

Enterprise Security Whitepaper – Feature Addendum

Table of Contents

1. Introduction 3
2. Meeting Booking 3
3. Texting 3
    3.1. Overview 3
    3.2. Data Encryption 3
    3.3. Infrastructure Management 4
    3.4. Network Monitoring 4
    3.5. The Campaign Registry 4
    3.6. Text Archiving 4
4. Social Media 5
    4.1. Overview 5
    4.2. Platform Connection 5
        4.2.1. Facebook 5
        4.2.2. Instagram 5
        4.2.3. LinkedIn 5
    4.3. Account Connection 5
    4.4. Compliance Workflow 5
5. Surveys 6
6. AI Content Generation 6
    6.1. Overview 6
    6.2. Content Selection and User Input 6
    6.3. User Privacy 6
    6.4. Data Access and Privacy 6
7. Handwritten Cards 7
    7.1. Overview 7
    7.2. Data Security 7
    7.3. Privacy and Encryption 7
    7.4. Logistics and Shipping 7
    7.5. Payment Processing 8
8. Websites 8
    8.1. Overview 8
    8.2. Disclosure Placement 8
    8.3. Website Review 8
    8.4. Consent for Solicitation 8
9. Conclusion 9

1. Introduction

Welcome to this feature-focused addendum to our comprehensive security whitepaper. In this document, we take a closer look at the individual features used by our clients, such as email campaigns, social media, texting, meeting booking, websites, and handwritten cards, to strengthen the security of our systems and services.

While our original whitepaper provided an overview of our security framework, this addendum hones in on the technical details that bolster our defenses and ensure a safer digital environment for you, our users. Here, you'll gain insights into the specific tools, practices, and technologies that drive our commitment to safeguarding your data and sustaining the resilience of our digital ecosystem. We encourage you to explore these features, showcasing our unwavering dedication to your safety and trust in our platform.

2. Meeting Booking

Levitate users can allow their contacts to book meetings directly against their calendars using customized links. For meetings booked with the Levitate meeting booking feature, Levitate will store metadata about email and meeting interactions, including the emails' recipients, the email's timestamp, the email's sender, meeting attendees, and the timestamp of the meeting.

This functionality is limited to users with a Google, Exchange, or Office365 email server. Users with an IMAP email server with Zimbra can use Meeting Booking if they also utilize Redtail CRM's Tailwag 2.0 application that allows you to synchronize your Contacts and Calendar Activities between Redtail CRM and a locally installed version (Non-Click-to-run) of Microsoft Outlook.

This feature's permissions are accepted when users connect their email server to Levitate using OAuth.

3. Texting

3.1. Overview

Levitate offers texting as an alternative form of communication between users and their clients. Levitate's texting API is provided through Twilio, a third-party communications service.

3.2. Data Encryption

TLS 1.2 encrypts data in transit between the customer application and Twilio over public networks. Databases housing sensitive customer data are encrypted at rest.

3.3. Infrastructure Management

All network access between production hosts is restricted, using AWS security groups to allow only authorized services to interact in the production network. Any inter-site or network connectivity is established through edge routers and security devices. All network and VPN connections terminate in edge zones. Outbound DNS requests from any zone travel through DNS resolvers and are auditable and traceable to a single device.

3.4. Network Monitoring

AWS Web Application Firewalls are used for external services with AWS Shield while leveraging AWS Security Groups and Access Control Lists (ACLs) to manage traffic. AWS VPCs (Virtual Private Clouds) are used to manage network segregation between different security zones in the Production environment. Firewalls are used to maintain segregation of the corporate networks; rules are reviewed quarterly. An intrusion detection system (IDS) monitors access events, security-related events, and API authentication.

3.5. The Campaign Registry

Levitate requires all users registering a phone number for SMS messaging to also register with The Campaign Registry (TCR). This ensures transparency regarding recipients and content, helping prevent fraud and spam. It also aligns with regulations mandating explicit consent from message recipients for marketing purposes. These measures guarantee responsible and compliant SMS practices while upholding data security and regulatory standards.

3.6. Text Archiving

Texting Archiving is on by default for Levitate accounts in the financial industry and can be turned on for other Levitate users. Exchanges held through Levitate's texting feature are viewable on the contact's profile in Levitate.

A consolidated view of the texting conversation is created as an email and silently sent from the Levitate user to a designated Levitate email mailbox (no-reply@levitate.ai) so that it will create a history of the conversation to be automatically archived by the user's existing email archiving service.

These silent emails will be in the user's Sent email folder along with an attached .txt file attachment. This file contains the full conversation, metadata for each message, and any images sent during the conversation.

4. Social Media

4.1. Overview

Levitate offers clients the ability to connect and post directly to their social media pages as another form of communication between them and their clients and promote their business.

4.2. Platform Connection

4.2.1. Facebook

Levitate users may only connect to a Facebook business page. Any Levitate user with posting rights to the page can schedule, post right away, and make edits before the post goes live.

4.2.2. Instagram

Levitate users may only connect to a professional Instagram account linked to a Facebook business page. Any Levitate user posting rights to the Facebook business page can schedule, post immediately, and make edits before the post goes live to the linked Instagram account.

4.2.3. LinkedIn

Levitate users may connect to a business or personal LinkedIn account. Any Levitate user with posting and/or admin rights to a LinkedIn account can connect and post directly through Levitate.

4.3. Account Connection

Each Levitate user can connect to their own respective social media accounts. Social media posts must be made in the account of the connected Levitate user. Administrators are not permitted to post on behalf of other Levitate users and their connected social media accounts.

4.4. Compliance Workflow

If your firm requires third-party approval for posts on social media, Levitate provides the ability to send a PDF of a social media post via email to the entity in charge of approving content. Similarly to a Levitate email campaign, the full compliance workflow is enabled for social media, where a post will stay pending until it is approved by either the user or an administrator.

5. Surveys

Levitate offers the ability to create and request ratings and feedback from their contacts through surveys. Users can request that these reviews be posted on their business Google or social media page.

Levitate users must provide their referral request link for the specific business page and attach it to the survey. Anyone with access to this link can post reviews to the affiliated business page. Levitate can not alter or delete any posts made by third parties and is not responsible for the posts/reviews left by others.

6. AI Content Generation

6.1. Overview

AI content generation is a core component of our platform, driven by the collaboration between OpenAI and ChatGPT. Our priority is safeguarding user data privacy and security.

6.2. Content Selection and User Input

Levitate offers content options from a library or lets users create content using the AI Content Generator. Levitate creates a tailored prompt based on user preferences and input, which is shared with OpenAI solely for content generation.

When users submit requests, we follow a clear process. Their content input combines with a prompt we designed that includes additional details such as message length, personality, and creative freedom for OpenAI to guide content generation. We do not inspect user submissions before sending them to AI.

6.3. User Privacy

User privacy is our utmost concern. We ensure that no user-identifying information is relayed to OpenAI. Our Success team actively advises users against including Personally Identifiable Information (PII) in their prompts. The sole security risk arises if a user intentionally adds PII to their prompt.

6.4. Data Access and Privacy

It is vital to clarify that Levitate has a closed API and is made inaccessible to OpenAI. This clear separation is crucial for maintaining data security. For a comprehensive understanding of OpenAI's privacy policies, please refer to the OpenAI Privacy Policy.

Our process focuses on delivering quality content while maintaining stringent data security and user privacy standards.

7. Handwritten Cards

7.1. Overview

Levitate offers Handwritten Cards, allowing clients to send personal, memorable messages to their contacts. We partner with a third party, making it easy for clients to express gratitude and build strong connections.

7.2. Data Security

The Handwritten Cards service collects data from the user's management system. We have implemented robust security measures to safeguard this data during transit and while it is at rest. Specifically, for Handwritten Cards, the following mandatory data elements are involved:

- Recipient Street Address
- Recipient Street Address 2
- Recipient City
- Recipient State
- Recipient Postal Code
- Return Street Address
- Return Street Address
- Return Street Address 2
- Return City
- Return State
- Return Postal Code
- Return "written" signature
- Message content

7.3. Privacy and Encryption

We share the content of each message exclusively with its intended recipient. To accomplish this, we execute an encrypted HTTPS request incorporating the user's request body, encompassing all the information mentioned above. It is imperative to note that this request is encrypted, adhering to the same stringent security standards as an HTTPS request made by a web browser.

7.4. Logistics and Shipping

We exclusively utilize USPS for all shipping, and our service is confined to U.S. addresses, employing Forever Stamps for postage. Our partner employs manual quality control procedures to validate the accuracy of formatting.

7.5. Payment Processing

Payment is managed through Maxio, a company firmly committed to adhering to industry standards of security, reliability, and confidentiality. Maxio's dedication to these principles is demonstrated through its compliance with ISO 27001:2013, SOC 1, and SOC 2, all subject to rigorous third-party audits. With their PCI DSS Level 1 compliance, you can trust that the secure handling of sensitive payment data is their top priority.

8. Websites

8.1. Overview

Levitate offers a complete solution for building and hosting clients' company websites. We start by discussing their needs, content, and features. Our skilled team designs and crafts the website to match their vision, ensuring a professional and appealing online presence. Clients can trust us to manage the entire process, delivering a quality, hosted website that represents their business effectively.

8.2. Disclosure Placement

Websites within the scope of financial services will feature a comprehensive disclosure statement at a conspicuous location, typically at the bottom of the site. This statement indicates the regulatory registrations, authorized entities, and relevant affiliations. It also specifies the securities offered through the platform and details data protection and privacy policies.

8.3. Website Review

Before a website's public release, the firm and/or Broker-Dealer's compliance team may conduct a content review to ensure adherence to regulatory requirements and internal policies. This review may be a live preview or an exported website version.

8.4. Consent for Solicitation

Prospective users accessing the site will be presented with a clear disclosure statement. This statement will explicitly state that the user consents to receive automatic messages by providing their information on the site. Additionally, a mechanism for email alerting the new prospect's designated financial professional should be implemented for optimal communication and compliance tracking.

9. Conclusion

This addendum has offered insights into the user-centric features that enhance our system and service capabilities. Our commitment to establishing a reliable and efficient digital environment remains unwavering. This commitment involves continuous updates and improvements to our platform, including the introduction of new user-based features and the refinement of existing ones.

Our determination to protect data and ensure an exceptional user experience remains resolute. We anticipate ongoing innovations and improvements that will guarantee a dependable and effective experience with our services.