



Maxxcloud

Enterprise, Unsanctioned

Location of Headquarters: Bohemia, United States
maxxvault.com

88

Cloud Confidence

Users:
 Sessions:
 Bytes Downloaded:
 Bytes Uploaded:
 Vulnerable: No

Summary

MaxxCloud is a cloud based Enterprise Content Management solution that allows documents and data to be stored in a world class Electronic Document Management System (EDMS) and made available instantly from user desktop, via the web or from within their other business applications. MaxxCloud organizes user documents based on index criteria, making them easily found through quick searches rather than fumbling through complex folder trees. MaxxCloud fully supports workflow, digital secure signatures and online forms design. MaxxCloud also can integrate with other 3rd party cloud solutions.

Similar Apps by Sessions

Pricing Plan

# of Users:	Cost / User / Month:	Estimated Cost:
-------------	----------------------	-----------------

Certifications and Standards

What compliance certifications does the app have?

- HIPAA
PCIDSS, SP800-53, GAPP, COBIT, TRUSTe, Privacy Shield, Not Supported by Vendor, Under Research

To what data center standards does the app adhere?

- SOC-2, SAS70/SSAE-16
SOC-1, SOC-3, ISO27001, ISO/IEC 27018, Not Supported by Vendor, Under Research

Data Protection

Does the app allow data classification (e.g., public, confidential, proprietary)?

- Yes

If yes, does the app allow admins to take action on classified data (e.g., encrypt, control access)?

- Yes

Does the app encrypt data-at-rest?

- AES
RSA, DES, BitLocker, Blowfish, Yes. Algorithm under research, Not Supported by Vendor, Under Research

Does the app encrypt data-in-transit?

- Yes

Does the app increase the risk of data exposure by supporting weak cipher suites?

- Under Research
Yes, No

If yes, what are the weak cipher suites supported by the app?

-

Does the app allow customer-managed encryption keys?

- Yes

Data segregated by tenant

- Yes

Which HTTP security headers does the app use?

- Not Supported by Vendor
Content Security Policy, XSS-Protection, HTTP Strict Transport Security, X-Content-Type-Options, X-Frame-Options, Under Research

Does the app vendor use a Sender Policy Framework to protect customers from spam and phishing emails?

- Yes

Does the app enable file sharing?

- Yes

File Sharing Capacity

- Greater than 10GB

Less than 5GB, 5GB to 10GB, Not Applicable, Under Research

Does the app allow anonymous sharing of data?

- Yes

Can the App Traffic be Proxied

- Under Research

Yes, No

Access Control

Does the app support role-based authorization?

- User-role based access

Does not provide role based authentication, Under Research

Does the app enforce authorization policies on user activities?

- Yes

Does the app support access control by IP address or range?

- Yes

Does the app enforce password best practices as policy?

- Yes

SSO/AD hooks

- SAML, AD/LDAP

OAuth, OpenID, Facebook, Twitter, Google Sign-in, Linkedin, Not Supported by Vendor, Under Research

Does the app support multi-factor authentication?

- Supports 2-factor/multi-factor authentication

Does not support multi-factor authentication, Under Research

Does the app support the following device types?

- iOS Device, Android, Windows Desktop, Browser

Windows Mobile, BlackBerry, Mac, Not Supported by Vendor, Under Research

Auditability

Does the app provide admin audit logs?

- Yes

Does the app provide user audit logs?

- Yes

Does the app provide data access audit logs?

- Yes

Disaster Recovery and Business Continuity

Does the app vendor provide infrastructure status reports?

- Yes

Does the app vendor provide notifications to customers about upgrades and changes (e.g., scheduled maintenance, new releases, software/hardware changes)?

- Yes

Does the app vendor back up customer data in a separate location from the main data center?

- Yes

Does the application vendor utilize geographically dispersed data centers to serve customers?

- Yes

Does the app vendor provide disaster recovery services?

- Yes

Which infrastructure or hosting provider is the app hosted on?

- Amazon Web Services

Legal and Privacy - Legal

Who owns the data/content uploaded to the application site? Does the customer own the data or does the application vendor own the data?

- Customer owns the data

Vendor owns the data, Under Research

Is the customer data available for download upon cancellation of service?

- Available immediately

Not Supported by Vendor, Under Research

Is all customer data erased upon cancellation of service? If so, when?

- Within a week

Within a month, Later than a month, Not Supported by Vendor, Under Research

Legal and Privacy - Privacy: Mobile

Does this application access contacts, calendar data and messages?

- Under Research

Yes, No

Does this application access other apps on the device?

- Under Research

Yes, No

Does this application perform system operations?

- Under Research

Yes, No

Legal and Privacy - Privacy: Browser

Does this app share users' personal information (e.g., name, email, address) with third parties?

No

Does this application use third-party cookies?

No

Vulnerabilities and Exploits

Vulnerabilities & Exploits

None

Heartbleed, OpenSSL CCS Injection, POODLE SSL v3 fallback, FREAK, Logjam, DROWN