

Levitate

Enterprise Security Whitepaper

Published 2026

Table of Contents

1. Introduction 3
2. Levitate Servers: Web, API, and Databases 3
    2.1. Overview 3
    2.2. Amazon Web Services security 4
    2.3. Data Security 4
        2.3.1. Data In Transit 4
        2.3.2. Data At Rest 5
        2.3.3. Data Backup 5
    2.4. Metadata 5
    2.5. Data Ownership 5
        2.5.1. Importing Contacts Through Spreadsheets 6
        2.5.2. Importing Contacts Through Integrations 6
    2.6. Network Firewall Standards 6
3. Levitate Web Application 6
    3.1. Authentication 6
    3.2. Logging 6
    3.3. Vulnerability Scans and Penetration Testing 7
4. Email and Calendar Integrations 7
    4.1. Overview 7
    4.2. Email Plug-ins 8
    4.3. Security 8
    4.4. Email Archiving For Financial Services 9
5. Mobile Device Security 9
    5.1. Overview 9
    5.2. iOS 9
    5.3. Android 10
6. Third-Party Disclosure 10
7. Levitate's Security Culture 10
    7.1. Employees 10
    7.2. Vulnerability Program 10
8. Conclusion 11

1. Introduction

Levitate helps relation-based businesses keep in touch with clients, prospects, and centers of influence personally and authentically. We provide software, custom content, and marketing coaching services to help advisors send personalized, authentic emails on a scale. By leveraging metadata from email, calendar, and CRMs, we help our customers strengthen and maintain personal relationships with their clients to drive organic growth and retention and cross-sell other services.

Levitate was started in 2017 by Jesse Lipson, a serial entrepreneur who founded ShareFile, a secure data storage and sharing software with over 70,000 customers and 20 million users worldwide. Similar to ShareFile, Levitate is a 'SaaS' platform.

SaaS or 'software as a service' means that security is simplified and automated (e.g., you are not responsible for personally updating software and applying patches). The technology is constantly updated, so you get new features, and any new security vulnerabilities that pop up (it is normal and expected that they will) can be neutralized by us.

2. Levitate Servers: Web, API, and Databases

2.1. Overview

Levitate's server infrastructure (application servers and databases) is hosted in Amazon Web Services. Fortune 500 companies and the United States Government trust this industry-leading cloud hosting provider.

All application data in Levitate is transferred using SSL/TLS encryption, stored in MongoDB databases hosted in AWS, and secured using MongoDB Atlas management service. The MongoDB Atlas service undergoes annual SOC 2 certifications by third-party auditors. All database content is stored on volumes that are encrypted at rest.

Levitate's application servers are regularly patched with the latest security updates, and all new code released must be reviewed and approved by at least two different engineering team members. The employee base with access to these EC2 instances is tightly controlled and monitored.

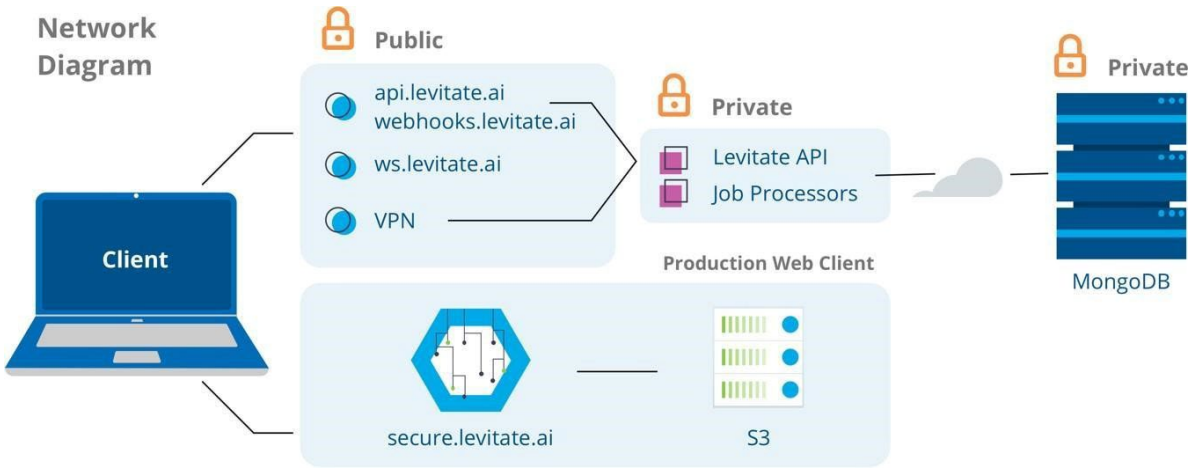


Figure 1: Illustrates the Levitate components. All traffic is via HTTPS and port:443

2.2. Amazon Web Services security

Levitate's server infrastructure (application servers and databases) is hosted in Amazon Web Services (AWS), the industry-leading cloud hosting provider trusted by Fortune 500 companies and the United States Government.

Amazon EC2 provides a firewall solution to enable security groups, a mandatory inbound firewall configured in a default deny mode that requires us to open ports allowing inbound traffic explicitly. The traffic may be restricted by protocol, service port, and source IP address (individual IP or CIDR block).

Amazon Web Services comply with key industry security, reliability, and confidentiality standards, such as ISO/IEC 27001:2005, SOC 1, and SOC 2, and undergo rigorous third-party audits.

AWS offers state-of-the-art physical protection for the servers and complies with an impressive array of standards. For more information on AWS Data Center Physical Security, see the AWS Security Whitepaper: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf.

2.3. Data Security

2.3.1. Data In Transit

Data is vulnerable to unauthorized access as it travels across the Internet or within networks. For this reason, securing data in transit is a high priority for

Levitate. All communication between the end user and Levitate's servers is transferred using 256-bit AES encryption and TLS 1.2 protocols.

2.3.2. Data At Rest

Similarly, all data at rest is encrypted using AES 256-bit symmetric key encryption, a FIPS-approved encryption algorithm.

If customers delete their data or cancel their accounts, we commit to deleting it from our systems. Information you delete from Levitate is automatically deleted from our customer database after 30 days.

2.3.3. Data Backup

We back up data on Mongo Atlas database storage by taking point-in-time snapshots. Snapshots are taken on an incremental schedule and retained in alignment with best practices for maintenance and restoration requests to reasonable restoration points.

2.4. Metadata

Metadata means 'data about data.' Levitate stores this metadata in its secure database to deliver service to you. While not an exhaustive list (we can customize what we pull into Levitate to suit your Keep-In-Touch plan better), we store the following metadata information:

- Name (First, Last, Suffix)
- E-Mail Address
- Phone Number
- Physical Address
- Birthdate
- Anniversary date
- Key Facts (custom added by you)
- Auditing/reporting statistics
- Contact Data

2.5. Data Ownership

As part of our customer service, Levitate stores metadata, including names, contact information, key facts, and notes in our system. While we store this data on behalf of our customers, our customers maintain ownership of data that they import or manually enter into the Levitate application.

2.5.1. Importing Contacts Through Spreadsheets

Customers may provide their Levitate Success Manager with spreadsheets (CSV, XLS, XLSX supported formats) to add contacts in bulk. These spreadsheets should only be shared via the provided link so that they may be securely uploaded and stored in ShareFile, the industry-leading secure file-sharing and transfer service mentioned above, for a limited time until they can be stored in our databases. The uploaded spreadsheets are automatically deleted per our expiration policy. Alternatively, customers may upload spreadsheets themselves directly to our S3 database.

2.5.2. Importing Contacts Through Integrations

Levitate offers various 3rd party integrations to improve your user experience. Any integration that requires a connection outside an email integration is opt-in only.

Opt-in integrations require administrator permission to allow our databases to pull and/or push data via API calls to the select vendors we have partnered with. By enabling these integrations, we pull only the same relevant metadata related to your contacts as we would manually through CSV spreadsheets but automatically refresh that data at specific intervals on your behalf.

This data is encrypted at rest and stored on our secured databases.

2.6. Network Firewall Standards

Strict network firewalls are in place to secure application servers, load balancers, and databases. Firewalls restrict access at each ingress/egress point on the network infrastructure.

3. Levitate Web Application

3.1. Authentication

Levitate user credentials are secured by WorkOS, a best-in-class identity management provider with SOC 2 certification. Levitate requires strong passwords for user accounts, implements lockout policies for multiple failed login attempts, and requires end users to answer a security question to reset forgotten passwords correctly.

3.2. Logging

Levitate leverages multiple logging tools to monitor and regularly fix application errors and review irregularities in system usage.

3.3. Vulnerability Scans and Penetration Testing

The Levitate application undergoes daily third-party vulnerability scans that check for over 50,000 of the latest hacking vulnerabilities. Levitate also undergoes an annual third-party penetration test and security audit to validate its security. Up-to-the-minute information about Levitate's system health, performance, and ongoing incidents can be found at status.levitate.ai.

4. Email and Calendar Integrations

4.1. Overview

Levitate stores metadata about email and meeting interactions, including the emails' recipients, the emails sent, the email sender, meeting attendees, and the meeting's timestamp. Levitate never stores the body content of any emails or meetings or the subject of emails not sent through Levitate.

Levitate does require the ability to access a user's email/calendar system to provide reminders to record notes for recent meetings and to compile reporting statistics about email/meeting activity. Sometimes, our system may scan the replies to emails sent through Levitate to detect whether the email message bounced or the recipient requested to unsubscribe from future emails. Still, we never store the contents of the message.

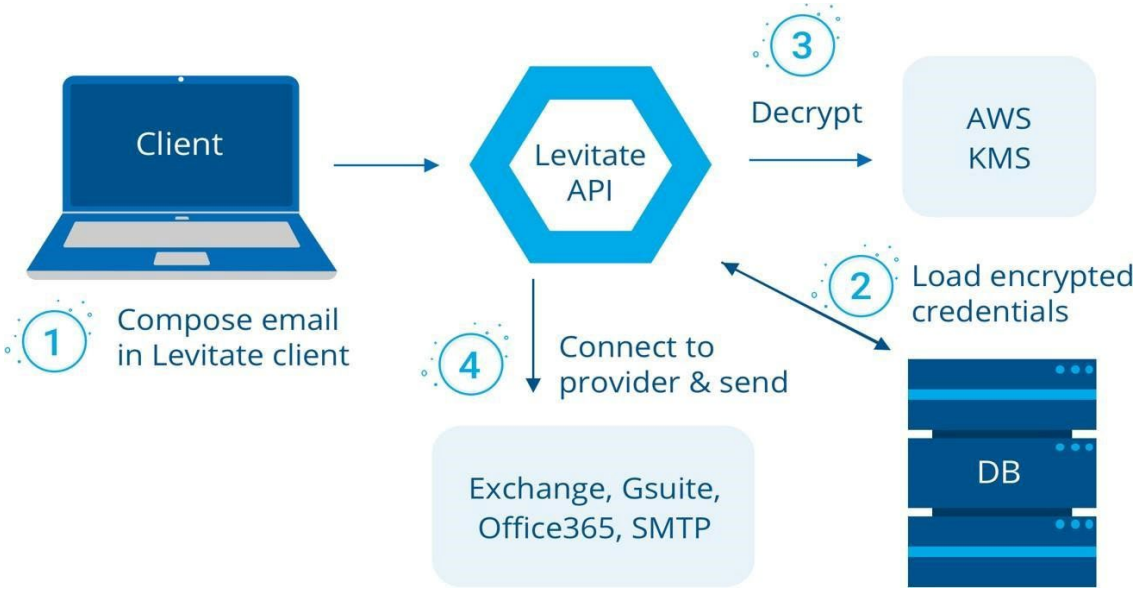


Figure 2: Diagrams the workflow for sending emails from Levitate through your email server.

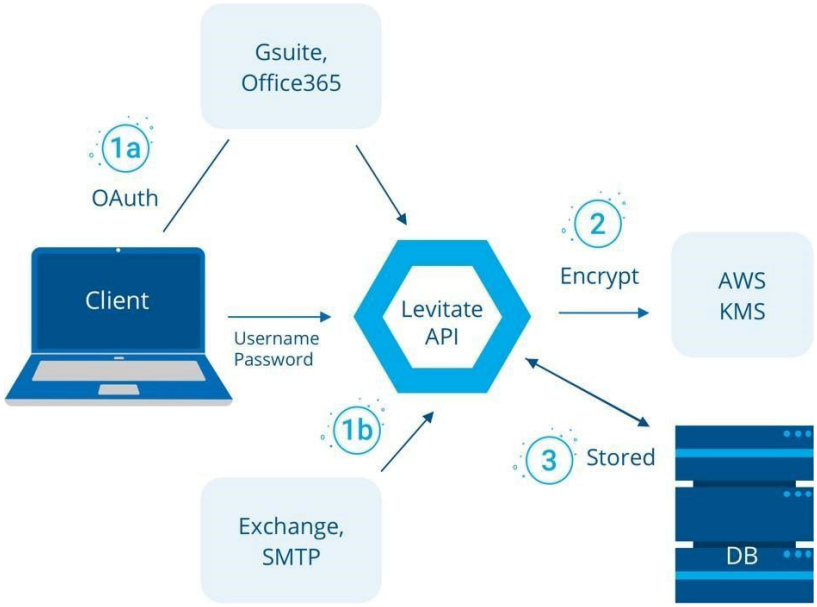


Figure 3: Illustrates how we connect to your email.

4.2. Email Plug-ins

Levitate offers optional client-side email add-ins for Microsoft Outlook and Gmail. Once installed, the add-in may parse the content of individual emails to allow proper functionality. This content is only sent to our servers with your active consent, such as saving content as a note in Levitate and saving email signatures into a contact's Levitate profile.

Microsoft Add-In approval was given by submitting an XML manifest file and proof of web application on a web server. Microsoft's App Source requires the plugin to use a Secure Socket Layer (SSL) to communicate, archive add-ins in read-only mode, and provide proof of identity, a contractual agreement, and a compliant privacy policy which can be found here: https://www.levitate.ai/privacy-policy. Levitate's plugin undergoes annual security audits that keep it in compliance with Google and Microsoft's Add-In security requirements.

4.3. Security

As an additional layer of protection, all highly sensitive data, including any user email/calendar OAuth tokens or stored credentials, is encrypted using AWS' Key Management Service (KMS). AWS KMS uses FIPS 140-2 validated hardware security modules to protect the security of the encryption keys, and each user has a unique encryption key to protect his/her email/calendar tokens. Access to Levitate's KMS

system is restricted to the company's Chief Architect and Founder/CEO. OAuth is an open protocol to allow secure authorization in a simple and standard method from the web, mobile, and desktop applications. All OAuth data transfer must take place on SSL (Secure Sockets Layer) to ensure the most trusted cryptography industry protocols are being used to keep data as safe as possible. Using OAuth 2.0, Levitate provides users with access to their data while protecting their account credentials. Levitate supports the OAuth 2.0 framework, enabling applications like the Levitate mobile application, email, and calendar integrations to obtain limited access to an HTTP service like Levitate.ai.

4.4. Email Archiving for Financial Services

Per SEC Rule 204-2, client-facing communications at registered investment firms, including emails, must be archived.

Levitate stores the content of any email sent through Levitate, but we do not store the content of any replies or emails sent through your connected email server. Levitate integrates directly with the users' email server; any existing archiving processes in place with the user's email server will happen automatically as if the message was sent out through the user's email client.

5. Mobile Device Security

5.1. Overview

Levitate offers iOS and Android applications as an alternative method or optional supplement for users to access the Levitate service. The mobile applications allow you to add contacts, update key facts quickly, and use mobile-specific features, like business card scanning.

All sensitive data, such as the Levitate OAuth tokens used for iOS and Android authentication, is encrypted if stored on the device. Each encryption key is stored using the platform's native KeyStore or Keychain, is generated per user, and uses the platform-provided implementations of AES.

5.2. iOS

OAuth tokens are further protected by being stored within the iOS Keychain. This eliminates the need to store credentials locally after entry on first use and only permits access after OS-level authentication (biometric or PIN).

5.3. Android

OAuth tokens are further protected by encrypting using AES CBC and stored within a local file, which eliminates the need to store credentials locally after entry on first use.

Certificate pinning is enabled for this application. Certificate pinning requires the leaf certificate thumbprint to match a specific, hard-coded value.

6. Third-Party Disclosure

We do not sell, trade, or otherwise transfer your Personally Identifiable Information to outside parties. Additionally, data that you enter into the Levitate application (including but not limited to notes, contacts, company names, and action items) is never sold, traded, or otherwise transferred to outside parties except for opt-in services for the sole purpose of your use elsewhere. Your data is your data!

7. Levitate's Security Culture

7.1. Employees

Levitate performs background checks on all employees, verifies an individual's education and previous employment, and conducts criminal and credit security checks. The extent of these background checks is dependent on the position.

During orientation, new employees agree to our Code of Conduct and Confidentiality Agreement, highlighting our commitment to keeping customer information safe and secure. Depending on their job role, additional training in specific security aspects may be required.

7.2. Vulnerability Program

We appreciate and encourage security researchers to contact us as part of our responsible disclosure/vulnerability program to report potential vulnerabilities identified in any application, system, or asset belonging to Levitate.

If you believe you have identified a potential security vulnerability, please share it with us by emailing security@levitateapp.com.

Levitate offers no reward or compensation in exchange for submitting potential issues associated with the Vulnerability Program.

8. Conclusion

With more than two decades of experience building software for businesses, Levitate provides a secure, user-friendly tool to help businesses focus on what they do best: build relationships.

We take security seriously at Levitate. If, after reading this whitepaper, you have any further questions, please don't hesitate to contact us at security@levitateapp.com.