Front

Security and Compliance Handbook

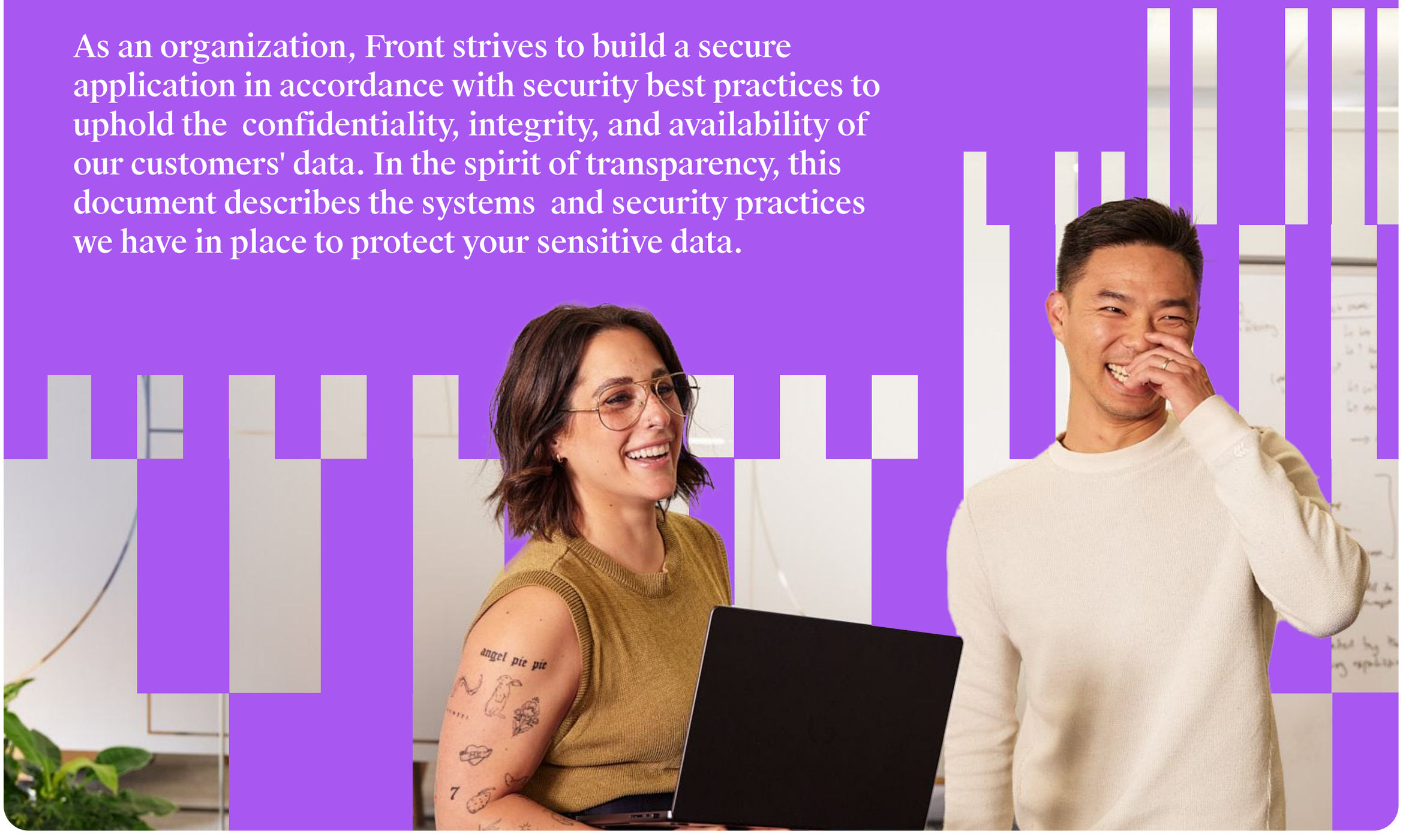
Introducing Front

Front is the modern customer service platform that helps companies delight their customers, engage their teams, and build stronger businesses. We've reimagined the help desk for real-time team collaboration across every customer communication channel, then powered it up with AI and automation to resolve issues and help teams work faster. Today, over 8,000 customers trust Front to protect their most sensitive assets.

Front's Commitment to Security

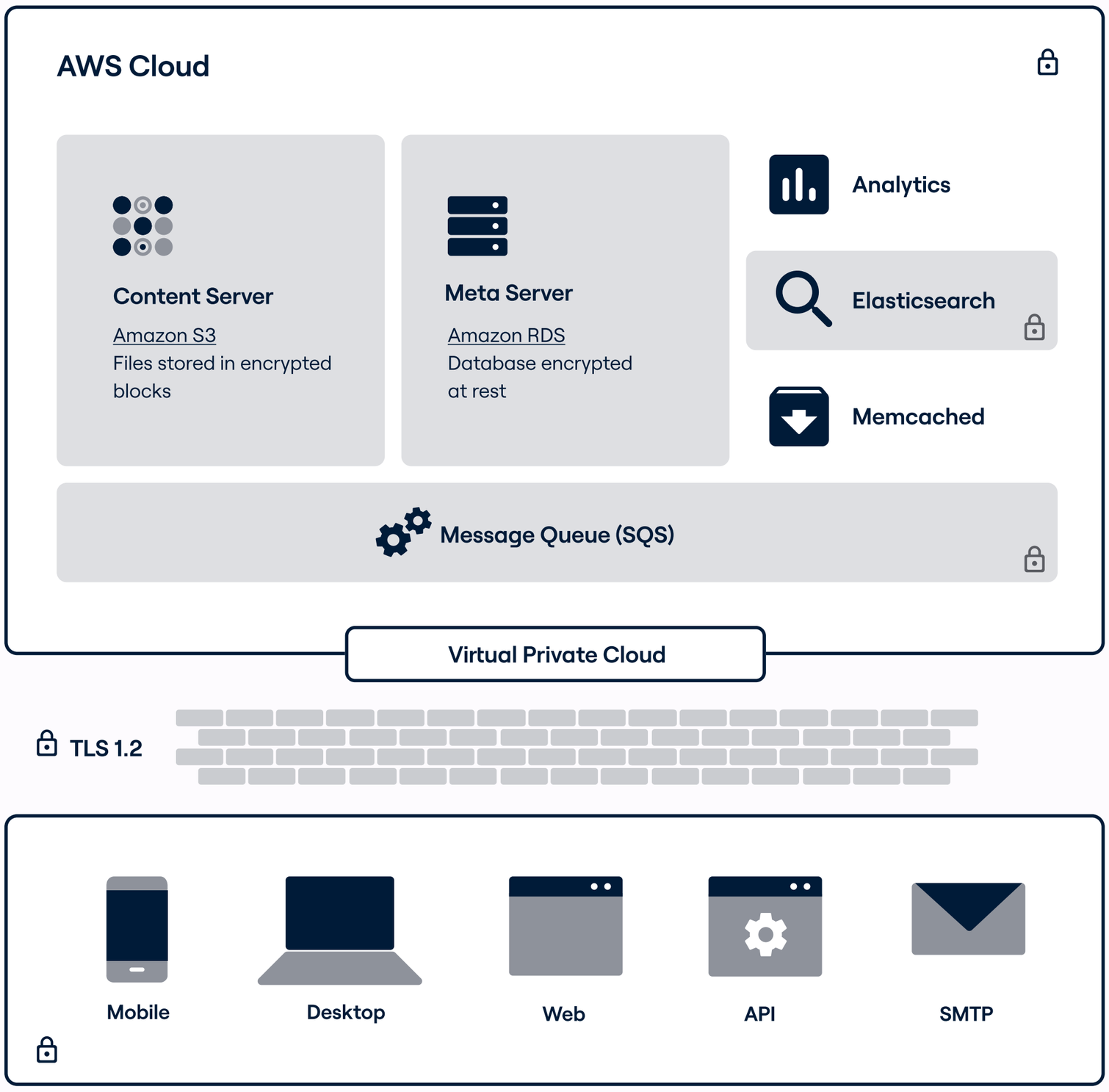
Since our customers' inboxes are their most extensive bank of confidential information, privacy and reliability have been at the core of our business since day one.

As an organization, Front strives to build a secure application in accordance with security best practices to uphold the confidentiality, integrity, and availability of our customers' data. In the spirit of transparency, this document describes the systems and security practices we have in place to protect your sensitive data.



Enterprise Architecture

- Hosted on Amazon Web Services (AWS), designed to provide 99.99% availability, with services hosted regionally from the US and the EU.
- Content Server is hosted on AWS S3 and Metadata Server is built on Amazon's Relationship Database Service (RDS).
- All systems and services are equipped with integrated failover and fault tolerance with multiple availability zones for redundancy.
- Built with a distributed architecture, where all services are contained within a protected VPC environment using individual security groups and AWS SQS message queues.



Security Controls

- All business systems follow the principle of least privilege.
- Sensitive administrative actions trigger notifications, which are reviewed in real time and are written to an immutable log.
- All production systems require VPN and multi-factor authentication.
- Application source code is stored in a secure environment and changes go through a peer review process.
- Front has dedicated staging environments for development and testing, separate from production.
- All company-owned assets are encrypted and have MDM technology installed, allowing Front IT admins to remotely wipe devices.

Data Privacy

- All data in transit is secured with TLS 1.2 encryption and data at rest is secured through RDS and S3 services using AES 256-bit encryption.
- All API and client communication (desktop, web, and mobile) require HTTPS connections.
- All customer data is logically separated and tied to an enterprise ID that is used to validate requests during data retrieval processes.
- Front has security monitoring technology in place to detect system anomalies.
- Customers can dictate which geographic location (United States or European Economic Area) to host their data.
- Front has a Data Processing Addendum that is incorporated in our SaaS agreement.

Compliance

- Front is SOC 2 Type 2 compliant.
- Front is ISO27001 compliant.
- Front adheres to the EU/US and EU/Switzerland Privacy Shield framework and is compliant with GDPR and CCPA.
- Front conducts annual third party vulnerability audits and security pentests.

Governance

- All employees go through background checks prior to employment.
- All employees undergo general security training and testing as part of Front's standard onboarding process.
- Engineers go through an annual security developer training.
- Front handles sensitive data through our mature information security management system to minimize risk and combat security breaches.
- Front has a defined information security response program to detect and respond to incidents, recover service, and maintain business continuity in the eventof a disaster.

Enterprise Application Security

Front was designed to create a secure and collaborative experience for companies and their teams. To ensure Front can be deployed in compliance with the security needs of your organization, we've developed a suite of security features, some of which are highlighted below.

Multi-Factor Authentication

Individuals and administrators can enable two-factor authentication, which adds an extra layer of security to their Front account. Authentication apps need to support "TOTP algorithm."

IP Restrictions

Company administrators can allowlist the IP addresses from which their employees can access Front.

Multi-Team Workspaces

The Teams feature allows organizations to build multiple workspaces, each containing its own resources like tags, rules, responses, and analytics within one Front account.

Roles & Permissions

Administrators can define user roles with a customized set of permissions, like allowing certain users to create rules or restricting them from responding to messages.

Data Retention

Data Retention Policy:
https://help.front.com/en/articles/2083

Data Deletion Policy:
https://help.front.com/en/articles/2133

Single Sign-On

Front's administrators can enable single sign-on (SSO) using any SAML-based identity provider (IdP) like Okta, Google, OneLogin, Microsoft Azure Active Directory.

Gmail/Office365 OAuth

Front securely connects to full Gmail and Office365 mailboxes through an OAuth process, enabling Front to import mailbox history and sync messages between both systems.

Conversation Audit Trail

All user, rule, or API activities will generate an activity history that will be logged to the conversation for audit purposes.

Delegated Inboxes

A Front user can delegate their individual workspace to another teammate, enabling them to manage their teammate's work queue without having to share login credentials.

Admin Access Controls

Front's admin console provides administrators access to manage teammate settings like signatures and preferences, giving them heightened control over each user's workspace.

Frequently Asked Questions

Does Front retain a copy of my communication data?

Yes. Front securely saves a copy of every communication received to our EU or US AWS servers. This enables Front to associate Front-specific actions like assignment and comments, which don't translate to Exchange and Gmail, to the conversation. Additionally, this allows Front to deliver a seamless and quick experience to end users as they navigate and search in the platform.

Can I request Front to delete my data?

In compliance with GDPR, Front will delete any company's data once an explicit request is submitted and the requester's identification is properly validated. All deletion requests will be completed promptly, but metadata can take up to 10 days to be purged from backups.

What types of personal data does Front store?

Customers may submit personal data to Front, the extent of which is determined and controlled by the customer in its sole discretion, which may include, but not be limited to the following categories of personal data: First and last name, Title, Job Title, Employer, Contact information (company, email, phone, physical business address, social networks), IP address, Localization data, Signature, Pictures, Interaction with end user, Web application usage, Data relating to data subject's interaction with email communication in connection with Frontapp's email tracking feature. More information can be found in Front's SOFTWARE-AS-A-SERVICE (SaaS) AGREEMENT (https://front.com/legal/saas-services agreement).

For AI features in Front, is my data used for model training purposes or any purposes other than to provide the AI output?

No. We use third-party AI models to power AI features within Front. These models are not trained on any Front customer data, and your data is only used to generate the AI output you see. In compliance with GDPR, the third-party provider is listed as a subprocessor on our website. Customers also have the option to disable AI-enabled features within their Settings.

Is Front HIPAA compliant?

Front complies with HIPAA in its role as a business associate for the personal health information (PHI) that may be contained in its customer data for customers who have signed Front's BAA.

What subprocessors does Front have?

Please refer to: https://front.com/legal/list-of-subprocessors