



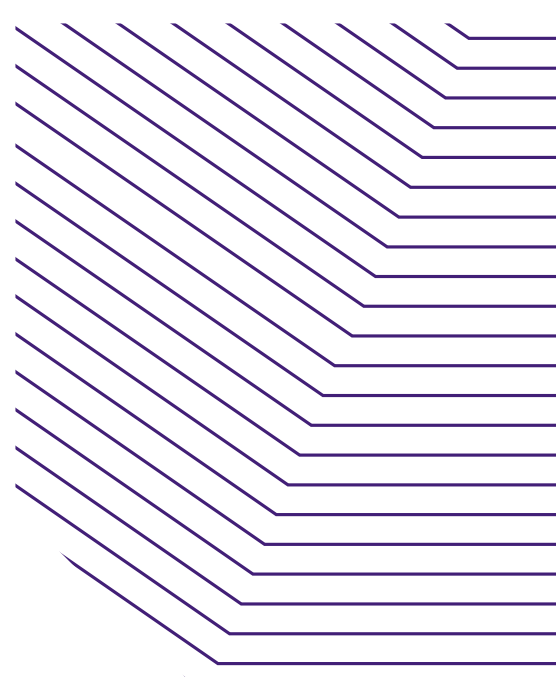
How (and why) Carbonite Server ensures data immutability for users

The evidence of a rise in ransomware attacks is all around us – at work, on the nightly news, it may even be what keeps us up at night. All types of serious studies back up what’s obvious to anyone with a passing interest in IT.

According to the Ransomware Task Force (RFT), a multi-disciplinary group of experts assembled by the non-profit Institute for Security + Technology, “in 2020, nearly 2,400 U.S.-based governments, healthcare facilities, and schools” alone were victims of ransomware, to say nothing of private sector facilities.

Another study, reported in InfoSecurity Magazine, reported a 150% overall jump in ransomware incidents in 2020. The average payment for ransomware incidents, also climbed significantly, by 171% in 2020 according to RFT.

Luckily, backup and recovery solutions are one of the most surefire ways to undermine ransomware actors’ demands for cash. In this paper, we’ll cover a few key steps for configuring Carbonite Server backup to ensure that, if the worst happens, your data backups cannot be tampered with and won’t be fooled into irrevocably backing up data encrypted by ransomware actors.



Designed for security

Since the first release of our Server Backup product in 2000, a key design goal has always been protection from unsolicited data modification, guaranteeing the fidelity of the restored data. Our initial product released in 2000 supported the latest encryption standards at that time and we have continually evolved the product to support the latest encryption standards including full support for AES-256. Apart from supporting the latest encryption standards, Carbonite® Server backup was designed to support a robust replication architecture that can be configured by each customer to ensure data is immutable and always available even if one or more vaults are offline or unavailable.

In addition, our datacenters are designed and built to industry standards with multiple layers of fault-tolerance and redundancy at the component and systems level, full adherence to industry standard regulations including HIPAA, FERPA, GLBA, PCI-compliant processes, and SOC compliance as outlined by the [Cloud Security Alliance](#) (CSA). Additionally, all Carbonite personnel (including contractors, and part-time and full-time employees) are required to sign confidentiality agreements. Employees are hired with appropriate training, industry experience and certifications for their roles.

Comprehensive security relies on multiple factors working in harmony – a well-configured network, highly available storage and computing infrastructure and proper configurations that takes advantage of the built-in security features. This paper builds on previous whitepapers that detailed numerous steps to protect the Carbonite Server backup infrastructure environment.

[Security Tips for Protecting your Carbonite Backup Servers](#)

- This paper focuses on measures and techniques to protect the backup environment, as well as the Carbonite Server backup multi-vector approach for securing your data, part of our cyber resilience philosophy.

[Carbonite: Complete Data Protection](#) - This e-book explains how Carbonite Server backup data protection platform ensures both the survivability and availability of data for various strategic purposes, including: information governance, regulatory compliance support, business intelligence, agility and user productivity

Best practices recommended by Carbonite include:

- Not broadcasting your backup server - When deploying a backup server, stealth can be your friend. Adding an Active Directory entry for your backup server is like a 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.

- Implementing network separation - One of the best security strategies involves separating your backup network into security zones. Security zones are groups of servers, systems and networks with 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 like 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.
- Updating OS and Carbonite server versioning – Follow the advice of your OEM software, hardware and application vendors and periodically update your system with the latest security and application patches. Using older versions of software potentially opens up your system to attackers who seek to exploit the vulnerabilities and weaknesses.
- Turning off unnecessary services and ports on your Carbonite Server backup servers - To reduce the attack surface area, software installed and maintained on your Carbonite Server backup servers 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 backup application components. The less you have on the system, the better.

Additional best practices for protecting your Carbonite Server backup environment can be found in the paper "Security Tips for Protecting your Backup Servers."

Addressing the Carbonite Server backup environment's security

After securing a network, physical infrastructure and the OS environment, it's time to address the Carbonite Server backup environment's security.

For starters, Carbonite uses AES 256-bit encryption for all jobs and data, with an encryption key being created for each job. The customer provides an encryption password, which is stored (encrypted) on the agent in the customer's environment.

The encryption password provided by the customer is used to generate the key for the AES 256 encryption. The encryption password is not stored in the UI system or transmitted to Carbonite. This limits access to data. Data is transmitted to Carbonite over a separately encrypted channel.

Carbonite recommends customers always carefully choose strong, random encryption passwords. Also, to prevent and detect malware from accessing the agent, we recommend you install reliable endpoint protection software.

Backups created by Carbonite Server are immutable – once a safeset is created, it cannot be changed or modified. Each safeset is a revision (or point-in-time capture) of the customer's data. Once safeset N is created, it is kept on the vault until it is ready to be expired, based on the customer's defined retention policy. When safeset N+1 is created later, it is simply an incremental backup that builds on top of safeset N. Safeset N remains completely unaltered/unmodified. Even if the source data is infected or has been changed by ransomware, the solution will not replicate or corrupt the existing backups. If the customer is using replication, and the attacker encrypts Director metadata or pool files on the satellite or cloud vault, replication from the satellite vault to the cloud vault or from the cloud vault to the passive vault will fail.

If the customer is backing up directly to the cloud and the production server files are encrypted, and assuming the attacker does not impede the ability for the agent to back up, the agent will back up the ransomware-encrypted files but they will look like a full seed. The key point is that the initial safesets are not impacted by the new Ransomware infected safesets, and the customer can restore from the previous (good) safesets. The recently launched ransomware detection feature in Portal 8.9 will clearly identify ransomware-suspected safesets and provide the user with suggested options to resolve the threat.

Another layer of security is the retention type. Properly specifying a retention type makes it impractical for an attacker to compromise offline/cloud backups by overwriting all good backups with ransomware-encrypted ones. When customers schedule or run a backup job, they must select a retention type for the resulting safeset. A retention type specifies:

- How many copies of a backup are stored online
- The number of days a backup is kept on the vault

Both conditions must be met before Carbonite Server backup removes expired backups. Thus, it is not practical for a bad actor who breached a customer environment to send many ransomware-encrypted backups to overwrite the good backups in the cloud – the attack would have to last longer than the number of days the customer chose to keep the data for all backups to be rendered useless.

As an example –

Assume that the customer chooses to keep 41 copies for 365 days. While the attacker might be able to send more than 41 new safesets in a relatively short period of time, Carbonite Server backup does not remove expired safesets unless they are more than 365 days old. Therefore, the attack will have to last at least 365 days for the attacker to be able to overwrite all good restore points.

The Portal is a key component of the overall solution and here again, each user with access to Portal is required to create a strong, complex password. Password settings are accessible in Profile Settings of the Portal interface. Also available in Profile Settings is the option to enable two-factor authentication (2FA), which will be requested on login to ensure only authenticated users can access the Portal.

When configured, 2FA provides an extra layer of security for logging in to the Carbonite® Sever Backup portal. Users can set up two-factor account authentication anytime by entering a phone number in their profile settings. Users 2FA configured will be prompted to enter a code periodically (every 30 days) when they sign into the portal, when they want to reset their passwords and when they sign into the portal from a new web browser. Users have the option to receive authentication codes via text (SMS) messages or automated voice calls.

Apart from these features, the Portal also supports role-based access controls so information and functionality are only assigned as needed to perform a job. For on-premise customers, the Portal supports six different user types or roles. For SaaS customers, it supports four user types or roles. All of these offer varying capabilities and access that can be customized to fit your respective environment.

Admins have the most access and should be protected with a strong, well-guarded password. Admins are also the only users with permissions to initiate deletion of data in the cloud. So, limiting the number of admin accounts and ensuring all are using 2FA minimizes the risk of a malicious actor tampering with protected data.

Customers are encouraged to judiciously tailor their access roles – only provide the absolute access required to complete the particular task. For SaaS customers, that means making good use of the Execute-only or Read-only access level; On premise customers have those access levels plus also the Support User, who can view reports, logs and status information.

Use Case #1: Configuring access for an admin at a branch office

In this case, admin access might be overkill. Instead, a user-level account is sufficient. Simply assign the respective agents to the user (under the "Agents" tab for the user) by dragging and dropping the agents from the "Available" to the "Assigned" box. Then click "Update" to save your changes. This user account can now create and run backup jobs, or run restores on computers to which they are assigned. A similar process can be followed to assign sites or vaults to a particular user.

Use Case #2: Configuring access for an execute-only user

An execute-only user can run backup jobs, run restores or view logs and status information for their assigned computers. This would be a good role for a Support Desk or in instances where a restoration or backup needs to be completed for specific computers.

Conclusion

Carbonite® Server Backup, in any configuration, provides options and features for securing your data. As new methods of cybercrime like ransomware come to the fore, we will continue to innovate to ensure we meet cybercriminals head on. When it comes to battling data loss, Carbonite will continue to develop and deliver new features to ensure customers have the best tools to safeguard against tomorrow's cyberattacks.

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.