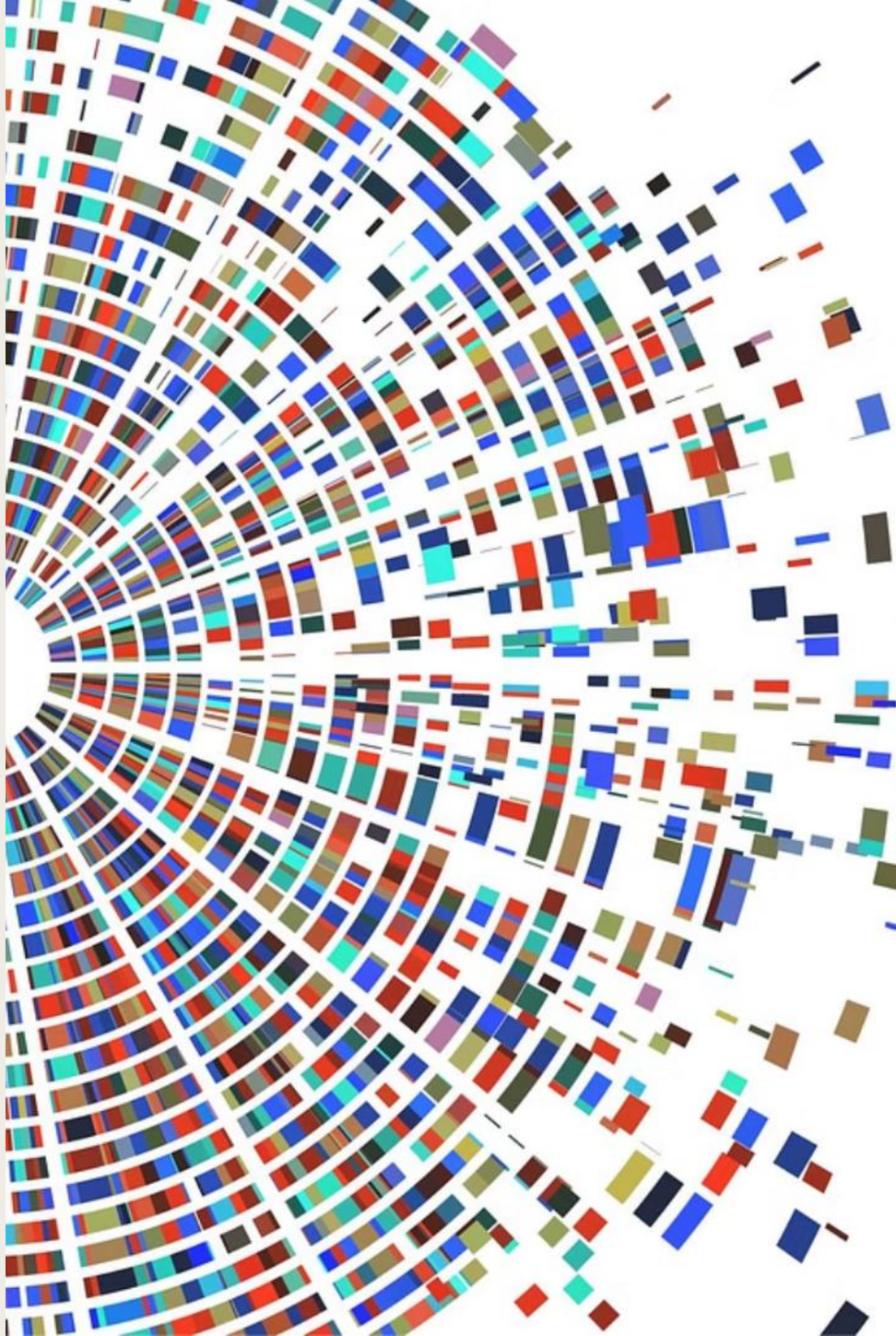
Security

Updated on 03 May 2025



Technical Capabilities, Integration & Reliability

Technical Capabilities

Karate Labs provides software that runs locally on user desktops with no cloud storage of user data.

Integration

Our products integrate with industry standard IDE platforms like IntelliJ and VS Code.

Reliability

We follow strict security protocols and offer enterprise-grade solutions with offline license activation options.

Vulnerability Management & Security Scanning

How We Monitor and Address Security Vulnerabilities

Maven & Sonatype Security Checks

Karate is released as a Java package via the Maven Central infrastructure. We cannot release in case of critical vulnerabilities. Example report. All releases can be seen here.

Automated Dependency Scanning

GitHub dependabot is a powerful tool that continuously scans the repository for known vulnerabilities and deprecated dependencies. This helps us stay on top of potential security risks and keep our codebase up-to-date.

Whenever dependabot identifies an issue, we get notified right away. In most cases, GitHub even auto-provides a pull request with the necessary updates, making it easy for us to review and merge the changes. This streamlined process helps us address vulnerabilities quickly and efficiently.

Overall, having dependabot integrated into our workflow is a huge advantage. It gives us peace of mind knowing that our repository is constantly monitored for security concerns, and that we can act on them promptly to maintain a robust and secure application.

Enterprise Community Security Alerts

Karate is in use at 600+ enterprises . Many of these customers use solutions such as Snyk for scanning their code, tools, artifacts and Docker containers. Whenever a scan reports an issue with Karate, they are quick to alert us and even provide a PR in some cases. Here is an example of us addressing the famous Log4J issue (even though we did not depend directly on it. Another example is our expedited release for Java 11 when a library we depended on did not have a safe equivalent for Java 8.

Plugin Security

Stringent level of checks done by JetBrains and Microsoft (VS Code) when publishing plugins to their marketplace.

Overrides

Karate allows users to override dependencies, in cases where waiting for an official release is not an option. This was suggested by one of our enterprise users along with a PR (Thomson Reuters). High CVE's in Karate core. To quote: *"With a non-shaded JAR, I can mitigate the new CVE by explicitly declaring a newer version of the dependency in my POM"*. Karate Labs code scanning.

Security Infrastructure & Controls

Is Karate cloud-based?

No. Karate Labs software runs locally on the user desktop and no user data is stored in the cloud.

Does your organization use industry standard repositories for secure check-in and check-out of code?

YES. We use GitHub.

Does your organization have security controls such as antivirus, file integrity monitoring, and logging?

YES. We have stringent controls in place at Karate Labs including antivirus and scanning of files, logging.

Does your organization have policies and procedures defining the security of user systems, infrastructure, and components?

Karate Labs software runs locally on the user desktop and no user data is stored in the cloud. Only billing and auth is delegated to industry-standard cloud providers. We offer offline license activation to enterprise customers.

Does your organization support, [where possible] keys provided by a Customer for the use of encryption protocols?

Not applicable. Karate Labs software runs locally on the user desktop and no user data is stored in the cloud. Only billing and auth is delegated to industry-standard cloud providers. We offer offline license activation to enterprise customers not wanting our licensed software making outbound calls to validate license.

Data Processing & Network Security

Customer production data in non-production environments	**Not applicable. Our software runs locally on the user desktop and no user data is stored in the cloud.**
Do we use AI in processing Customer information?	**No**.
Network security controls for attacks detection	**Not applicable. Karate Labs software runs locally on the user desktop and is not exposed as something that can be connected to via the network.**
Restriction of service or utility accounts	**No. Karate runs abstracted within industry standard IDE platforms (IntelliJ & VS Code).**
Do we follow principle of least privilege?	**Yes. After license activation we enable only features allowed by the license tier.**
Support for Customer account creation and federated authentication (Okta, SAML)?	**Yes. We use WorkOS to manage identity and SAML. When a non-offline license file is provisioned locally by a product that requires a subscription (e.g. the IDE plugins) it is encrypted and cached locally. This allows the user to freely use the product without connecting to the internet until the file expiry (max 30 days).** **We include cost details in our quote to enterprise customers.**

Open-Source Libraries & Standards

Open-Source Usage

YES. Karate Labs uses open-source libraries.

The core framework is open source, and the dependencies are listed here (example): https://central.sonatype.com/artifact/io.karatelabs/karate-core/1.5.0.RC3/dependencies

Karate IntelliJ plugin dependencies:

- io.karatelabs:karate-core
- io.netty:netty-handler
- net.minidev:json-smart
- JetBrains IntelliJ platform (depends on IDE version)

More details: https://plugins.jetbrains.com/plugin/19232-karate

Karate VS Code extension dependencies:

- posthog-node
- uuid
- VS Code platform (depends on IDE version)

More details: https://marketplace.visualstudio.com/items?itemName=karatelabs.karate

Karate is a developer tool and is not used in a production critical environment, we encourage our enterprise customers to always update to the latest version of Karate and the latest IDE plugin version (for IntelliJ or VS Code).

OWASP does not apply to Karate products (IDE Plugins / Xplorer) as they run on the desktop and not as a web-application in the cloud.

Third-Party Security & Data Management

Third-Party Security Assessment

Karate Labs does not store any data on behalf of users and delegates to the following providers:

1. Stripe - for billing
2. Google Cloud and Microsoft Azure for OAuth flows

Stripe security policies can be referred here: https://stripe.com/docs/security

Data Encryption

Not Applicable. Karate Labs products run locally on the user-desktop and do not use a database.

Data Backups

Karate Labs software runs locally on the user desktop and no user data is stored in the cloud. Only billing and auth is delegated to industry-standard cloud providers.

Security Training & Disclosure

Development and testing is owned by a single team that has access to development tools such as GitHub and Sonatype for real-time feedback on security. Code checked-in to GitHub is continuously scanned for vulnerabilities.

YES. We disclose all vulnerabilities that affect the security of our software. Refer https://ossindex.sonatype.org/component/pkg:maven/io.karatelabs/karate-core@1.5.0.RC3 and https://github.com/karatelabs/karate/security

Security Incidents & Documentation

Security Incidents

NO. Karate Labs has not experienced a security incident in the past 3 years.

Multi-Factor Authentication

NO. Karate Labs does not require multi-factor authentication on all enterprise applications and production systems.

Security Documentation

We maintain comprehensive security documentation for both open source and IDE plugins.

Open Source Security Documents:

1. Karate SBOM (PDF example): https://github.com/karatelabs/karate/releases/download/v1.5.0.RC3/karate-1.5.0.RC3-sbom.pdf
2. Karate Security status on Sonatype (Maven example): https://ossindex.sonatype.org/component/pkg:maven/io.karatelabs/karate-core@1.5.0.RC3
3. Karate Security status on GitHub: https://github.com/karatelabs/karate/security

IDE Plugins Security Documents:

1. VS Code: https://code.visualstudio.com/docs/editor/extension-marketplace#_can-i-trust-extensions-from-the-marketplace
2. JetBrains: https://plugins.jetbrains.com/docs/marketplace/jetbrains-marketplace-approval-guidelines.html

Updates Management

Open Source

For open source, the user is always in control of upgrading and can choose when to upgrade and which version to upgrade to. This typically achieved by editing the Maven or Gradle build configuration or explicitly downloading the binary artifact. All releases along with detailed release notes can be viewed here: https://github.com/karatelabs/karate/releases

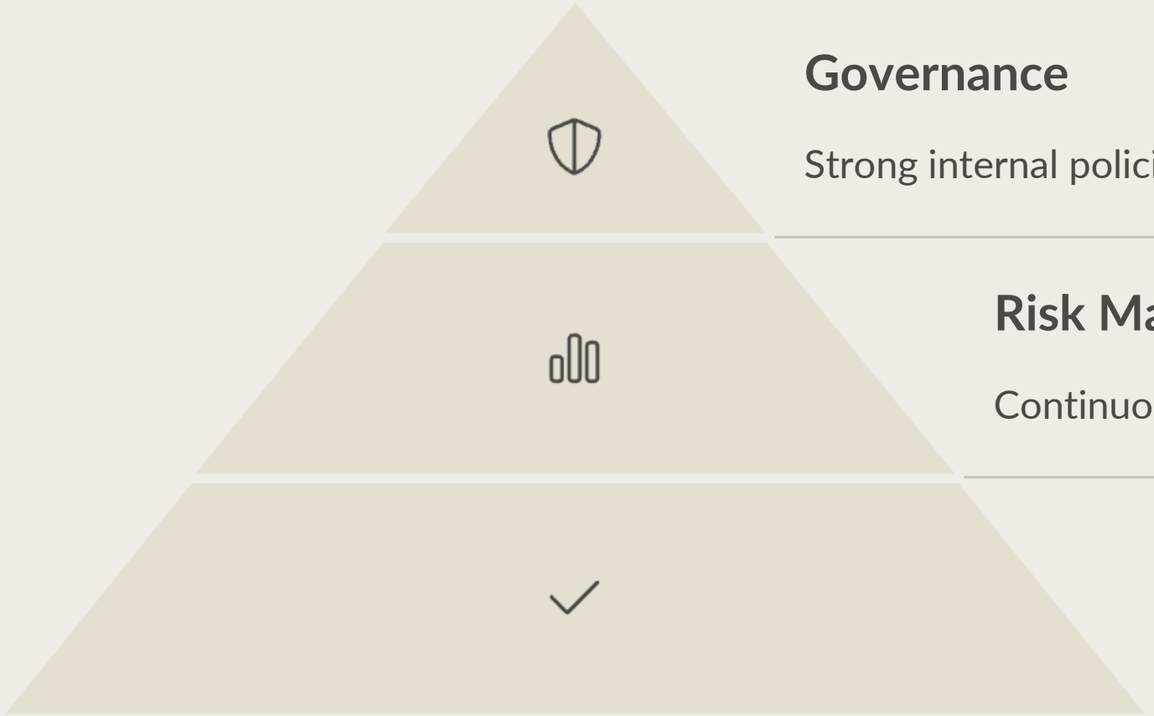
VS Code Extension

By default, new versions of extensions will be installed automatically as documented here. However, users or organizations have the option to disable this. The user always has an option to un-install updates or switch to any previous version which is available, at any time. Note that for a plugin to be published on the VS Code Marketplace, there is a review and approval process involved.

IntelliJ Plugin

By default, plugins are not installed automatically, and the user can see if there are available updates and choose to install them. This behavior can also be changed by a configuration setting. The user always has an option to un-install updates or switch to any previous version which is available, at any time. Note that for a plugin to be published on the JetBrains Marketplace, there is a review and approval process involved.

Governance, Risk & Compliance



Governance

Strong internal policies

Risk Management

Continuous monitoring and assessment

Compliance

Meeting regulatory requirements

Karate Labs maintains a comprehensive governance, risk, and compliance framework to ensure our products meet industry standards and regulatory requirements while protecting customer data and privacy.

Regulatory Compliance

Will any Customer data be shared with your partner (4th Party to Customer)	**NO.**
Does your organization provide system or platform level training with a discussion on secure use of the product?	**YES. We include pricing for this in our enterprise quotation.**
CCPA Compliance	**YES (https://www.karatelabs.io/privacy-policy)**
NYDFS Compliance	**Not applicable to Karate Labs as we do not collect any personal resident data.**
CTA Compliance	**YES.**
CTDPA Compliance	**Not applicable to Karate Labs as we do not collect any personal resident data.**
UCPA Compliance	**Karate Labs is exempt from the UCPA under category of "small businesses".**
VCDPA Compliance	**Not applicable to Karate Labs as we do not collect any personal resident data.**

Note: Karate Labs does not sell any data for direct marketing purposes.

Business Oversight and Continuity

Disaster Recovery

We back up all our data using One Drive for our business operations

Customer Control

Customers maintain their own DR controls for their Karate implementations

Service Providers

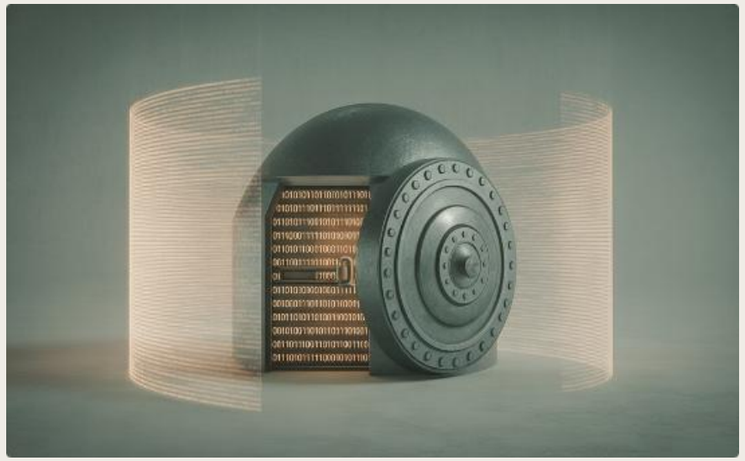
We delegate to Stripe for billing and WorkOS/Google/Microsoft for authentication

Local-First Approach

Karate runs locally on user desktops with no cloud storage of customer data

Karate Labs has documented Disaster Recovery controls we follow internally. There are two aspects to DR here: our own business continuity and our role as a software provider to customers.

Data Protection & Auditing



Data Protection

Local-first approach means customer data never leaves customer firewall

Breach Notification

Well-defined internal processes for security incidents

Access & Activity Audits

Available upon customer request

(costs borne by customer)

One amongst many of Karate's biggest differentiators is our "local-first" approach, meaning Karate is a local solution (not a cloud hosted SaaS offering). When using Karate for test automation, customer data never leaves customer firewall. This amongst others has been a primary driver for companies to migrate from SaaS providers to Karate.

Our commitment to security, privacy, and compliance makes us a trusted partner for enterprises worldwide.

Zero Security Incidents

In the past 4 years

100% Local Processing

Customer data never leaves customer firewall

Trusted by 600+ Companies

Across various industry sectors

Thank You

Our local-first approach ensures your data never leaves your control.

We're committed to maintaining the highest standards of security, privacy, and compliance.