Leaptree Security Whitepaper

This document provides information about the security of all Leaptree applications.

Address

5 Lamps Place
Amiens St.
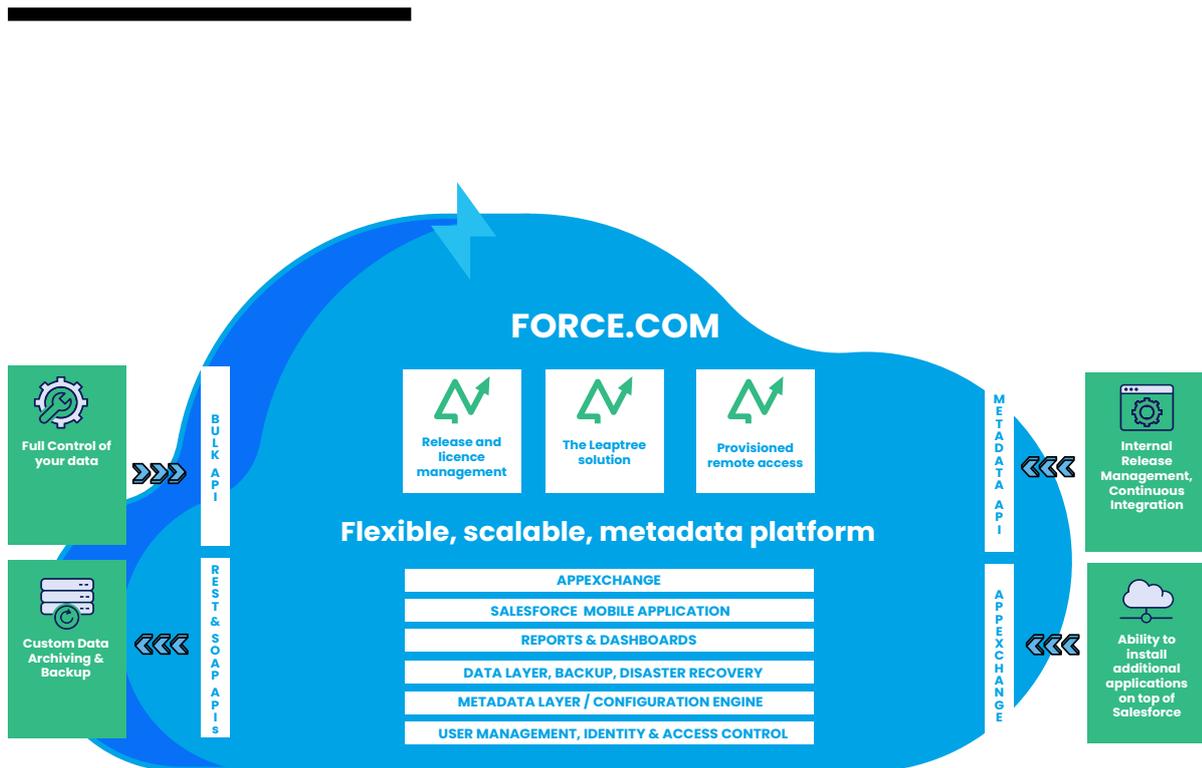Dublin 1
Ireland

Phone

Phone: +353 1 547 7758

Online

Email 1:   help@leaptree.com
Email 2:   info@leaptree.com
Website: https://www.leaptree.com/

01.
Built on the Salesforce Platform

FORCE.COM

Full Control of your data

Custom Data Archiving & Backup

BULK API

REST & SOAP APIs

| Release and licence management | The Leaptree solution | Provisioned remote access |

Flexible, scalable, metadata platform

| APPEXCHANGE |
| SALESFORCE MOBILE APPLICATION |
| REPORTS & DASHBOARDS |
| DATA LAYER, BACKUP, DISASTER RECOVERY |
| METADATA LAYER / CONFIGURATION ENGINE |
| USER MANAGEMENT, IDENTITY & ACCESS CONTROL |

METADATA API

APPEXCHANGE

Internal Release Management, Continuous Integration

Ability to install additional applications on top of Salesforce

Leaptree

Leaptree takes security very seriously. Our platform was built from the ground up to information-security best practices.

The document provides an overview of the Leaptree platform, including frequently asked questions, which can help our customers to assess our security practices.

02.
Salesforce AppExchange Security Clearance

All four Leaptree products were built on Force.com, a mature platform for cloud applications provided by Salesforce. All Leaptree data is stored on the Salesforce platform and is never processed outside of it. That means Leaptree never has access to any of our user's data unless you explicitly grant Leaptree time-based access to your Salesforce environment.

Leaptree is listed on the Salesforce AppExchange, their cloud applications marketplace. All AppExchange apps go through an intensive review process to ensure they fulfill a comprehensive list of security standards and data protection best practices before they are publicly listed. This includes stringent testing of customer data protection and includes threat-modeling profiles that are based on common security vulnerabilities, including:

- SOQL and SQL injection
- Cross-site scripting
- Non Secure authentication and access control protocols
- Vulnerabilities specific to the Salesforce platform, such as record-sharing violations

As a result, Leaptree meets our customer's (including those in Government and Healthcare) most rigorous data security requirements.

Leaptree Release Management

Leaptree gets access from the Force.com platform to automatically upgrade Leaptree to a new version for our customers. This is fully seamless and causes no downtime. A Leaptree release will always be communicated and agreed upon in advance with our customers before being executed. In the case where a customer prefers to make manual upgrades, Leaptree will provide an upgrade link so that the customer can make and control the version upgrade themselves.

Leaptree Installation

Leaptree installation is done by our customers themselves either by an installation link we provide or by installing Leaptree directly from the Salesforce AppExchange. Our customers can uninstall Leaptree at any time from their Salesforce environment if they wish.

Leaptree Data

Leaptree data is saved only on the Salesforce database and Leaptree has no access to any of your data. You can control access permission to your Leaptree data via Salesforce configurations. Additionally, your Leaptree data can use the same backup and disaster recovery features that Salesforce provides to any Salesforce data. If you stop your Leaptree license you still have access to your Leaptree data, but not to any Leaptree features. You can grant Leaptree temporary access to your Salesforce instance to troubleshoot any issues but otherwise, Leaptree has no access to your data and your data never leaves the Salesforce environment. All your Leaptree data is available to consume and manage via the Salesforce API–just like any other Salesforce data.

Leaptree Licences Control

Leaptree can control how many licenses each customer has and view the number of licenses in use by each customer. Aside from that, Leaptree has no control or access to your Salesforce instance.

Data Compliance

Leaptree has the capability to fit in with your CCPA, HIPPA and GDPR protocols. Our customers are responsible for ensuring that they comply with applicate data protection laws.

Frequently Asked Questions

1. Please provide details for any Compliance/ Regulatory attestations (SOC2 type 2, PCI-DSS, ISO, etc.) and reports where applicable.

We've been reviewed and approved by the Salesforce security review which is required by any application on the Salesforce AppExchange.

2. Do you use a public cloud (AWS, Azure, GCP, etc.) or a private cloud? Please also provide geographic location(s).

Our product is using the Force.com (Salesforce) platform. Since our product sits on top of Salesforce, the geographic location is the exact same as your Salesforce server.

3. Will there be any QA environment or is testing done on your production environment?

You can install our application in your Salesforce sandboxes which are your own Salesforce testing environments. This way you can test and check our product, make sure it works well with the rest of your Salesforce implementation.

In addition to this, when Leaptree develops the application we have our own development environments and testing environments to make sure our application can work with different types of Salesforce environments and configurations.

4. HTTPS Access – please provide details of protocol (eg: TLS v1.2), supported ciphers, minimum key length, key exchange details, etc.

Access to our application is done via the same access to your Salesforce application. You can access Salesforce API, the main browser application, or via a mobile app. All access to Salesforce requires TLS 1.2. See more details here:
https://help.salesforce.com/articleView?id=000351980&language=en_US&mode=1&type=1

Frequently Asked Questions

5. Is our data encrypted at rest? Provide details if so (eg: disk-level encryption or data encryption; is a different key used for each tenant/ customer/survey, etc).

Salesforce allows you to encrypt data at rest using an additional feature of Salesforce called Salesforce Shield encryption. See more details here:

https://help.salesforce.com/articleView?id=security_pe_overview.htm&type=5

6. What Single Sign-On methods do you offer?

Salesforce offers a wide range of out-of-the-box Single Sign-On solutions and allows you to create custom solutions as well. See more details here:

https://help.salesforce.com/articleView?id=sso_about.htm&type=5

7. Do you offer HRIS synchronization with ADFS?

Salesforce support an out- of-the-box ADFS integration. See more details here:

https://help.salesforce.com/articleView?id=identity_provider_examples_3p_adfs.htm&type=5

8. Does your product provide Role-Based Access Controls (RBAC)? If so please share details of the roles and access.

Access to our application is done via the same access to your Salesforce application. You can access Salesforce API, the main browser application, or via a mobile app. All access to Salesforce requires TLS 1.2. See more details here:

https://help.salesforce.com/articleView?id=admin_userprofiles.htm&type=5
https://help.salesforce.com/articleView?id=perm_sets_overview.htm&type=5

Frequently Asked Questions

9. Do you have a REST API for user provisioning/ automation/orchestration?

Yes. You can use the Salesforce REST API to access our product, its

data, its configuration, and automate the access and the roles of our product on top of

Salesforce. See additional details here:

https://developer.salesforce.com/docs/atlas.en-us.api_rest.meta/api_rest/

10. What kind of logging/ accountability are available for user login and activity?

Salesforce provides a login activity history for every user login attempt:

https://help.salesforce.com/articleView?id=users_login_history.htm&type=5

11. Data Access

a. Do you have access to any of our data by default?

No. Your data is saved in your Salesforce environment. Leaptree has no access to that

data by default.

b. Are you able to gain access without us explicitly allowing you?

No. Salesforce won't give us any default access to any of your Salesforce data.

Salesforce won't give us any default access to any of the Leaptree data you have stored

on your own Salesforce environment.

c. Do you have any need to ever access our data?

No. Salesforce gives you the option to allow Leaptree to get temporary access to your

Salesforce if you wish. Sometimes we ask you to grant us access using this option

to your testing Salesforce environment (Sandbox) in order to troubleshoot an issue.

However, that's not required and Leaptree can work around that if that's not possible.

Frequently Asked Questions

Some of those products (such as BitGlass) have an out of the box integration into Salesforce. See more details here:

https://www.bitglass.com/casb-salesforce-security

13. Please provide details of the system components for your product (Operating System, Web and Database platform(s), eg: RHEL v7.5; Apache v2.4.37 ; MySQL v8.0.13).

Our Leaptree application is deployed fully on the Salesforce platform.

14. Does your product rely on or transfer data between any 3rd party or service (eg: for integration)? Please provide details and list the 3rd parties.

Your data is stored in your Salesforce platform and never leaves it. The Leaptree product won't send your data anywhere or pull data from any 3rd party system.

15. How are tenants prevented from affecting the performance or availability for others?

The Salesforce platform supports a secure multi- tenant platform which makes sure every tenant has limits to how many resources they can use so that they don't affect any other tenants. Our Leaptree application is reviewed and approved by the Salesforce security review team to make sure we don't abuse the Salesforce resources. The use of Salesforce resources by Leaptree is NOT counted against the usage of those resources by the client. See more details here:

https://developer.salesforce.com/wiki/multi_tenant_architecture

16. Please provide details/ documentation for the following security controls:

Frequently Asked Questions

a. Privacy/confidentiality (especially what is in place to prevent tenants from accessing each other's data)

https://developer.salesforce.com/wiki/multi_tenant_architecture

b. Integrity of data (what is in place to monitor for or prevent data from being modified inappropriately)

https://help.salesforce.com/articleView?id=000329320&type=1&mode=1

c. Identity management

https://developer.salesforce.com/docs/atlas.en-us.identityImplGuide.meta/identityImplGuide/identity_overview.htm

d. Records management

https://help.salesforce.com/articleView?id=mc_bp_data_management.htm&type=5