Checklist for Enterprise-Readiness—Why CrashPlan Ranks #1 for Enterprise Endpoint Backup

It's no secret IT organizations have a large number of applications available to them, but how do they determine which are worthy of their implementation? Cloud app analytics and policy company, Netskope, outlined criteria for enterprise-ready applications in its recent Cloud Report™.

Netskope's Cloud Report rankings are based on the Netskope Cloud Confidence Index™, a database of 2,600 cloud apps in which each app is assigned a score of 0-100 based on its enterprise-readiness.

The result? Code42's enterprise endpoint backup solution, CrashPlan, took the #1 spot for cloud backup providers and #3 overall out of 2,600 cloud applications. Read on for a list of Netskope's key criteria that led to CrashPlan's top placement.

CRASHPLAN ENTERPRISE ENDPOINT BACKUP: KEY ENTERPRISE-READINESS CRITERIA

☑ ACCESS PERMISSIONS

Whether the cloud app provides capabilities for multi-factor authentication and/or IP filtering

By their very nature, cloud services are readable from any public Internet connection. Enterprise deployments require the ability to uniquely identify and authenticate users so only those approved may access the services. Client backup with self-service restore further complicates the issue by allowing essential, private corporate data to be restored from anywhere in real time. Code42 offers the ability to run private master authentication servers so IT departments can utilize their existing directory services credentials (AD/LDAP) to approve devices for protection and give permissions to restore data at will.

☑ APP COMPLIANCE CERTIFICATIONS

Whether the cloud app complies with HIPAA, PCI, SP800- 53, GAPP, COBIT, or has Safe Harbor or TRUSTe notifications

CrashPlan enables enterprises to maintain HIPAA and Safe Harbor compliance by autonomously determining which of Code42's global cloud destinations should be utilized by given users. This capability can even be programmatically driven using the customer's directory services (AD/LDAP) information, saving manual administrator intervention.

☑ AUDIT LOGGING

Whether the cloud app makes logs available on administrator, user, and data access activities

All actions, including admin and client activities, as well as automated maintenance, are logged and centrally accessible in the CrashPlan admin console. Administrators can also remotely access and read client-side logs from the same interface.

DATACENTER COMPLIANCE CERTIFICATIONS

Whether the cloud app's datacenter provider is certified as SOC-1, SOC-2, SAS70/SSAE-16 or ISO27001 compliant

Code42 operates its own global data centers, all of which are SAS70/SSAE-16 and/or ISO27001 compliant. These certifications ensure operational requirements are met and regularly audited by a third party.

DATA CLASSIFICATION

Whether the cloud app enables the classification of data (e.g., "confidential" or "sensitive") in order to treat them differently or set policies on them

CrashPlan has extensible capabilities to "include" or "exclude" backup of certain data types or directories on endpoint devices. Administrators can even set up different backup "sets" so that specific data is backed up and protected to different destinations or at different frequencies.

DEVICE RESTRICTIONS

Whether the cloud app enables the restriction of certain device types (e.g., mobile) from accessing the app

CrashPlan administrators can specify device quotas to limit the number of devices or types of devices for each user.

DISASTER RECOVERY AND BUSINESS CONTINUITY

Whether the cloud app offers a published disaster recovery plan and geographically dispersed data centers for redundancy

Code42 customers get a choice of six global data centers. In addition, CrashPlan's multi-destination backup capabilities allow enterprises to choose a hybrid cloud storage solution by seamlessly adding on-premises private cloud destinations with no additional licensing costs.

ENCRYPTION KEY MANAGEMENT

Whether the cloud app enables customer cloud customers to manage their own encryption keys

By utilizing the CrashPlan private master server, enterprises maintain full control (escrow) of their data while still protecting it in the cloud. All data is locally de-duplicated and encrypted client-side where the encrypted data is stored directly in the Code42 cloud. As such, Code42 lacks any mathematical ability to view customer data.

ENCRYPTION OF DATA AT REST

Encryption of data that is not currently active, either in storage or archive

With CrashPlan, all data is encrypted as soon as it's read from disk on endpoint devices. Data remains encrypted in-transit and at rest, meaning it is not decrypted until restored. Maintaining encryption during the complete data life cycle is paramount while protecting and storing vital enterprise data.

ENFORCEMENT OF COMPLEX PASSWORDS

Whether the cloud app allows the administrator to require complex user passwords (e.g., special characters, expiration rules)

Code42 builds its clouds so enterprises can take its technology completely out of the authentication loop. Clients authenticate directly to the onsite private master for AD/LDAP accounts or can use third-party identity providers.

GEOGRAPHICALLY DISPERSED DATA CENTERS AND BACKUP TO A SEPARATE LOCATION

Whether the cloud app is hosted in geographically dispersed datacenters and backs up customer data to a separate location

Code42 offers the ability to treat each global data center discretely. Customers can then use CrashPlan's multi-destination capabilities to provide two completely independent data stores in the cloud.

GRANULAR ROLE-BASED POLICIES

Whether the cloud app provides the ability to set granular policies or permissions based on role

CrashPlan features an extensible role builder where all possible application permissions can be individually chosen as needed. Administrators can then save and programmatically match users to their appropriate role permissions using JavaScript scripting or directory services data.

SEPARATION OF CUSTOMER DATA IN THE CLOUD

Whether the cloud app provider separates each tenant customer's data in the cloud so the data are not comingled

Single tenant cloud storage is available at an additional cost for CrashPlan users. For these customers, Code42 offers a "cloud to managed private cloud appliance" migration in case they prefer to keep data on-premises and behind their own firewall.

CONCLUSION

Data security is top-of-mind for any company choosing a cloud application. Add to that the extra trust involved in critical data backup, and IT is left with a heavy implementation decision. CrashPlan has the sophisticated, enterprise-grade features necessary to satisfy a wide range of security requirements while still providing the ease-of-use requested by IT and end users alike.

Download a free trial to experience why Netskope ranked CrashPlan the highest-scoring enterprise cloud backup application and #3 overall in a total of 2,600 cloud apps.

DOWNLOAD YOUR FREE, 30-DAY CRASHPLAN TRIAL TODAY!
www.crashplanproe.com/download

OR CONTACT CRASHPLAN SALES
www.crashplanproe.com/contact

CODE42 **CORPORATE HEADQUARTERS** 1 MAIN STREET SE #400 / MINNEAPOLIS, MN 55414 / 612.333.4242 / WWW.CRASHPLANPROE.COM/CONTACT / WWW.CODE42.COM