SOTA Cloud Security Overview

Contents

Scope

This document describes at a high level the controls that exist to ensure SOTA Cloud Imaging application security. This document is not an intensive or technical summary of all security protections in place, but rather a high-level description of the basic features of the security apparatus.

sotaCLOUD

Introduction

SOTA Cloud Imaging follows industry best practices to ensure that SOTA Cloud Imaging remains secure post-deployment. This document describes at a high level what steps are taken to protect the SOTA Cloud Imaging servers and application executables, runtime environment, resources, assets, and data. The steps taken to ensure application security during and after deployment are summarized according to the sections presented in Section 5 of the FDA guidance document entitled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff."

Protective Controls

This section provides a high-level summarized list of protective controls that ensure system integrity post-deployment.

Identify and Protect - Limit Access to Trusted Users Only

HTTPS using Secure TLS/SSL Signing Certificates

All customer facing endpoints are encrypted using secure, signed TLS/SSL encryption.

Insecure Protocols

HTTPS is enforced on all endpoints. All non-secure connections are rejected by the server. Insecure/outdated protocols are also rejected automatically, including TLS 1.0/1.1.

Static IP Restrictions on Application Resources

The only machines authorized to access resource storage infrastructure directly are IP addresses under SOTA Imaging control. All other IP addresses are rejected automatically from accessing database or file storage resources directly.

Stateless, Containerized Backend

The application backend is designed around the use of stateless containers. Stateless containers do not make use of local storage, can be completely erased and re-provisioned with updated or known-good binaries almost instantly, and provide robust protection against DDoS and other attacks due to their distributed nature. Finally, because they do not make use of local storage, they may be configured as read-only, making malware attacks far more difficult to carry out.

Authentication and Authorization, Multi-Factor Authentication

All connections to the application must be both authenticated and authorized. In other words, for any machines or users to access the system and its resources, they must first provide proof that they are an authorized entity.

The authentication and authorization systems used by SOTA Cloud Imaging are state of the art and implement controls ranging from available adaptive multi-factor authentication to bot detection, brute force prevention, and suspicious IP detection. Password requirements, timeouts, expiration dates, and more are available for customers to customize according to the needs of their organization.

In-Azure Resources

All resources are hosted on Microsoft Azure, renowned as one of the most secure hosting services available. Because all resources are stored within the Microsoft Azure network, the connections between the back-end server containers, database servers, and storage servers cross no network boundaries. In other words, in addition to SOTA Imaging's security protocols, SOTA Cloud Imaging inherits and leverages the security infrastructure of the Microsoft Azure ecosystem.

Application Secrets

All resource keys that are used to access back-end resources are secured independently of the system, ensuring that they cannot be accessed even if an attacker gains access to application source code or documentation.

Layered User Roles and Permissions

Customer Facing

Users may be assigned specific roles or permissions which restrict their access to the application to what is necessary to perform their role or function within the customer's organization.

SOTA Imaging Employees

SOTA Imaging employees are assigned permission to access areas of the system and administration dashboards within Azure only in accordance with their role.

Rigorous Administrative Access Rules

SOTA Imaging employees must use multi-factor authentication, including hardware/physical 2FA tokens, to access sensitive system resources. In addition, activities that could impact the performance and security of the system require users to re-authenticate.

Automatic Session Timeout

Users are automatically signed out from their application sessions due to inactivity.

Identify and Protect - Ensure Trusted Content

Code Versioning, Signing, and Authentication

All code deployed by SOTA Imaging is versioned, signed, and authenticated.

Secure Deployment

Code delivery to CI/CD systems is encrypted.

Secure Access

When a customer's workstation accesses the application and downloads resources, all communication is encrypted.

Detect, Respond, Recover

System Monitoring

System monitoring happens 24/7 through Azure Application Insights. SOTA Imaging has developed a proprietary dashboard and notification triggers for anomalous system events, ensuring the appropriate people within the company are notified if an attack or system degradation status is detected.

System Audit Logging

SOTA Cloud Imaging makes use of four levels of audit logging:

Authentication Logging

Authentication related activity for all users (both SOTA Imaging and customers) are logged including timestamps, actions taken, and risk profile.

Application Logging
The activity of all users is logged to an application audit log (including action taken and timestamp) to ensure traceability of any suspicious activity to a particular source or account.

Administrative Logging
All administrative actions are logged within Azure (including action taken, timestamp, and risk profile) to ensure traceability of any suspicious activity to a particular source or account.

API Integration Logging
All API use is logged (including action taken, timestamp, and risk profile) to ensure traceability of any suspicious activity to a particular source or account.

System Redundancy

SOTA Imaging has several layers of protection in place to ensure the system will remain available even in the event of a security breach or regional datacenter failure. This includes multi-region system redundancy.

System Backups

In the event of data corruption or data loss, data may be restored from historical backups. Backups are made for the entire system at several time intervals and the backup data is securely isolated from the rest of the system. Backups are distributed across multiple datacenters in different regions within the United States.

User Management and Permissions

User Roles

SOTA Cloud uses a role-based permissions system to control access to patients and sensitive settings within the SOTA Cloud service. The roles are as follows:

Role	Create Users	Edit Users	Create Patients	Edit Patients	View Patients	Billing Info	Analytics
Global Administrator	Can create users in any practice	Can edit users in any practice	Can create patients in any practice	Can edit patients in any practice	Can view patients in any practice	Can view and update billing information	Can access analytics for all practices
Administrator	Can create users in own practice	Can edit users in own practice	Can create patients in own practice	Can edit patients in own practice	Can view patients in own practice	No access	Can view analytics for own practice
User	No access	Can only edit their own account	Can create patients in own practice	Can edit patients in own practice	Can view patients in own practice	No access	No access
Limited User*	No access	No access	Can only create patients when bridged from practice management and patient does not already exist	Can only update patients when done through the PMS bridge	Cannot search, can only view patients when bridged from PMS	No access	No access

*Limited user is a good choice for IT teams that want to primarily enforce restrictions through the PMS system. Limited users can only access patients when bridged from the PMS.

User Password Requirements

By default the password requirements in SOTA Cloud are as follows:

- Minimum length 8 characters, maximum 256 characters
- Uppercase and lowercase characters required
- Numbers required
- Special characters NOT required

New password cannot be the same as the last used password The user's login will be locked for 3 minutes after 10 failed login attempts within 60 minutes. Tokens are valid for up to 10 hours.

These settings can be changed for a nominal one-time fee, contact your sales representative for information.

User Two-Factor Authentication

Two factor authentication is available. SMS and time-based Authenticator applications (such as Google Authenticator) are supported.

Single Sign On

Single Sign On is supported for enterprise customers. A variety of options including SAML v2, OpenId Connect, and Federated login are available.

SSO configuration requires payment of a one time fee. Contact your sales representative for information.

Third Party Integrations and APIs

SOTA Cloud supports a variety of third party integrations, and robust APIs are available for enterprise customers. All third party integrations authenticate using OAuth 2.0, the industry standard for secure communication between applications.

Contact your sales representative for information.