DocRaptor Security Policies & Information

Whitepaper

Spring 2016

OVERVIEW

This document provides a high-level overview of DocRaptor's Security Policies and the security features within the DocRaptor application. It addresses the most common concerns customers may have about security and privacy, while outlining the security controls available within DocRaptor.

TABLE OF CONTENTS

1. SECURITY PROGRAM OVERVIEW

DocRaptor is committed to the security of your data. As part of this commitment, we use a variety of industry-standard security technologies and procedures to help protect your information from unauthorized access, use, or disclosure.

The DocRaptor security program covers the following areas:

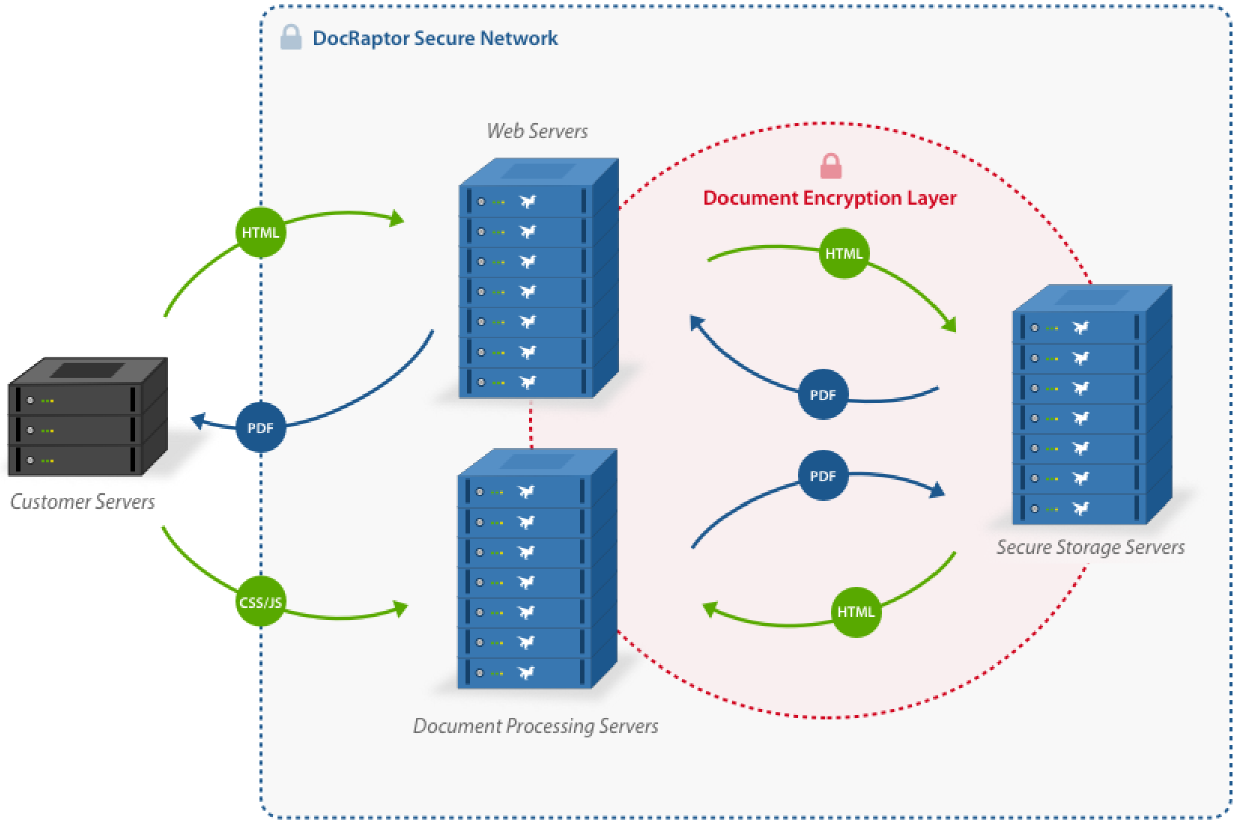
- Processed Data Security
- Data Privacy
- Infrastructure & Network Security
- Application Security
- User Management Security
- Corporate Security Policies

2. PRODUCT OVERVIEW

DocRaptor's services are used by our customers to convert HTML, CSS, and JavaScript into PDF, XLS, and XLSX documents. This is accomplished by enabling customers to transmit their content to DocRaptor's services, which converts and sends the resulting document back to the customers.

A single document request flow through DocRaptor:

- A customer who runs applications and/or servers in data center, cloud, or hybrid environments, supplies DocRaptor with a URL or content via an API call over an SSL-encrypted (by default) connection after authenticating with a unique API key.
- The DocRaptor services optionally run JavaScript content.
- The DocRaptor services render the resulting HTML into PDF/XLS/XLSX.
- The resulting document is encrypted using certified public encryption standards and stored to allow download by the customer.
- The customer downloads the resulting document (a limited number of times depending on Data Retention Configuration) over an SSL-encrypted (by default) connection after authenticating with a unique API key.
- Customer input and output are deleted based on their Data Retention Configuration.



3. APPLICATION SECURITY

DocRaptor's developers review application code changes for security vulnerabilities, as well as run automated vulnerability checks on library dependencies. Additionally, vulnerability disclosure lists are monitored regularly to ensure timely updates and patches of security issues.

DocRaptor employs industry standard security measures concerning server management including:

- No password-based SSH access
- No shared developer credentials
- No global AWS access
- Strict firewalling between servers/groups of servers

4. USER MANAGEMENT

DocRaptor users access management, billing, and debugging information on the website via an email address and a password. The DocRaptor API is accessed by account API key. User passwords are stored in an industry standard encrypted hash format.

5. DATA PROCESSED

DocRaptor only processes content that you send the DocRaptor API (directly or via URL). Generally, this includes HTML, CSS, and JavaScript that make up a web page. This may involve multiple requests since content may link to external images, scripts, or stylesheets. The customer can control the security of these requests in a number of ways, including:

- Specifying SSL for assets in their HTML
- Protecting assets using HTTP Basic Auth and providing the username and password to access those assets using DocRaptor's API parameters
- Using assets that are only available for a short time window
- Using assets that are limited to a specific number of downloads
- Using asset URLs containing large random strings
- Using IP whitelisting to firewall asset access to only DocRaptor servers
- Proxying requests through a secured proxy server they control

6. TECHNICAL FEATURES

DocRaptor has certain built-in technical features to offer flexible security options:

- DocRaptor encrypts content in transit to and from DocRaptor's servers. HTTPS encryption is enabled by default for data being sent to DocRaptor in transit.
- DocRaptor encrypts document input and output during internal transit between its servers.
- DocRaptor encrypts document input and output at rest.
- Communication from the DocRaptor Client Libraries to the DocRaptor servers is outbound on either port 80 or 443. DocRaptor Client Libraries do not receive inbound connections.

- DocRaptor does not have the ability to auto-update DocRaptor Client Libraries installed on customer servers. All updates must be manually installed.
- Limited data retention. By default DocRaptor will store document input and output for 7 days in order to allow customers to open a Help Request on any document in that time frame. Opening a Help Request allows us to access your document input and output in order to assist with any technical or styling issues. This time frame can be configured on an account basis with various options ranging down to “As Short As Possible”. In this case customer input content is deleted immediately after it is converted, only one download is allowed, and the document is deleted immediately after download. This feature is highlighted in our blog post https://docraptor.com/blog/fine-tuning-your-document-storage.
- Secure Random Hash codes are used for download and status URLs

7. SECURITY CONFIGURATIONS

DocRaptor offers the following security configuration options:

- Data Retention Time can be configured to control the length of time document input and output content is stored.
- By default, Client Libraries are configured to send requests over HTTPS.
- Users can control asset transmission encryption by specifying HTTPS for HTML assets.
- SSL certificates for HTML assets are verified by default, but verification can be disabled.
- External assets can be additionally protected by HTTP Basic Auth and a username and password can be sent to DocRaptor that will be used to fetch assets.
- PDF output can optionally be encrypted using a PDF standard “user password”.
- Several other post-render security features, such as disallowing PDF modification, disallowing printing of PDF output, disallowing copy from PDF output, can be found at https://docraptor.com/documentation/api#api_advanced_pdf

8. DATA CENTER SECURITY & LOCATION

DocRaptor is hosted in the Amazon Web Services (AWS) US-East region, across three availability zones with fully redundant power backup systems, fire suppression systems, and security guards. More information about AWS security can be found at https://aws.amazon.com/security.

9. PRIVACY

DocRaptor is committed to protecting the privacy of our customers.

The information we collect as part of doing business with our customers, in addition to the content we process as part of our provision of services is protected under our privacy policy.

More information on our privacy practices is available at https://DocRaptor.com/privacy.

10. ADDITIONAL CONSIDERATIONS

Customers with specific security or compliance concerns should consider use of the security configurations described above or as further described in the DocRaptor Documentation available at https://docraptor.com/documentation/api.

To further understand how to address security and privacy, customers are encouraged to read the materials, best practices, and other guidance that is made available on the DocRaptor website. If you require further information, please visit https://DocRaptor.com/contact.