hello@pageproof.com
www.pageproof.com

PageProof's technology for IT professionals

Version 1.4

PageProof is a fully-encrypted review and approval platform for artwork, images, documents, video, audio, html, banner ads and email templates. PageProof gives your team a red pen so they can put feedback directly on your work and press a green button. We remove the email chaos associated with gathering feedback into a simple to use system which you can use on your computer, tablet or mobile phone.

The technology stack which underpins PageProof is Microsoft Azure which brings a large number of benefits in terms of scale, security and features.

In this document, we will outline the technology stack we use at Microsoft and provide some detail around how we use encryption inside PageProof.

PageProof and Microsoft Azure

Introduction

Microsoft Azure is a very large scale cloud computing platform which is heavily certified by a large number of certification agencies all over the world. Azure is designed, run and maintained by Microsoft globally.

Azure platform services

Microsoft provides the following managed platform & services to PageProof:

- Data centers
- Networking & firewalls
- Computing hardware
- Storage
- Operating systems (including versions and patching)
- Application software (including versions and patching)
- Webserver software (including versions and patching)
- Database servers (including versions and patching)
- Penetration testing and IDS (Red/Blue Team Attack/Defense)

PageProof deployed application

The PageProof application itself runs on Microsoft Azure. The entire stack is managed by Microsoft, and PageProof deploy the following application components:

- PageProof .NET application
- Managed microservices
- HTML / JS / CSS for the PageProof front-end & website

Inherited benefits

Using Microsoft Azure at scale enables PageProof to inherit a number of features provided by the Azure stack. These include:

- Geo-replication (in region) of storage and database
- Encryption at rest (Database and storage)
- Microsoft controlled infrastructure firewalls and intrusion detection
- Microsoft's Red / Blue team penetration testing of the entire Azure stack
- Auto-scaling of resources on-demand

PageProof data sovereignty

PageProof Enterprise customers can (optionally) nominate a data region for their account to provide data sovereignty. This means all proofs, comments, snapshots and attachments will reside in the nominated data region only.

Data regions supported are:

- West USA \ East USA \ Central USA \ South Central USA
- Canada
- Australia
- France
- Germany
- UK
- South Africa
- Brazil
- UAE
- Japan

Each region has in-region replication pairing for live snapshots. (Example: WestUSA pairs with EastUSA)

Microsoft Azure platform certifications

Microsoft Azure has the broadest set of compliance offerings with over 90 compliance certificates. These cover major areas for:

- Platform management
- Patch and deployment
- Data center access
- Data center management
- Networking and power redundancy
- Hardware and storage wipe and decommission
- Firewall and IDS
- Resilience
- Data controls

These certifications include:

- ISO 27001
- ISO 27018
- SOC 1
- SOC 2
- SOC 3
- FedRAMP
- HITRUST
- MTCS
- IRAP
- ENS

See https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/ for a comprehensive list.

Platform Configuration

PageProof uses multiple Azure subscriptions and roles to manage access to the environments inside of Azure. We run the following:

- Development
- Testing
- Staging
- Production

Development and Testing exist in the DEV Azure subscription where the development team are further managed into roles of front end and back end teams.

Staging and Production exist in the LIVE Azure subscription and can only be accessed by the deployment team who run all changes and configurations through Development, Testing and Staging before it is swapped into Production.
Every Production change is checked post swap - and can be swapped back to its previous state within 1-3 minutes.
The development teams have no access to the Production environment.

PageProof's encryption explained

PageProof's use of encryption in review and approval is a world-first (US Patent No. 10515227). This next generation approach to encryption takes data encryption to a new level. PageProof is the only review and approval platform which offers encryption and security to these levels.

PageProof uses multiple levels of encryption to keep data secure. These are:

- Pre-transmission content encryption (AES256 & RSA 2048)
- Encrypted transport over HTTPS (with the latest TLS version)
- Database encryption at rest (RSA 2048)
- Storage account encryption at rest (RSA 2048)

When a proof, comment, attachment or version is added to PageProof, we go through the following technology to get it to the PageProof servers.

1. On the user's device (pre-transmission), the data is encrypted using AES256.
2. A RSA 2048 key is added to the envelope of users able to decrypt the data.
3. Using HTTPS, we transmit the encrypted data to the PageProof servers.
4. The encrypted data is put into Azure storage (encrypted at rest).

The RSA 2048 key pair are stored against the user's profile in PageProof - with the private key stored encrypted by the user's password. These can only be used if the user provides their password in order to decrypt the keys. PageProof has no access to these keys.

To decrypt, the data must be retrieved to the user's device along with the RSA 2048 keys which are decrypted using the password provided by the user. The AES256 key is then decrypted, and used to decrypt the data.

The decrypted data is then presented to the user. This process happens entirely on the user's device.

Enterprise authentication

PageProof Enterprise can be configured to authenticate with the following single sign-on identity providers:

- Okta
- Centrify
- OneLogin
- Microsoft Azure AD (On premise AD is possible using SAML2)
- Google G Suite
- Ping Identity

Single sign-on can be set to enforced if required. This means a PageProof password field is not displayed and SSO must be used.

Features such as multi factor authentication and biometric authentication is provided for by your identity provider.

PageProof SCIM can be optioned and configured to provision users from your identity provider into your PageProof team.

PageProof's notifications and access whitelisting

PageProof uses SendGrid (https://sendgrid.com) to deliver email notifications. Every notification comes from the same email address. We recommend adding this email address to your company whitelist:

team@pageproof.com

For those running firewalls with inspection modes in play, please add the following domains to the whitelist to ensure the best experience for your reviewers:

pageproof.com	
api.pageproof.com	
app.pageproof.com	
*.static.pageproof.com	(required for HTML proofing)
*.pageproof.app	(required for Enterprise CDN delivery)
amp.azure.net	(required for Azure Media Player - video)

For the best review experience, we recommend reviewers access PageProof on a fast internet connection (Fast VDSL+ or Fibre). As PageProof's servers deliver high quality artwork, documents, html, video and audio content, these connections are very important for the overall experience.

PageProof supports all modern browsers. We recommend:

- Google Chrome
- Firefox
- Microsoft Edge
- Safari
- Microsoft Internet Explorer 11 (Note: Edge is recommended over IE)

Chrome, Firefox, Safari or Edge are required for HTML proofing using the PageProof browser extension.

Notes:

A PC with Windows 7 and IE11 are our bare minimum specification.

Performance is moderate for this configuration of PC. We recommend these users simply upgrade to Edge for dramatically improved performance.

IE11 will be deprecated 1st September 2020 and users advised to move to Microsoft Edge according to Microsoft's own guidance.

PageProof data processing outline

PageProof collects and processes a customer email address to login to PageProof. No other personal information is required to use PageProof.

Definition

In relation to a customer, PageProof is defined by data protection mandates, such as the European GDPR, as a processor.
Data is defined as the email address provided to PageProof by the customer to login to the PageProof platform.

Confidentiality of processing

PageProof will ensure that any person it authorizes to process the data will protect the data in accordance with PageProof's privacy agreement https://pageproof.com/privacy

Security

PageProof will implement technical and organisational measures to protect the data from a security incident.

Subprocessors

PageProof uses the following companies as subprocessors of the data:

- *microsoft.com (Azure platform)*
- *intercom.io (Customer support platform)*
- *chargify.com (Billing platform)*

Each companies maintains a data processing policy for subprocessing of data.

Customer and data rights

PageProof will co-operate with customers to provide:

- The data held by PageProof, upon request
- Removal of all personally identifiable data (PID), upon request

These requests will be processed in reasonable and timely manner. Requests can be made by emailing team@pageproof.com.

Further questions?

If you have any further questions regarding PageProof security or IT, please email your question to **security@pageproof.com**

PAGEPROOF