Bloomfire

SECURITY AND REDUNDANCY:
Knowledge Sharing For Your Digital Workplace

Hundreds of organizations and hundreds of thousands of users across multiple industries including financial services, retail, direct marketing, and technology depend on Bloomfire to keep their information secure within our robust architecture. To that end, we proactively apply stringent security controls in all layers ranging from facilities to network infrastructure, IT systems and information and applications.

The purpose of this document is to describe the security practices at Bloomfire regarding our approach to software development, hosting, and access controls.

Development

PROCESS

At Bloomfire, we adhere to a strict development process that ensures that our code base is reliable and secure. All changes to the code base are peer reviewed before being added to our environment.

After peer review, it is tested using both automated and manual testing methods to ensure that no stability issues are introduced. Code scanning tools are utilized to ensure that complexity is kept at a minimum and to limit possible exploits.

While we pride ourselves on shipping software to production almost everyday, we take steps to ensure that only authorized members of the engineering team can send code to production.

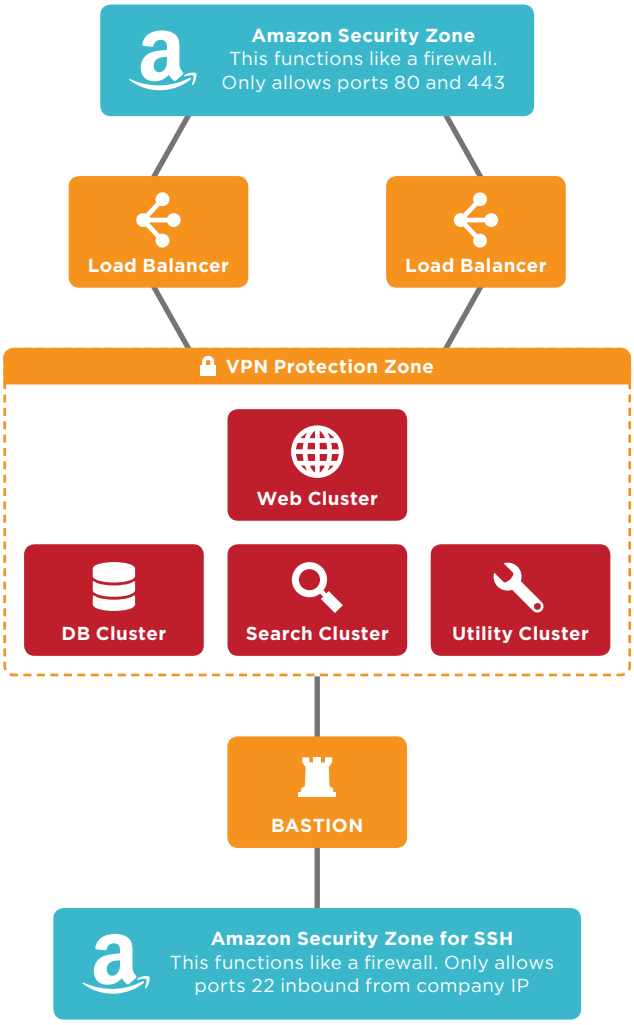
SECURITY

Our codebase is hosted in a secure Git Repository. Access is only permitted via private/public key. Any web based access to our codebase requires two factor authentication to gain access. Each user is uniquely identified, and every check in is tracked to the individual.

Hosting

Bloomfire is SOC2 compliant and uses Amazon Web Services (AWS) as its cloud-hosting platform. This platform, which is trusted by very large Internet properties such as Netflix and Reddit, ensures locked down, privately known locations and uses multiple security layers to prevent unauthorized access to the hardware and infrastructure. You can read more about the security measures taken, and view certificates at their Security and Compliance Center.

All communication to and from Bloomfire's servers is done over robust industry standard 256-bit SSL (Secure Socket Layer) encryption to our secure cloud platform. Our production servers are all behind a VPN to limit any external access. The diagram below describes our environment.



The primary components of AWS that Bloomfire uses are:

- **Elastic Computing Cloud (EC2)** — EC2 provides virtual machines that we use to host all Bloomfire communities. EC2 permits deployment into Availability Zones that represent the redundant parts of Amazon's network. By deploying our servers into multiple Availability Zones (AZ), we can ensure that we will remain online in the event of a loss of an AZ.
- **Relational Database Service (RDS)** — Amazon managed database infrastructure that provides redundancy, failover, encryption, and reliable snapshots.
- **Simple Storage Service (S3)** — This is network storage service used for storing file assets for our communities. S3 is architected to be highly available and redundant.

Backup and Recovery

Bloomfire's database is replicated across multiple AZs in real time, allowing us to continue operation with the loss of any single AZ. We also take snapshots of our data and store them apart from our servers throughout the day. If there were a multiple permanent loss of data on all AZs, Bloomfire could reconstruct operations from these snapshots. In the event of a full rebuild, Bloomfire could reconstruct basic operations within 6 hours.

We maintain virtual machine images of our servers to rapidly create new machines as needed. In the event of a major long term Amazon outage, we would be able to recreate all Bloomfire communities in a different datacenter.

Customer Data Separation

Customer data hosted on Bloomfire is segmented into two sections, file assets and organizational data.

File assets (including video, documents and presentations) are hosted directly on Amazon S3. We rely on Amazon's infrastructure for redundancy and encryption. All customer assets are currently stored in common S3 buckets, but independently secured with the customer's unique identifier. Files are real-time copied to a backup bucket in a different region to ensure that even the most catastrophic of events will not result in data loss.

Bloomfire also has a relational database built on Amazon RDS that is used to store organizational data. This data is stored on a single logical database, but relationally segmented by the customer's unique identifier.

Each request for data or content on Bloomfire is secured by evaluating the user's credentials. When a user makes a request for a community page, that user's credentials are evaluated and the user's session authenticated. The system is architected to prevent users from viewing content in a community that has not been made public. Amazon's S3 product allows us to restrict access to file assets at a fine-grained level. When a download or view request is made, the URL is constructed on the fly and can be configured to expire very quickly. This prevents the user from distributing the URL to unauthorized 3rd parties.

This logical separation of data is a standard practice across SaaS providers. We employ internal security controls to ensure that only authorized Bloomfire employees are able to view customer data. We also utilize external audit services to ensure that we are protected against common attacks that would permit a user to see content they are not authorized to view. Should a customer require additional security or architectural audits, Bloomfire will make the appropriate resources available.

Identity Management

In addition to traditional username/password, Bloomfire's system supports the use of Single Sign On (SSO) providers. We support SAML and our own custom SSO API for other proprietary solutions.

Using our API, customers are also able to set specific roles for users using any authorization system already deployed by the customer.

Internal Access Controls

Internally, Bloomfire controls access to your data by role. Our customer support team is able to login to your community to assist with any support issues. When a support team member logs into your community, they are required to utilize a two-factor login to securely access your data. Any action that a support user does on a community is logged and can be audited and/or exported by the customer.

All web-based logins to production or administrative systems also enforce 2-factor authentication and full auditing. Access to our production systems requires a private/public key pair that can be revoked and changed at any time.

Audit Logs

The Bloomfire system records all activity to an audit log. This audit log contains changes to content and the system, and records which user is doing the action. This can be used to determine the source of any unknown activity.

Proactive Security Policies

In addition to the above, we continually work to ensure that we are providing a secure platform for our customers. We monitor well-known security lists for new exploits and ensure that our servers are patched with the most recent updates in a timely manner. We also utilize third party services to perform penetration testing on all of our software, both web and mobile. We continually investigate and evaluate new approaches to protecting the data that we store.

Deployed inside or outside firewalls, Bloomfire's security and privacy features are designed to meet the requirements of the most tightly regulated global industries and government agencies. For more information about Bloomfire's security policies contact us to schedule a technical call.