Security and compliance for Carbonite EVault solutions

Here at Carbonite, we know how important security is for personal privacy and for business confidentiality. That's why we take every necessary precaution to make sure our systems, policies and procedures conform to strict industry-standard regulations. This document outlines the safeguards and procedures we put in place to ensure the security of our customers' data.

Security, privacy and comprehensive protection

Carbonite takes many steps to safeguard the integrity of data and prevent unauthorized access to information maintained on behalf of customers. These protections cover information security and privacy, including governance, infrastructure, physical security, data handling and operations. As part of Carbonite's continuing commitment to risk management, controls such as authentication, monitoring, auditing and encryption are built into the design, implementation and day-to-day practices of our operating environment. These measures are designed to avoid corruption or loss of data, prevent unknown or unauthorized access to systems and information and above all, to comprehensively protect the critical data customers entrust to us.

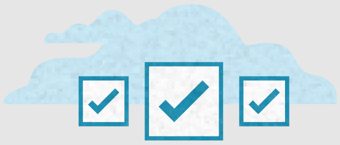
Governance

Audits, external reviews and certifications

Internal and external audits of the control environment are an integral component of assessing the effectiveness of the existing controls. External audits, which are conducted by an outside third party, provide an unbiased, independent opinion of the security in place. Carbonite EVault™ operates control frameworks in line with industry-standard regulations like Service Organization Controls (SOC 2) and Health Insurance Portability and Accountability Act (HIPAA).

Incident response

A security incident can occur in any company, regardless of the size or the technologies used. A properly developed incident response program is important to reduce the impact on the business, its customers and their data. Carbonite has a purpose-built incident response application that is based on asset classification and is operated by highly trained analysts. Carbonite also utilizes advanced host protection and forensic tools, which enable rapid investigations and escalations, when necessary.



Carbonite operates a control framework based on adherence to several industry-standard regulations including:

- SOC 2
- HIPAA
- FERPA
- GLBA

Additionally, Carbonite adheres to PCI-compliant processes for customer payment transactions.

Least privilege and appropriate access

A cornerstone of all security programs is access control that aligns with the industry standard known as least privilege. Following this principle, employees are granted only the access required to perform their duties, utilizing access management and provisioning processes based on defined roles and responsibilities.

Information classification

Carbonite identifies sensitive information wherever it exists as part of its efforts to effectively protect customer and proprietary data. Proper identification and classification of sensitive data assist in the measurement of risk and the subsequent application of efficient security controls.

Vendor management

Vendor system access is limited to only the information that is necessary to fulfill vendor responsibilities. Carbonite performs security assessments of third-party operations prior to engagement to minimize risk.

Employee screening, training and awareness

Many of today's cyber attacks exploit human behavior—whether by clicking an email attachment, going to a harmful website or providing information in a telephone conversation. Carbonite regularly conducts formal security-awareness training that all employees are required to take. In addition, background checks are part of the standard pre-employment screening used during the hiring process.

Policies and procedures

Carbonite maintains policies and procedures, including a written information security program (WISP), that specifies physical, electronic and behavioral security of workspaces and information. Carbonite has a security and compliance committee that reviews Carbonite policies and procedures, making adjustments as the compliance and threat landscape evolves.

Infrastructure

Network architecture

Carbonite's network leverages numerous technologies to maintain its security, including next-generation firewalls, access control lists (ACLs), intrusion prevention, anomaly detection and regular scanning. The network is segmented by asset sensitivity, with only the appropriate access granted via centrally managed network credentials. All remote access to the network requires multifactor authentication. Independent penetration tests and internal vulnerability assessments are conducted on a regular basis.

Wireless access management

Unprotected or insecure wireless access ("Wi-Fi") can act as an entry point for hackers to gain access to a network. Carbonite uses security measures to prevent unauthorized access, including network segmentation, tunneled guest access, strong authentication and encryption. Carbonite monitors its wireless networks for insecure network traffic.

System configuration

Carbonite engineers all its internal and externally facing systems according to strict configuration management protocols, shutting down unnecessary services, installing endpoint protection and enabling operating system-level security settings. Additionally, Carbonite monitors for indicators of attack or compromise at the host level.

Passwords and authentication

Carbonite has implemented robust password controls across its entire network. These controls regulate multiple parameters including: password length, complexity, lock-out thresholds (for repeated incorrect attempts) and reuse history (disallowing the same password).

Business continuity/disaster recovery

Carbonite uses redundant high speed communication links, rigorously engineered systems and storage and access to support personnel to meet its business continuity requirements. In addition, Carbonite's third-party data center partners' business continuity disaster recovery plans are regularly reviewed.

Physical security

Data center controls

Carbonite's data centers restrict access to unauthorized individuals by physical and technological controls. These may include combinations of cameras, human security guards, visitor logs, card reader locks, badge-enabled electronics, biometrics, fences, audible alarms and special location tactics employed at key points throughout Carbonite data centers and operational facilities. Fire detection is implemented through visual and audible alarm systems and industry-accepted systems are utilized for fire suppression. In the event of a commercial failure, multistage autonomous generators provide redundant power to the data center.

Data handling

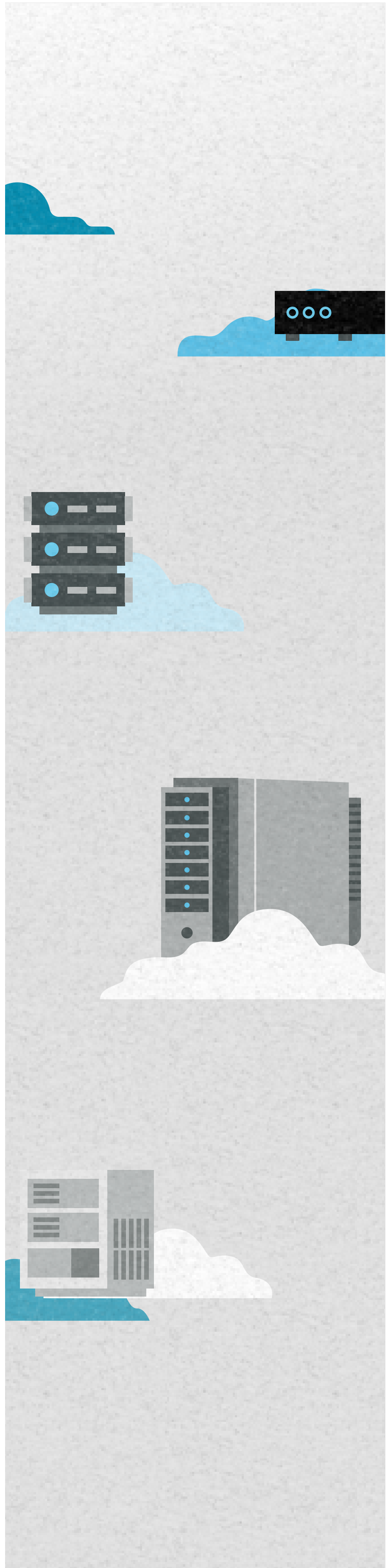
Data encryption

To protect customer data, Carbonite uses TLS, SSL or IPSEC encryption for data transmission and requires AES256 encryption for all new backups since version 8.0. Prior to the release of version 8.0, customers could choose less secure encryption methods, or opt out of encrypting their data. Contact customer care if you have any questions regarding the status of your company's data encryption.

Security and compliance for Carbonite EVault solutions

CARBONITE

Carbonite leverages segregation of duties to ensure only those employees with a need to know have the ability to access customer data for jobs configured as unencrypted. Decryption of customer information cannot be performed without customer authorization. Decryption of jobs configured as encrypted can only be done by the customer.



Operations

Patching

Maintaining a robust security posture on servers and networks is a key aspect of delivering secure services. Keeping these devices at the current operating system version and vendor-recommended patch level is a significant part of ensuring their security. Carbonite regularly updates servers and workstations and applies patches following a thorough testing process.

Access management

Authenticated and authorized Carbonite credentials are required for access to any of Carbonite's networks, servers, operating systems, databases, applications and physical locations. Access is granted strictly on a least privilege basis, and periodic reviews are conducted to ensure adherence to this practice. Upon separation from the company, whether for an employee or a third party's contracted relationship, the applicable account(s) are deactivated and access is revoked.

Logging and monitoring

In addition to protecting our computing environment through preventive controls, Carbonite has also implemented automated log collection and monitoring. By integrating the logged events into a centralized SIEM, Carbonite provides an audit trail for key transactions and actions, delivers forensic information for security investigations and intelligently correlates events from disparate sources to provide holistic awareness of anomalies and suspicious activity.

Change management

Carbonite has documented change management standards that are in line with industry best practices. All production implementations are tested, reviewed and approved by appropriate managers prior to implementation. Separate environments are maintained for internal development, quality assurance and production.

Software development lifecycle

Carbonite practices a well-defined SDLC that includes network segmentation of development, testing, staging and production environments. Promotion of code requires rigorous reviews and approvals. Development personnel do not have access to the staging or production environments, and production releases are tested extensively both prior to and after a deployment.

Security and compliance for Carbonite EVault solutions

About Carbonite

Carbonite provides data protection solutions for businesses and the IT professionals who serve them. Our product suite, including Carbonite EVault and Carbonite DoubleTake™, provides a full complement of backup, disaster recovery and high availability solutions for any size business in locations around the world, all supported by a state-of-the-art global infrastructure.

Contact us to learn more

Phone: 800-683-4667
Email: DataProtectionSales@carbonite.com
www.evault.com