WHITE PAPER

CARBONITE
an opentext company

WEBROOT
an opentext company

Security Tips for Protecting your Backup Servers

The Problem

The rapid rise of malware attacks in the past few years has brought to the attention of administrators and C-level roles alike the increased risk businesses face today regarding data loss, crippling production delays and harmful reputation hits. Not only is the frequency of malware on the rise, but the ever-changing complexity or polymorphic characteristics of malware creates a huge hurdle for detection to find and isolate. In fact, in 2019, 93% of malware strains seen by Webroot were polymorphic.[1]

This has led to businesses evaluating and implementing a multi-layered approach to securing and protecting company data. This paper will focus on additional measures and techniques to specifically protect the backup environment, as well as the Carbonite multi-layer approach for securing your data, part of our cyber resilience philosophy.

The Cyber-Resilience Approach

Cyber Resilience is the ability to continuously deliver the intended outcome despite adverse cyber events. Think of cyber resilience as digital fitness.   It's the ability to absorb punches and get back on your feet, no matter what threatens. The concept of cyber resilience is critical for companies of all sizes, as is the ability to not only be as secure as possible from breaches, but also quickly recover and continue business as usual even if a breach does occur. Put simply, strong cyber resilience could make the difference between continuing to grow your business and going under. Carbonite and Webroot have a full suite of cyber resilience solutions for every business.

- **Webroot® Security Awareness Training** is for your first line of defense: your people. It provides a phishing simulator, robust training courses, and reporting, and helps support compliance requirements.
- **Webroot® DNS Protection** is the first DNS Protection service to marry DoH (DNS over HTTPS) privacy with security. This solution provides enhanced connectivity, helps reduce latency and stops up to 88% of known malware.[2] It's also simple, fast and easy to deploy.
- **Webroot® Endpoint Security** is our leading next-generation security solution. It provides advanced security and detection, simplified security management and integrated support and remediation.
- **Webroot BrightCloud® Threat Intelligence** is the primary driver behind our power-in-prediction and cyber resilience platform.

These solutions are complemented by offerings from Carbonite, including:

- **Carbonite® Endpoint** provides comprehensive protection of all the data that resides on your endpoints to help prevent data loss, while providing advanced administrative control and award-winning support.
- **Carbonite® Backup for Microsoft 365** is a complete backup solution for the entire suite of Microsoft 365 applications, including protection from data loss due to human error and ransomware attacks.
- **Carbonite® Recover** enables rapid recovery in the cloud for your entire business through continuous real-time replication.
- **Carbonite® Availability** uses continuous, byte-level replication to maintain an up-to-date copy of your operating environment.
- **Carbonite® Migrate** moves server workloads across different hardware platforms, storage types and operating systems with minimal risk and near-zero downtime.
- **Carbonite® Server** offers efficient, comprehensive, all-in-one protection for servers with flexible deployment and optional local failover.

Tips to Secure Your Backup Environment

Backup is your copy of your most valuable digital assets. Implementation of secure backup policies is necessary to facilitate disaster recovery protocols when adverse events threaten to disrupt operations. It requires a deep understanding of the different types of data under protection and the urgency of the data for the users who depend on it.

With the right tools for protecting data, any organization can establish secure backup policies that help ensure the availability of data. The important thing to remember is that backup security is not a project, but a process that requires constant monitoring and improvement.

The sections listed below serve as tips for implementing a more secure backup infrastructure. We will primarily focus on securing the Carbonite® Server director. The director serves as the storage repository for your backups. It also performs other tasks like replication to maintain multiple copies of your data through N:1, 1:1 and N:1:1 replication.

1 Do not broadcast your backup server

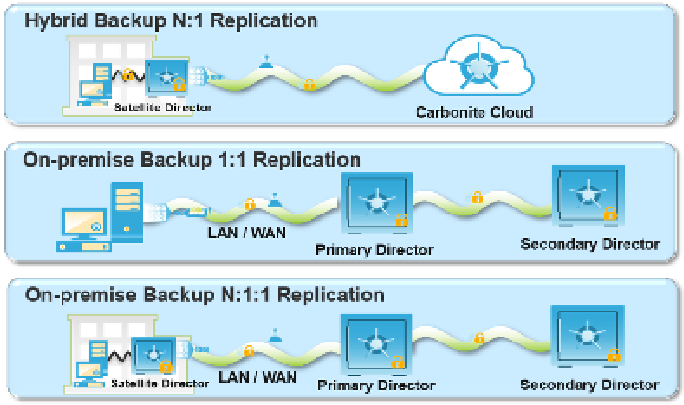
When deploying a backup server, stealth can be your friend. Adding an Active Directory entry for your backup server is like providing an advertisement message saying, "I'm right here." Instead, use window workgroups or connect agents to the backup server via static IP address. The less information known about the backup server, the better.

Hide OS services and application version numbers when possible. Some services and applications installed on the protected server may display version information via an HTTP header. Providing this version information can also provide an attacker with useful information regarding potential exploits. It may be simple to remove this information by deleting it from the HTTP header of its greeting banner. Since the director runs on a Windows Server operating system, examine the protected server's OS for specific Windows services. You may wish to scan those service and application ports with a tool such as Nmap or Netcat to verify the information presented. For specific services or applications, you should refer to the product support documents or vendor website. Also use caution before modifying any application settings.

These types of procedures are often referred to as "Security through obscurity" or STO. The technique can be a useful way to reduce the chances of attack, but only when employed along with other security components that form a complete security strategy. STO should never be looked upon as an all-encompassing security practice.

2 Implement a replication configuration

Carbonite® Server supports multiple replication architectures. The N:1 configuration allows multiple local (often referred to as satellite) directors to replicate to a single primary director. The 1:1 configuration allows a single primary director to replicate to a single, passive secondary director. This ensures that data is available for restore even if one vault is offline or unavailable. It also ensures that a redundant copy of your backup data exists and can be accessed if any compromise to your primary director were to occur. Typically a secondary director will be placed at a separate data center facility, often at a specified DR site. Examples of Carbonite replication configurations are illustrated here.



Since Carbonite® Server writes to storage in a proprietary format, if data is corrupted on the primary director, replication (N:1, 1:1 or N:1:1) would fail. If data is corrupted (e.g. disk failure) or changed by a foreign process (e.g. malware) the director would detect the issue, stop replication, and alert the administrator to prevent the push of corrupted data to a secondary director.

Additional steps can be taken to enhance security and further protect the redundant backup data housed on the secondary director, as detailed in the next section.

3 Network separation

It is critical to ensure secure communication with your backup server. One of the best security strategies is to separate your backup network into security zones. Security zones are groups of servers, systems and networks that have similar security requirements. Each zone consists of a single interface or a group of interfaces to which a security policy is applied. These zones are typically separated using a layer-3 device such as a firewall or through virtual local area network (VLAN) segmentation. If configured correctly, VLAN segmentation hinders access to backup environments by limiting packet sniffing across security zone trust boundaries and by limiting broadcast domains.

Using Carbonite® Server, this can be accomplished by separating the agents, primary director and secondary director (passive backup server) into separate VLAN segments or security zones. You should then lock down the backup and replication traffic to the specific ports required by Carbonite® Server for agent-to-director communications or director-to-director replication. Section 7 discusses port requirements in greater detail. It is recommended that you place the secondary director in a security zone with other disaster recovery equipment if you are performing 1:1 vault replication.

Keep in mind, backup traffic from the agents to the director is always encrypted with AES 256-bit at rest and SSL/TLS in transport. Replication traffic is also encrypted between directors.

4 Update OS and Carbonite Server versioning

Periodic update of the operating system and application software on a server is a crucial step in keeping it safe from security risks.

Outdated software versions have typically already been explored for weaknesses and vulnerabilities, leaving them open for attackers to exploit those known weaknesses and vulnerabilities. Keeping everything up to date minimizes the number of vulnerabilities.

Software manufacturers are continually updating versions for new features and efficiencies. However, they are also patching potential security vulnerabilities. Keeping software up to date is a key method for securing your assets, including your backup infrastructure.

The question is how often should you update and upgrade your backup server and agents.

Automatic updates are one way to guarantee that no updates are forgotten. However, allowing the system to automatically make such changes on its own also introduces risk. Before you update your backup server or agent, download the release notes and research the update notes for potential impacts. The Carbonite® Server portal does have an optional automatic agent update capability. However, many, if not most, administrators prefer a scheduled agent update.

One of the best methods for a solid update/upgrade strategy is to define a scheduled time to periodically review the agents and the server versions (for instance, monthly or quarterly). Download the release notes and evaluate necessity and required effort of the updates/upgrades. Then define the right date and time to implement.

Verify any installation dependencies before installing software. Make sure you are not adding anything to the system that is unnecessary. Also, determine if any of these dependencies will be auto-started on the director and make sure those auto-starts are required. The best rule of thumb is to not install any software that is not necessary to manage the Carbonite® Server backup process.

A word of warning: Do not let your updates/upgrades fall too far behind. Not only will you be easing your way into a less secure environment, but you also risk a more complex upgrade scenario (for instance: multi-step dependent upgrade) which may require more time and effort.

5 Limit and monitor access

Who has access and the level of privilege they maintain to your backup server needs to be closely monitored. Most security comes down to having responsible people. The backup administrator has access to a vast amount of a company's data. That individual must be trustworthy and well versed in security policy. Basic steps like pre-employment background check and review of references can reveal potential issues. Security policy training, reviews and audits are activities the backup administrator should regularly participate in. Periodic operational audits can ensure that all the correct procedures are maintained.

Administrators need to periodically review access to backups. Some common tasks to perform are:

- Look for older unused Admin or user accounts and immediately disable or remove.
- Review the need for access. Often accounts are created on the fly with more privilege and rights than necessary to perform their appropriate tasks.
- Review any audit logs for unusual access and activity. Report and anomalies or violations to the security manager.

When evaluating backup solutions, verify the backup solution provides the appropriate amount of auditing and security capabilities that are consistent with the company's security policy requirements.

6 Establish and enforce a password policy

One of the major access risks is weak password enforcement. Weak passwords can be easily acquired through password guessing and brute-force attacks. In order to minimize the risk, there are certain steps that can be taken. These steps should be detailed in a password policy.

The first thing is to set a password policy that must be followed by all members on the server, no exceptions. Some steps to enforce are:

- Root out and correct all empty or default passwords on the server.
- Enforce a minimum password length and complexity.
- Implement a lockout policy that is triggered by a specified number of failed attempts.
- Do not store passwords using reversible encryption.
- Force session timeout for inactivity.
- Enable two-factor authentication.
- Set an expiration date for a password. Monthly or quarterly are typical, however, for higher privileged accounts, setting a faster expiration time may be prudent.
- Use passphrases instead of passwords. Often, they can be just as easy as passwords to remember. For example: **I-WantToDrinkBourbonAt1255CenterSt!**

The password policy should be required to access the administrative consoles as well as encryption security. Keep in mind, job encryption passwords need to be well planned out and secured. It's best not to change them, because if they are changed it will require the reseed of the job data.

7 Turn off unnecessary Windows services and ports

It's simple math: More employed services will require more access and more open port traffic. Increase the backup server security by reducing the attack surface area.

To reduce the attack surface area, software installed and maintained should consist of only the bare minimum necessary to maintain requirements and keep the application and server running. Only enable the network ports used by the OS and required by Carbonite® Server application components. The less you have on the system, the better. Here's a list of Carbonite® Server ports:

Agent Port	Communication	Protocol
Outbound:8086, 8087	To Portal	TCP
Outbound: 2546	To vault	TCP
Outbound: 2548, 8031	To Windows Central Control	TCP (optional)
807, 2547, 12547	Vault Replication - 1:1	TCP (Only if Replicating)
807, 2547, 12547	Vault Replication - N:1	TCP (Only if Replicating)

A Windows OS server should only have required services to maintain that backup application. For instance, it is unlikely that the Carbonite® Server director will require the Bluetooth Support Services (bthserv) to maintain the backup application. Please refer to Microsoft support documentation for a full list of services and their purpose. Also, several security publications exist regarding the process of hardening Windows Server configurations. You may wish to research them, especially if your organization falls under compliance or regulatory mandates.

A few useful guides that provide information on this topic but are beyond the scope of this document are listed below:

- NIST Special Publication 800-123 - Guide to General Server Security
- CIS Benchmarks - Securing Microsoft Windows Server
- Microsoft - Windows security baselines

If possible, disable Remote Desktop Protocol (RDP) on the Carbonite® Server director. If remote access is required, look at methods for locking down RDP. Always make sure to only allow RDP access when combined with VPN access. You should never expose port 3389 directly.

When you purchase an appliance from Carbonite or implement an appliance using Carbonite professional services, much of this work is done for you up front. However, Carbonite provides the option for customers to provide their own server hardware, as long as it meets the backup workload requirements. Therefore, our customers will often implement and configure their own backup server(s). If this is the case, there are certain steps and considerations regarding which Windows services are necessary.

8 Test your backups

It's essential to periodically test your backups. However, the process for testing backups and Disaster Recovery (DR) can often dictate the results. A successful result can often be misleading. When testing the backup recovery or DR procedure, a few general rules of thumb include:

- Test with real data. Don't create a special backup as a recovery demonstration. Randomly, select safe set data from historical backups.
- Spot check file system backups. Since most recoveries are single file or folder recoveries, perform multiple recoveries from different point-in-time backup safe sets. Set a minimum of at least three recoveries for three separate backups. It's also recommended to select separate or multiple server backups to recover from.
- Test full system recovery via a Bare Metal Recovery (BMR). Verify that all applications and their associated data are correctly operating as expected after the recovery.
- Document your results, including:
  - Data size
  - Recovery time
  - Any recovery issues
  - Any work-around steps required
- Incorporate the results into your DR plan

Summary

Carbonite® Server, whether it is deployed as an on-premises or cloud backup solution, provides many options and features to secure your data. Carbonite is committed to the security of your data, exemplified by our approach to security within our cloud service offering. For more information on our own internal procedures, read this datasheet.

However, when deploying any hardware or software solution on-premises, it is important to secure the infrastructure that supports it.

[1] 2020 Webroot Threat Report
[2] Based on Webroot's internal testing

Contact us to learn more – Carbonite US
Phone: 877-542-8637
Email: carb-data_protection_sales@opentext.com

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.