CARBONITE

Global deduplication

How Carbonite Endpoint reduces storage requirements and network utilization

Data deduplication reduces storage needs by eliminating redundant data and storing only one unique instance of the data.

Data deduplication options

Current data deduplication techniques fall into two broad categories:

- Client-side deduplication occurs at the source (where the data is created and stored).
- Target-side deduplication takes place on the server (after the data has already been transported to its archival storage location).

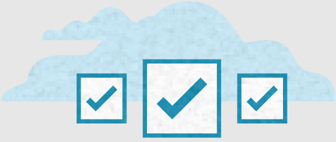
While both forms of deduplication generally provide the same level of storage savings, client-side deduplication provides additional efficiences through reductions in network bandwidth consumption.

Carbonite Endpoint uses a client-side deduplication process that also provides enhanced security for enterprise businesses.

Deduplication of encrypted data

End-to-end security and privacy of data are core pillars of Carbonite Endpoint.

- **Automated key management**: By utilizing our automated key management and encryption technology in conjunction with our unique data deduplication technology, Carbonite has solved the problem of deduplicating encrypted data.
- **No compromises**: Other forms of data deduplication technology require a choice between decryption on the server (which compromises security, privacy, multi-tenancy, etc.) or deduplication that is limited to data from individual data sources (instead of data across the enterprise).



Key benefits

- Increase end user satisfaction and productivity by reducing backup-related WAN traffic by up to 98% during business hours
- Reduce total storage requirements by 50-60% by only storing unique data
- Reduce cost of long-term data storage
- True global deduplication across all users and their data—not per user, per server, or per storage location like other vendors
- Global deduplication over encrypted data provides efficiency and security

How it works

- **Client-side processing**: With Carbonite Endpoint, each block of data is completely processed on the client. So from the server's point of view, each block is an opaque unit. In fact, no data analysis is even possible on the server, which just files the data in the data store. Each file is disassembled into a set of variable length blocks that are then processed on the client. After scoping rules have been applied to a data block, a unique block encryption key is deterministically generated.

- **Block encryption**: This key is then used to encrypt the block using AES 256-bit encryption. The block encryption process ends after each data block has been encrypted. And as a final step, the block encryption key is then itself encrypted and any clear text representation of the key is removed from the system.

- **Data deduplication**: Following data deduplication, each file can be represented by a simple index that associates a list of unique data blocks required with their order of arrangement and identifies the block encryption key required to completely reassemble an instance of the original data.

Contact us to learn more

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