



Security Whitepaper

“digitalbucket.net has streamlined our processes, simplified internal document transfer and collaboration, and made it extremely simple to push out files to our customers. I'm recommending db.net to my business colleagues as they share similar file and document management issues. We're very pleased, and wanted to let you know.”

Lindsay Garrison
President & CPS (Chief Problem Solver)
On the verge, incorporated

Security and availability are two important factors that set our service apart from any other online storage and collaboration provider. We take security very seriously and rest assured that your data is safe and secure. Below is an overview of how digitalbucket.net utilizes security in different levels.

Security Overview

Digitalbucket.net utilizes some of the most advanced technology for Internet security available today. Secure Socket Layer (SSL) technology protects your information using both server authentication and data encryption, ensuring that your data is safe, secure, and available only to registered Users in your organization.

Data Access Control

Uploaded files to your account are only accessible by you. You have a choice of sharing your data privately or publicly.

- **Private Sharing:** Any digitalbucket.net user can Share a folder with other registered users privately. Depending on the given permission for your Shared folders, users can upload, delete and rename files or just to view, download.
- **Public Sharing:** Any digitalbucket.net user can Publish files or folders and make it available publicly. Generated links allows non-register users to access the files and folders. Published files and folders can be protected by passwords and expiration date

User Access Security

Digitalbucket.net provides each User in your organization with a unique user name and password that must be entered each time a User logs on.

- **Authentication** – Authentication of user's credentials ensures user's privileges on every operation. Unauthorized operation will cause appropriate errors.

- **Validation** – User actions will be validated on different stages of the application to prevent unauthorized operation.
- **Activity tracking** –Users can get complete log of their usage activity. Business and Enterprise Users are able to track activity of the sub-accounts.

Data and Server Security

Amazon Web Services is utilized to bring you the most secure, efficient and scalable Storage and Cloud Computing platform possible.

- **Server in the cloud** –Amazon EC2 (Elastic Compute Cloud) is utilized to provide our users a powerful compute capacity in the cloud. Security within Amazon EC2 is provided on multiple levels: The operating system (OS) of the host system, the virtual instance operating system or guest OS, a stateful firewall and signed API calls.
- **Secure data storage** – User’s data are encrypted and stored in Amazon S3 (Simple Storage Service). Data stored in Amazon S3 is redundantly stored in multiple physical locations across the US. All requests to access data goes through our servers and no direct access to the data stored in Amazon S3 is possible.
- **Application monitoring** – We are monitoring our Application 24x7 to ensure security, integrity and availability. This will help us to provide the best uptime possible to our customers.

Network Security

Digitalbucket.net utilizes some of the most advanced technology for Internet security available today.

- **SSL** – digitalbucket.net provides 256-bit SSL (Secured Socket Layer) security to encrypt all the data transfers between the end user and digitalbucket.net. This feature is available only for paid users.
- **Secure Published links** – Links to your published files/folders are encrypted and won’t be discovered by search engines.