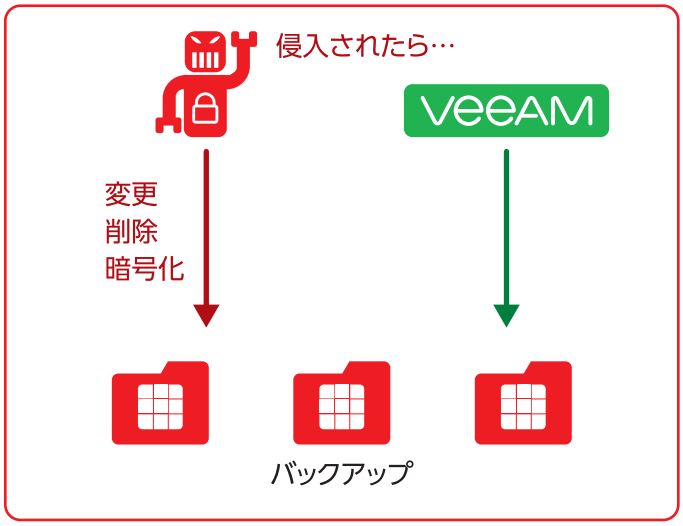
Windowsだけでランサムウェア対策

Blocky for VEEAM

- 追加Linuxサーバや高価な専用ストレージ不要
- Veeam Windowsリポジトリを20分でイミュータブル/ゼロトラスト構成に
- オールインワン構成から分散/マルチサイト構成まで、大規模でも簡単導入

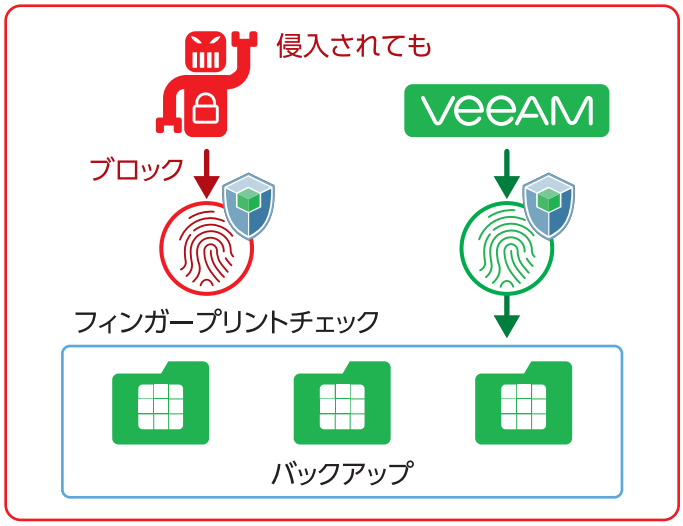
Blockyなしの場合

バックアップシステムにランサムウェアが侵入すると…
ランサムウェアはバックアップデータに自由にアクセスできるため、
変更/暗号化/削除され、ユーザからはアクセスできない状態に…

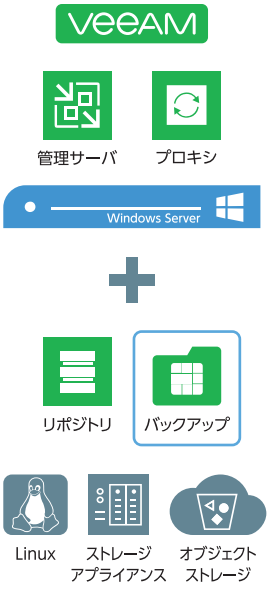


Blockyありの場合

ホワイトリストに登録したアプリケーション以外からは
変更/削除できないようにBlockyがリクエストを制御します。
独自フィンガープリントチェックで改ざんや偽装されたリクエストも
ブロックされバックアップデータは保護されます



Veeamでランサムウェア対策するには?



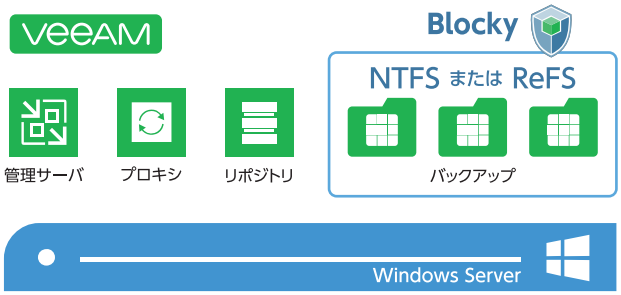
管理サーバのため、Windowsが必須

Veeam管理サーバがサポートしているOSはWindowsのみです。このため、Veeamを利用するには少なくともWindowsマシンが1台は必要になります。

Veeam機能での
ランサムウェア対策には
追加Linuxまたはストレージが必要

Veeam機能でランサムウェア対策するには保存先となるリポジトリで不変性をサポートする必要があり、現在、これに対応しているリポジトリはLinux、ストレージアプライアンス、オブジェクトストレージのみです。Windowsリポジトリで不変性はサポートしておらず、Veeamのみでランサムウェア対策するには別途Linux またはストレージを追加する必要があります。

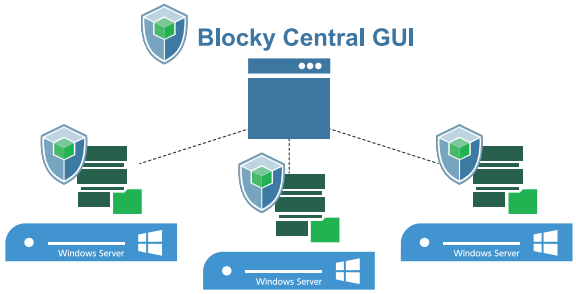
Windows Server 1台でもランサムウェア対策



WindowsのNTFSとReFSのボリュームをBlockyで保護できます。これにより、オールインワンなVeeam管理サーバで、ローカルにバックアップをとっているような構成でも、追加サーバやストレージなしに既存バックアップ環境へランサムウェア対策を追加できます。

分散/マルチサイト構成も統合管理

複数のWindowsリポジトリが構成されている環境や、マルチサイトでVeeamを使用しているような場合でも、Blocky Central GUIを用いて、ボリューム保護の構成やアラート通知設定などを統合管理できます。



従来アプローチでは難しいゼロデイ攻撃にも ホワイトリストアプローチ で対応

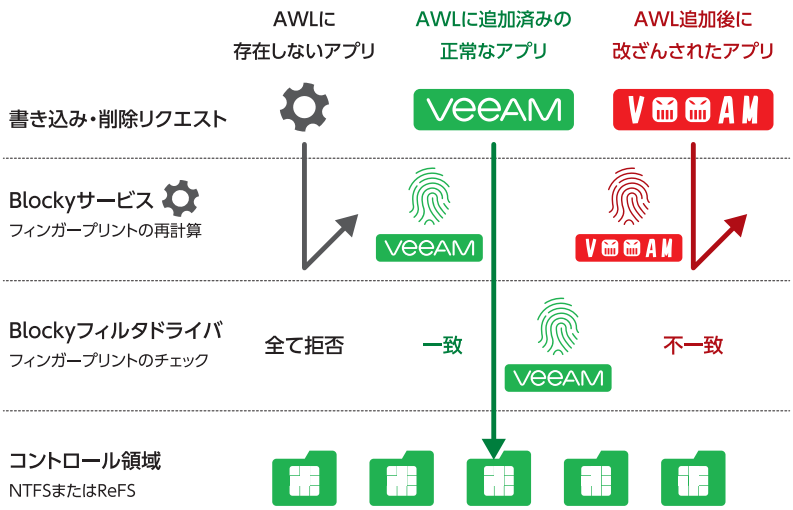
ブラックリストアプローチ

Blockyのアプリケーションホワイトリスト（AWL）アプローチは、どのアプリケーションも信頼しておらず、デフォルトでは全てブロックします。そしてAWLに追加したアプリケーションからのアクセスについても、その信頼性をフィンガープリントでチェック、改ざんや偽装されたアクセスでないことを保証します。このように信頼できるかどうかをチェックすることでバックアップを確実に保護します。

ウィルス対策ソフトなど、リストに載っている脅威を識別してブロックするブラックリストアプローチでは、常に定義ファイルを最新にしても、新規の脆弱性を利用するゼロデイ攻撃を防ぐことはできません。脅威であるかどうかをチェックするのではなく、全てのアプリケーションが脅威になる前提でゼロトラスト構成を実現する必要があります。

アプリケーションホワイトリスト（AWL）アプローチ

改ざん/偽装アプリケーションからの変更・削除リクエストもブロック



Blockyのコアコンポーネントをインストールすると、Blockyサービスと Blockyフィルタドライバが構成されます。Windows上にロードされたBlockyフィルタドライバはコントロール領域への変更/削除リクエストをチェックし、AWLに存在していないアプリケーションからのリクエストはシステム含めすべて拒否します。AWLにアプリケーションを追加すると、Blockyサービスがそのdllや属性、アプリケーション固有の動作からハッシュ値を計算し、フィンガープリントとして記録、AWL追加済みアプリケーションから変更/削除リクエストがあると、ハッシュ値を再計算し、一致する場合にのみ許可します。改ざんや偽装されたアプリケーションの場合、このフィンガープリントチェックを通過できないため、正常なアプリケーションからのリクエストのみがコントロール領域へ実施されることが保証されます。また、Blockyサービスが変更または停止された場合にはフィルタドライバは完全保護モードになり、全ての変更/削除リクエストを拒否し、管理者に通知します。

よくある質問

保護ボリュームに制限はありますか?

はい、保護ボリュームを他のアプリケーションで、たとえばキャッシュやダンプなどで使用してはなりません。
また、以下のボリューム構成やWindows 機能にも対応していないことに注意してください。

- システムドライブ（C:\）
- ダイナミックディスク
- ReFSの重複排除（NTFSの重複排除はサポート）
- NAS（SMBやNFS）
- Microsoft フェールオーバクラスタ構成
- Active Directory ドメイン コントローラ構成

ボリュームの一部のみを保護できますか?

はい、保護はボリューム全体に対して、またはボリュームの最初のディレクトリ レベルの個別ディレクトリに対して有効化できます。
これにより、一部のディレクトリを他の目的で変更/削除可能にしておくことができます。

不正な書き込み試行などはどのように通知できますか?

電子メール、Windowsアプリケーションイベントログ、Blocky ログ（GUIのMonitoring項目）に通知できます。

Blocky をウイルス対策ソフトウェアなどのセキュリティツールと併用できますか?

もちろん、ウイルス対策ソフトウェアなどのセキュリティツール併用可能です。ウイルス対策ソフトからの不要な通知を回避するには、下記をウイルス対策ソフトウェアのリアルタイム スキャンおよび動作監視から除外する必要があります。
C:\Program Files\GrauData\Blocky\BlockyAccessCntrlSvc.exe

Blocky 自体はどのように保護されていますか?

Blocky for Veeam はパスワードで保護されています。インストールまたは初回起動時にパスワードを設定する必要があり、Blockyのアップデート、アンインストール、保護機能の有効化/無効化で入力を求められます。

■ サポートOS

Windows Server 2012, 2016, 2019, 2022
※Serverのみクライアント OSはサポートしていません。

■ 対応ボリューム

Windows NTFS, ReFS
※ネットワーク接続ストレージはサポートしていません。
※iSCSIやFC、USBなどで接続されたストレージもサポートしていますが、Blockyがインストールされた Windowsでのみ保護されます。

Climb Inc. Growing to Meet Your Needs 株式会社クライム
www.climb.co.jp
本　社／〒103-0014 東京都中央区日本橋蛎殻町1-36-7 蛎殻町千葉ビル4F
Tel:03-3660-9336 Fax:03-3660-9337 E-mail:soft@climb.co.jp
大阪営業所／ Tel:06-6147-8201 名古屋営業所／ Tel:052-462-1282
福岡営業所／ Tel:092-686-8637