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/
● 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. 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, but typically twice 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.

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 is encrypted at rest, via a managed service by Amazon Web Services, 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.
Authentication

Passwords 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.

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/