Bluebeam Studio
Security & Disaster Recovery

2017

Table of Contents

Introduction

From time to time, we receive questions from Bluebeam Studio™ users about the safety of the files they're uploading to Bluebeam Studio. These concerns usually revolve around the overall level of document and system security, access control, and questions about the consequences of an infrastructure failure.

To help clarify these important points, we'll provide an overview of these areas in the following sections.

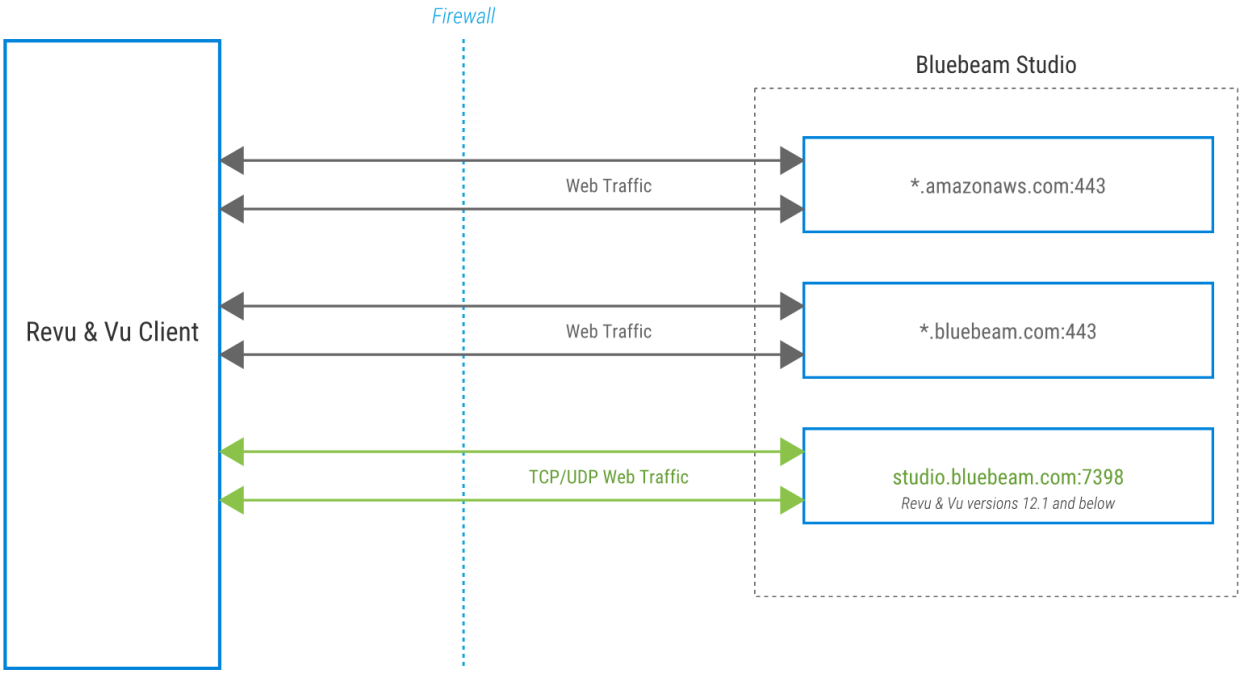
Note: *Information about Studio Prime and Studio Enterprise can be found on the Bluebeam Support site.*

Accessing Bluebeam Studio

All end-users interact with Studio through the Revu application. In order to participate in Studio Sessions and Projects, users must enter a username and encrypted password.

Note: *Bluebeam® Vu® users may also access Studio, but they must be invited to a Studio Session or Project by a Revu® user first. Any information in this document pertaining to Revu (including version numbers) will also apply to Vu, assuming this prerequisite is met. For this reason, Revu and Vu may be used interchangeably throughout this document.*

Studio server connections are initiated by Revu clients, but the system does not send inbound connection requests back to the client. Primary communication and transmission of files, markups and other rich data uses the HTTPS protocol, while encryption and authentication uses the Transport Layer Security (TLS) protocol.



Firewall Requirements

Revu 12.5 and later need access to the following domains in order to communicate with the Studio Server:

*.amazonaws.com:443

*.bluebeam.com:443

Note: *Revu 12.1 and below also communicate with Studio via TCP/UDP protocols. studio.bluebeam.com:7398 should be open for these clients.*

Studio-Related Email Domains

We use the following domains to communicate with end-users for support, licensing and Studio-related information. Please make sure they are white-listed to ensure successful email transmission:

@bluebeam.com

@bluebeamops.com

@bluebeam-support.com

Note: *These emails are sent on our behalf by amazonses.com. If these emails are not being received by your users, please ask your Email Server Administrators to check the Sender Policy Framework (SPF) record, and make sure that amazonses.com is also whitelisted as a trusted domain.*

End-User Authentication & Access Control

The following protocols have been implemented for secure end-user authentication and access control:

Certificate Requirements

Access to the Studio server (studio.bluebeam.com) is handled by a certified SSL issued by the Root Certificate Authority, DigiCert®.

The certificate may be viewed by going to https://studio.bluebeam.com and clicking the padlock icon, located near the beginning of the URL in the address bar.

Password Requirements & Encryption

All passwords *must* be between 8 and 32 characters, with at least one uppercase letter, one lowercase letter, one number and one special character, such as !@#$%^&*.

Password encryption is achieved using a one-way salted hash algorithm.

Along with this, an 'exponential back-off' algorithm locks accounts for progressively longer periods of time with each failed login attempt using an incorrect password. Login failures are logged, and our Operations Team is alerted if the quantity rises above a preset level.

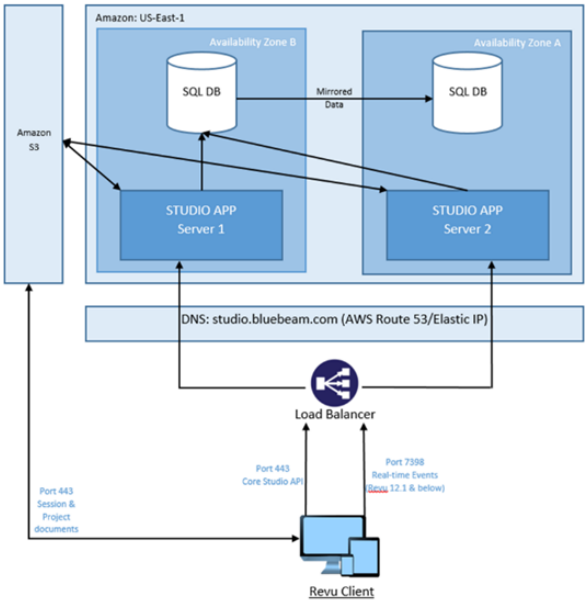
Note: *The system does not store any Personally Identifiable Information. Only user login credentials and company contact information.*

Data and System Security

The measures described below have been implemented to address data and system security concerns.

Infrastructure and Data Storage

Although Bluebeam Studio is accessible from anywhere in the world, the system is hosted in the US, in two zones, on Amazon Elastic Compute Cloud (EC2) managed by Amazon Web Services (AWS).



The Studio infrastructure is comprised of application servers which serve Revu clients on Windows®, Mac OS®, and iOS, as well as a backend processing system and a data tier.

User data, Project and Session metadata, and Session markups are stored on SQL servers, and actual Project and Session documents reside on Amazon Simple Storage Service (Amazon S3) servers.

SLA's for Amazon EC2 and Amazon S3 can be found in following locations:

- https://aws.amazon.com/ec2/sla/
- https://aws.amazon.com/s3/sla/

Data Protection

In addition to the encryption of all SQL server backups and developer hard drives, all documents are automatically encrypted when uploaded to a Studio Session or Project using Revu 2015 and above, as described below.

Encryption

Encryption is done by AWS using a combination of an Amazon Resource Name (ARN) and an AWS Key Management Service (KMS) key ID.

All data is encrypted at-rest (AES-256 encryption) and in-transit. Data transfer is encrypted in transit via SSL/TLS between the Revu client and Amazon S3. In the server environment, files are encrypted in Amazon's S3 service. SQL database backups are stored on encrypted volumes.

Note: *Files uploaded using earlier versions of Bluebeam Revu are not encrypted.*

System Security

We've ensured that all server instances perform in the same manner and are subjected to the same network policies and restrictions by building them with a validated and tested "template." Once they've been deployed, the following steps and policies are in place in order to provide additional security while maintaining consistency across the infrastructure:

Controlled Administrator Access

Only a select group of engineers and developers have administrative rights within the Bluebeam Studio infrastructure, and system access is controlled via Multi-Factor Authorization (MFA).

Change Control & Auditing

All system changes and enhancements are documented, and must be approved before they can be tested and eventually implemented in the production environment.

Audit logging is handled by AWS CloudTrail, Tripwire, and SumoLogic for the system, its configuration, and all server changes.

Logs are retained for the following timeframes: CloudTrail – 2-weeks; Tripwire – perpetual; SumoLogic – 30-days. Only DevOps engineers have access to these logs and developers when required to troubleshoot issues.

Vulnerability Assessment and Remediation

We've implemented a comprehensive vulnerability assessment and remediation process to address any security issues that may arise. These measures include antivirus protection on all servers, proactive system patching policy, and file integrity monitoring (which detects unauthorized changes to the systems).

The system undergoes monthly security scans using Rapid7's AppSpider dynamic web application security testing tool. Results of scans are also reviewed by a 3rd-party Security Engineer, and any issues not OWASP compliant are immediately addressed.

Inventory of Authorized Devices

Regular system audits are performed, which ensures that unauthorized devices are never connected to the infrastructure.

Infrastructure & System Monitoring

To ensure a steady state of operations, a comprehensive monitoring and alert system is in place for the following:

- Server infrastructure: CPU, memory, disk space, and uptime.
- Applications: errors, performance degradation, and uptime.
- Network Performance: usage and bandwidth, server response time, throughput, and web requests.

System Maintenance

Regular quarterly patches and emergency patches are in accordance with our established Change Control process.

Disaster Recovery (DR)

In case of emergency, Bluebeam Studio includes proactive infrastructure monitoring, which provides information and alerts on system availability as well as performance and error conditions. Additionally, the Bluebeam Studio team regularly tests their disaster recovery procedures.

To handle the unfortunate event of an infrastructure failure, we've also put the following contingencies in place:

Backup Protocol

Full backups of the SQL Databases and Files Stores are performed on a daily basis. The backup files are stored away from production servers, and their integrity is checked periodically.

Scheduling

SQL Database Backups

- Hourly: incremental backups are taken every hour.
- Daily: full backups are taken once a day.
- Weekly: full backups are taken once every weekend.

Full daily backups are stored for up to 60 days in Amazon snapshots.

The latest daily and weekly backup files are also stored in an isolated Amazon S3 bucket.

PDF File Backups

PDF file changes uploaded to Amazon S3 servers are copied to an isolated S3 bucket every night. These backup files are stored away from production servers, and their integrity is checked periodically.

Infrastructure Redundancy

There is full redundancy for all Studio application servers. If a primary server fails, all traffic will automatically be switched to a secondary server.

Application servers run in a cluster behind a load balancer. Studio SQL servers include active-passive mirroring. DNS redundancy is provided by AWS Route53.

Bluebeam, Inc.
55 S. Lake Ave. Ste. 900
Pasadena, CA 91101, USA
www.bluebeam.com