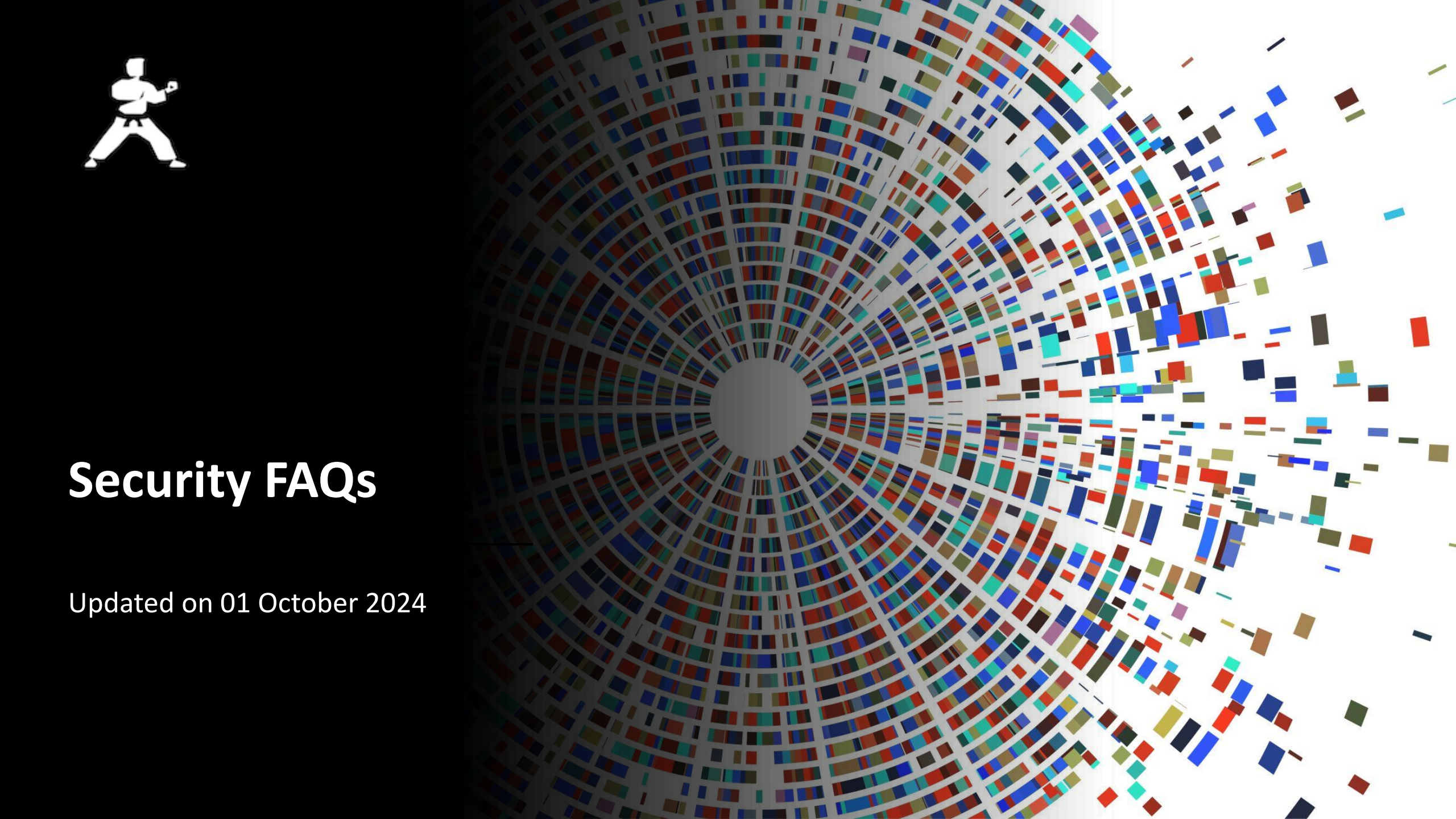

Security FAQs

Updated on 01 October 2024

Technical Capabilities, Integration & Reliability

Does your organization have policies and procedures for detection, disclosure, and review of vulnerabilities within source code, deployed applications, infrastructure, and system components (e.g., network vulnerability assessment, penetration testing)? Do you use automated tools for security testing or code review? Do third parties conduct security assessments on your products? Do you regularly review your list of open-source libraries for updates and vulnerabilities?

Karate security scans and release process

1. **Maven & Sonatype**: Karate is released as a Java package via the Maven Central infrastructure. We cannot release if we have any critical vulnerabilities. Here is an example report (https://help.sonatype.com/iqserver/reporting/application-composition-report/reviewing-a-report) and shows the level of checks when a release is attempted. Maven has a very good reputation and track record when it comes to tracking and resolving vulnerabilities in dependencies. We have been successfully releasing to Maven Central since 2017. All releases can be seen here (https://central.sonatype.com/artifact/com.intuit.karate/karate-core?smo=true).

2. **GitHub Dependabot**: GitHub dependabot continuously scans the repository for known vulnerabilities and deprecated dependencies. We get notified and in most cases GitHub even auto-provides a Pull Request so that the remediation can be performed in minutes. Here is an example of a pull request initiated by GitHub to upgrade one of Karate's dependencies: Bump Netty Version (https://github.com/karatelabs/karate/pull/1473).

3. **Community**: Karate is in use at 550+ enterprises across sectors. 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 (https://github.com/karatelabs/karate/issues/1866) of us addressing the famous Log4J issue (even though we did not depend directly on it), and you can see the discussion and feedback from the community. Another example is our expedited release for Java 11 (https://github.com/karatelabs/karate/issues/2148) when a library we depended on did not have a safe equivalent for Java 8.

4. **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) and you can see the discussion here: High CVE's in Karate core (https://github.com/karatelabs/karate/issues/1834). 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"*. https://github.com/karatelabs/karate/security/code-scanning

5. **IDE Plugins**: there are stringent level of checks done by JetBrains (https://www.jetbrains.com/legal/docs/plugins_site/approval-guidelines/) and Visual Studio Code / Microsoft (https://code.visualstudio.com/docs/editor/extension-marketplace#_can-i-trust-extensions-from-the-marketplace) when publishing plugins to their marketplace.

Is it 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, processing Customer information, 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 support, [where possible] keys provided by a Customer for the use of encryption protocols, protection of sensitive data in storage (e.g., file servers, databases), data in use, at rest, and transmission (e.g., public networks, and electronic messaging)

Not applicable to Karate Labs. 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.

Does your organization have policies and procedures defining the security of user systems (e.g., workstations, laptops, and mobile devices), infrastructure, and components?

YES. We use WorkOS for identifty and SAML SSO management. WorkOS security compliance documents can be shared for reference.

Karate Labs software runs locally on the user desktop and no user data is stored in the cloud. **Note**: Karate Labs offers enterprise customers the option to activate licenses offline. Which means WorkOS need not come into the picture if this is of any concern to enterprise Cybersecurity teams.

Can your organization ensure that any use of Customer production data in non-production environments, receives documented approval and comply with all legal and regulatory requirements?

Not applicable to Karate Labs. Our software runs locally on the user desktop and no user data is stored in the cloud. This means Karate Labs will have no access to any customer data (production, non-production environments).

Will your organization utilize Artificial Intelligence in the processing of Customer information?

NO.

Does your organization have network security controls implemented to detect network-based attacks (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks, in timely manner?

Karate Labs has stringent security controls for our internal requirements. That said, this is not applicable to us. Karate Labs software runs locally on the user desktop and is not exposed as something that can be connected to via the network.

Does your organization restrict service or utility accounts, capable of modifying or overriding system, object, network, virtual machine, and/or application controls?

NO. Karate runs abstracted within industry standard IDE platforms (IntelliJ & VS Code).

Does your organization follow the principle of least privilege for provisioning and de-provisioning entitlements?

YES. After license activation we enable only features allowed by the license tier.

Does your organization offer support for Customer account creation, federated authentication, and group authorization (e.g., SailPoint, Okta, MFA, SAML, nested groups, multiple forests)?

YES. We use WorkOS to manage identity and SAML. On request, we are happy to share the WorkOS security compliance documents for your reference.

We include this in our commercial quote for enterprise tier. **Note**: Karate Labs offers enterprise customers the option to activate licenses offline.

Do you use open-source libraries?

YES.

Please list open-source libraries used in your software.

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

Karate IntelliJ plugin (Java / Gradle based) has the following dependencies:
io.karatelabs:karate-core:1.5.0.RC3
io.netty:netty-handler:4.1.109.Final
net.minidev:json-smart:2.5.1
JetBrains IntelliJ platform (depends on IDE version)
More details can be found here: https://plugins.jetbrains.com/plugin/19232-karate

Karate VS Code extension (JS / NPM based) has the following dependencies:
posthog-node:3.6.2
uuid:9.0.1
VS Code platform (depends on IDE version)
More details can be found here: https://marketplace.visualstudio.com/items?itemName=karatelabs.karate

How long do you offer support and security patching for each version of your software? E.g. N-2, N-3?

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).

Are your organization's applications designed, developed, deployed, and tested in accordance with industry standards (e.g., OWASP)?

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.

Does your company assess the security and privacy practices of all third-party companies with access to customer data?

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

Does your company's product/service encrypt any data prior to insertion into databases (i.e., row level encryption)?

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

Are backups of data performed?

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 (see above)

What training do your development and testing teams receive specific to application security?

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. And code checked-in to GitHub is continuously scanned for vulnerabilities.

Do you disclose to customers all vulnerabilities that affect the security of your software?

YES. Refer https://ossindex.sonatype.org/component/pkg:maven/io.karatelabs/karate-core@1.5.0.RC3 and https://github.com/karatelabs/karate/security

Has your company experienced a security incident in the past 3 years?

NO.

Do you require multi-factor authentication on all enterprise applications and production systems?

NO.

Recent security documents.

Open Source

1. Karate SBOM for latest version (PDF): 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): 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

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

How do you manage updates? Can we manage obtaining and applying updates or do you push automatically?

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

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.

Does your organization meet current regulatory requirements (CCPA, NYDFS, CTA, CTDPA, UCPA, VCDPA)?

CCPA - YES (https://www.karatelabs.io/privacy-policy)
NYDFS - Not applicable to Karate Labs as we do not collect any personal resident data.
CTA - YES.
CTDPA - Not applicable to Karate Labs as we do not collect any personal resident data.
UCPA - Karate Labs is exempt from the UCPA under category of "small businesses".
VCDPA - 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.

Does your organization have documented Disaster Recovery controls they follow internally

YES.

There are two aspects to DR here.

1. DR for our own business: We back-up all our data using One Drive.
2. Software Provider to customers: Karate Labs does not store any data on behalf of users and delegates to the following providers:
    - Stripe - for billing
    - WorkOS for SAML SSO, Google Cloud and Microsoft Azure for OAuth flows.

Customers of Karate need to follow their own DR controls.

Business Oversight and Continuity

Does your organization have a method in which Cybersecurity can request Data Loss or Breach Notification?

YES. We do have well defined internal processes. Please note we do not touch or store any customer data..

Does your organization have a method in which Cybersecurity can request or conduct Access & Activity Audits?

YES. The cost of such audits (if any) will need to be borne by the Customer.

Does your company publish a list of sub-processors with respect to GDPR or CCPA?

Not applicable to Karate Labs.

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.

Thank You