MITRATECH

Architecture, Security, Compliance & Data Policies

Architecture

CaseCloud™ is built on and runs on the Salesforce platform, which is known for its industry-leading Platform-As-A-Service capabilities. This provides best-in-class technology infrastructure for security, reliability, and performance. To that end, it is a platform for “out-of-the-box” reporting, analytics, mobile access, integrations, and a modern ecosystem of add-on/downloadable capabilities.

CaseCloud™ on the Salesforce platform supports the ability to encrypt client data and make it available without inadvertently accessing another client's data. The architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions (e.g., testing and production).

Data Center Infrastructure

All CaseCloud™ client data is managed through a world-class data center infrastructure. Each customer's solution is hosted from a primary and secondary production data center, with near real-time replication occurring between the two sites. A given customer's data will be stored in 2 of these co-located data centers, with one acting as the primary location and the other as the fully redundant secondary site. Customers will be primarily hosted from a production instance hosted in a data center within the region where the customer is based. We technically cannot restrict the location where customer data is stored, but customers do have a choice in deciding where they want their data to reside. Data centers for government agencies will be located within the U.S.

All data centers provide only power, environmental controls, and physical security. Salesforce employees manage all other aspects of the service at the data centers. Co-location data center personnel do not have a network or logon access to the systems.

MITRATECH
Empower. Automate. Elevate.

Security, Compliance & Auditing

CaseCloud™ automatically inherits all security, compliance, and auditing protocols established by Salesforce. Independent audits confirm security design and features (see Compliance Certifications Section). Using the latest firewall protection, intrusion detection systems, and TLS encryption – CaseCloud™ gives you the peace of mind only a world-class security infrastructure can provide.

CaseCloud™ does not have access to any customer data, unless the customer specifically gives us user access to assist with questions, etc.

PROTECTION AT THE APPLICATION LEVEL

Client administrators assign data security rules that determine which data users can access and how this data can be accessed. Sharing models define company-wide defaults and data access based on a role hierarchy.

Security can be applied at the:

- Record level – which matters, documents, and other records a user can access and how these can be accessed.
- Screen level – which screens or data on a record can be accessed and how these can be accessed.
- Field level – which fields on a matter or other type of record a user can access and how these can be accessed.

All data is encrypted in transfer. Data can be encrypted at rest using the Salesforce Shield Feature (add-on feature). All-access is governed by strict password security policies. Multi-factor authentication can be enabled for additional security. Passwords are hashed with a per-user salt, using PBKDF2. Applications are continually monitored for security violation attempts. System activities and events are logged, and audit logs can be reviewed or exported as needed

PROTECTION AT THE NETWORK LEVEL

Multi-level security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only HTTP and HTTPS traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.

PROTECTION AT THE FACILITIES LEVEL

Security standards are on par with the best civilian data centers in the world, including the world's most security-conscious financial institutions. Authorized personnel must pass through multiple levels of two-factor authentication (including biometrics) to reach the dedicated space with systems hosting client data. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. No media containing client data leaves the data center.

THIRD-PARTY VALIDATION

Security is a multi-dimensional business imperative that demands consideration at every level, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, third-party certification is continually obtained, including ISO 27001, PCI-DSS, FedRAMP, and SOC 1 (SSAE 18) and SOC 2 Type II audits. Third parties also conduct periodic vulnerability scans and penetration testing.

MITRATECH
Empower. Automate. Elevate.

COMPLIANCE CERTIFICATIONS

CaseCloud™ inherits all Salesforce compliance certifications, and meets all compliance standards and regulations – including:

- ISO 27001
- ISO 27017
- ISO 27018
- HIPAA
- C5 (ISAE 3000)
- DoD IL2
- DoD IL4
- FedRAMP
- GDPR

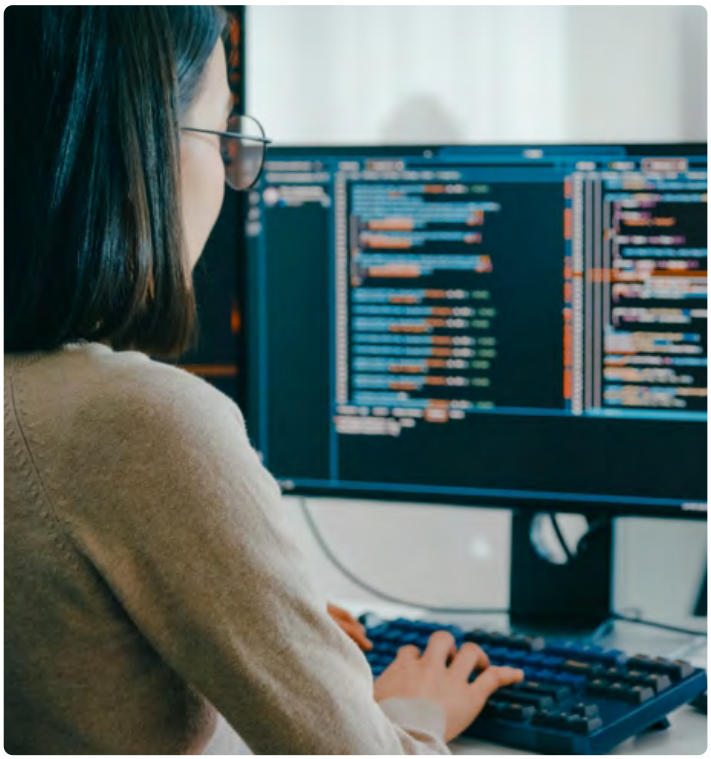
CJIS COMPLIANCE

To support the advanced security and compliance needs of our U.S. public sector customers, the Salesforce platform uses the CJIS-compliant infrastructure provided by Amazon Web Services, Inc. ("AWS"). AWS enables clients to exercise exclusive control over where data is stored – and the methods used to secure data in transit and at rest – through the AWS Key Management Service and AWS Nitro System. AWS Key Management Service uses hardware security modules validated under FIPS 140-2 and enables clients to create, own and manage their own master keys for all encryption. These master keys never leave the AWS FIPS-validated hardware security modules unencrypted and are never known to AWS personnel.

The AWS Nitro System uses purpose-built hardware and servers designed specifically to run a virtual compute hypervisor—nothing more – removing all extra and unnecessary ports, components and capabilities found on traditional servers. The AWS Nitro System's security model is locked down and prohibits administrative access, eliminating the possibility of human error and tampering. Clients can also choose AWS Nitro Enclaves if they require a security model that includes no persistent storage, no interactive access and no external networking to create isolated compute environments to further protect and securely process highly sensitive data.

MITRATECH
Empower. Automate. Elevate.

Data Backup & Disaster Recovery



DATA BACKUP

At any given time, your CaseCloud™ instance is actively served from one location with transactions replicated in near real-time to a completely redundant and geographically diverse secondary location. Each location can be considered a complete backup (files and data) of the other. This approach supports Salesforce's ability to provide a seamless customer experience while working on site maintenance, compliance, and disaster recovery items.

We also strongly recommend that clients regularly back up their own files and data to their own server or other location to address other potential issues such as accidental client user data deletion, a need to roll back to a particular point in time due to a third-party software update or custom coding issue the client is trying to address, etc. Clients can choose to set up a completely automated process for periodic data backups through third-party apps or scripts. There is also a defined process for a client's system administrator to set a schedule for automatically copying all files and data for backup purposes to a zip file that can be saved to a hard drive, server, etc. Clients can choose a full backup and/or a backup of certain objects with associated files. The schedule can be set for as often as once a week. Each table that is copied is saved in a separate .csv file., server, etc. Clients can choose a full backup and/or a backup of certain objects with associated files. The schedule can be set for as often as once a week. Each table that is copied is saved in a separate .csv file.

DISASTER RECOVERY

CaseCloud™ automatically inherits all the disaster recovery protocols established by Salesforce. Salesforce has developed a global Business Continuity and Disaster Recovery Program hired Certified Business Continuity Planners ("CBCP") and retained the services of leading consultants to assist in the ongoing development of Business Continuity and Disaster Recovery plans and procedures. This program is overseen by senior management for each of the key functional areas within Salesforce and is supported by executive leadership at the highest level.

A global Crisis Management Team ("CMT") comprised of select executives from key departments manages this process. The CMT is mobilized when a crisis or significant event occurs and is responsible for evaluating the situation and responding accordingly. Depending on the severity and nature of an incident, the CMT Leader may request engagement from various support teams to assist with the mitigation of the incident. The CMT meets periodically for training, education, and review of the documented CMT Action Guide, or as required due to a

crisis or significant event. CMT members have specified roles and responsibilities and are available 24/7/365. The CMT conducts table-top exercises, at a minimum of once annually.

Salesforce maintains a Mirror Site that is a 100% staged warm site with block-level data replication. The secondary data center is replicated at 100% of the capacity (host, network, and storage) of the Production data center. As part of developing a viable Disaster Recovery plan and program, Salesforce schedules Disaster Recovery exercises which are conducted several times per year.

Additionally, disaster communication processes are exercised using the mass notification system during each exercise, which includes call-outs with response requests to the Crisis Management Team and the Production Disaster Recovery Teams. The disaster recovery plan is tested at a minimum on an annual basis and will continue to enhance and develop processes and technology related to disaster recovery to further reduce RPOs and RTOs. Additional procedures, processes, and plans have been developed, including a Pandemic plan. The DR/BCP Plan Summary and recent DR postmortem can be provided to customers under NDA/MSA upon request.

ABOUT MITRATECH CASECLOUD™

CaseCloud™®, is a leading enterprise legal management solution that helps law firms and general counsel automate unique business processes and simplify legal matter management. The CaseCloud™ cloud-based enterprise solution centralizes matter management, conforms to unique workflows and practice standards, and provides industry leading security and reliability. Built on the leading cloud platform, Salesforce® and Mitratech, CaseCloud™ offers comprehensive configuration and integration with thousands of add-on applications to extend the solution to meet specific business needs.