CloudFin

Security, Privacy and Architecture of CloudFin, CloudFin True Capture and CloudFin Framework Processing

CloudFin’s Customer Commitment

CloudFin is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that considers data protection matters across our line of products and services, including data submitted by customers to our services (“Customer Data”).

Services Covered

This documentation describes the architecture of, the security- and privacy-related audits, and the administrative, technical and physical controls applicable to, the services branded as CloudFin, CloudFin True Capture and CloudFin Framework Processing.

This documentation does not apply to other CloudFin services that may be associated with or integrate with the Covered Services, such as CloudFin Connector.

Architecture and Data Segregation

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides a different physical data separation for different customers via separated data physical files, customer-specific "IDs" and allows the use of subscription, project-customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing (sandbox) and demo. The specific infrastructure used to host Customer Data is described in the “Infrastructure and Sub-processors” documentation.

Certain customers may have the option to subscribe to Covered Services hosted on the infrastructure of a public cloud provider (“Public Cloud Infrastructure”). This infrastructure is described in the “Infrastructure and Sub-processors” documentation. For customers who elect Public Cloud Infrastructure, this will mean the underlying physical infrastructure on which your Customer Data is stored will be with a public cloud provider for what is commonly referred to as “Infrastructure as a Service” and/or Platform as a Service, and the Covered Services will run on top of the public cloud provider. Unless otherwise noted in this documentation, customers who choose Public Cloud Infrastructure will receive the same services, software functionality and operational processes as described here.

Control of Processing

CloudFin has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by CloudFin and its sub-processors. Compliance with such obligations as well as the technical and organizational data security measures implemented by CloudFin and its sub-processors are subject to regular audits. The “Infrastructure and Sub-processors” documentation describes the sub-processors and certain other entities material to Salesforce’s provision of the Covered Services.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to the Covered Services.

● **Rules for Processors**: Customer Data submitted to the services branded as CloudFin, CloudFin True Capture and CloudFin Framework Processing is within the scope of the CloudFin Rules for Processors (except when hosted on the Public Cloud Infrastructure). The most current version of the CloudFin Rules for Processors is available on CloudFin's website, currently located at https://www.cloudf.in.

● **ISO 27001/27017/27018 compliance**: CloudFin's efforts are scoped in operating aligned with the ISO 27001, ISO 27017 and ISO 27018 international standards.

Additionally, the Covered Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

Security Controls

The Covered Services include a variety of configurable security controls that allow customers to tailor the security of the Covered Services for their own use.

Security Policies and Procedures

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

● Customer passwords are stored using a one-way salted hash.

● User access log entries will be maintained, containing date, time, user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted).

● If there is suspicion of inappropriate access, CloudFin can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis.

● Data center physical access logs and system infrastructure logs, are logged, kept and maintain in Microsoft Azure Datacenter and are according to its standards.

● Passwords are not logged.

● Certain administrative changes to the Covered Services (such as password changes and adding custom fields) are tracked in logs.

● CloudFin personnel will not and cannot set a defined password for a user. Passwords resets are executed through a limited time access URL and delivered automatically via email to the requesting user.

Intrusion Detection

CloudFin, or an authorized third party, will monitor the Covered Services for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. CloudFin and/or Microsoft Azure may analyze data collected by user's web browsers for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

Security Logs

All systems used in the provision of the Covered Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

CloudFin notifies impacted customers for security incidents without undue delay of any unauthorized disclosure of their respective Customer Data by CloudFin or its agents of which CloudFin becomes aware to the extent permitted by law. CloudFin typically notifies customers of significant system incidents by email, and for incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and CloudFin's response.

User Authentication

Access to Covered Services requires authentication via one of the supported mechanisms as described in the CloudFin Guide, including user ID/password, SAML based Federation, OAuth, Social Login, or Delegated Authentication as determined and controlled by the customer. Following successful authentication, an encrypted random session ID is generated and stored in the user's browser to preserve and track session state. Additionally for every project session, CloudFin will create an additional unique hashed user-project-session token. Every user must showcase both Authentication and user-project-session tokens in order to be able to operate the software. Should any of those tokens is missing, user must re-authenticate.

Physical Security

CloudFin services are operated end-to-end through Microsoft Azure PaaS. CloudFin applications are operated through Microsoft Azure webapps and Microsoft Azure SQL is used for storage. Microsoft Azure data centers used to provide the Covered Services have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

Reliability and Backup

All networking components, network accelerators, load balancers, Web servers, Database servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Covered Services is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the Covered Services is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Covered Services, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and backed up to localized data stores. Backups are verified for integrity and stored in the same data centers as their instance.

Disaster Recovery

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance up to 99,99%. The Covered Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Microsoft Azure production facilities at the primary data centers were to be rendered unavailable.

Microsoft Azure has disaster recovery plans in place and tests them at according to their standards.

Viruses

The Covered Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Covered Services by a customer. Uploaded attachments, however, are not executed in the Covered Services and therefore will not damage or compromise the Covered Services by virtue of containing a virus.

Data Encryption

The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128 bit symmetric encryption keys at a minimum. Additionally, all data, including Customer Data, is transmitted between data centers for replication purposes across a dedicated, encrypted link utilizing AES-256 encryption.

Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Covered Services (to the extent such data has not been deleted by Customer). CloudFin shall provide such Customer Data via a downloadable file in comma separated value (.csv) format and attachments in their native format.

Deletion of Customer Data

After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days.

Sensitive Data

Important: Customers must not submit the following types of sensitive personal data such as: information related to an individual’s physical or mental health; and information related to the provision or payment of health care.

For clarity, the foregoing restrictions do not apply to financial information provided to CloudFin for the purposes of checking the financial qualifications of, and collecting payments from, its customers.

Analytics

CloudFin LTD may track and analyze the usage of the Covered Services for purposes of security and helping CloudFin improve both the Covered Services and the user experience in using the Covered Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

CloudFin LTD may share anonymous usage data with CloudFin’s service providers for the purpose of helping CloudFin in such tracking, analysis and improvements. Additionally, CloudFin may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show percent of success trends about the scanning mechanism.

Interoperation with Other Services

The Covered Services may interoperate or integrate with other services provided by CloudFin LTD or third parties. Security, Privacy and Architecture documentation for services provided by CloudFin is available at https://Cloudf.in . CloudFin LTD also provides a variety of platforms and features that allow

CloudFin users to learn about CloudFin products, connect third party applications, and participate in pilots, testing and assessments, which are outside the scope of this documentation. CloudFin may communicate with users that participate in such platforms and features in a manner consistent with our Privacy Statement. Additionally, CloudFin may contact users to provide transactional information about the Covered Services; for instance, through system-generated messages, such as notifications. CloudFin LTD offers customers and users the ability to deactivate or opt out of receiving such messages.