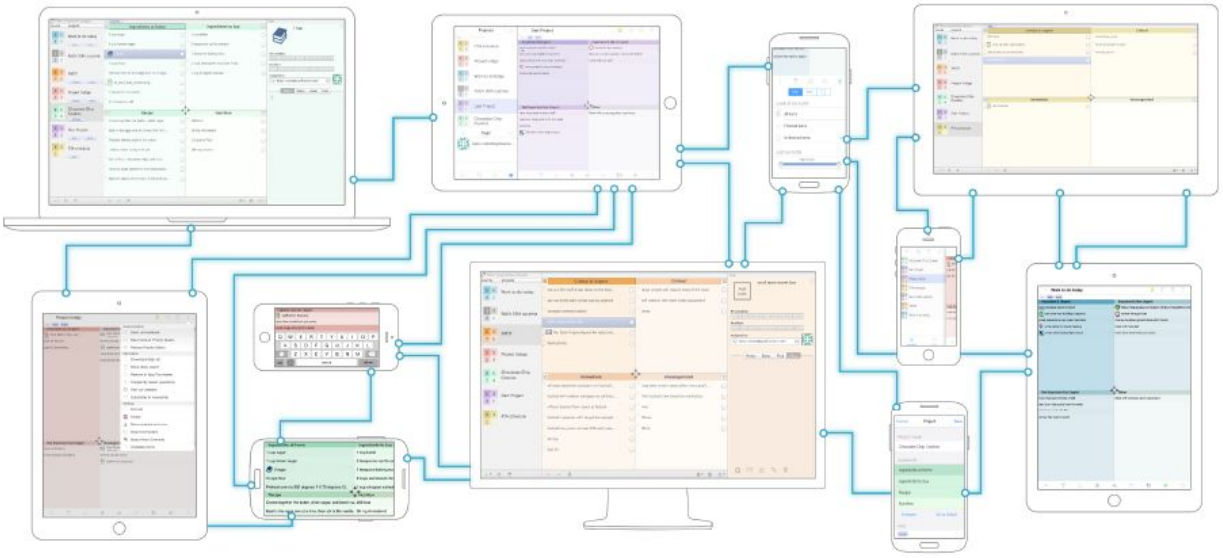

Appfluence Inc & Priority Matrix

Security Protocol Overview

Last revision: September 25, 2020
Endorsed by: Appfluence Executive Team

EXECUTIVE SUMMARY

- Services run by Appfluence Inc and Priority Matrix are hosted on Amazon AWS and Microsoft Azure commercial cloud systems
- Therefore, many components of our security protocols share similarities with, and rely upon, the professional services provided by said vendors
- Amazon AWS Security Overview is available at https://aws.amazon.com/security/
- Microsoft Azure Security Overview is available at: https://microsoft.com/en-us/trustcenter/security/azure-security
- Further information provided upon request

SECURITY PROTOCOL

Key takeaways

- **Physical security.** Servers where Appfluence stores its data are large-scale data centers with military grade perimeter control berms. Physical access is controlled by professional security staff with video surveillance and state of the art intrusion detection.
- **Backups.** Hourly and daily backups are made automatically by AWS RDS and stored in multiple physical locations for added reliability.
- **Firewall.** Our Amazon EC2 instances are deployed behind a bank-grade firewall solution and configured in a default deny mode, with only the necessary ports open for inbound traffic, which can be further restricted by IP addresses, protocol, or service port.
- Various **security protocols** are automatically in place to provide significant protection against DDoS, MITM, IP Spoofing, and Port Scanning.
- Our codified **business processes and practices** ensure that each employee only has the absolute lowest access level that permits them to do their job, thus limiting the risk of unauthorized access.

Data access

Access to production database is limited to senior engineering management. Only authorized individuals have keys to access production database and only selected IP addresses are allowed even given those keys. Furthermore, access to the production database is limited by policy on only specific cases for data recovery or other special circumstances.

From the infrastructure point of view, administrative access to our servers, which sit in private address space behind firewalls, is restricted by IP to specific authorized locations, and directed through a hardened bastion server to minimize the potential attack surface. No SSH/shell password access is allowed under any circumstances, and a strong passphrase rotation is enforced systemwide for all our authorized personnel. All our servers are physically managed by Amazon Web Services. All user data is encrypted both at rest on the server side, and on transit.

Continuous security

Security is a journey, and cannot be something we think about once a year. In order to preserve the secure state of our systems, we subscribe to a continuous security monitoring service to receive prompt alerts about newly detected vulnerabilities, thus allowing us to patch every server with the latest stable updates on a daily basis. We strive to minimize the number of software packages used in our environment, to limit the opportunity for potential attacks.

On a regular basis (at least once a year), we contract the services of an external security specialist to perform **penetration tests** and report on their findings so we can continue improving our security practices. Additionally, we subscribe to a number of automatic, independent services to continuously monitor security risks and keep our services up to date. This includes both public interface scanning and internal log monitoring. Finally, we run our own (static and dynamic) vulnerability scans on a quarterly basis, in order to continuously reduce the attack surface offered to an adversary. Some of these scans are integrated in the development process, which prevents the introduction of vulnerable source code in the first place.

Secure development

We operate a secure-by-default environment. Whenever a new service is built, we start from a zero-access environment, and then open access only as required by the service, and not further. Since we run a container-based service, the following specific precautions are taken as part of our process:

- Operate an updated container environment, on the development, staging and production sides, with all patches applied, especially security related ones
- Only use trusted, up to date container images, only after verifying their signature, and chosen for their limited application scope

- Reject container images with unnecessarily available services, and inspect for known vulnerabilities using an up to date scanner run on a regular basis
- Do not store credentials, secrets or other identification means in the images; Instead use our deployment infrastructure to provide these details at runtime
- Maintain updated automatic vulnerability scans of all modified code at the time of commit

Communication protocols

- Communicate to and from our Amazon EC2 sync servers use the 256-bit SSL/TLS encryption signed by Verisign Class 3.
- Secure Server - CA security certificates. The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and DHE_RSA as the key exchange mechanism.The connection does not use SSL compression.

Secure data storage

Server side data (projects, items, and generally everything beside attachments) is encrypted at rest, via the managed database service RDS by Amazon Web Services (details at https://aws.amazon.com/rds/features/security/) using industry standard **AES-256** encryption, and on transit using industry standards (HTTPS/SSL with modern encryption).

Client (local apps) data is stored in user folders on client computers. These folders can be encrypted by the client's IT department as needed. Assuring the security of these folders is beyond the scope of our engineering team, given that access control is controlled at the operating system level, and the client's IT department should make the appropriate decisions.

File attachments are stored using in one of two commercial systems: **AWS S3** and **Microsoft OneDrive**. By default, attachments are stored in an Amazon-managed S3 bucket. The specific location is in a scrambled, not guessable location. However, in order to facilitate collaboration across the internet, files in this S3 bucket are publicly accessible to anyone who knows their scrambled URL. Therefore, users who have concerns about the confidentiality of their documents should request access to our other storage option. In an *opt-in basis* for users with an appropriate subscription level, it is possible to use the client's own OneDrive account for document storage. This gives IT administrators more control over the access rights and lifetime of their internal files. For users with enhanced security requirements, we recommend enabling the alternative storage solution based on the client's own OneDrive account. With this approach, attached files are maintained inside the organization control, in a special folder inside the administrator's account. Microsoft may levy additional charges depending on the total storage space being utilized.

Authentication

Customer passwords for Priority Matrix are **never** stored in plain text, and are encrypted with keyword hash and salt. We also have recommended minimum password requirements. User data can only be accessed by authorized users with the correct email and password.

Single-sign-on is supported against various identity providers (currently Google and Microsoft), in order to facilitate comprehensive user management from the customer side.

Multi-factor authentication is offered to our enterprise customers as agreed by contract. Similarly, custom password rules can be enforced by admins at this subscription level. For more information, see our pricing documents or contact support.

Environment isolation

During our development work, there are several backstops that prevent the leaking of potentially confidential information across legitimate areas of concern. A brief list includes:

- Our development, staging and production environments run on independent infrastructure and without sharing access to common data, networks, databases or authentication credentials.
- By default, customer data is co-located on the same production environment, and a data ownership protocol is used to grant or deny access to each project, task or attachment in the system. It is possible for customers to request a private cloud or on-premises deployment, under our enterprise plan.
- Internal employees do not have access to customer data, with the exception of privileged support personnel who may access customer data via a limited, monitored dashboard, with user permission. Such access is restricted to a few commonly requested operations in order to facilitate common tasks, and it is logged and audited.

The appropriateness of these backstops is tested automatically with every software release, and it is also evaluated at least once every 12 months as part of our internal risk assessment process.

Further reading

Additional information regarding our data management and other policies can be derived from our other publicly available documents:

- Privacy policy: https://appfluence.com/privacy/
- Terms of service: https://appfluence.com/eula/