Box Security Overview

Information That Should Help You Sleep at Night

More than 100,000 businesses use Box for sharing and accessing their data, and we work continuously to earn their trust. Box invests heavily in the security and resiliency of our data center, software, and our entire business operation.

We recognize that security has to be integrated in every phase of product development and daily operations. This paper describes some of the many measures and practices that we implement on a daily basis to ensure the security of your business data.

It starts by taking an end-to-end look at the path of a file from your desktop to Box storage. We also look at the policies and practices implemented both in our headquarters and our data centers that help us achieve SSAE 16 Type II compliance throughout the stack. Finally, we briefly describe the availability and resiliency measures that allow us to offer a 99.9% uptime guarantee.

> *“ Box’s security controls and the ability to turn on and off folder access are key for us. ”*
>
> **Brian Davis**
> President,
> Net Generation

Box Sales
Call 877-729-4269
www.box.com

End-to-End Security: Follow the Data

One of the best ways to understand the multiple levels of security in Box is to follow the path of a file from your desktop to the Box cloud and beyond, to collaboration and storage in the cloud. So, let’s take a look at what happens when you upload a file to Box.

Account Access and Authentication

Before any file upload occurs, you have to log in to your Box account. We do everything we can to help businesses implement and enforce the policies they need to protect access to their applications.

Strong and Configurable Password Policies

Businesses can configure the password policies for their users, including:

- Password strength factors (minimum number of characters, required numbers of numbers, special characters or uppercase characters, restriction from using email addresses)
- Password resets (a configurable time period)
- Password re-use restriction
- Notification after a configurable number of failed attempts
- Prevention of persistent logins
- Overall maximum session duration

“ *Box provides valuable administrative features, which let us easily set granular permission controls across all our content and all our users.* ”

Christopher High
Sales & Marketing
Development,
Alere

Box Sales
Call 877-729-4269
www.box.com

Single Sign-on

Box offers Active Directory/LDAP integration for Enterprise accounts. This gives businesses centralized control over user accounts in Box. When a business removes an individual’s Active Directory account, for example, that person can no longer login to his Box account.

Box supports the SAML (Secure Assertion Markup Language) 2.0 protocol, which enables easy integration with multiple identity and cloud SSO providers. SAML is a federation protocol that lets organizations securely exchange authentication and authorization information in a trust relationship. Box also supports ADFS 2 (Active Directory Federation Services).

Box works with several providers of cloud SSO to offer secure single sign-on to the Box cloud. These providers include Ping Identity (PingFederate), Citrix (NetScaler Cloud Gateway), VMware (VMware Horizon App Manager), Okta, OneLogin and Symplified.

Box supports multi-factor authentication through these cloud SSO providers or other third-party MFA services. For more information on strong authentication options, contact support@box.com.

Mobile Access

Mobile users can access their Box accounts through mobile browsers or specific Box applications for various mobile devices (iPhones, iPads, Android phones and others). Using Box, you can extend corporate SSO and security policies out to mobile devices; users can login to Box from a mobile device using corporate single sign-on credentials.

All data passed between the server and the mobile application is encrypted using SSL. If a mobile device is stolen or lost, the administrative console can cut off access in real time.

Upload/Transit

Once you have securely logged in, you can upload your file. While upload itself is simple from the user’s perspective, behind the scenes Box is working to optimize the performance and security of data in transit.

For Business and Enterprise accounts, the data is encrypted with 256-bit SSL encryption on file transfer.

For Enterprise accounts, we use multiple Content Delivery Networks (CDNs) such as Akamai and EdgeCast to speed the process of file uploads from dispersed locations.

The upload opens an encrypted SSL tunnel to the local point of presence for the CDN. The CDN likewise sends the data encrypted to the Box data center. This strategy takes advantage of the high bandwidth and TCP optimization offered by the CDNs to provide a better upload performance.

The same general path is reversed on downloads.

Within the Application: File Permissions and Audit

Once the file has reached the Box service and ready for sharing, collaboration or storage, it is subject to the authorization and audit security within the application itself.

Flexible Permissions

Once uploaded to the Box cloud, the file inherits the permissions of the folder or the account that contains it. You can set very detailed access/sharing permissions on the file.

- *Private/public*: By default, files uploaded to Box are private to the file owner. You must explicitly decide to share files. Files that have been shared can be made private at any time.
- *Password protection*: You can choose to add a password requirement to a file you are sharing, so that users need a password to access the file.
- *Notification*: You can configure Box to notify you by email when someone views, downloads, comments on, edits or uploads files or folders. Notifications can occur on each event or in daily summary form, depending on your preference.
- *Links*: One way to share files is to send people a link to the file in Box; the links are unique, randomly-generate IDs. You decide whether recipients can download or simply preview the file.
- *Time-based access controls*: You can set expiration dates for file access.
- *Collaboration*: Create collaboration folders to collaborate with others, and invite collaborators using detailed roles-based permissions (for Business and Enterprise accounts). For example, you can restrict partners to a Previewer role, so they can see but not download files, or an Uploader role, to securely drop files without seeing what else is there.

Global Settings

At a global level, administrators can set certain restrictions across all users in a Business or Enterprise account, including:

- Who can create folders or upload files
- Whether users can share links to content
- Whether link recipients can download content
- Who can invite collaborators
- When links expire
- When collaboration expires

Audit Trail

Box automatically logs all file and user activities on the application and maintains a complete audit trail of all activity within the account. The audit log provides administrator insight into what is being done in the system, facilitates discovery, and demonstrates compliance with relevant industry regulations.

Audit logs are date/time stamped, and tracked by user name, email address, IP address, and action taken. You can sort by these attributes or drill down to particular groups, ranges of dates, files or users. You can also export the audit log as a CSV-formatted file.

> *“ We thought an online file server was the way to safely share information with investors and throughout the company. ”*
>
> Melissa Gannon
> Head of Corporate Operations,
> MCR Development LLC

Box Sales
Call 877-729-4269
www.box.com

A comprehensive set of reports lets you report on data along these dimensions. Predefined security reports provide valuable insight into the potential misuse or abuse of data. You can also configure Box to alert you to failed login attempts, requests for forgotten passwords, or password changes.

Box retains audit logs for one year.

In Storage

Once uploaded, the file itself is stored within the Box storage cloud.

Encryption

For Enterprise accounts, data is encrypted in storage using 256-bit AES encryption. The encryption key itself is encrypted with a Key Encryption Key (KEK). The key encryption key is stored securely, separately from the data, and rotated frequently according to best practices for key management. All access to the keys is logged and audited.

Because data is encrypted in storage, even if someone were to access the file in storage, they could not see the data in the clear.

As mentioned in the data transit section, data is also encrypted in transit using SSL/ HTTPS (Business and Enterprise accounts).

Backup/Replication/Disaster Recovery

Not only is Box storage resilient to device failure, but the company also sends encrypted data to secure offsite storage for redundant backup, which essentially replicates the file to a different location to protect it from site-wide disasters

Remember that the off-site storage retains the encrypted data, without the encryption keys necessary to decrypt the data.

Data Retention

You've shared your file and completed the project. What happens once you delete the file?

The file, once deleted, goes to the Trash. You can configure exactly how long things stay in the trash, ranging from 7 days to forever. If you decide you still want that file, you can retrieve it from the trash during this time period.

Once a file has been deleted from the trash, Box retains the ability to retrieve deleted data from the backup for a limited time period. Contact support@box.com if you need to reclaim files already deleted from the trash.

> *" In today's enterprise, there's definitely a need for both an internal and an external sharing solution. Sharepoint helped us internally, but from an external communication and collaboration standpoint we needed Box to allow us to manage files with greater flexibility, particularly with users that might not be part of our enterprise. "*
>
> Sean Andersen
> Director of Interactive Services,
> Six Flags

Box Sales
Call 877-729-4269
www.box.com

SSAE 16 Type II Throughout the Stack

When most cloud companies talk about SSAE 16 compliance, they're talking about the data centers that they hire to host their services. Obviously, it is critical that these data centers meet high standards for security and availability.

At Box, we maintain SSAE 16 Type II compliance and audits for our corporate operations as well, beyond the hosted data centers. So, we're SSAE 16 throughout the stack – something that few other cloud-based service companies can boast.

Data Center Security and Availability

Box uses multiple data centers to host its application and data, providing essential redundancy.

Box data centers are SSAE 16 Type II compliant and use advanced measures for redundancy, availability, physical security and continuity. Here are some of the highlights of their security and availability measures.

- *Availability*: Data centers have n+1 (or greater) redundancy for all critical components, including cooling systems, power, connectivity, and other essential systems. (N+1 means that there is at least one spare for any single point of failure.)
- *Physical security*: All equipment is secured within locked cages or vaults, secured with separate keys or biometric scanning. Access to the facility is protected by 24-hour onsite monitoring and guards, biometric authentication, CCTV with video archives, access control lists, and access and surveillance audit logs.
- *Environmental controls and continuity*: Data centers include full Uninterruptible Power Supply systems, backup systems, and uptime guarantees. Data center facilities have advanced fire suppression and flood control measures.

All facilities are regularly audited for SSAE 16 Type II compliance.

Inside Box: Our Policies and Practices

Security begins right in our offices, with our facilities, procedures and policies. Every employee is trained on our security policies and procedures.

We have a complete SSAE 16 audit report, but just to give you the highlights, we maintain and audit policies for:

- Employee background checks
- Corporate facility access
- Acceptable use
- Removable media
- Corporate passwords and production passwords
- Access privileges

> *" Box has certainly saved us money, but more importantly it's saved us time and energy. I take one or two fewer aspirin each month. "*
>
> **Bill Bocash**
> IT Manager,
> Stonewall Kitchen

Box Sales
Call 877-729-4269
www.box.com

- Incident response procedures
- Security training
- Patch management
- Standards for hardened systems
- System configuration
- Change management

Box also works to maintain the security of its corporate networks and files, with:

- Network intrusion detection systems and host intrusion detection
- System, network, and application log reporting, analysis, archiving and retention
- Network device baseline standards
- Continuous internal monitoring
- Regular vulnerability scanning
- Remote network access through VPNs with multi-factor authentication

In addition, Box regularly engages third-party network security testing to find potential vulnerabilities.

An Incident Response Team handles any significant security or service events according to defined policies.

Data Breach Practices

In general, the Box Incident Response Team handles any security incidents.

- If, despite all other protections in place, your data is accessed without authorization, we will notify you.

- If personal information about you or your employees is breached from the Box files, Box will notify you in accordance with California Law (California Civil Code Section 1798.29 and Section 1798.82).

Software Development Processes

Ultimately, a commitment to security has to start with the software development process itself. At Box, security is part of the design from day one.

- QA is integrated into the development process. Changes in various stages of development are tested on a daily basis.
- Our automated test framework includes both positive and negative testing, with end-to-end testing from authentication onward.
- We use network security testing and third-party penetration testing to verify the resilience of the system.

> *" What's great about Box is that it keeps great records of everything going on, I can control who has access to what... I have complete transparency of every file on our system...I don't have to worry about having a redundant server up, I don't have to worry about backups, I don't have to worry about someone going in and kicking the cable out on the machine. All of that is taken care of for me, and that's a big load off my mind. "*
>
> **James Bambauer**
> Director of IT,
> Eveo

Box Administrators and Your Data

Box Customer Support or Engineering may occasionally need access to some of your data to provide support and address technical issues. Here, too, we have policies in place to limit that access to the least access necessary to provide superior support (a “least privilege” strategy).

Box carefully enforces role-based segregation of access. For example, access to customer data is limited to specific support roles and levels, and includes limited views, such as:

- Ability to see the file tree, but not file names
- Ability to edit and view user account information (contact info, account status), but not files

Exceptions to role-based access policies may be granted on a case-by-case basis, and all customer data access is always logged.

Availability and Resiliency

We’ve built end-to-end n+1 or better redundancy into the Box service. This means we have at least one extra of everything, ready to take over automatically in case of a failure.

While this paper will not outline the entire system architecture, here are some of the highlights.

Data Center Redundancy

Box is replicated across separate data centers, providing redundancy atop the n+1 (or better) resiliency offered by each data center individually.

This redundant architecture gives us a concurrently maintainable infrastructure - we can fix things without ever interrupting service.

Across the data centers, we use four distinct Internet providers, ensuring that our service remains online even if an Internet connection fails.

Application Architecture Redundancy

Within each data center, Box maintains n+1 or better redundancy, with:

- Redundant load balancers, routers and switches in failover configurations
- Segmented clusters of application servers handling different functions
- Master/slave database clusters, replicated in real-time across data centers
- Multiple log databases replicated in real-time across data centers
- Resilient storage technologies in multiple storage clouds
- Backups (encrypted) in offsite storage files

In addition, all layers of the application stack are isolated in distinct network segments, with strict Access Control Lists maintained through each, to isolate potential risk.

As previously mentioned, encrypted data is also stored in redundant, offsite backups to provide a further layer of protection in the case of failure.

> *“ It’s been amazing the amount of time and effort that Box has saved us versus the status quo of how we were used to doing things. ”*
>
> **Josh Stein**
> Managing Director,
> Draper Fisher Jurvetson

Box Sales
Call 877-729-4269
www.box.com

Summary

Today’s computing environment is complex, requiring many different layers of security. At Box, we make the security of your data our number one priority. Box is committed to offering you an absolutely safe way to manage, share and access your information. This paper just touches the surface of many of the measures. If you need more detail on a specific area, please contact Box and we’ll be happy to answer your questions.

> *“ I don’t know what we would do if we didn’t have Box. It would just be a disaster. ”*
>
> **Jordan LaRusso**
> Marketing Coordinator,
> Crocs Footwear

Box Sales
Call 877-729-4269
www.box.com