Blocky for Veeam®

Safeguarding Veeam® Backups with Application Whitelisting

GRAU DATA
Your data \ Your control _

Contents

Introduction 3

The Challenge for Reactive Blacklisting Security Methods 4

Blocky for Veeam® A Proactive Approach to Malware Protection 5

Lower Resource Utilisation and Tamper Proof Resilience 6

Blocky for Veeam® Deployment Best Practices 7
- 1 Security and Contingency Planning 7
- 2 AWL Deployment 8
- 3 Monitoring and Simulation 8
- 4 Create AWL Rules 9
- 5 Lockdown 9

Conclusion 10

References 10

Blocky for Veeam®

INTRODUCTION

There is no question that the increase in frequency and severity of cybercrime attacks it set to continue as cybercrime groups and their Malware payloads become more and more sophisticated. Corporate IT departments play out a constant battle of implementing cyber security where they are always one step behind the bad guys. While high-profile, headline-grabbing ransomware cases and data breaches are likely to continue, it is the small and medium-sized businesses (SME) that are the most attractive targets for hackers as they either do not have sufficient resources to defend against an attack, or they do not take cybersecurity as seriously as they should. According to the UK Cyber Security Association which is a not-for-profit organisation providing expert advice and cyber security resources, 65% of UK SMEs experience a data breach at least once per month, only 29% have written a formal cyber security policy to protect their business and only 51% took recommended action to identify the risks to their business from cyber attacks[1].

The total cost of a ransomware attack extends far beyond the ransom payment if one is made. Remediation costs of the network and company data need to be factored alongside potential brand and reputation damage if the interruption to business operations is severe enough. Ransomware actors have also begun hijacking customer data from victims and threatening its release which adds the risk of 3rd party liability claims if demands are not met.

An effective cyber security strategy requires a multi-level approach encompassing not only the obvious protection of vulnerabilities at all points within the technology stack, but also employee education to drive awareness and security best practices.

Ensuring the integrity and security of Veeam® backups is an important part of any resilience and recovery plan should ransomware become an issue within your IT environment. The stance on ransomware from Veeam is quite simple: do not pay the ransom, and restore from backups. Of course this strategy can only succeed if the hackers have not encrypted your backups first before issuing their demands, an alarming trend that is currently being frequently reported.

This white paper will outline how Blocky for Veeam® can proactively ensure that Veeam backups remain a vital insurance policy against ransomware attacks.

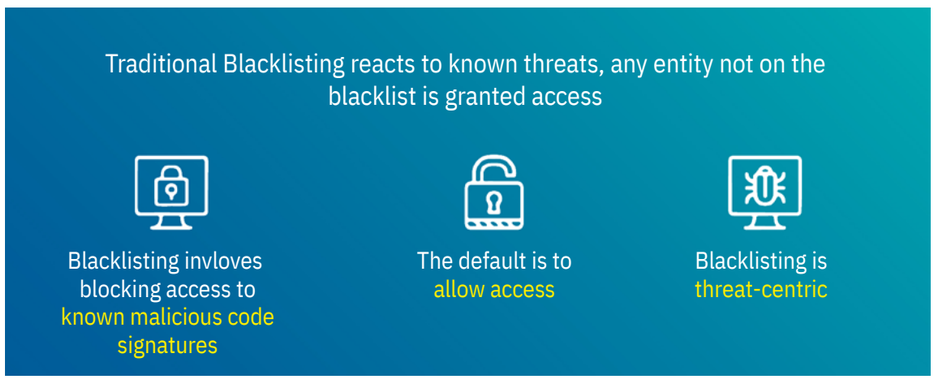
GRAU DATA
Your data \ Your control _

The Challenge for Reactive Blacklisting Security Methods

Traditional malware protection systems, including firewalls and antivirus software, use a protection technique known as blacklisting. This approach is based on maintaining a list of protective signatures for codes that should be denied access to the network. This is an effective technique but a time consuming one; both for the security software companies that constantly have to maintain definition files to detect and isolate all known malware codes, and for the IT staff who have to ensure that all system patches and definition files are kept up to date.

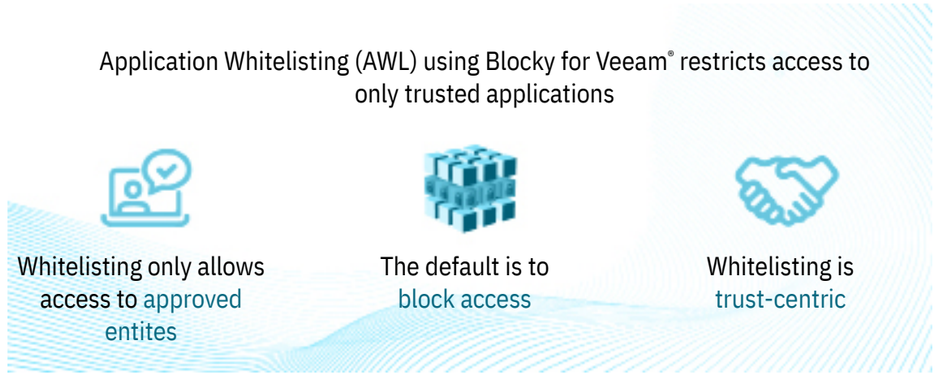
Malware and virus payloads are designed to exploit vulnerabilities that have been found within the technology stack, these could be within an operating system, the network infrastructure, an application or anything in between. Herein lies the key failing of the blacklisting approach; you are constantly patching security holes that are already known and being exploited, hence the reason IT security teams are always on the back foot against cybercrime.

The traditional blacklisting approach is a reactive one which allows new and unknown malware codes to infiltrate and propagate undetected before they wreak their havoc. These unknown codes are known as ‘zero day’ exploits. Until these vulnerabilities are mitigated, hackers can continue to exploit them to adversely affect system applications, company data and additional computers on the network.



Blocky for Veeam®

Blocky for Veeam® A Proactive Approach to Malware Protection



Blocky for Veeam® uses a trust-centric approach known as application whitelisting (AWL). This turns the security protocol around from the traditional blacklisting protocol of “default allow” to a much more robust “default deny for any unknown application”.

With AWL the system administrator creates a list of trusted applications that are allowed to access and modify files on a particular storage volume. In the case of Blocky for Veeam®, the Veeam application can be set if required as the only system process permitted to modify files on the storage volume used for backups.

Of course it is not quite as simple as selecting a set of named executable files that can be granted access to a particular volume. The AWL within Blocky uses application fingerprinting technology to create a unique hash value signature for each permitted application based on attributes such as the dynamic-link libraries used in addition to other behaviours that are representative of an applications unique identity.

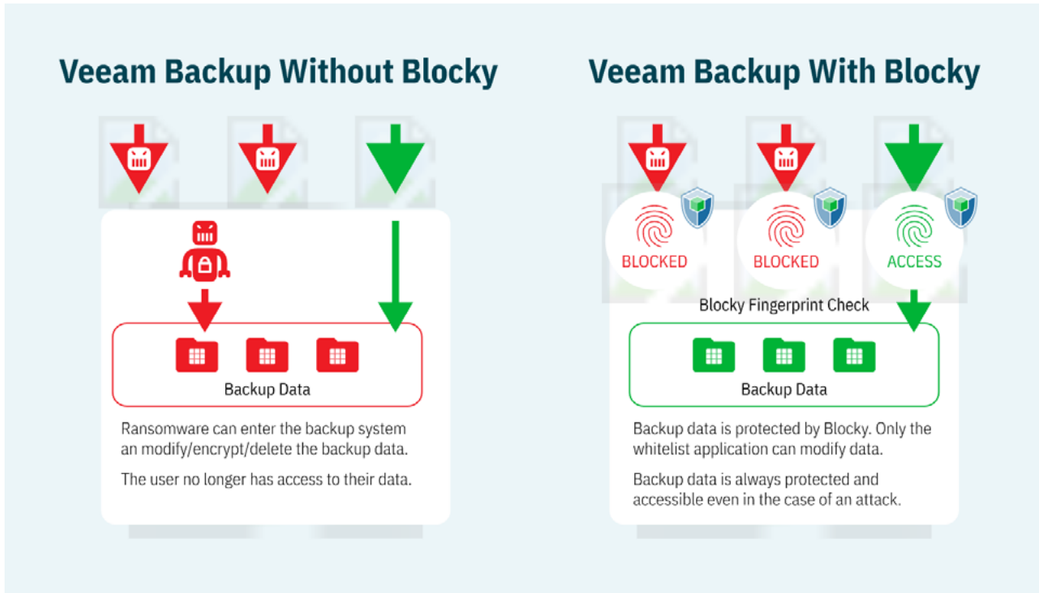
Any malware that masquerades as a known or trusted application should not get past Blocky’s identity checks. With Blocky system administrators can proactively protect Veeam backups while simplifying their job in the process.

GRAU DATA
Your data \ Your control _

Lower Resource Utilisation and Tamper Proof Resilience

Unlike the traditional blacklisting approaches Blocky does not require a vast list of excluded malware code signatures to be maintained and constantly updated. It is consequently far more system resource efficient than traditional antivirus applications and integrated deeper into the operating system, rather than being an add-on application.

Once a whitelist has been established for a particular storage volume or 1st level directory within that volume, the Blocky filter driver ensures that only the applications matching the previously authorised fingerprints have write access. AWL is operationally simpler with no lapse in malware protection if the system is, waiting for, or in the process of applying security patch updates.
In addition to the deeper operating system integration, Blocky includes deactivation and de-installation protection built into the standard feature set resulting in an extremely tamper proof security solution.



Blocky for Veeam®

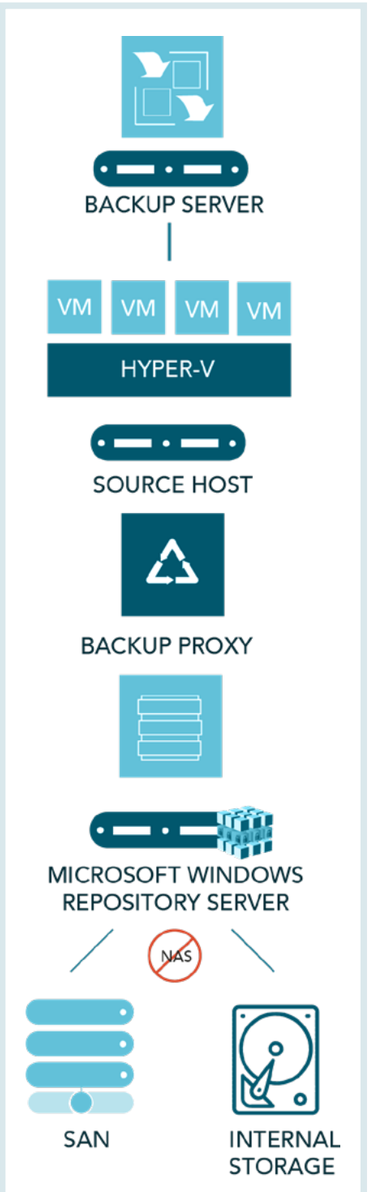
Blocky for Veeam® Deployment Best

1 Security and Contingency Planning

A key starting point for any organisation is the development of a robust cyber security plan that meets risk assessment profiles and recovery time objectives. Blocky provides a powerful addition to the practical cybercrime prevention tips recommended by Veeam such as the 3-2-1 rule.

The 3-2-1 rule states that for best practice three different copies of your production data should be taken, using two different types of storage media, one of which should be off-site. To further mitigate ransomware protection Veeam suggest adding another “1” to the rule whereby one of the media is offline[2]. Examples of offline storage include tape, removable hard drives, cloud connected immutable storage and replicated VMs hosted on a different domain. The offsite and offline techniques suggested within the 3-2-1 rule are certainly effective but could add complexity beyond the resources available to some SMEs and may increase data recovery times following an attack.

Blocky is installed on the Microsoft Windows Repository server and provides protection for NTFS and ReFS volumes residing on internal storage, directly attached disk based storage such as block storage connected via iSCSI or a Fibre Channel SAN.



GRAU DATA
Your data \ Your control _

Blocky for Veeam® Deployment Best Practices

It therefore provides vast recovery time benefits over backup images residing off-site or offline; however, your risk assessment should determine what recovery time objectives are acceptable to meet your business continuity goals.

2 AWL Deployment

Blocky works with all versions of Microsoft Windows that meet the system requirements for a Backup Repository Server as outlined in the Veeam Backup & Replications User Guide[3]. Volume sizes should then be determined for systems holding backups or other business critical information that needs protection. When determining volume licensing it is recommended that a capacity growth of 10% be factored per annum, however data growth should be determined based on individual company growth rates and expansion plans. Every system that has a storage volume requiring protection should be checked for malware with an applicable scanner using the very latest virus signature definitions before proceeding to install the Blocky for Veeam® executable.

3 Monitoring and Simulation

The most important step towards combating cyber-attacks is to ensure that you have the best possible real-time visibility into suspicious behaviour. This can help to mitigate the propagation of malware onto other systems within your infrastructure.

Veeam ONE 9.5 introduced a new predefined alarm called “Possible ransomware activity” which triggers if there are excessive writes on disk or high CPU utilisation. Similarly, Blocky for Veeam® provides extensive monitoring and reporting functionality that will show and log all write requests received by protected volumes and folders.

Following installation Blocky can be run in Automatic Whitelisting mode for a period of up to 24 hours. When using Automatic Whitelisting, ALL program requests are granted and are added to the Whitelist. This can be dangerous as this does NOT protect against Viruses, Worms, Ransomware, or human error. This feature should only temporarily be used to configure systems which can be rated as clean and “secure”. After the countdown timer has ended, automatic
whitelisting is turned off and all further unauthorised requests are blocked.

The list of trusted applications should be checked after automatic whitelisting has ended to remove any unwanted applications from the list. It is recommended to keep only absolutely
required applications!

Alternatively applications can be manually whitelisted from the Blocky GUI main menu by selecting applications that you

Blocky for Veeam®

Blocky for Veeam® Deployment Best Practices

wish to allow unrestricted file access using the FileBrowserDialog . If the whitelisting process was successful the application is displayed in the table “List of Trusted Applications”

It is also possible to whitelist applications via the Blocky request table if the administrator GUI is running. During this time, if a file modification is attempted which cannot be assigned to any currently whitelisted program, the attempt will be displayed in the request table so that an administrator may then manually control file access. If there is no answer to a request within 1 minute, the access is automatically denied. Access can be manually set to one of four options: GRANT, DENY, AUTHORIZE PID (write access is granted to all files for the specified process ID until its termination (NT kernel and system processes are excluded)) and WHITELIST PROGRAM (write access on files is granted for the specified program in general).

This monitoring period is useful to ensure that all applications needing write access permission are accounted for. In addition, during this time the administrator can attempt to create files on a target volume to simulate a malware attack and in doing so become familiar with the monitoring, logging and authorisation mechanisms available within Blocky. For more information regarding volume monitoring and whitelisting control please refer to the Blocky for Veeam® Administration Guide.

4 Create AWL Rules

Following a period of monitoring the administrator will be in a position to identify and confirm all application processes that should be granted write access permission to each of the volumes and/or 1st level directories that Blocky has been set to protect. If over time, new data sets and application processes require protection within the monitored storage volumes, then appropriate authorisation can be added within the Blocky for Veeam® administrator GUI. Also during this stage notification reporting via email should be configured to ensure administrators receive immediate warning of any unauthorised access attempts.

5 Lockdown

The final stage in the AWL process is to set each chosen machine into lockdown with only the permitted applications authorised to make any write modifications to protected volumes.

GRAU DATA
Your data \ Your control _

Conclusion

With so many ransomware attacks succeeding through ‘zero-day’ vulnerabilities, many of which are manually controlled in real-time by increasing sophisticated cyber-criminal teams, it is vitally important to use a proactive security solution to prevent Veeam® backup files from being compromised.

Traditional techniques based on blacklisted code patterns are always one step behind in the fight against cybercrime and while they are still an important part of any security strategy, Blocky for Veeam® offers a resilient solution that consumes very little system resources, is easy to install, configure and maintain.

AWL should form a key part of any robust security plan alongside traditional measures throughout the technology stack. Human behaviour is a major contributory factor to corporate cyber security, whether it be unintentional or malicious. Therefore, for maximum chances of success any technical security measures must be supported with clear security policies, adequate training and a regular review of best practices.

References

1. Anon. (2020) Some worrying Statistics [online] http://cybersecurityassociation.co.uk Available at http:// cybersecurityassociation.co.uk/membership-benefits/ [Accessed 7 Sep. 2020]

2. Vanover, R. (2016). 7 Practical tips to prevent ransomwareattacks on backup storage [online] http://veeam.com Available at http://veeam.com/blog/tips-to-prevent-ransomware-protect-backup-storage.html [Accessed 7 Sep. 2020]

3. Anon. (2020) Veeam Backup & Replication 10 User Guide for VMware vSphere [online] http://helpcenter.veeam.com Available at http://helpcenter.veeam.com/docs/backup/vshere/system_requirements.html?ver=100/#repo [Accessed 7 Sep. 2020]