How does Comet Backup protect your data against ransomware?

Every company has—or should have—a security suite to safeguard their data. However, with millions of dollars lost to security breaches annually, cyber criminals are constantly releasing new forms of ransomware that threaten our data, and the constant rate of change can be hard to keep up with.

Backing up data is your last level of defense against ransomware, to ensure business continuity in the event of a security breach.

Comet Backup Strengthens Your Backup Strategy With Three Layers Of Protection Against Ransomware

Policy settings to restrict end user permissions

#1

Comet's Policy settings allow administrators to restrict what actions can be taken from the client end. This will minimize the risk of data loss if the end point's security is breached and becomes compromised by ransomware. Additionally, this limits the risk of data loss due to human error.

Specifically, the following permissions can be restricted:

- Add, edit, or remove backup types
- Add, edit, or remove storage vaults
- Access or view the client interface
- Change password or email settings

For end users who need complete control over their environment, there is the option to turn off the setting, 'Allow administrator to reset password', which gives the end user full control and password management.

#2

Encryption during data transit and rest

Comet always encrypts all user data before storing it, as well as during transit and at rest, using strong AES-256-CTR with Poly1305 in AEAD mode with high-entropy randomized keys.

Even in a scenario where the storage destination is compromised, the data remains unreadable.

Encryption keys are automatically generated and managed by the client software. The data encryption keys are then encrypted against the customer's password, and stored on the Comet Server.

This means that (A) the service provider is unable to decrypt data without the customer's password; and (B) in the event of a disaster or data loss, only the customer's password is necessary to log in to the account and restore and recover data.

Object lock support for data immutability

#3

Some of the ways that bad actors operate is by threatening to delete data, or to encrypt data which would render it unusable, unless a ransom is paid. This can be countered by making data immutable.

Immutability is a state where data cannot be altered or deleted. Even if malware gains access to the storage credentials used by Comet, malware is unable to delete or tamper with any of the backed-up data.

Comet supports features to make data immutable, such as S3 Compliance mode object locking and Backblaze B2 Hide Files. This offers another layer of protection, even if ransomware were to penetrate the other security measures you have in place.

Ready to make a plan to protect your business?