SEPTEMBER 2022

CARBONITE® + WEBROOT®
OpenText Security Solutions

Product Update Bulletin

Carbonite® Server Backup – Recent updates

This month we have introduced new enhancements to Carbonite Server Backup to help make your data even more resilient against loss or compromise. We are excited to introduce potential ransomware detection alerts for VMware vSphere environments, expanded support for two-factor authentication, E3 data protection solution and support for hourly AIX backups. Together, these enhancements help safeguard your business-critical data.

New features in this release

Potential ransomware detection for VMware vSphere environments

Ransomware is the current bane of every business. Our new potential ransomware detection alerts for VMware vSphere environments automatically flag potential threats and provide multi-level alerting tools like dashboard warnings, threat views and automatic email notifications.

If a threat is identified and confirmed, uncompromised data can be quickly restored and recovered. In the Portal, Administrators can choose to clear the ransomware status from a safeset and all its incremental backups or restore from a previously saved safeset.

Our ransomware resilience management also includes the enabling or disabling of ransomware threat detection for a specific backup; seeing the status of an affected safeset and in the restore dialogue and even deleting the safeset from the Portal UI. See it in action here.

Support for hourly AIX backups

To help your business be even more resilient against data loss, our AIX Agent users can now schedule a backup job to run multiple times per day, as often as hourly. To schedule a backup job to run multiple times per day, create an intra-daily schedule using the Portal. Each backup job can have one intra-daily schedule. If the job has other schedules, the intra-daily schedule has the lowest priority. Two retention types are available for intra-daily schedules: 24-Hours (where each backup is kept for at least 24 hours and at least one backup is stored online) and 48 hours (where each backup is kept for at least 48 hours and at least one backup is stored online).

Expanded support for two-factor authentication (2FA)

On-premises Carbonite Server Backup users and MSPs can now use Twilio Verify, a third-party service, to send account verification codes to users and verify codes entered in the Portal. This enhancement gives on-premises customers the flexibility to choose the multi-factor authentication that is best for their business. It also lowers the total cost of ownership for MSPs by reducing their 2FA costs.

E3 data protection solution

Our E3 data protection solution is a combination hardware and cloud service that lets you protect critical data both onsite for rapid recovery and in the cloud for disaster scenarios. We provide and maintain the onsite appliance and we store an entire year of backups in the cloud, giving you a wide range of recovery points. For more information on our E3 data protection solution, review the E3 product bulletin on carbonite.com.

Support and product information resources

Please refer to the release notes for information on current and recent releases. To view the status of Carbonite products, including Carbonite® Server Backup, please visit the Carbonite Support page.

Benefits of Newly Created Functionalities

Reduce the amount of data loss with more frequent AIX backups

Experience more flexibility with additional 2FA options

Act quicker with potential ransomware alerts

Complete hybrid data protection