CASENGINE

Cloud Application Security

OVERVIEW

Casengine is a web-based software application package that can be accessed through the web browser. The software and database reside on a central server rather than being installed on the desktop system and is accessed over a network. With a computer connected to the network, a web browser and the right user-name and password you can access the systems from any location in your network with no further configuration on client Pc or Laptops. Web-based applications are easy to use and can be implemented without interrupting your existing work process. The Application Relies on Stable Application such as Microsoft ASP.net and MS SQL

Application Security and infrastructure Security

Casengine System adheres to the security standard and has implemented solutions to secure Web Application Security Risks identified in OWASP Top 10. Secure HTML sanitization to avoid malicious inputs. As the system support uploading file on almost each page, a secured process or validating the uploaded file is implemented which checks the extension, magic number and content type of the file and only processes the allowed type of files. We perform frequent Vulnerability tests and Penetration test to ensure the Application security.

We have implemented automated and custom checks to apply security patches using Azure automation services to protect from common vulnerabilities and other known security threats.

Authentication Module	-Only users who are Authenticated are allowed to use the application -To prevent a user id and/or password from being hacked, failed logins will trigger a lock-out after a determined number of attempts -Strong password rules should be applied. -Email Based OTP
Authorization and Access Control	-The user will not be able to access an unauthorized page by entering the location into the URL (DFA) -Users are allowed access only based on the roles.
Session Management	Session token stored once user successfully authenticated in Encrypted cookie We use token-based authentication for each session and without active token no page is accessible
Cross Site Scripting (XSS) and CSRF	Anti XSS is implemented and measures are implemented to prevent Cross-Site Request Forgery (CSRF) attack

SQL injection Protection	Methods are implemented in the application to prevent SQL injection
Input sanitization	Security feature is implemented on input fields to prevent XSS
Upload sanitization	Uploads are tested for Valid content type on server side and Direct File access is denied. Only authorized users are allowed to access contents
Error Handling, Logs and Alerts	Custom Error pages are maintained, All Events are Logged in Detail with Include time and date, user id, error code and Application is integrated with a syslog server for Alerts
Administration by Codengines	RDP protocol is Disabled by Default to the Application server. And is allowed on demand via a Gateway VM for Administration Controlled and protected by authorization, authentication and MFA Authorized users are protected by endpoint protections and Microsoft intunes.
Secure IIS Configuration	SSL enabled – Only secure https traffic. SSL can provide authentication, confidentiality, and integrity for data as it is transported to and from web services HTTP Headers – Will be securely configured Such as Content Security Policy, X-Frame-Options, Referrer-Policy, cache-control Session Timeout is configured.
Secure Server Configuration	Secure policies are applied to the server. Best Practices Cipher Suites are applied Antivirus solution.
Encryption	We encrypt data both at-rest and in-transit using 256-bit AES encryption for SSL/TLS web traffic and 2048-bit RSA public keys A Combination of Application-level encryption and Hosting solution-based encryption is used to protect Data at rest to prevent Data Leak User Authentication such as passwords are stored always encrypted.
Firewall	Only port 443 is exposed to the clients. Network security group (NSG) is configured to restrict to allow only port 443

Hosting

We use Microsoft Azure cloud as data centers which are SOC2 certified, and employ the strictest physical and logical security— If you'd like to learn more about the security practices of our hosting providers, please refer to the following links:

https://docs.microsoft.com/en-us/azure/compliance/

Casengine infrastructure

Casengine is hosted on multiple nodes for availability (windows based virtual machines) in a multi-tenant model where tenants share the same compute.

IAAS Shared responsibility

https://azure.microsoft.com/mediahandler/files/resourcefiles/shared-responsibility-for-cloud-computing/Shared%20Responsibility%20for%20Cloud%20Computing-2019-10-25.pdf

Data Security

Unique databases are provisioned for each tenant for segregation of Data. Documents and files are stored in Azure file share logically separated at folder level access via file API server.

We encrypt data both at-rest and in-transit using 256-bit AES encryption for SSL/TLS web traffic and 2048-bit RSA public keys.

Software Development

We embed security best practices into every step of our development lifecycle. These practices include, but are not limited to, manual and automated code reviews and internal compliance scans.

Backup Strategy

We are using Azure Backups for our Backup requirements

Backup Policy:

Daily Backup taken for 7 Day(s)
Weekly Backup taken retained for 4 Week(s)
Monthly Backup taken retained for 3 Month(s)
