CHOICE ONE

An ISO 9001 & 27001 Certified Company

Tech Brief

ChoiceOne's Data Security Systems and Practices

Defence-in-Depth Architecture Protects Against Wide Range of Threats

Executive Overview

ChoiceOne is fundamentally transforming cloud storage with the industry's most affordable and highest-performing storage solution. You can use ChoiceOne Cloud Storage for a variety of purposes including primary storage for on-premises or cloud-based workloads, secondary storage for backup and recovery, or archival storage for long-term data retention. ChoiceOne is engineered to meet stringent security and compliance requirements and to safeguard the integrity and privacy of customer data.

This tech brief provides a short overview of ChoiceOne Cloud Storage and reviews the strong security systems and best practices ChoiceOne uses to protect customer data against a wide variety of threats.

Data Encryption in Transit and at Rest

ChoiceOne enhances data security for our customers' data by enabling Transport Layer Security (TLS 1.2) cipher for data in transit. All ingress or egress data to and from ChoiceOne's cloud service will be encrypted using TLS 1.2 to prevent third party snooping.

Data at rest in ChoiceOne's storage is encrypted with Advanced Encryption Standard 256bit (AES256) cipher that ensures data is safe and secure. Our IT infrastructure is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1, 2 and 3
- FISMA, DIACAP and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- SO9001 / ISO27001
- ITAR
- FIPS 140-2
- HIPAA

Strong Security Systems and Practices to Safeguard Customer Data

ChoiceOne Cloud Storage is engineered for extreme data durability, integrity, and security. The service is built and managed according to security best practices and standards and is designed to comply with a range of industry and government regulations including HIPAA, HITECH, FINRA, MiFID, CJIS and FERPA.

ChoiceOne takes a “defence-in-depth” approach to security to protect against the widest range of threats. We ensure the physical security of our data centres; employ strong authentication and authorization controls for all cloud compute, storage and networking infrastructure; and encrypt data at rest and in transit to safeguard confidential data.

Physical Security

The ChoiceOne service is hosted in premier Tier IV data centre facilities that are highly secure, fully redundant, and certified for SOC-2 and ISO 27001 compliance. Each site is staffed 24/7/365 with on-site security personnel to protect against unauthorized entry. Security cameras continuously monitor the entire facility—both indoors and outdoors. Biometric readers and two-factor or greater authentication mechanisms secure access to the building. Each facility is unmarked so as not to draw attention from the outside.

Secure Network Architecture

ChoiceOne employs advanced network security elements, including firewalls and other boundary protection devices to monitor and control communications at internal and external network borders. These border security devices segregate customers and regulate the flow of communications between networks to prevent unauthorized access to ChoiceOne infrastructure and services.

Data Privacy and Security

ChoiceOne supports a comprehensive set of data privacy and security capabilities to prevent unauthorized access and disclosure. Strong user authentication features tightly control access to stored data. Access control lists (ACLs) and administratively defined policies selectively grant read/ write and administrative permissions to users, groups of users, and roles.

ChoiceOne encrypts data at rest and data in transit to prevent leakage and ensure privacy. All data stored on ChoiceOne is encrypted by default to protect data at rest. And all communications with ChoiceOne are transmitted using HTTPS to protect data in transit.

Data Durability and Protection

ChoiceOne Cloud Storage is engineered for extreme data durability and integrity. ChoiceOne provides eleven 9s object durability, protecting data against hardware failures and media errors. In addition, ChoiceOne supports an optional data immutability capability that protects data against administrative mishaps or malicious attacks.

An immutable object cannot be deleted or modified by anyone—including ChoiceOne. ChoiceOne data immutability protects against the most common causes of data loss and tampering including accidental file deletions, viruses and ransomware.

Customer Responsibilities

Customers typically interface with ChoiceOne using third-party file management applications and backup tools. Customer IT organizations must ensure the storage management tools and applications they use are configured to take advantage of ChoiceOne security features. For example, HTTPS must be enabled to encrypt data in transit.

Customers must also ensure they have strong security systems and practices in place to safeguard other elements of their on-premises and cloud-based infrastructure. The ChoiceOne storage service is typically employed as part of a larger public or hybrid cloud IT implementation that includes multiple compute, storage and networking components.

Summary

ChoiceOne is a leading cloud backup platform on a mission to ensure that businesses never lose data again. To be the platform of choice for data backup and protection, security is at the core of the product management and development process at ChoiceOne.

ChoiceOne is engineered to meet stringent data security and privacy requirements. The service is built and managed according to security best practices and standards and employs a defence-in-depth approach to protect against a wide array of threats. We ensure the physical security of our data canters, implement strong authentication and access controls to safeguard infrastructure and services, and encrypt data at rest and in transit to protect privacy and prevent unauthorized disclosure.

Take comfort in knowing that your data is always safe and secure. ChoiceOne engages independent/external entities to conduct regular application-level and infrastructure-level vulnerability tests. We also continue to scan and test the ChoiceOne application internally, and on a regular basis, preforming regular security patches or upgrades. Results of the external vulnerability testing and remediation are shared by the entire team including management and the board of directors.