opentext™

WHITE PAPER

5 Security tips for protecting Carbonite™ Endpoint Backup

Data is your most valuable digital asset. Implementing secure backup policies is necessary to facilitate disaster recovery protocols when adverse events threaten to disrupt operations. Successful backup requires a deep understanding of the different types of data under protection and the urgency of recovering data that users depend on.

With the right tools for protecting data, any organization can establish secure backup policies that 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 five tips listed below help you implement a more secure backup infrastructure. We will primarily focus on securing the Carbonite™ Endpoint Backup Vault by OpenText™.

1. Update Carbonite Endpoint Backup agent

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Outdated software versions have typically already been explored for weaknesses and vulnerabilities, leaving them open to attackers.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

Software manufacturers are consistently 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.

Make sure to install and update the Endpoint Backup agents on Windows and Mac endpoints. Generally speaking, the version installed on the endpoints should be within a year of the most recent release. However, please check the release notes for each update because some versions may have urgent security patches. To assist with keeping current, the recent auto-upgrade enhancement will allow for the agents to be upgraded automatically with each new release.

2. Update OS and Carbonite Endpoint Backup vault

Automatic Windows OS updates on your Endpoint Backup vault 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 vault software or OS, download the release notes and research the update notes for potential impacts.

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

Verify any installation dependencies before installing software. Make sure you are not adding anything unnecessary to the system. Also, determine if any of these dependencies will be auto-started on the server 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 Endpoint Backup service.

A word of warning: Do not let your updates and upgrades fall too far behind. Not only will you decrease security, but you also risk a more complex upgrade scenario—for instance, a multi-step dependent upgrade—which may require more time and effort.

3. Secure SQL Server

The SQL Server is part of the Endpoint Backup on-premises vault installation. So you should also make sure the SQL Server is also updated and secure. Comprehensive guidance for securing the SQL Server can be found on the Microsoft site: Securing SQL Server and Security Considerations for a SQL Server Installation. Of particular note, configure unique credentials for the database, and restrict network access to only communicate with the vault server.

4. Limit and monitor access

Closely monitor whoever has the access and privilege to maintain your Endpoint Backup vault server. 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 a pre-employment background check and a 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 on the server and immediately disable or remove them.
- Review the need for access—accounts are often created on the fly, with more privileges and rights than necessary.
- Review users with dashboard access within the Endpoint Backup service.
- Ensure that each user has the proper role for their job functions.
- Leverage your identity provider for secure authentication and authorization to the dashboard—Endpoint Backup supports any SAML 2.0 identity provider, such as Entra ID, Okta, Ping, and others.

Resources

Endpoint Backup: Endpoint protection of the evolving workforce

Read the datasheet ›

Endpoint Backup: An in-depth look at encryption technology behind our premium endpoint backup solution

Read the whitepaper ›

Endpoint Backup: Streamline the device replacement process

Read the technical guide ›

5. 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 Endpoint Backup vault security by reducing the attack vector.

To reduce the attack vector, 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 Endpoint Backup vault components. The less you have on the system, the better.

The required ports for the Endpoint Backup vault are 443 HTTPS (over TLS v1.2):

- Inbound from agents
- Outbound to external address https://license.mysecuredatavault.com

If another Endpoint Backup component, such as QuickCache or LDAP server is included, please see this article for more information.

A Windows OS server should only have the required services to maintain the backup application. For instance, it is unlikely that the Endpoint Backup vault will require 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

Lastly, If possible, disable Remote Desktop Protocol (RDP) on the Endpoint Backup vault. 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.

To learn more, please visit https://www.carbonite.com/business/products/endpoint-protection/

opentext™