Device Magic Product Security

Web Application Security:

- Our services and data are hosted by Amazon Web Services, on the east coast of the USA (AWS us-east-1 and us-east-2). They are deployed across multiple availability zones, so we are resilient against any single data center failure.
- Our product architecture aims to minimize coupling between components to further mitigate failures (A complete outage of submission deliveries should not take down our website, or API access, or interfere with mobile form completion).
- All data is encrypted at rest, with technology appropriate for how it is stored (encrypted EBS volumes and S3 buckets, database storage engine encryption, etc.).
- Data in motion is encrypted with HTTPS / TLS (‘A’ or better ratings in the Qualys SSL Labs tests on all our endpoints).
- Passwords have minimum complexity requirements and are never stored directly (salted bcrypt hashes).
- Role-based permissions are built into the product.
- 2 factor authentication is configurable for any user, and can be enforced by an administrator within their organization.
- All payment information is processed and stored by our PCI compliant billing providers (Recurly security except South African customers, where we use Snapbill).
- All data stores are backed up at least daily to Amazon S3, and stored for at least 30 days.
- Audit logging and SSO are included in our Enterprise plan.

Mobile Security:

- Our iOS app uses Apple’s Data Protection to encrypt stored data (including form submission data and reference data) when the user has configured a passcode. We use the NSFileProtectionCompleteUnlessOpen protection level.
- We have not found you can reliably encrypt stored data across the wide range of Android handsets without using a Mobile Device Management (MDM) solution. If you require encryption-at-rest on Android, we strongly recommend you deploy the app via an MDM wrapper. Our app is compatible with a number of these.
- All communication from our app to our servers is encrypted with HTTPS / TLS. (Android 4.x and older have limited TLS 1.1+ support)
- Data retention periods after successful submission are configurable.
- Storage of captured images in the device albums / gallery is configurable.
- Removal of devices from organizations on the website will cause apps to wipe their stored data.
- Submission delivery from the app to the servers is done in multiple steps (to support intermittent slow connectivity) with each step including integrity checking and retries of uploaded data.
- Forms and resources access within the app is configurable per device group on the website.

Human Security:

- Background checks are performed on Device Magic employees (in accordance with local laws).
- US employees are subject to employment verification and criminal checks.
- All employees sign a confidentiality agreement to protect customer data.
- 2 factor authentication is enforced for all Device Magic employees.
- Administrator access is limited to authorized employees who require it to do their jobs.