mangoapps®

SECURITY & COMPLIANCE at MangoApps

A white paper for MangoApps compliance cloud customers

www.mangoapps.com

Table of Contents

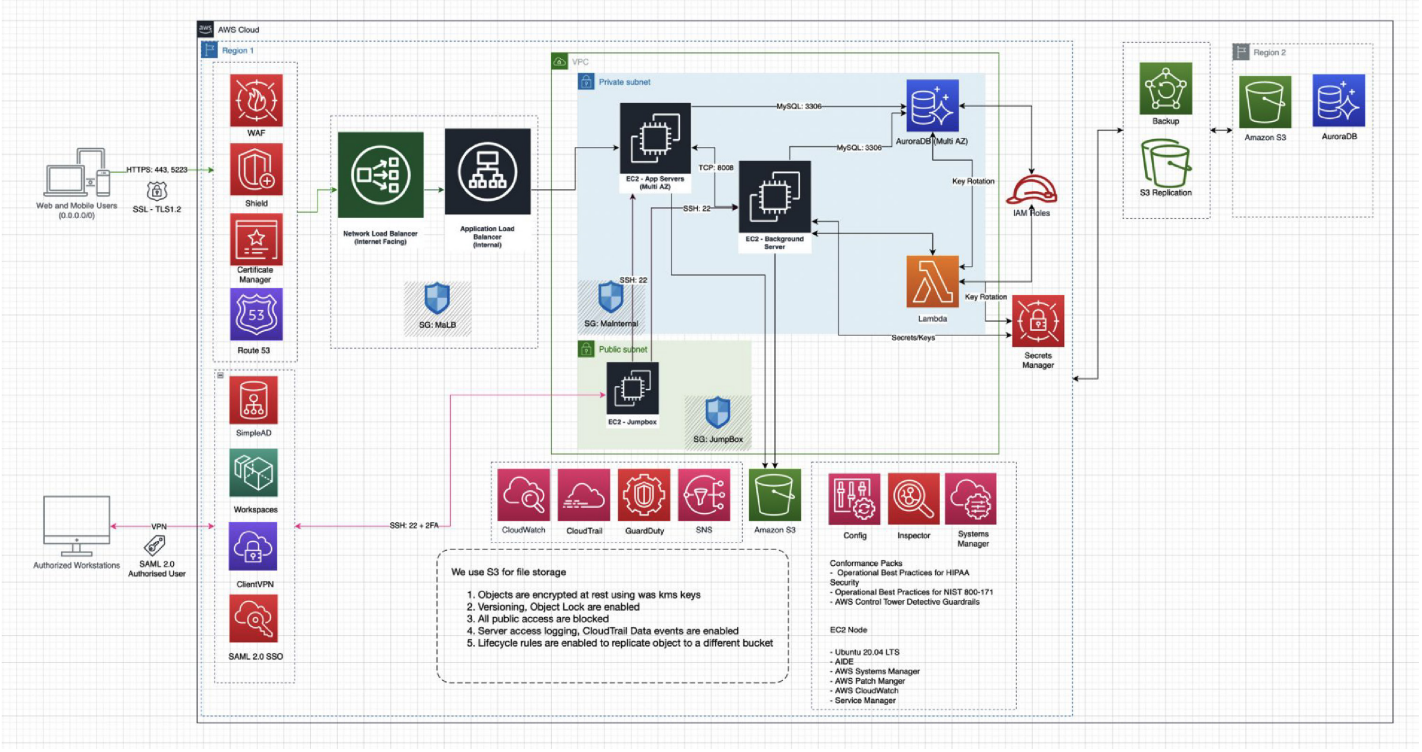
Introduction

At MangoApps, our mission is to help companies create a friction-free, empowered workplace so every employee has an opportunity to produce extraordinary results. For companies, efficiency creates new investment opportunities. For employees, success at work drives happiness and satisfaction. This cycle makes organizations more efficient every day.

We know that intranet & communications are the front doors to your company's data, and we have a special responsibility to keep it safe and secure. We're committed to being transparent about our security practices and helping you understand our approach.

Security Architecture

The reference security diagram below reflects the deployment structure, connections between the components of that structure, and actions undertaken to ensure the security of the service and customer data for MangoApps compliance cloud customers.



Organizational Security

MangoApp's industry-leading security program is based on the concept of defense in depth: securing our organization and your data at every layer. MangoApps is HITRUST CSF and SOC 2 Type II certified. Additionally our security program is GDPR compliant and is aligned with ISO 27001, FISMA, and NIST standards and constantly evolves with updated guidance and new industry best practices.

MangoApps' security team, led by our Chief Information Security Officer (CISO), is responsible for implementing and managing our security program. The CISO is supported by the members of the MangoApps Security Team, who focus on security architecture, product security, security engineering and operations, detection and response, and risk and compliance.

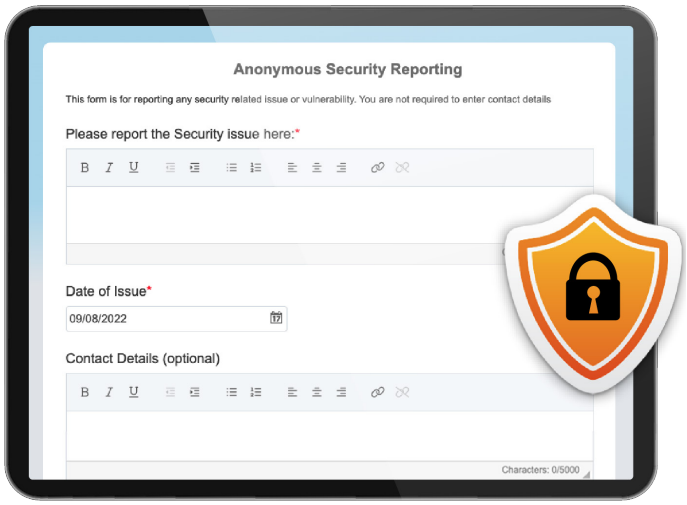
Protecting Customer Data

MangoApps' security program focuses on securing and preventing unauthorized access to customer data. To this end, our team of dedicated security practitioners, working in partnership with peers across the company, take specific steps to identify and mitigate risks, implement best practices, and constantly develop ways to improve.

Secure by Design

MangoApps' product security team has built a robust, secure development lifecycle, which primarily leverages open-sourced tools. The MangoApps security team also does web application scanning & vulnerability testing using Qualys and static code analysis using Brakeman.

While we strive to catch all vulnerabilities in the design and testing phases, we realize that sometimes mistakes happen. With this in mind, we have created a public security reporting program (located here) to facilitate responsible disclosure of potential security vulnerabilities. All identified vulnerabilities are validated for accuracy, triaged, and tracked to resolution.



End-to-End Encryption

Data in Transit

All data transmitted between MangoApps clients and the MangoApps service is done using robust encryption protocols. MangoApps supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.2 protocols, AES256 encryption, and SHA2 signatures. At MangoApps, we use AWS Certificate Manager to automate the deployment & management of SSL/TLS certificates.

Data at Rest

MangoApps has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials. Data at rest in the MangoApps production network is encrypted using FIPS 140-2 compliant encryption standards, which apply to all types of data at rest within MangoApps systems-relational databases, file stores, database backups, etc. All encryption keys are stored in a secure server on a segregated network with limited access.

MangoApps hosts all customer data in our shared infrastructure, logically separated from other customers' data. MangoApps also provides the option of single-tenant deployments where the infrastructure & data is physically separated from other customers' data (e.g., dedicated VPC, Compute, etc.). We use a combination of storage technologies to protect customer data from hardware failures. The MangoApps service is hosted in AWS data centers, offering state-of-the-art physical protection for the servers and infrastructure that comprise the MangoApps operating environment. MangoApps also offers data residency, which allows organizations to choose the country or region their resting data is stored.

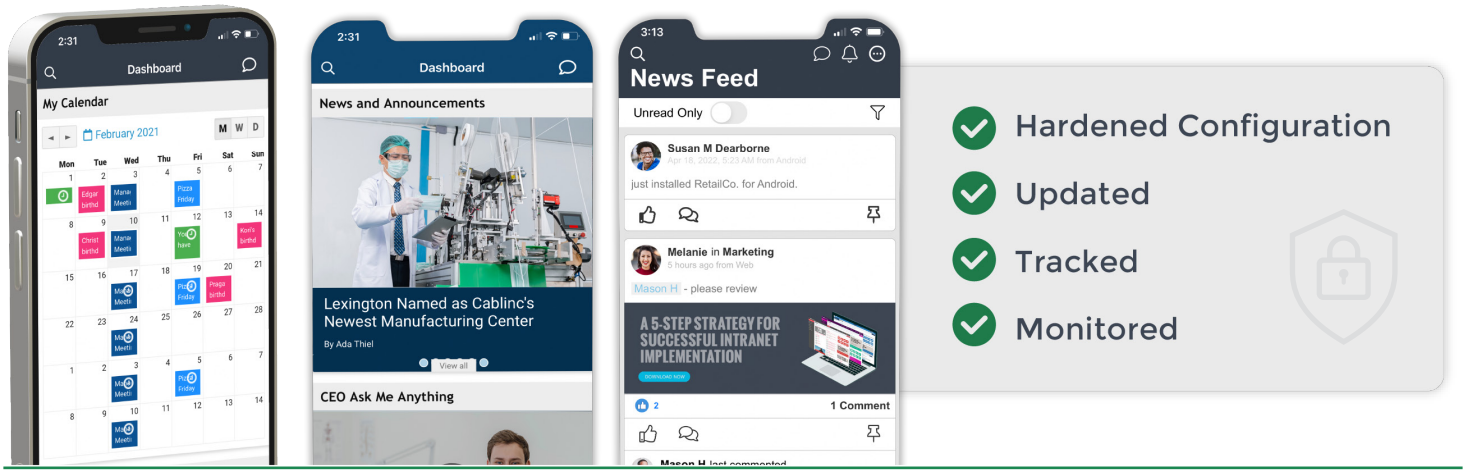
Network Security & Server Hardening

MangoApps segregates its systems into separate networks to protect sensitive data effectively. Systems supporting testing and development activities are hosted in a different network from the production infrastructure. All servers within the production fleet are hardened (e.g., disabling unnecessary ports, removing default passwords, etc.) and have a base configuration image applied to ensure consistency across the environment (using AWS Trusted Advisor & AWS Systems Manager). MangoApps has deployed AIDE (advanced intrusion detection environment) on all production servers to check the integrity of files & directories for enhanced security.

Direct network access to MangoApps production environment from open, public networks (the Internet) is entirely restricted. Only those network protocols essential for delivering MangoApps service to its users are available at the MangoApps perimeter. There are mitigations against distributed denial of service (DDoS) attacks deployed (using AWS shield) at the network perimeter. MangoApps uses intelligent threat detection on all production setups (using AWS GuardDuty). Additionally, for host-based intrusion detection and prevention activities, MangoApps has automated logging, monitoring, and auditing of all system calls (using AWS Inspector) and alerting in place for system calls that indicate a potential intrusion.

Endpoint Security

All workstations issued to MangoApps personnel are configured by MangoApps to comply with our standards-based security framework. These standards require all workstations to be set with hardened configuration, updated, tracked, and monitored by an endpoint management solution (MangoApps uses TrendMicro) with a configuration policy to encrypt data at rest, strong passwords, and lock when idle. Workstations run up-to-date monitoring software to report potential malware, unauthorized software, and mobile storage devices. Mobile devices used to engage in company business are enrolled and managed by MangoApps remote device management app to ensure they meet MangoApps security standards.



SOC 2 TYPE II CERTIFIED | HITRUST CSF Certified | HIPAA COMPLIANT | NIST 800-171 Comliant | aws PARTNER • Public Sector • Healthcare Software Competency

Identity & Access Control

Provisioning

To minimize the risk of data exposure, MangoApps adheres to the principles of least privilege and role-based permissions. Employees are only authorized to access data to fulfill their assigned job responsibilities (using AWS IAM). In addition, all production system access is reviewed every 60 days.

Authentication

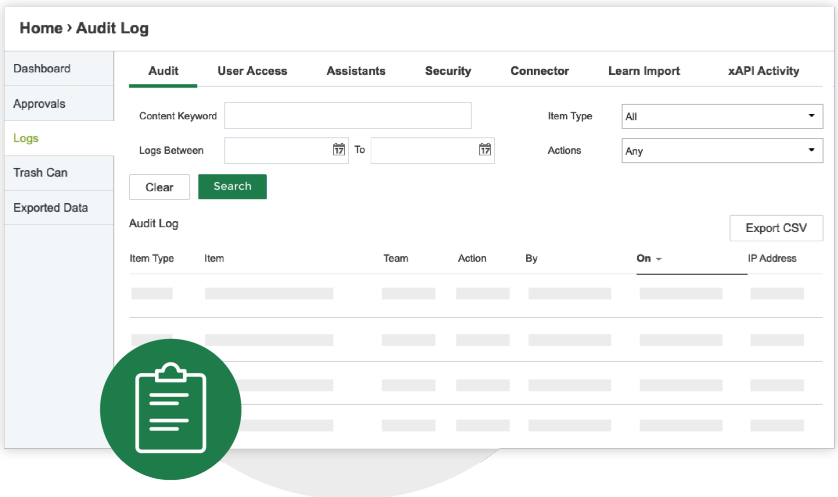
To further reduce the risk of unauthorized access to data, MangoApps deploys multi-factor authentication (MFA) for all access to production environments, which houses customer data. Wherever possible and appropriate, MangoApps uses private keys for authentication, in addition to the previously mentioned multi-factor authentication on a separate device. Additionally, access to production environments is over a secure VPN via a JumpBox only for isolation & network segregation, which is monitored & logged.

Password Management

MangoApps requires personnel to use an approved password manager (1Password). Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks.

System Monitoring, Logging & Alerting

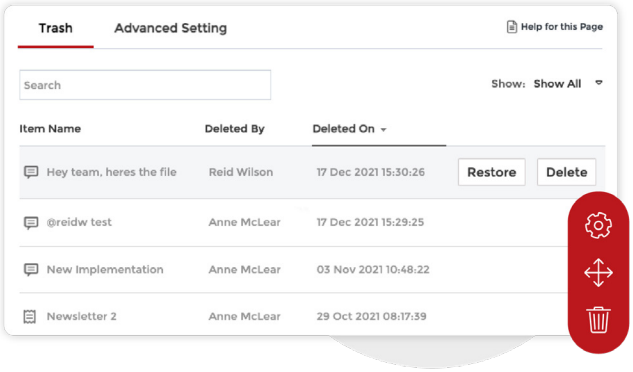
MangoApps monitors servers, workstations, and mobile devices to retain and analyze a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on all servers inMangoApps production networks are logged (using AWS CloudWatch & AWS CloudTrail) and retained. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel. All production logs are stored in a separate network restricted to only the relevant security personnel.



Data Retention & Disposal

Customer data is removed immediately upon deletion by the end-user or upon expiration of message retention as configured by the customer administrator. MangoApps hard deletes all information from currently running production systems, and backups are destroyed within 30 days after termination.

Disaster Recovery & Business Continuity Plan



MangoApps utilizes services deployed by AWS to distribute production operations across multiple availability zones. These availability zones are within one geographic region but protect MangoApps service from loss of connectivity, power infrastructure, and other common location-specific failures. Production transactions are replicated among these discrete operating environments to protect the availability of MangoApps service in a location-specific catastrophic event. MangoApps also retains a full backup copy of production data in a different region significantly distant from the region of the primary operating environment. Full backups are saved to this remote location once per day and transactions. MangoApps tests backups at least quarterly to ensure they can be successfully restored (Using AWS Backup & Restore).

Responding to Security Incidents

All security incidents are managed & responded to by the MangoApps security team. MangoApps has established policies and procedures (that are HITRUST CSF certified) for responding to potential security incidents. The policies & procedures define the types of events that must be managed via the incident response process and classifies them based on severity. MangoApps incident response procedures are tested and updated at least annually. In the event of an incident, affected customers will be contacted by out customer success team via email and their dedicated support channel.

Vendor management

MangoApps' in-house DevOps & Security team manages the entire operations of all the staging & production environments. No external vendor or third party is allowed in our production & testing environments.

Product Security Features

MangoApps includes a robust set of security and data protection product features that give you the control, visibility, and flexibility you need to manage all your security challenges without compromising agility.

Identity & Access Controls

Securing your information starts with identity controls, no matter where your users are located. MangoApps allows you to manage users and groups, streamline authentication using your identity provider, and assign roles and permissions. We give you the solution to ensure that only the right people can access your company's information in MangoApps. MangoApps' critical features in identity & access controls include:

- SAML & OAuth based single sign-on
- Two-factor authentication
- Auto virus scan of documents
- Session duration management
- Custom admin roles
- Custom IP ranges to limit access
- Strong password enforcement
- User and group provisioning via SCIM/JIT

Device Management

MangoApps provides remote device management to give you the solution to ensure that only the proper devices can access your company's information in MangoApps. MangoApps' key features in device management include:

- Remote mobile device management (device wipe out, retire)
- Mobile PIN & face identification
- Minimum app version
- Mobile app deep linking
- Automatic file compression
- Self destruct messages
- Lockdown android app (integrated with BlueFetch)
- Microsoft Intune protection policies ready

Data Protection

MangoApps encrypts data at rest and in transit as part of our foundational security controls. We also provide tools that give you even further visibility and control. MangoApps' key features in data protection include:

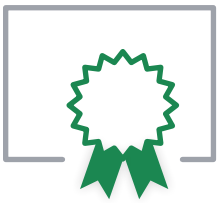
- Data Loss Prevention (DLP)
- Virus scan & quarantine of infected files
- Audit & user access logs
- Security alerts
- Network trash can

Information Governance

Every company needs an ongoing strategy to reduce the risk of compromised data, and there's no one-size-fits-all approach. MangoApps offers governance and risk-management capabilities that are flexible enough to meet your organization's needs, no matter what they are. MangoApps' key features in information governance include:

- Data retention policies
- eDiscovery / Legal Holds
- Data exports
- Custom terms of service (TOS)

Compliance Certification & Attestations



External / 3rd Party Compliance Certification

MangoApps compliance cloud is HITRUST CSF v9.3 certified and SOC 2 Type II certified. MangoApps also has received 3rd party attestation for following the NIST cybersecurity framework. MangoApps is hosted on the AWS cloud, so it inherits AWS security & compliances like FedRAMP and others. Additionally, MangoApps is an AWS partner that has received AWS healthcare competency attestation.

External / 3rd Party Penetration Testing

In addition to our compliance audits, MangoApps engages independent entities to conduct application-level and network-level penetration tests annually. Results of these tests are shared with senior management and are triaged, prioritized, and remediated promptly. Customers may receive executive summaries of these activities by requesting them from their designated MangoApps contacts.

Customer-Driven Audit & Penetration

Our customers are welcome to perform either security controls assessments or penetration testing on the MangoApps environment. Please contact your designated technical account manager (TAM) to learn about options for scheduling either of these activities.

Conclusion

At MangoApps, protecting our customer's data is our first priority. Every person, team, and organization expects their data to be secure and confidential. Safeguarding this data is critical. Contact us if you have questions or concerns.

HITRUST
6175 Main Street
Suite 400
Frisco, TX 75034

July 8, 2022

Mangoapps, Inc.
1495 11th Avenue NW.
Issaquah, WA 98027

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an Authorized External Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST® Assurance Program requirements, the following platform, facility, and supporting infrastructure of the Organization ("Scope") meets the HITRUST CSF® v9.3 Risk-based, 2-year (r2) certification criteria:

Platform:
- Compliance cloud MangoApps SaaS residing at Amazon Web Services (AWS)

Facility:
- AWS (Data Center) managed by Amazon Web Services located in Unknown, East Virginia, United States of America

The certification is valid for a period of two years assuming the following occurs. If any of these criteria are not met, HITRUST will perform an investigation to determine ongoing validity of the certification and reserves the right to revoke the Organization's certification.

- No data security breach reportable to a federal or state agency by law or regulation has occurred within or affecting the assessed environment,
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST Risk-based, 2-year (r2) certification criteria, and
- Timely completion of the HITRUST Interim Assessment for r2 Certification as defined in the HITRUST Assurance Program Requirements.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information protection. With input from leading organizations, HITRUST identified a subset of the HITRUST CSF controls that an organization must meet to be HITRUST Risk-based, 2-year (r2) Certified.

HITRUST performed a quality assurance review to ensure that the control maturity scores were consistent with the results of testingperformed by the Authorized External Assessor. Users of this letter can refer to the document Leveraging HITRUST Assessment Reports: A Guide for New Users for questions on interpreting this letter and can contact HITRUST customer support at support@hitrustalliance.net. Users of this letter are assumed to be familiar with and understand the services providedby the organization listed above, and what specific services are being used by the user organization.

A version of this letter with a more detailed scope description has also been issued by HITRUST which can also be requested from the organization listedabove directly. A full HITRUST Validated Assessment Report has also been issued by HITRUST which can also be requested from the organization listed above directly. Additional information on the HITRUST Assurance Program can be found at the HITRUST website which can also be requested from the organization listedabove directly. A full HITRUST at https://hitrustalliance.net.

HITRUST

HITRUST

MangoApps Compliance Cloud US

SOC 2 TYPE II REPORT

An Independent Service Auditor's Report has been issued after completion of SSAE18, SOC 2 Type II Audit throughout the audit period
June 1st, 2023 - October 31st, 2023

DIWAKAR KAMATH

DIWAKAR KAMATH,
CERTIFIED PUBLIC ACCOUNTANT
AICPA # 98033086

ACCORIAN ASSURANCE

December 4th,2023

*** Valid till December 2024**

GLO CERT ™

CERTIFICATE

The Independent Conformity Assessment Body Glocert International Certifications (UK) Limited

certifies that the "Information Security Management System" of

MangoApps, Inc.

1495 11th Ave NW,
Issaquah, WA 98027,
United States Of America

"has been assessed, registered and found to conform the requirements of

ISO/IEC 27001:2022

(Information Security Management Systems Standards Requirements)

applicable to the scope of:

MangoApps Information Security Management System (ISMS as ISO/IEC 27001:2022) applies to MangoApps covering the departments – Product Engineering, Security and Compliance, Human Resources, and DevOps at MangoApps Headquarters.

Statement of Applicability (SoA), Document Version No, 1.0, Dated 03rd May 2023

Initial Certification Date
07/08/2023
1st Surveillance due before
07/08/2024

This certificate is valid till
06/08/2026
2nd Surveillance due before
07/08/2025

Global Business Manager
Glocert International Certifications (UK) Limited,
Crown House, 27, Old Gloucester Street,
London, WC1N 3AX, England and Wales,
United Kingdom

Certificate No.
23ISMS-1026

Issue Date
07/08/2023

GLO CERT ™
MSCB 273

IAS ACCREDITED
Management Systems Certification Body

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF