Security Information

How Marq Protects Your Data

Marq is the intuitive brand templating platform that empowers anyone to easily create on-brand materials. The power, simplicity, affordability, and security of Marq have driven its adoption by hundreds of thousands of individuals and teams from numerous businesses and educational institutions.

The following paper introduces Marq security policies, practices, and procedures. Review it to gain an understanding of how Marq employees, service providers, and partners safeguard customer data.

marq.com
(888) 705-4096
sales@marq.com

About Marq

Marq is delivered through a software-as-a-service model that avoids upfront costs and IT operational burden. It is designed to be seamlessly compatible with several software platforms.

Marq integrations

Storage

- Google Drive
- Dropbox
- Facebook

Social Media

- Facebook
- Twitter
- LinkedIn

Search

- Bing
- Iconfinder

Email

- Constant Contact

Marq import and export

Import

- InDesign

Export

- PDF
- Images (JPEG and PNG)
- Hosted webpage

Marq is designed to provide guardrails and oversight to protect your brand throughout the entire templating process. Designers can follow their normal process by seamlessly importing InDesign IDML files and converting them to Marq documents.

Admins can set up brand assets usable by everyone on their account. They can also convert any document, imported from InDesign or created in Marq, into a brand template. Converting a document into a template locks down the original file while still allowing custom copies to be created.

To aide in collaboration, Marq offers integrations with Slack and G Suite.

End users can export the created documents as a unique URL in a published document, post directly to social media, order prints through Alexander's Print Advantage, or download the document as a PDF for their own use.

Secure

To learn more about the security procedures employed by AWS, please review their documentation. Marq delivers secure design through a defensive application architecture, a system of internal controls, and a set of policies governing partnerships and integrations. Marq provides security across many dimensions, including data secrecy, authentication, authorization, and auditing.

Secure infrastructure

Marq is powered by Amazon Web Services (AWS), the industry’s leading pro-vider of secure computing infrastructure. AWS meets stringent security measures that include a variety of physical controls to the data centers, data privacy guarantees, and robust controls to its services. AWS has pub-lished white papers on risk and compliance and security processes. AWS has achieved the following certifications and third-party attestations:

AWS certifications

- SAS70 Type II audits
- Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS)
- ISO 27001 certification
- U.S. General Services Administration FISMA Moderate level operation authorization

Data encryption

Marq understands the sensitivity of private business documents, communication-, and personally identifiable information. To ensure the privacy of this information, all data is transferred between user devices and Marq servers using a 256-bit encrypt-ed connection via TLS 1.2 and a world-class certificate provider.

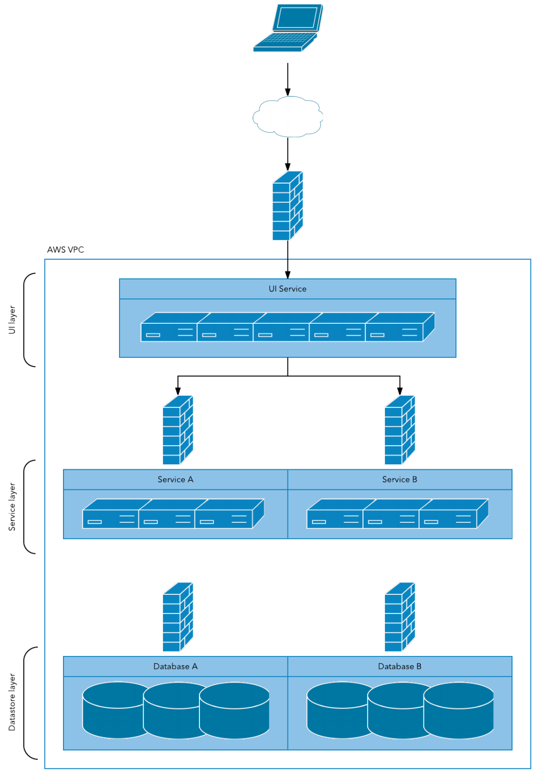
Marq also employs encryption at rest to protect the secrecy of all data persisted by the application. All databases, data-base-backed caches, and other components with persisted data have their disks initialized with random data using a high-entropy, random data source. During use, the disks encrypt their contents with 256-bit AES with ESSIV. The cryptographic keys are protected by a pair of redundant passphrases stored in separate environments.

Network protection

Marq runs in an AWS Virtual Private Cloud (VPC) that is not accessible from the public Internet. All traffic to and from the public Internet must travel through specific gateways.

The Marq operations team uses secure connections for working on VPC machines. Network access to the environment happens through an industry-standard VPN solution that is locked down to a strict set of clients. SSH connections to the VPC servers use Diffsotie-Hellman 2048 for key exchange and encrypt the entire session with industry-standard Blowfish cipher and 2048-bit unique keys. Keys are generated per user and can be shut off individually upon termination.

To provide rigorous access control, the various-services and service tiers are segregated by network layer (IP) and transport layer (TCP & UDP) firewalls. The firewalls are implement-ed by AWS Security Groups and limit all in-bound network connection attempts, except with strict sets of client machines for each service (see Figure 1 below).



Availability

An integral part of the Marq service is the ability to securely access the tool at any time and from any device or location. Documents, account information, access control lists, and other persistent data is rep-licated across availability zones using industry-standard database management systems, replication, and failover solutions.

All services are clustered and served through AWS Elastic Load Balancers (ELBs), giving users access to their documents whenever they need it. One of the benefits to software-as-a-service is that users always get the latest version of the software at no cost and without any work by IT. That is true for Marq, plus our bi-weekly upgrades are done with no downtime. Users will never receive a “down for sched-uled maintenance” page when they need to finalize critical documents for a meeting or deadline.

Because components may fail on occasion, the Marq operations team maintains a robust automated live site monitoring system and a 24/7 on-call rotation to ensure that the redundancy, failover, and self-healing mechanisms work properly at all times.

Disaster recovery

Customer documents and related data are backed up hourly to multiple physical environments across availability zones in encrypted format. The Marq operations team performs regular validations of these snapshots to ensure that they can be used for restoration in the event of an emergency.

Content controls

Application

Authentication

Marq gives team administrators the flexibility to set the password policy for their account. They can set the required password length, required character classes, and frequency of password changes. Admins may also manually force all team members or individuals to reset their passwords.

Passwords are never transmitted in plain text. Only salted one-way hashes of passwords are ever stored by Marq servers, never the passwords themselves. Individual user identity is authenticated and re-verified with each transaction, using a secure token created at login.

Authorization

We follow security best practices and protect your data by using the principle of least privilege access. A simple role-based permissions system allows administrators to manage access to documents owned by the account.

There are two primary sets of access controls: account controls and document controls. Four roles exist in regards to account management: account administrator, team administrator, user, and billing administra-tor. The following table lists the features that each role may access.

Permission	Account Admin	Team Admin	User	Billing Admin
List team members	☑	☑	☑	☑
Manage group membership	☑	☑		
Set (not view) user passwords	☑	☑		
Manage team settings	☑	☑		
Manage integrations with other apps	☑	☑		
Manage team admins Manage subscription level	☑	☑		☑
Manage payments	☑			☑

The account management tools allow account and team admins to remove users from their account, as well as delete users that are part of their account. In the latter case, the admin has the option to take ownership of any documents that the deleted user owns. Through the team settings page, admins can:

- Restrict document sharing on social networks.
- Restrict publishing of documents as web pages, exportable documents, and images.
- Restrict the generation of public links to documents.
- Restrict sharing to users with email ad-dresses under certain domains.

In relation to Marq documents, there are four roles that users could have: owner, editor, commenter, and viewer. The creator of the document automatically occupies the role of owner, though this setting can be changed. Documents are private by default, i.e. no other user has any level of access to the document. The following table lists the features that each role may access.

Permission	Account Admin	Team Admin	User	Billing Admin
View document	☑	☑	☑	—
Edit document	☑	☑		
Comment on document	☑	☑	—	
Delete document	☑			
Share document	☑			

Data ownership

Marq claims no ownership over any documents created through our services. Users retain copyright and any other rights, including all intellectual property rights, on created documents and all included content. We respect your privacy and will never make your documents or other information publicly available without permission.

Internal controls

Marq uses a multidimensional control framework to ensure that security is maintained and continually improved. Company leaders support security and provide a positive control environment. Risk assessment is performed by both internal and external system reviews. Security information and objectives are openly shared among team members, and security measures are continually monitored and improved.

Operations

Administrative access to the production environment of Marq is controlled.
Only authorized members of the Marq operations team have access to the AWS console that manages the environment. Least privilege access is designed so that team members with a legitimate need to access components, such as production logs, may do so without administrative access to critical processes and secure drives.

Internal reviews

Security reviews are performed at multiple stages in the development process. All critical architecture designs are reviewed by several Marq team members. Code reviews of implemented designs include security reviews. These reviews verify secrecy, authentication, authorization, and other security needs of each feature or component.

Partners

Many users are attracted to Marq because of its easy integration with a variety of popular business applications.

Single sign-on

Marq supports single sign-on (SSO) using the popular OpenID technology. Supported OpenID providers include Google and Yahoo.

Marq also supports single sign-on through Security Assertion Markup Language (SAML). SAML is an XML-based framework for communicating user authentication, entitlement, and attribution information. When a customer enables SAML integration, Marq acts as the service provider and the customer's SAML service acts as the identity provider.

Cloud-based applications

Because these applications use OAuth, user passwords are never entered into or stored by a third-party application. The integrations require minimal configuration by the admin.

Print Partners

Marq integrates with a variety of print partners to satisfy the needs of an expanding customer base. Information shared with print partners is limited to:

- A PDF of the document to print
- Selected print options
- Addresses for shipping

Print partners are required to delete order Information within one month of order fulfillment. Access to documents and addresses are limited to only the printer via a signed URL.

Summary

Marq employs powerful defense procedures to keep its customers' documentation secure.

The architecture implements secrecy through encrypted transmissions and storage of data. That data is made highly available and reliable through modern replication, backup, failover, and monitoring techniques. Authentication and authorization are foundational features of the service, with administrative controls to tune the system to meet different corporate guidelines and policies. In its integrations with several popular business tools, Marq applies the same rigorous security standards.

Marq is also committed to following information systems best practices of internal controls and external reviews.

To explore Marq's features, join our sales team for a live demo of the software. We're happy to demonstrate its ease of use and answer any questions you might have.

Resources

https://aws.amazon.com/security/
http://media.amazonwebservices.com/AWS_ Risk_and_Compliance_Whitepaper.pdf
http://media.amazonwebservices.com/pdf/ AWS_Security_Whitepaper.pdf
https://aws.amazon.com/security/
http://openid.net/

https://www.oasis-open.org/committees/
tc_home.php?wg_abbrev=security#samlv20

http://oauth.net/
http://self-issued.info/docs/draft-ietf-oauth-json-web-token.html