Introduction to Security and Data at Robocorp

13 January 2021

In today's rapidly changing world, we believe security must be at the heart of everything. Robotic Process Automation is a powerful way to save time, but we recognise the risks it also poses to companies leveraging its numerous beneficial capabilities. Therefore, we have developed and keep improving Robocorp's secure ecosystem to enable automation and champion modern ways of working.

RPA is used to automate business critical functions for many organizations. Data that is fed to a software robot can be potentially very sensitive by nature or the automated task itself could pose a significant risk if it was to be used for malicious purposes.

That's why we're committed to ensuring that

- Data handled in our tools remains confidential
- Robocorp Cloud platform can be used in a secure manner, and
- Users can leverage powerful security features to protect data

This whitepaper goes through how Robocorp continuously improves security and data protection . We'll also show you how you can make the most of our powerful security features to apply segregation between different duties and operations for powerful orchestration.

Robocorp's Security culture and operational security

Security is central to Robocorp's mission - we believe that modern ecosystems do not operate without security in place. We include our employees to empower them to work in a security aware manner, from onboarding to regular company-wide security training. We also leverage both internal and external security knowledge to test and verify our solution. Operational security consists of the technical measures we take to make sure security and data protection is in place and possible misuses can be detected.

Security training for employees

All of our employees undergo thorough security training when they start. . We enforce secure usage of services and leverage services like multi-factor authentication and encryption of assets whenever possible.

We also host regular company-wide and team-specific training whenever shifts in our ways of working or new vulnerabilities are detected.

Privacy training and awareness for employees

Our employees regularly undergo privacy-related training. Teammates are empowered to enable encryption for assets and proactively limit access to sensitive information related to our end users.

Security audits and penetration testing

Upon every major architectural change, we conduct a rigorous internal assessment of the solution. We also invite external consultants to conduct thorough penetration tests. If a vulnerability is discovered, we prioritize its fix above other development work and roll out a patch as soon as possible.

Our web application has been tested and verified to be resilient according to OWASP best practices and OWASP top ten.

We understand that security is an ongoing commitment and despite our great efforts to secure our tools, sometimes what is required to discover a problem is to have multiple pairs of eyes looking at the same solution. That's why we also have a responsible disclosure policy for security researchers in case they happen to find a vulnerability in our tools.

Operational security

Our security motto is to follow the principle of least privilege. We restrict both human and programmatic access to services and data.

We remain vigilant for any potential misbehavior in our systems. If we encounter anything that implies a security-related incident has occured, we have a process in place to conduct a thorough security incident response.

Robocorp products security and data protection overview

Robocorp Cloud

Robocorp Cloud is used to orchestrate software robots that can be run either directly in the cloud with the usage of cloud containers or on local machines and servers with Robocorp App.

Robocorp Workforce is the collection of software robots in your arsenal.

Robocorp Assistants are the handy robots that can provide assistance for users to complete tasks that can be partially automated.

We use Amazon Web Services (AWS) as our datacenter provider. AWS maintains SOC2 and ISO 27001 compliance certifications among others and provides robust means to provide secure services to host Robocorp Cloud services securely.

Whenever data travels to Robocorp Cloud we assure that it is:

- Encrypted in transit
- Encrypted at rest using industry standard encryption algorithms
- Data stored in Robocorp Vault is also encrypted in application-level

Robocorp Cloud infrastructure is hosted in European regions and data storages for our infrastructure are therefore located in the European region. However, we use some vendors that may process data outside of the EU/EEA region.

Our Privacy Policy[1] has up-to-date information on how personal data is collected, where it is stored and which third-party vendors we are using to provide the cloud services.

Robocorp cloud container runtime

Robots can be run fully in a Robocorp-managed container. The technology in use is Docker and for each individual run we deploy a short lived container to provide a runtime for the software robot. The containers are segregated from one another and are deployed on an isolated and CIS hardened host server instance.

Robocorp Lab, Robocorp Command-Line and RPA Framework

Robocorp Lab is an IDE that allows smooth integration with Robocorp Cloud to develop software robots and push them to the cloud.

Robocorp Lab integrates with the cloud by storing credential tokens on the local machine. Permissions for Robocorp Lab are based on *user credentials*, which means it has the same access to Robocorp Cloud as the user that created the credentials.

Note: User credentials, as with login credentials, are the most secure if they are used by an individual person or process. Robocorp recommends using strong passwords and to avoid sharing user credentials.

Robocorp Command-Line

Robocorp Lab relies on RCC as a command line tool. It can also be directly used from the command line for access to the cloud to upload or download packages and so on. It uses *user credentials* that are stored locally on the machine.

[1] https://robocorp.com/privacy-policy

RCC has a built-in certificate validation which makes it harder to conduct Man-in-the-Middle[2] attacks against Robocorp tools.

RPA Framework

RPA Framework is the core of software robots. It has its roots in Robot Framework, a Python-based framework designed originally for test automation. With RPA Framework, we further develop Robot Frameworkand to streamline interactions with IDE, Robocorp Lab.

We control the contributors and code submitted to our RPA Framework repository. In this manner, we ensure the core of RPA Framework remains in Robocorp's supervision.

Robocorp App

Robocorp App enables remote orchestration of Robocorp Workforce and Assistants from Robocorp Cloud. It can be hosted on a computer, server or a container. We support Windows, Mac and Linux operating systems.

The initial authentication between Robocorp App and Cloud can be done by logging in with Robocorp credentials or copy-pasting a short-lived one-time token from Robocorp Cloud into a local App. All linked Apps can be viewed within Robocorp Cloud portal. One token cannot be used multiple times for security reasons to prevent fraudulent App linking.

All communications are encrypted between Robocorp App and Robocorp Cloud starting from the initial authentication sequence to websocket communication between the cloud and local App.

Leveraging Security features to protect data in Robocorp products

We want to empower users of Robocorp tools to make secure design choices when creating Robocorp Workforces and Assistants.

Role-based access control

Robocorp Cloud allows fine-grained role-based access[3] control to restrict access for users. This helps to segregate user roles from one another on both Organization and Workspace level, and protect data from unauthorized access.

---

[2] https://owasp.org/www-community/attacks/Man-in-the-middle_attack
[3] https://robocorp.com/docs/product-manuals/security/role-based-access-control

Organization roles

It is possible to limit access to Organization settings, Compliance features and billing with the Organization roles. Adjusting these roles can also restrict access to Workspaces in an Organization.

	Plan & Billing	Management, compliance	Promote and demote Admin to Owner	Promote and demote member to Admin	Add and remove users to organization	Edit and view workspaces and permissions	Add org users to workspaces	Add users only to workspaces they are admin of	See only workspaces they belong to
Owner	x	x	x	x	x	x	x		
Admin				x	x	x	x		
Member								x	x

Workspace roles

Workspace roles are made for adjusting access rights within a single Workspace. This includes who can access and link new Apps or upload software robot code and whether the user can only view and execute processes.

	add or remove users	view and edit workspace permissions	edit processes	view and edit robots	view and edit vault	run, stop and schedule processes	view processes
Administrator	x	x	x	x	x	x	x
Editor			x	x	x	x	x
Member						x	x

Use case: Consulting company with multiple clients

A consulting company creates an Organization in Robocorp Cloud. They work with a multitude of customers to provide Robocorp Workforce and Assistant services to automate menial tasks.

This company creates workspaces to isolate each individual customer from one another. After this, the consultancy assigned roles such as Workspace Editor and Workspace Member to allow clients' software robot developers to collaborate with them. Workspace Members are the business users of the customer, who then use Robot Workforce and Assistants.

Robocorp Vault

Hard-coded credentials and secrets in source code are a major security risk in case the code is exposed to third parties accidentally. Robocorp Vault is a secure means for storing credentials, API tokens or other secrets needed by software robots.

Everything stored in Robocorp Vault is encrypted at rest. In addition to this, they are encrypted two-fold during transit - both by strong HTTPS encryption and by application-level encryption using an envelope encryption pattern. This means that even if the HTTPS traffic were to be decrypted, the token within the HTTP message body remains encrypted.