CRASH PLAN PRO™
Continuous Backup for Business

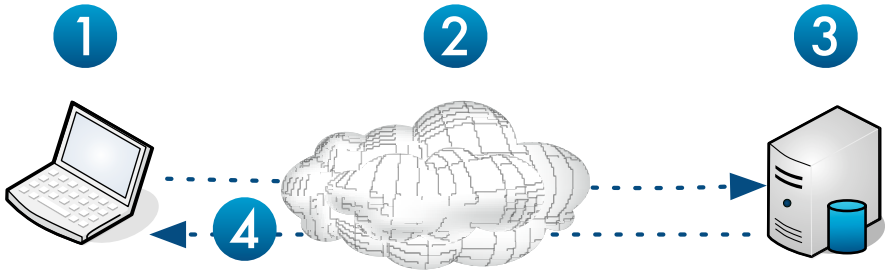
CrashPlan PRO Security Overview

Multi-layered security strikes a balance between security and convenience.

CrashPlan PRO is a continuous, multi-destination backup solution engineered to back up mission critical data whenever and wherever it is created. Because mobile laptops are often connected to unsecured networks, a very high standard of security implementation is required to ensure privacy. CrashPlan PRO's multi-layered approach to security was engineered to meet this high standard and exceeds industry best practices, while balanced against an enterprise's need for convenience and flexibility.

Security Data Flow

To understand the security of CrashPlan PRO it helps to have a high level familiarity with how CrashPlan PRO works:



1. CrashPlan PRO backup begins with the PRO Client recognizing file modifications the user makes in real time. Files are analyzed quietly in the background to identify what is unique about the change. Unique information is broken into blocks, then compressed and encrypted symmetrically using a local private key.
2. The encrypted information flows through unsecured networks to multiple destinations as specified by an administrator. This is secure because the private key is unknown to third parties.
3. Data remains in its encrypted state on disk at the destination. Decryption occurs only when authorized personnel supply the password to restore the data.
4. CrashPlan PRO restore begins when the user or administrator select files to restore. Steps 1 & 2 are conducted in reverse: encrypted blocks are received by the client, decrypted using the local private key, decompressed and written out locally to disk to complete file recovery.

Security Highlights

- Multi-layered security
- Unique cryptographic keys per user, machine and organizational unit
- Secured 128, 256 or 448-bit file encryption
- Secured 128-bit communication encryption with unique session keys
- Flexible key escrow policy
- Open-sourced symmetric cipher (Blowfish)
- Secure globally unique identifiers
- Logged and audit-able restores
- Integrates with existing enterprise identity management systems
- Automated data retention policies and life-cycles
- Tamper-proof backup archives
- Centralized administration and event logging
- Flexible configuration policy management

Account Security

All CrashPlan PRO customers have a CrashPlan account, which uniquely identifies them in the CrashPlan database. Accounts may be created and maintained within the CrashPlan PRO Server (an "internal account" setup) or delegated to a third party identity management system (an "external account" setup) via LDAP. Within an account, users are assigned roles as a means to limit and control account access.

Roles

In CrashPlan PRO, a user account may be authorized with the five roles below, listed from the least to the most permissions:

- **CrashPlan Desktop** (CPD) - Permission to backup to a CrashPlan PRO Server (default).
- **CrashPlan PRO Server** (CPP) - Permission to access the CrashPlan PRO admin console. Access is restricted to the users' computers and their data. (default)
- **Manager** - Read only access to all users in their respective organization and all child organizations
- **Admin** - Read/write access to all users in their respective organization and all child organizations
- **Sysadmin** - Read/write access to all users, all organizations, all children, and all servers

Internal Accounts

Accounts can be created by end users without IT intervention provided the user knows the following information:

- **Registration Key** (aka Organization ID) - A unique and secure GUID (globally unique identifier) containing 16 letters and/or numbers, which is cryptographically secured to prevent a brute force dictionary-style attack to join the environment.
- **CrashPlan PRO Server hostname** - the resolvable hostname to the IP address of the CrashPlan PRO Server

Accounts created via this method are limited to CrashPlan Desktop User (CPD) and CrashPlan Web User (CPP) roles. These roles have no administrative or managerial permissions.

External Accounts

Identity management within an enterprise can greatly enhance security. CrashPlan PRO supports this approach by communicating through a proxy to your identity management system for user information and access. User account states can be updated in real time (pushed) or delayed (pulled), depending on the identity management system used. With this model CrashPlan PRO does not store user login information in its server. This model offers the highest level of user account security.

Account Lifecycle

Accounts can move from one state to another. Account states include:

- **Active** - Account may interact with their data and computer(s)
- **Inactive** - Account is no longer considered in use, but users may reactivate themselves
- **Blocked** - Account is considered inactive and blocked from all activity. Users may not reactivate themselves

From a security point of view, these states can be transitioned and subsequently trigger predefined data retention polices. For example, if an employee's status becomes inactive, CrashPlan PRO no longer accepts backups from this user, until the user is reactivated. The data is escrowed for 30 days, after which it is deleted or securely destroyed.

Password Security

There are two types of passwords in CrashPlan PRO:

- **Account Password** - validates the identity of a user with a minimum of a 6 character password
- **Private Password** - an optional password used to encrypt the backup data key
- **Private Key** - an optional password generated on demand by the user (PRO Client only)

Account Password

The account password is never stored or transmitted to the CrashPlan PRO Server in plain text. On the client, the account password is cryptographically salted with a 64-bit secure random number and repeatedly hashed using SHA-1. Repeatedly hashing the password greatly exceeds the RSA PKCS5 standard, creating a virtually unbreakable password from whatever easily identifiable word the user might have entered. It is this salted and strengthened password that is transmitted and stored in the CrashPlan PRO Server and then later used for verification when authenticating access to a user's account.

An account password is used only to authenticate the user during installation or remote access to files via the web interface. It is not used to encrypt backup data and may be changed or reset at any time without affecting existing backup data.

Because the salt process and repeated secure hashing, the account password cannot be reverse engineered using pre-computation or "rainbow table" attacks.

Private Password

In this model, backup data is encrypted with a 448-bit data key. This key can be escrowed in the CrashPlan PRO Server allowing administrators to easily restore and decrypt data on behalf of a user. However, if additional security is required, the user may elect to symmetrically encrypt the data key with a private password. The resulting encrypted data key can then be escrowed in the PRO Server while the private password is not. This provides the convenience and security of key escrowing while preventing administrators from restoring protected data. If the private password is lost, the backup can never be restored by anyone. Because forgetting the correct password can render the backup data inaccessible, CrashPlan PRO provides the administrator the option to disable this feature for individual users or for the entire enterprise.

Encryption Key Security

Keys must be present on a system before the first backup occurs. Typically, keys are created at the time of installation either using the built-in algorithm in the CrashPlan Client or it is a custom key provided by the IT department.

Key Creation

Keys are created using a secure random number generated from Sun Microsystem's Java Cryptography Extensions framework. This framework is an audited open source implementation proven to exceed industry standard practices.

Key Storage within CrashPlan PRO Client

The key used to backup data is stored locally on the computer itself in an unsecured location. This is acceptable as the data itself is not secured. If one has access to the key, presumably one has access to the data as well. An exception to this rule is if you are using Mac OS X File Vault or Windows Full Disk Encryption. In this case, the key is stored in the users home directory and leverages the existing disk-based encryption.

Escrowing Keys in the CrashPlan PRO Server

Keys are typically escrowed at the CrashPlan PRO Server and optionally in each backup archive (securely encrypted, of course) at the destination. Keys remain in these locations until changed or requested for a restore. Keys may be securely or insecurely escrowed depending on an organization's needs. This policy setting can be applied to an individual computer, user, a group of users or enterprise-wide.

Unsecured Key Escrowing - For installations that require IT to have access to user data (i.e., the ability to restore files for users), select an unsecured key escrow policy. This policy is typically used when PRO Server is running within your own IT infrastructure. This is the most convenient method while remaining reasonably secure.

Secured Key Escrowing - When running PRO Server in an untrusted environment (e.g., third party data center) it makes sense to utilize a secured key escrow policy (or no escrow policy at all). With secured key escrow, keys are encrypted using a private data key prior to transmission and stored on the CrashPlan PRO Server. This policy strikes a fair balance between ease of use and security.

No Key Escrow -To insure 100% security in untrusted hostile storage environments that are not under direct IT control, you may elect to not have the key escrowed at all. This requires you to manually manage your own keys but provides 100% assurance that there is no way a third party can retrieve your data. This is the most secure and least convenient policy.

Striking a Balance Between Security and Convenience

The best approach to security strikes a balance between flexibility, convenience and enterprise policies. CrashPlan PRO's multi-layer security offers the ability to strike the balance you need while protecting you three ways:

- Encryption security protects your data
- Password security prevents unauthorized restores
- Account security controls user access