:

- Zero-trust backup security through application whitelisting at repository level,
- simple integration into existing Veeam environments,
- new opportunities for differentiation, margin and customer retention.

For the portfolio, Blocky is not a "nice-to-have" but a strategic element that lets you set your offering apart from the market while optimizing your own risk and cost base.

Sources

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