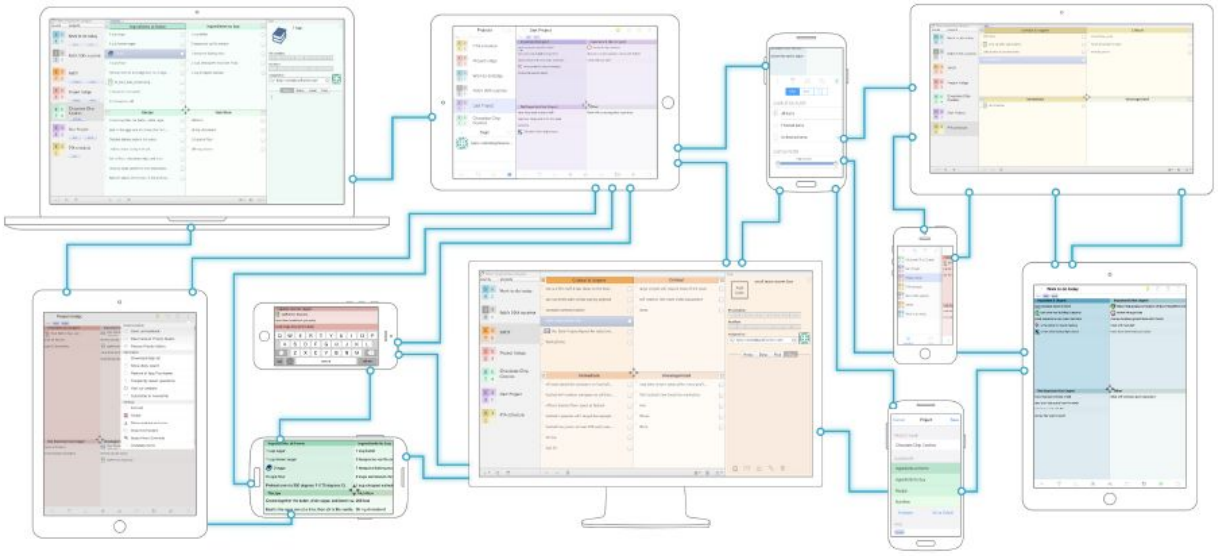

Appfluence Inc & Priority Matrix

2018 Security Protocol Overview

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 LLC 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 policies

Access to production database has extremely limited personnel access. 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.

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.

Client data storage

Client (local apps) data are stored in user folders on client computers. This folder can be encrypted by the client IT department as needed.

Password storage

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.