Blocky for Veeam®

Play Book

Introduction:

Blocky and Veeam® have teamed up to meet a crucial customer requirement: providing powerful ransomware protection that removes the complexity and cost typically associated with deploying ransomware protection.

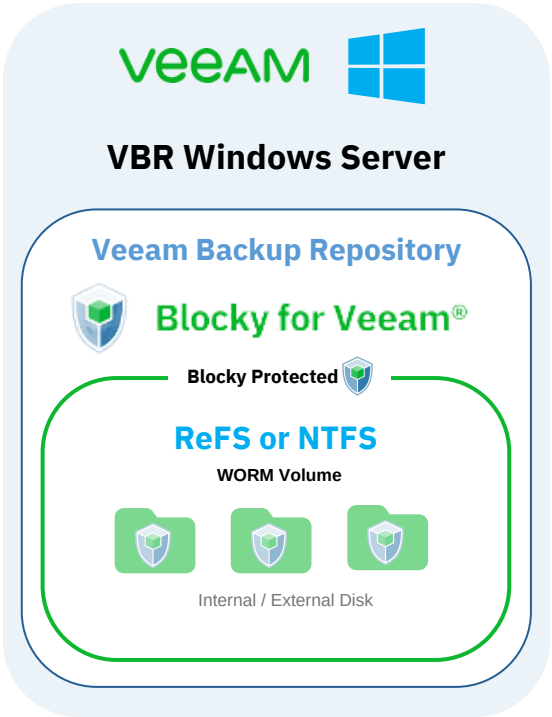
What is Blocky?

Blocky is the only ransomware protection solution that runs on the Veeam Windows server. It complements Veeam® Backup & Replication (VBR), offering an on-premise deployment that doesn't require Linux, extra hardware, or cloud services. Blocky hardens the Windows VBR against ransomware threats by transforming the ReFS and NTFS volumes into a zero-trust, immutable Write Once Read Many (WORM) volume. This creates an robust ransomware protection for Veeam backup volumes, precisely tailored to meet the stringent demands of Veeam customers.

What is unique about Blocky?

Blocky is the only ransomware solution for Veeam that:

1. Runs on the the Windows VBR
2. Does not require Linux, additional servers, or specialized storage.



What problem does Blocky solve?

Blocky stops ransomware attacks. Veeam does not provide ransomware protection without adding an additional Linux server. Many Veeam customers do not want the added complexity or cost to add a Linux server. Blocky is designed to address the specific challenges related to ransomware threats particularly experienced by SMB, ROBO (Remote Office/Branch Office) configurations, and SLED (state, local government, and education).

Blocky for Veeam®

Why does Veeam need ransomware protection and why Blocky?
Blocky addresses a critical gap in Veeam's backup solution, specifically in the area of ransomware protection. Veeam itself does not natively offer this safeguard unless customers opt to add a dedicated Linux server, a choice that many find undesirable due to its added complexity and cost. Moreover, alternative ransomware protection solutions often demand additional dedicated hardware, like servers and specialized storage, or necessitate the use of cloud services to establish an immutable protective layer—both of which can significantly drive up costs and complexity.

In contrast, Blocky offers a streamlined and cost-effective solution by directly running on the existing Veeam Windows server. It transforms this server into an immutable, hardened repository capable of stopping ransomware attacks, effectively adding a robust layer of protection against data loss or corruption due to such threats. This approach eliminates the need for additional hardware or specialized storage solutions, making Blocky a highly convenient and financially prudent choice for organizations using Veeam. Blocky ensures that Veeam users can continue to benefit from their existing setup, now enhanced with robust ransomware protection, without incurring extra costs or complicating their system architecture.

Key Selling Points:

Unparalleled TCO: Blocky maximizes the customer investment by enhancing Veeam backup security without significantly increasing costs, thereby optimizing Veeam's Total Cost of Ownership (TCO).

Seamless Integration & Enhanced Protection: Blocky's seamless compatibility with Veeam Windows servers not only preserves the user-friendly experience but also transforms the setup into a fortified, ransomware-resistant environment.

Ransomware Protection: Blocky layers in essential security measures to make the Veeam environment cyber resilient to ransomware attacks. It stops all unauthorized access for write, delete, and encryption to the backup volumes. Featuring real-time threat detection, it not only guards against intrusion but promptly alerts to unauthorized access attempts, ensuring customers' data remains uncompromised and secure.

Rapid Recovery Time: Customers can achieve the fastest recovery times with a protected VBR in their data center, dramatically reducing the impact of potential downtime.

No Additional Hardware Required: Blocky's architecture allows it to run on the existing Veeam Windows server, eliminating the need for extra servers or specialized storage, thus minimizing both capital and operational expenditures.

Transformative Solution: By converting the Veeam Windows server into an immutable, hardened repository, Blocky provides an effective shield against unauthorized modifications or deletions, including those initiated by ransomware.

Seamless Integration: Blocky is engineered to integrate effortlessly with Veeam and requiring no Veeam or server modifications.

Preservation of Veeam's Simplicity: Despite its advanced security features, Blocky retains Veeam's original ease-of-use.

Unified Management: Blocky's centralized control simplifies administrative tasks by providing real-time monitoring and quick policy implementation, leading to uniform security across all locations.

Flexibility in Pricing: With pricing models based on both the protected capacity and the number of VBR servers, Blocky offers customizable solutions tailored to an organization's specific needs.

Adaptable for Multiple Locations: Whether operating a single site or multiple geographically dispersed locations, Blocky's flexible pricing and deployment options ensure comprehensive, consistent protection.

Target Audience

1. **Organizations using Veeam for backup solutions:** These businesses are already invested in Veeam's ecosystem and are looking to further enhance their security, particularly against ransomware threats.
2. **Centralized IT teams managing ROBO (Remote Office/Branch Office):** Such teams oversee geographically dispersed sites and aim for uniform data protection across all locations. They look for solutions that provide robust security without adding undue complexity or incurring significant costs.
3. **Businesses that prioritize both robust protection and cost-effectiveness:** Any organization conscious of the challenges posed by ransomware, but also wary of the expenses associated with most protective solutions, would be interested in Blocky's offerings.
4. **Companies with a budget-conscious approach:** Organizations that seek to maximize the Total Cost of Ownership (TCO) of their Veeam environment while also ensuring protection against modern cyber threats like ransomware would find Blocky appealing.

A salesperson would target the following departments to sell Blocky:

1. **IT Department**: This is the primary department as they are directly responsible for the organization's technology infrastructure, including backup solutions and cybersecurity. Within this department, they should focus on:
   - IT Managers/Directors
   - System Administrators
   - Backup Administrators
   - IT Infrastructure Teams
   - Cybersecurity Teams

2. **Information Security Department**: Given that Blocky addresses ransomware threats, professionals focused on information security will be interested in solutions that bolster an organization's defenses.
   - Chief Information Security Officers (CISO)
   - Security Analysts
   - Security Engineers

3. **Risk Management Department**: Ransomware is a significant risk to business operations, and this department is concerned with mitigating various risks, including IT-related threats.
   - Risk Managers
   - Risk Assessment Teams

4. **C-Level Executives**: They are key decision-makers, especially in smaller to medium-sized enterprises where top executives might be directly involved in significant IT decisions.
   - CEO (Chief Executive Officer)
   - CIO (Chief Information Officer)
   - CTO (Chief Technology Officer)
   - CFO (Chief Financial Officer) – given the financial implications of ransomware attacks and the potential cost savings of Blocky.

5. **Finance Department**: While they may not be the primary decision-makers, the finance department often plays a role in budget allocations for IT solutions. Presenting Blocky's cost-effectiveness and potential savings in the event of a ransomware attack can be persuasive to this department.

6. **Business Continuity/Disaster Recovery Teams**: These professionals are responsible for ensuring business operations continue smoothly in the face of disruptions, including cyberattacks. A solution like Blocky would be of interest to them.

In any sales approach, understanding the specific pain points and needs of each department and tailoring the pitch accordingly will be crucial to success.

Which roles should I target for Blocky?

1. **IT Director/Manager**:
   - Role: Oversees the IT infrastructure of the organization, including backup and disaster recovery strategies.
   - Challenges: Ensuring robust data protection, managing IT budgets, and overseeing multiple remote office locations.
   - Motivations: Looking for reliable, cost-effective solutions that integrate easily into existing systems and offer comprehensive protection against ransomware.
2. **Backup and Recovery Specialist**:
   - Role: Directly responsible for creating, implementing, and managing backup and recovery strategies.
   - Challenges: Keeping up with the volume of data, ensuring backups are consistent and recoverable, and protecting backup data from threats like ransomware.
   - Motivations: Streamlined tools that easily integrate into the current backup infrastructure, like Veeam, and enhance its protection capabilities.
3. **Cybersecurity Officer**:
   - Role: Tasked with ensuring the organization's cyber health, formulating security policies, and managing cybersecurity teams.
   - Challenges: Protecting against an ever-growing array of cyber threats, including ransomware, with often limited resources.
   - Motivations: Solutions that provide robust protection without incurring prohibitive costs or demanding extensive deployment efforts.
4. **Systems Administrator**:
   - Role: Manages and maintains the organization's IT systems.
   - Challenges: Deploying and maintaining new solutions, ensuring system uptime, and securing systems.
   - Motivations: Tools that are easy to install and manage, and that can improve the overall security posture without adding significant overhead or complexity.
5. **CFO/Financial Decision-Maker**:
   - Role: Manages the financial health of the company and oversees budget allocations.
   - Challenges: Balancing the IT department's requests for new tools and solutions with the company's financial constraints.
   - Motivations: Solutions that offer a good return on investment and protect the company from potential financial pitfalls, like the costs associated with a ransomware attack.

Each of these personas would approach Blocky with their unique needs and concerns, but all share a common interest in robust, efficient, and cost-effective ransomware protection for their Veeam environment.

Here's why you should consider offering Blocky to your customers:

In today's fast-evolving cybersecurity landscape, your customers are constantly on the lookout for robust, integrated solutions that can secure their critical data without breaking the bank. This is where Blocky for Veeam comes in, and why it should matter to you as a reseller. By including Blocky in your product offerings, you're arming yourself with a solution that's perfectly aligned with the market's needs—today and in the foreseeable future. It's not just about adding another product to sell; it's about enriching your portfolio with a solution that solves real-world problems efficiently and economically.

Capitalizing on Veeam Sales*:* If you're already selling Veeam, consider this: most customers lack robust ransomware protection. Many are keen to learn about ransomware protection options and are willing to invest if the solution is cost-effective. Blocky provides an opportunity to boost your margins not only for new Veeam sales but also for existing customers. Consider introducing Blocky during maintenance renewals—it's an avenue for added revenue and heightened customer satisfaction.

Holistic Security Offering: With Blocky in your portfolio, you'll not only be offering backup solutions but also a premium ransomware protection, strengthening your position as a one-stop-shop for all things related to data protection.

Meet Market Demands Head-On: Ransomware attacks are on the rise, and businesses are actively seeking robust protection solutions. Blocky addresses this critical need, making you a problem-solver in the eyes of your clients.

Improved Profit Margins: Blocky doesn't require additional hardware, which means higher cost savings for your customers and better profit margins for you, especially when considering the potential for volume-based discounts.

Build Customer Loyalty: Offering an integrated, simple, and cost-effective ransomware protection solution like Blocky can significantly enhance customer satisfaction and loyalty, leading to longer contract periods and recurring revenue.

Stand Out from the Crowd: In a saturated market, differentiation is key. Blocky gives you an edge, highlighting your focus on innovative, high-value solutions that go beyond just fulfilling basic needs.

New Revenue Streams: Blocky's subscription model generates recurring revenue.

Brand Enhancement: Being able to provide a timely and effective solution to one of the industry's most pressing challenges elevates your brand, reinforcing your reputation as a proactive and customer-centric reseller.

Easy to Learn, Easier to Sell: GRAU offer comprehensive training and support to ensure you're well-equipped to market Blocky, allowing you to sell with confidence and expertise.

Flexible and Adaptable: Blocky's flexible pricing models mean you can cater to businesses of all sizes, from small local companies to large enterprises.

Qualifying questions. These customer questions will help you determine whether a Blocky is a good fit for a potential customer given its integration with Veeam and its focus on ransomware protection for backup data.

1. **Existing Backup Solution**:
   - Are you currently using Veeam for your backup solution?
   - If so, do you have ransomware protection?
   - If so, does that protect all your locations?
   - Do you have other backup applications?

2. **Ransomware Concerns and Protection**:
   - Have you ever experienced a ransomware attack or data breach?
   - What measures do you currently have in place to protect against ransomware?
   - Are you satisfied with your current ransomware protection strategy?

3. **Backup Infrastructure**:
   - How many VBR servers do you operate across your locations and how many locations have Veeam?

4. **Backup Data Storage and Capacity**:
   - How much backup data (in TB) do you currently store per location?
   - Are you expecting this capacity to grow in the near future?

5. **Operational Complexities**:
   - Are you looking for a ransomware solution that seamlessly integrates with your existing backup environment without adding operational complexities?

6. **Budget Considerations**:
   - Do you have a budget allocated for ransomware protection?
   - Are you concerned about the potential additional costs of hardware or specialized storage when considering ransomware solutions?

7. **Future Expansion**:
   - Are you planning to expand or change your backup infrastructure in the near future?
   - Do you anticipate opening more locations or sites that will require backup protection?

8. **Maintenance and Renewals**:
   - When is your next maintenance renewal for Veeam?
   - Are you open to considering additional security features during the renewal process?

9. **Decision-making Process**:
   - Who is involved in the decision-making process for IT security solutions in your organization?
   - What challenges or pain points are you hoping to address with a new solution?

10. **Current Challenges**:
   - Are there any specific challenges or concerns you've encountered with your current backup and security setup?

11. **Evaluating a New Solution**:
   - Would you be interested in trialing a ransomware solution that seamlessly integrates into your environment without any disruptions and is available at no cost?

By asking these questions, you can gauge the customer's current setup, their concerns about ransomware, their familiarity with Veeam, and their openness to integrating a solution like Blocky. This will help in determining if Blocky is a good fit for their needs.

How is Blocky priced? Blocky's pricing model is based on two factors: the capacity being protected on the VBR server and the number of VBR servers.

To calculate the capacity for each individual physical location:

1. **Determine Total Capacity**: First, ascertain the total storage capacity needed to protect Veeam server at the specific physical location. This will include all the data that requires ransomware protection.
2. **Count the Number of VBR Servers**: Identify the total number of VBR servers at that location which will be managing the data backup.

Example:

- **Location:** Dallas
- **Number of VBR servers:** 4
- **Total capacity across all 4 servers:** 250 TB

For organizations with multiple locations, this pricing is determined separately for each location.

What is a VBR server? A VBR server is the server where the Veeam repository resides.

Can customer test Blocky? Yes, customers can put Blocky to the test with a 30-day risk free trial, no credit card required. This gives your customer an excellent opportunity to evaluate Blocky's features and benefits firsthand without any commitments.In addition, our world-class global support team is on standby around the clock to assist customers whenever they need help.

How do I size Blocky?

We need to know a few details about the Veeam environment, answering the following questions will help us size Blocky:

1. How many terabytes of Veeam data are you backing up?
2. Is Veeam deployed on more than one site? If yes, how much data per site?
3. How many Veeam servers (VBS) are you protecting?
4. Do you need a one-year subscription, three years, or five years?

Will GRAU protect my deal or does it provide deal registration? GRAU's deal registration can be conveniently completed at our website www.blockyforveeam.com/partner.

How does implementing Blocky potentially influence an organization's cyber insurance premiums given its impact on ransomware protection and recovery times?

1. **Potential Premium Reductions**: Insurance providers often assess the cybersecurity posture of an organization when determining premiums. Implementing robust cybersecurity solutions like Blocky might signal a proactive approach to cyber threats, potentially leading to reduced premiums or better terms.
2. **Faster Recovery Times**: Should an organization face a cyber attack, having a secure and uncorrupted backup ensures quicker recovery times. This speed in recovery can minimize business interruption costs, which is a primary concern for many cyber insurance policies.
3. **Possible Requirement in the Future**: As cyber insurers become more knowledgeable about specific cybersecurity solutions and their effectiveness, insurers may starting to require or recommend specific solutions like Blocky as a precondition for coverage or to qualify for specific premium rates.
4. **Educative and Consultative Role**: Insurers often play a role in educating their clientele about the best cybersecurity practices. Solutions like Blocky are becoming part of this educational framework, helping businesses understand the importance of ransomware protection for backups.

It's essential to consult directly with cyber insurance providers to understand if and how they recognize solutions like Blocky in their policy considerations. As the cybersecurity landscape evolves, insurers might update their stances on various protective measures and their impacts on policy terms and premiums.

Considerations To Discuss With Your Customer Before Deploying Blocky. These prerequisites can help ensure a smooth implementation and optimal functioning.

1. **Backup Infrastructure**:
   - VBR Server Availability: Confirm the number and locations of your VBR (Veeam Backup & Replication) servers.

   - NTFS or ReFS Volumes: Since Blocky hardens NTFS and ReFS volumes, you need to confirm that your backup data resides on these file systems.

2. **Security Considerations**:
   - Admin Rights: You might need administrative rights on the Veeam servers to install and configure Blocky.
   - Current Security Software: Ensure that any existing security software, like antivirus or intrusion detection systems, are compatible with Blocky or can be configured to avoid conflicts.

3. **Operational Considerations**:
   - Maintenance Windows: Determine when it would be best to deploy Blocky, possibly during periods of low activity or scheduled maintenance windows to minimize disruptions.

4. **Technical Support**:
   - Contact Information: Have contact details for Blocky's technical support handy in case of any issues during deployment.
   - Documentation: Familiarize yourself with Blocky's installation and configuration documentation.

5. **Training**:
   - Blocky training is available online and take about 30 minutes to complete. Once completed a certificate of completion is issued.
Https://blockyforveeam.com/certification/

6. **Licensing**:
   - Ensure you have the necessary licenses for the deployment of Blocky and understand the licensing model (e.g., based on protected capacity and the number of VBR servers).

By addressing these prerequisites, you can ensure a smoother deployment of Blocky and better integration with the Veeam setup.

Objection Handling

Is Blocky a Proven Technology? Veeam® customers worldwide, from small businesses to large enterprises and government organizations, trust Blocky's distinctive WORM technology to protect their backups.

Does Blocky add Complexity? Blocky is designed to simplify ransomware protection. Its easy installation process and "set and forget" design prevent users from being burdened by complicated management or monitoring tasks. Despite its sophisticated protection capabilities, it is user-friendly and does not require expert knowledge to operate. Users can test it risk-free!

Is Blocky Scalable: Blocky is designed to protect one or more repositories, and its centralized management simplifies monitoring across multiple sites, making it a scalable solution for growing businesses.

Cost Concerns: Blocky is priced to win. Blocky with Veeam® delivers an unbeatable TCO compared to other data protection solutions.

Why can I find more Information on Blocky? www.BlockyforVeeam.com

Sample Email: Blocky Introduciton

Subject: Elevate Your Veeam Environment with Comprehensive Ransomware Protection

Dear [Customer's Name],

I hope this email finds you well. My name is [Your Name] from [Your Company Name], and I wanted to introduce you to an innovative solution that addresses one of the most pressing concerns in today's IT landscape: ransomware.

If you're utilizing Veeam for your backup needs, you've already taken a significant step towards ensuring the continuity and safety of your data. However, as the threat landscape evolves, it's crucial to enhance your Veeam environment with dedicated ransomware protection.

Enter Blocky for Veeam. Blocky seamlessly integrates with your existing Veeam deployments, providing a fortified line of defense against ransomware without incurring the costs or complexities associated with additional hardware. Blocky is the **only solution** that runs on the Veeam VBR, transforming your Veeam Windows server into an immutable, hardened repository, Blocky ensures your backups are shielded from potential ransomware attacks.

Key benefits include:
- **Enhanced Ransomware Protection**: Blocky offers a dedicated layer of defense, safeguarding your Veeam backups against threats.
- **Optimized TCO**: Integrate Blocky without hefty hardware or operational costs, maximizing your Veeam investment.
- **Simplicity**: Deployed within minutes, Blocky works harmoniously with your Veeam environment, maintaining its inherent simplicity.

We believe that Blocky could be a transformative addition to your data protection strategy. I'd love to discuss how it can specifically benefit your organization and answer any questions you may have.

Would you be available for a brief call or meeting next week to explore this further? Please let me know a time that works for you, and I'll ensure it's in the calendar.

Thank you for considering **Blocky for Veeam**. We're excited about the potential benefits it can bring to organizations like yours, and I'm looking forward to our conversation.