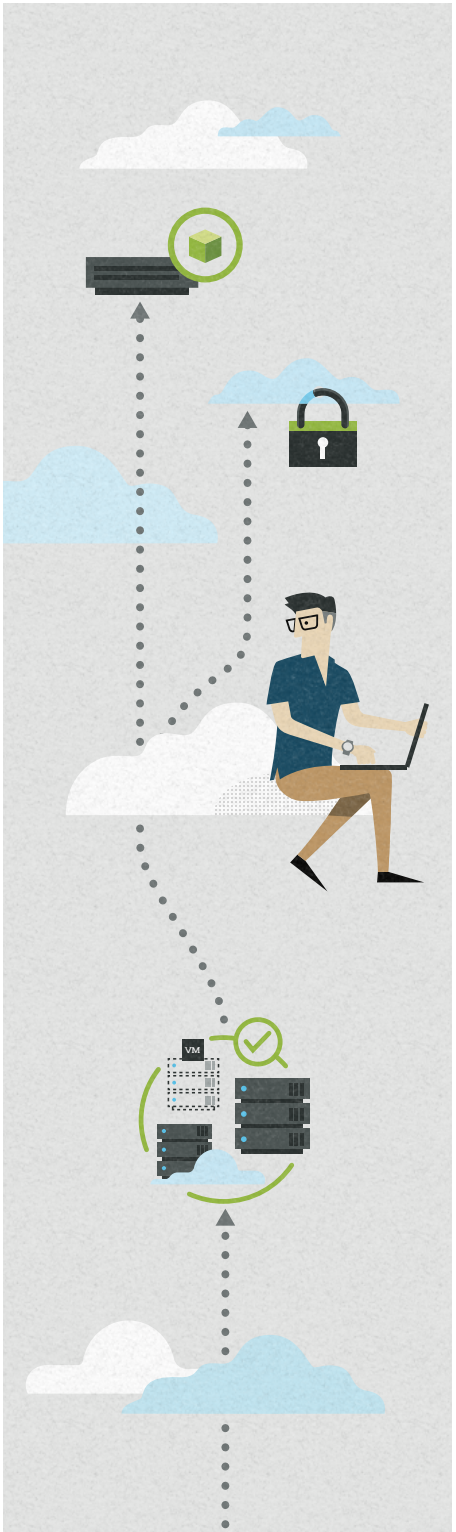
Security, Compliance and Carbonite

How Carbonite ensures data privacy and information security for organizations and consumers

Data security is a concern for both consumers and regulators. As an organization that handles personally identifiable information (PII) in the U.S. and abroad, Carbonite is committed to the protection and privacy of PII wherever it's held.

Carbonite uses advanced technology to protect consumer data from unauthorized access. Our solutions include administrative features that make it easier to handle requests that fall under a regulatory framework. We also employ numerous administrative, physical and technical safeguards to help support compliance with current data handling regulations.



Information security

Carbonite ensures organizational awareness of security and privacy policies through three governance committees.

CARBONITE INFORMATION SECURITY GOVERNANCE

Committee	Purpose	Composition
Compliance Committee	Responsible for maintaining awareness and ensuring compliance of applicable data security and privacy legislation requirements	Includes members of the Security, Privacy and Compliance teams
Security Council	Responsible for the development, documentation, and implementation of security policies and standards	Includes the CISO, General Counsel and other cross-functional executive staff members
Information Security Risk Committee	Oversees the implementation of information security strategy, monitors compliance with information security policies and procedures, and evaluates enterprise-level security risks	Includes the CISO and a subset of the Board of Directors

© 2020 Carbonite, Inc. All rights reserved.

Human resources

Carbonite performs background checks on employees upon hire. Once someone is hired, and on an annual basis thereafter, the company requires employees to complete security awareness training. This includes best practices, relevant data protection regulations and role-specific compliance requirements. Employees are updated regularly on privacy and security matters through corporate communications channels. Additionally, all Carbonite personnel (including contractors, 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.

Industry-standard requirements

Carbonite employs dedicated staff and committees to monitor and improve the company's control frameworks, comply with new regulations and meet the privacy needs of the industry and our customers. The company undergoes annual audits and assessments from third parties to ensure compliance with necessary regulatory and industry controls and best practices.

Carbonite operates formalized control frameworks based on SOC 2, HIPAA, SOX and GDPR. Carbonite also complies with various state security requirements, including Massachusetts' 201 CMR 17.00. Carbonite can provide a SOC 2 Type 2 report to customers upon request and under NDA, to attest to security, confidentiality and availability controls.

Carbonite may be able to assist customers who need to comply with security guidelines and requirements under additional regulations. Please reach out to compliance@carbonite.com for more information.

Business continuity

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 regularly reviews the business continuity and disaster recovery plans for our third-party datacenter partners.

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 on a least-privilege basis and periodic reviews are conducted. Upon separation from the company, employee accounts are deactivated and access is revoked immediately. Remote access is controlled by multi-factor authentication (MFA).

© 2020 Carbonite, Inc. All rights reserved.

Password management

Carbonite implements robust security protocols for access to our network. This includes password controls with strict parameters concerning length, complexity, lock-out thresholds and disallowing previous passwords. Users must change their passwords on a quarterly basis. All system-level passwords, at a minimum, are stored in an enterprise-grade password repository with restricted access. Any user accounts with system-level privileges granted through group memberships must have a unique password.

Network security and incident response

Carbonite implements preventive controls around network security and incident response that align with industry standards. The program is overseen by Carbonite's information security team, led by the CISO. Carbonite leverages automated log collection and monitoring, integrated into a centralized SIEM, which provides an audit trail for key transactions and actions, and forensic information for security investigations. The SIEM provides visibility into anomalous and suspicious events occurring within the enterprise.

Carbonite performs vulnerability scanning at least monthly, where criticality is assessed and escalated appropriately for triage and remediation. We perform enterprise and application penetration testing at least once annually, and application code scanning is integrated with our development pipelines.

Carbonite's incident response team follows a procedure that leverages host protection and forensic tools, which enable rapid investigations and escalations, when necessary. Firewall policies are implemented on a least privilege basis and audited periodically.

Vendor management

Carbonite's vendor management program ensures that vendors are compliant with Carbonite policies, procedures, contractual obligations and applicable laws and regulations. As part of compliance for GDPR, we execute Data Processing Agreements (DPAs) with vendors where personal data may be shared. As part of compliance with HIPAA, Carbonite executes Business Associate Agreements (BAAs) with healthcare providers upon request to ensure rights around Protected Health Information (PHI). Carbonite obtains and reviews the annual SOC 2 report from sub-service organizations to monitor and evaluate the adequacy and effectiveness of their controls. Carbonite additionally performs regular visits and walkthroughs.

Software development lifecycle

Carbonite's defined software development cycle includes network segmentation of development, testing, staging and production environment. Code development goes through rigorous reviews and approvals. Threat modeling, scanning and penetration testing are performed during the product development process. Additionally, development personnel do not have access to staging or production. Production releases are tested extensively both prior to and after deployment. Where issues may be found, they are reviewed and prioritized to be remediated, deferred or declared a false positive.

© 2020 Carbonite, Inc. All rights reserved.

CARBONITE INFORMATION SECURITY GOVERNANCE				
	Infrastructure	**Encryption (at rest)**	**Encryption (in flight)**	**Encryption Keys**
Carbonite Safe Backup	Windows and Linux servers in colocation Data Centers	128-bit Blowfish for Carbonite managed keys	Transport Layer Security (TLS)	Carbonite supports and recommends managing consumer encryption keys, but for some users, private encryption key may be supported.
Carbonite Safe Server Backup	Google Cloud AWS	128-bit Blowfish for Carbonite managed keys	Transport Layer Security (TLS)	By default, Carbonite manages your encryption key for you. Customers can choose to manage their own private encryption key.
Carbonite Server	Windows or Linux servers in colocation Data Centers	AES 256-bit encryption for all new backups since 8.0	Transport Layer Security (TLS)	Customers manage their own encryption keys.
Carbonite Endpoint 360	Azure	AES 256-bit encryption	Transport Layer Security (TLS)	By default, Carbonite manages encryption keys through an enterprise key controller. Customers have the option to manage their own key.
Carbonite Backup for Office 365	Azure	AES 256-bit encryption	Transport Layer Security (TLS)	By default, Carbonite manages unique encryption keys for each customer. Customers have the option to manage their own key.
Carbonite Recover	Windows and Linux servers in colocation Data Centers	AES 256-bit encryption	Transport Layer Security (TLS)	Keys are managed through a third-party key manager. For an additional layer of security, customers can choose to encrypt using VPN or SSH.
Carbonite Availability	Consumer-hosted data	N/A (Customer Hosted Data)		
Carbonite Migrate	Consumer-hosted data	N/A (Customer Hosted Data)		

Contact us

For additional information about our information security practices and procedures – or for information about our portfolio of data protection solutions – please contact us directly.

Phone: 877-542-8637
Email: DataProtectionSales@carbonite.com

© 2020 Carbonite, Inc. All rights reserved.