

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 1 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

RUNGUTAN FOR ORGANIZATIONS

White Paper

Enterprise Features



THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 2 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

Revision History

Revision	Originator	Date	Description of Change
1.0	Marius Mitrofan	31-Jan-2021	Release of document

Approvals

Roles	Approver Name	Signature
Chief Technical Officer	Marius Mitrofan	
Chief Executive Officer	Costina-Madalina Mitrofan	

Useful Resources

Resource Name	Resource Location
Landing page	https://rungutan.com
Blog	https://rungutan.com/blog/
Documentation website	https://docs.rungutan.com/index.html
CLI tool	https://pypi.org/project/rungutan/
GitHub organization	https://github.com/rungutan/

THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 3 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

Table of Contents

1. Intro	4
2. Purpose of document	5
3. Scope of document	5
4. Definitions	5
5. System Overview	8
6. Use cases	8
6.1. Business as Usual Performance Testing	8
6.2. Load Testing as part of Chaos Engineering	9
6.3. Cyber-Attack Simulation	9
7. Valuable Features	9
7.1. API Workflow simulation	9
7.2. Team Collaboration	11
7.3. Unattended test automation	12
7.4. DDoS-level of request simulation	15
8. Relevant technical details	17
8.1. Authentication	17
8.2. Data encryption	19
8.3. Monitoring	21
9. Testimonials	23
9.1. Before using Rungutan	23
9.2. After using Rungutan	23
10. Final notes	24

THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 4 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

1. Intro

Rungutan for Organizations is your own Load Testing platform capable of running the entire Performance Testing suite.

Due to its advanced and flexible design, the Serverless technology behind the Rungutan platform can help organizations simulate application traffic spikes up to the point of orchestrating Distributed Denial of Service cyber-attacks while offering real-time reports with 1-second granularity of data.

The **Rungutan for Organizations** version of the platform has been designed so that it caters specifically to the needs of the customer for which it is intended towards, providing therefore 100% data security and integrity.

Upon deployment of the **Rungutan for Organizations** software platform, the customer may decide upon the following:

- **Datacenter location** to store data (e.g., US or EU)
- **Authentication methods and policies** for its employees and contractors
- **Single Sign-On integrations** with existing customer platforms
- **Administrative organizational UI** to monitor stats for teams, users and tests
- Granular level **audit log** of all user actions
- **Network tunneling** capabilities between customer's and platform's endpoints
- Ability to generate tests routed **through the Internet** or **through the network tunnel**
- **Full ownership** of data stored
- **Platinum-level support** through dedicated development team
- Custom membership **permission matrix**
- **Advanced alerting system** based on failures and response times to custom channels
- **Custom development** as requested by the customer

All the features mentioned above are **on top** of the existing standard Rungutan offering:

- CLI support for all platform tasks
- API support for all platform tasks
- Schedulable tests
- Full CI/CD integration with virtually any such system
- Granular 1-second level report resolution for all test graphs
- Configuration management
- Secret management

THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 5 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

2. Purpose of document

The purpose of this document is to define the enterprise features, technical specifications and environment details that are generated by the **Rungutan for Organizations** Platform as part of its infrastructure and software deployment.

Within this document all details regarding the infrastructure that is being used, how the platform is being monitored, all steps that encompass and ensure the security of the platform as well as encryption of the platform itself and its customer's data are outlined hereafter.

3. Scope of document

The scope of this document includes:

- Platform Overview
- Platform Enterprise Features
- Platform Technical Specifications
- Platform Environment Details

4. Definitions

Stress Testing - This test pushes an application beyond normal load conditions to determine which components fail first. Stress testing attempts to find the breaking point of the application and is used to evaluate the robustness of the application's data processing capabilities and response to high volumes of traffic.

Spike Testing - This testing evaluates the ability of the application to handle sudden volume increases. It is done by suddenly increasing the load generated by a very large number of users. The goal is to determine whether performance will suffer, the system will fail, or it will be able to handle dramatic changes in load. This testing is critical for applications that experience large increases in number of users; for example, utility customers reporting power outages during storms. This can be considered a component of stress testing.

THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 6 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

Load Testing - The purpose of load testing is to evaluate the application’s performance under increasingly high numbers of users. Load, or increasing numbers of users are applied to the application under test and the results are measured to validate the requirements are met. This load can be the expected concurrent number of users on the application performing a specific number of transactions within the set duration. This test will give out the response times of all the important business critical transactions. If the database, application server, etc. are also monitored, then this simple test can itself point towards bottlenecks in the application software.

Endurance Testing - Endurance testing evaluates the performance of the system under load over time. It is executed by applying varying loads to the application under test for an extended period to validate that the performance requirements related to production loads and durations of those loads are met. Endurance testing can be considered a component of load testing and is also known as soak testing.

Volume Testing - Also known as flood testing, this testing is used to evaluate the application’s ability to handle large volumes of data. The impact on response time and the behavior of the application are analyzed. This testing can be used to identify bottlenecks and to determine the capacity of the system. This type of performance testing is important for applications that deal with big data.

Scalability Testing - This testing is used to determine your application’s ability to handle increasing amounts of load and processing. It involves measuring attributes including response time, throughput, hits and requests per second, transaction processing speed, CPU usage, Network usage and more. Results of this testing can be used in the planning and design phases of development which reduces costs and mitigates the potential for performance issues.

CI/CD pipeline - In software engineering, CI/CD or CICD generally refers to the combined practices of continuous integration and either continuous delivery or continuous deployment. CI/CD bridges the gaps between development and operation activities and teams by enforcing automation in building, testing and deployment of applications. Modern day DevOps practices involve continuous development, continuous testing, continuous integration, continuous deployment, and continuous monitoring of software applications throughout its development life cycle. The CI/CD practice or CI/CD pipeline forms the backbone of modern-day DevOps operations.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 7 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

Continuous integration - Developers practicing continuous integration merge their changes back to the main branch as often as possible. The developer's changes are validated by creating a build and running automated tests against the build. By doing so, you avoid integration challenges that can happen when waiting for release day to merge changes into the release branch.

Continuous delivery - Continuous delivery is an extension of continuous integration since it automatically deploys all code changes to a testing and/or production environment after the build stage. In theory, with continuous delivery, you can decide to release daily, weekly, fortnightly, or whatever suits your business requirements. However, if you truly want to get the benefits of continuous delivery, you should deploy to production as early as possible to make sure that you release small batches that are easy to troubleshoot in case of a problem.

Continuous deployment - Continuous deployment goes one step further than continuous delivery. With this practice, every change that passes all stages of your production pipeline is released to your customers. There is no human intervention, and only a failed test will prevent a new change to be deployed to production. Continuous deployment is an excellent way to accelerate the feedback loop with your customers and take pressure off the team as there is not a Release Day anymore. Developers can focus on building software, and they see their work go live minutes after they have finished working on it.

Multi-factor authentication (MFA) - is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA protects the user from an unknown person trying to access their data such as personal ID details or financial assets.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 8 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

5. System Overview

Rungutan for Organizations software is a single-tenant **Software-as-a-Service** platform model deployed into its own Amazon Web Services cloud provider fully separated from any of its other customer deployments.

Because there are no other customer deployments deployed into that specific Amazon Web Services organizational account, data integrity and separation are 100% achieved for all customer information and customer storage data. In such a scenario, each tenant's data is therefore isolated and remains invisible to other tenants.

Through its single-tenant deployment, **Rungutan for Organizations** offers the possibility of running all types of Performance Testing:

- Stress Testing
- Spike Testing
- Load Testing
- Endurance Testing
- Volume Testing
- Scalability Testing

6. Use cases

6.1. Business as Usual Performance Testing

For day-to-day releases and code updates, Rungutan would help track any infrastructure fails in less than 10 minutes, assist in the optimization of caching mechanisms and infrastructure behavior, as well as code breakpoints.

Rungutan for Organizations, combined with a Performance Monitoring solution (e.g., Sentry, NewRelic or Dynatrace), would therefore run a few API calls at each release to provide valuable insights about the infrastructure with the least effort invested.

THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 9 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

6.2. Load Testing as part of Chaos Engineering

Relevant data can be obtained for important releases and any major future events that might cause disruptive effects, such as Black Friday Sales, can be tested and measured through ***Rungutan for Organizations***.

As an organization, offering a service faster than the competition is as important in the digital environment, as it is in an offline scenario. But for doing this, it is very important to know what kind of traffic spikes the infrastructure is capable to support.

Being able to simulate up to 10 Million requests per Minute from 15 concurrent regions around the globe, is a requirement for doing this.

6.3. Cyber-Attack Simulation

Rungutan for Organizations is useful for simulating Distributed Denial of Service scenarios. Through this use case, an organization would be able to monitor the effects of complex physical and cyber-attacks on its infrastructure and take precautionary steps in defining, mitigating and automating the processes of responding to such attacks in order to achieve better resilience.

7. Valuable Features

7.1. API Workflow simulation

Workflow simulation is not a new concept, but one that is currently being overlooked by many such solutions currently existing on the market.

Rungutan for Organizations knows that stressing an API call is not enough to understand a platform's security and maintainability, hence the reason why it defined a method of defining test cases to support user interaction with your APIs.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 10 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

This method uses a JSON-based configuration language to define test cases and simulate steps in the workflow as such a normal user would.

The test case definition system fits any user case definition and can be used by even non-technical persons due to its simple design.

```

"workflow": [
  {
    "path": "/login_path",
    "method": "POST",
    "headers": {
      "Content-Type": "application/x-www-form-urlencoded"
    },
    "data": "user=user&password=pass",
    "extract": [
      {
        "parameter_name": "authtoken",
        "location": "headers",
        "key": "PHPSESSIONID"
      }
    ]
  },
  {
    "path": "/my/profile",
    "method": "GET",
    "data": "",
    "headers": {
      "Authorization": "Bearer ${authtoken}"
    }
  }
]

```

Figure 1 - JSON-based workflow test case definition

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 11 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

In Figure 1, the workflow performs the following steps:

1. Sends a **POST** API call towards path **/login_path** with the necessary payload parameters defined as string within the **data** field and **extracts the header** with key “PHPSESSIONID” and stores it as parameter name “authtoken” to be reused.
2. Sends a **GET** API call towards **/my/profile** with previously defined parameter “authtoken” as a header within the key “Authorization”.

7.2. Team Collaboration

Organizations that use **Rungutan for Organizations** benefit from having the possibility to collaborate not just between members of the same team, but cross-team as well.

All roles within use a permission matrix to define which role has access to which action on the platform. The default roles are:

- Owner
- Admin
- Editor
- Reader

The Owner role is assigned to the first person that either created or is responsible for the team upon its creation. The rest of these roles can be assigned to any other member of the team and the default actions defined on the platform for each role are documented under the **Permissions** section of each of the topics on the official documentation website.

Sample permissions to interact with the alerting system for instance can be found here ->

<https://docs.rungutan.com/Alerts/index.html#permissions>

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 12 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

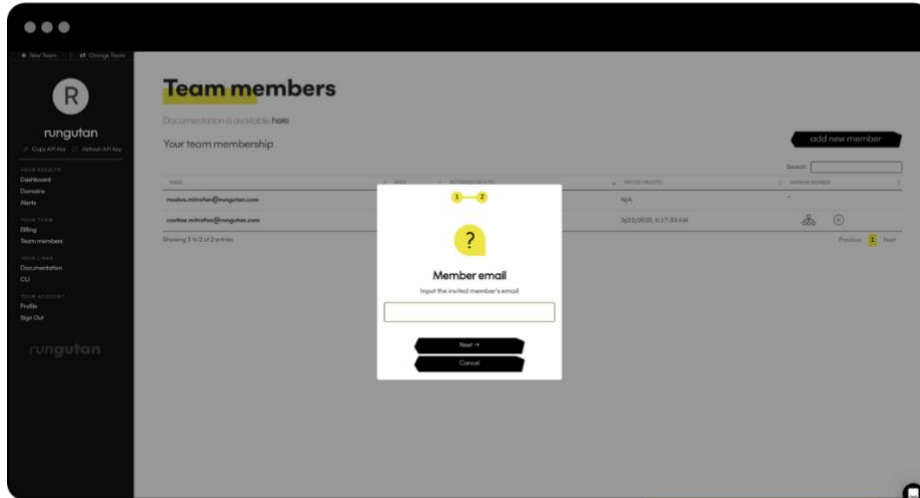


Figure 2 - Adding a new team member in a team

The team collaboration feature has been extended to fit all these purposes, and more:

- Share test results between team members
- Define tests cases together
- Collaborate on alerting events
- Interact simultaneously with result graphs

7.3. *Unattended test automation*

The **Rungutan for Organizations** allows of course its usage through a responsive web UI platform available for all devices, but it can be used of course unattended through the following methods:

1. Schedulable jobs
2. Terminal command line
3. API calls
4. CI/CD pipeline definitions

THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 13 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

7.3.1. *Schedulable jobs*

Rungutan for Organizations makes use of [AWS CloudWatch](#) to define test cases that can be executed either at regular intervals or at later dates, depending on user definition.

Full control of the timeframe of the schedulable events is offered to the customer’s team based on the roles assigned to its team members.

Such jobs execute the test cases as defined and their results are published on the same dashboard as the other tests, with the specific note that the test name specifically defines that test case as a scheduled job by adding the prefix “CRON” to it.

7.3.2. *Terminal command line*

Rungutan for Organizations had developed an open-source CLI to use with its platform that has been open-sources within its GitHub organization repository.

The CLI tool can be installed using **PIP** (<https://pypi.org/project/rungutan/>), supports Python 3 systems and its source is available in the **Rungutan/rungutan-cli** (<https://github.com/Rungutan/rungutan-cli>) repository.

Any action that can be performed through the web platform version has an equivalent in the CLI and authentication against a current organization and/or team is done through an API key which is uniquely generated for any member on the platform.

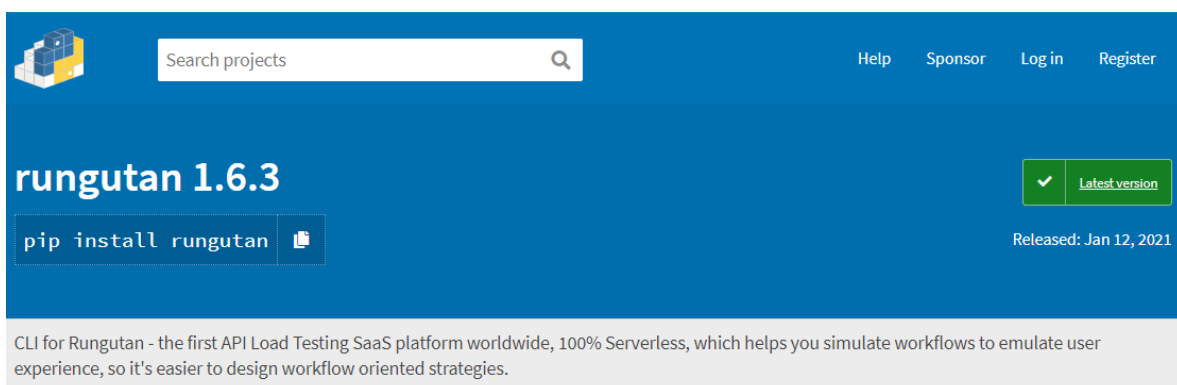


Figure 3 - PIP project of Rungutan CLI

THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 14 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

7.3.3. *API calls*

Like the CLI utility, any action within the web platform or through the CLI has an equivalent as an API call.

All calls towards the platform, regardless of method of execution, return the same results, with no exception.

Our exposed API calls offer the customer the possibility to react, interact, and query any component of the platform's infrastructure or database granting him full ownership and control of the data that is stored.

The authentication against API calls uses the same method as the CLI, specifically:

- Organization ID
- Team ID
- API Key

7.3.4. *CI/CD pipeline definitions*

Due to **Rungutan for Organizations**'s ability to understand and process API calls from either a CLI, an API call or actions on the web-platform, generating CI/CD pipeline using Rungutan should be simple.

The list of actual CI/CD system integrations is pretty much limitless, all needing to happen for that is simply reusing the CLI or provided Docker container to do your job.

There are however built-in integration out-of-the-box with some systems, such as GitHub Actions through its Marketplace offering.

The latest version of the **GitHub Actions Marketplace** offering for Rungutan allows you to run tests by referencing git-versioned test case files from any GitHub repository that the customer has access to.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 15 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

A sample CI/CD pipeline through GitHub actions looks like this:

```

name: Load test with Rungutan

on:
  release:
    types:
      - created

jobs:
  load:

    runs-on: ubuntu-latest

    steps:
      - uses: actions/checkout@v2

      - name: Load test your platform with Rungutan
        uses: Rungutan/rungutan-actions@1.0.0
        env:
          RUNGUTAN_TEAM_ID: ${ secrets.RUNGUTAN_TEAM_ID }
          RUNGUTAN_API_KEY: ${ secrets.RUNGUTAN_API_KEY }
          RUNGUTAN_TEST_FILE: test_file.json
          RUNGUTAN_TEST_NAME: ${ github.repository }-${ github.ref }

```

Figure 4 - GitHub Actions CI/CD pipeline using Rungutan Marketplace offering

7.4. DDoS-level of request simulation

The platform has been built from the ground up using the Serverless Design model which launches short-lived containers through the use of [AWS Lambda](#) services which can spawn in different regions and as many times as needed within a few milliseconds of each other, therefore being able to deliver and sustain high volume application level (OSI Layer 7) traffic towards the customer’s endpoints.

The normal version of the platform can currently reach 10.000.000 (ten million) requests/minute within 15 concurrent regions concurrently.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 16 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

The **Rungutan for Organizations** version of the platform can reach virtually unlimited number of requests since all originating threads are served towards the customer’s sole purpose use, instead of being shared with other customers.

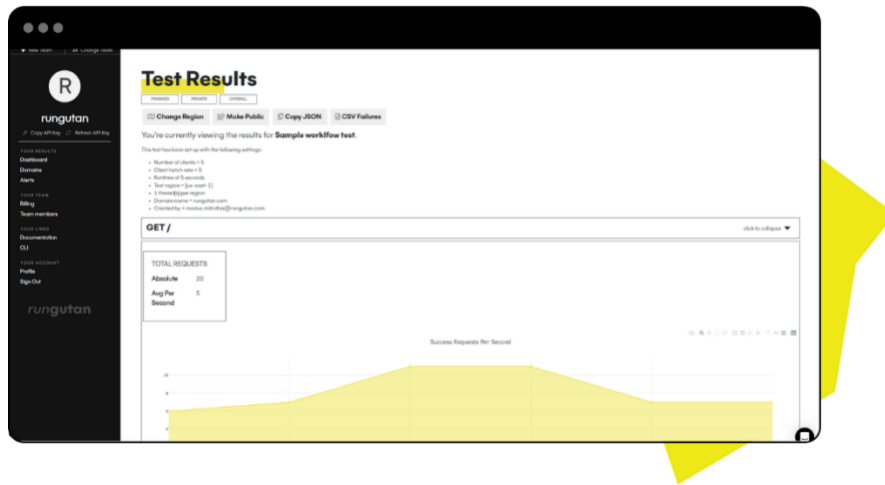


Figure 5 - Result page of a sample test

The current regions that can be used to concurrently spawn tests are:

- ap-northeast-1 = Tokyo
- ap-northeast-2 = Seoul
- ap-southeast-1 = Singapore
- ap-southeast-2 = Sydney
- eu-central-1 = Frankfurt
- eu-west-1 = Ireland
- eu-west-2 = London
- eu-west-3 = Paris
- us-east-1 = North Virginia
- us-east-2 = Ohio
- us-west-1 = North California
- us-west-2 = Oregon
- ca-central-1 = Canada (Central)
- ap-south-1 = Mumbai
- sa-east-1 = Sao Paulo

THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 17 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

8. Relevant technical details

8.1. Authentication

8.1.1. Authentication systems available

The *Rungutan for Organizations* platform supports 2 types of authentication to access its internal resources, based on method of access:

- User-based signing request -> available only for the web-platform
- API key -> available for direct API calls or through the CLI

Based on the type of access, the platform checks different headers that are sent through the request and verifies the authentication and authorization tokens within them to understand if:

- User generating request
- Access grant for user
- Permissions for specific resource to be accessed

These authentication methods have been developed using the [AWS Cognito APIs](#) and the API Keys specification from within [AWS API Gateway](#).

8.1.2. Multi-Factor Authentication support

Multi-Factor Authentication support is provided for the user-based signing request within the web-platform for accounts that are being maintained within the platform.

The MFA supports Software Token for day-to-day usage of the platform and can be easily configured through the "*Profile*" once the user is logged in.

All keys pertaining to the MFA authentication system are being handled securely and responsively by AWS through the Cognito offering.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 18 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

In case there is a problem accessing the account, additional verifications will be performed through the SMS-based method which uses the user's *verified phone number*, which is defined through the "*Profile*" page as well.

8.1.3. *AI-based login threat detection*

Rungutan for Organizations employs a strict AI model of security regarding the location, time zone and method of authenticating a user.

Therefore, each time a user authenticates through the web platform, a series of AI based mechanisms verifies if the requests is valid or not by checking current logged in sessions, usual places of login and normal timeframes of work.

If any irregularities are discovered, an initial prompt is made towards the user to enforce a secondary method of verifying the account, which based on the user's profile, these can be:

- Software Token
- SMS
- Email

In any of these cases, a notification is sent towards the user via email about the possible problem that was detected to ensure that no accounts can be compromised.

Should any problems arise, the user is afterwards invited to contact the Rungutan Support Team to verify all login activities and ensure system integrity.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 19 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

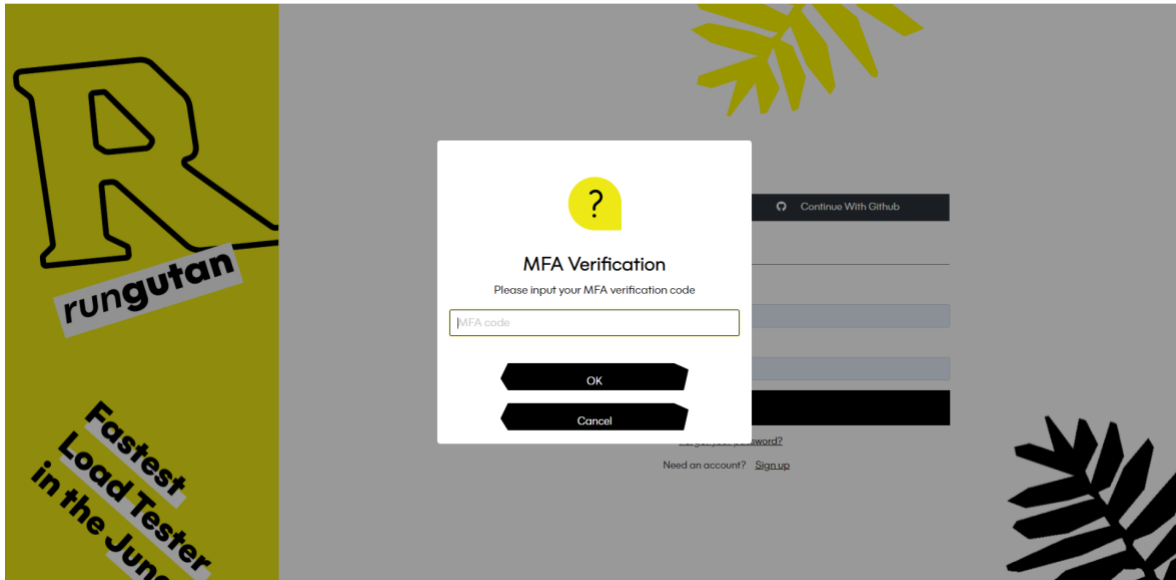


Figure 6 - MFA verification sample pop-up using Software Token

8.2. Data encryption

8.2.1. Object storage privacy

Object storage is used by **Rungutan for Organizations** to employ the storage of the following types of files:

- CSV report of failures for each test
- CSV of detailed responses

All files are stored as blobs using **AWS S3** service in separate buckets that are hidden from the Internet and can only be accessed through the Platform itself.

The objects within the bucket are stored privately as well and each time they are requested by the customer, an **AWS S3 Presigned URL** is generated which allows the user, for a very short period of time, to download the object.

THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 20 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

8.2.2. *Object storage encryption at rest*

All files that are stored within AWS S3 buckets are encrypted at rest.

This type of encryption is being performed through **AWS KMS** and upon customer’s request, the KMS key can be shared with the customer’s AWS account and data within those buckets replicated in customer-defined AWS S3 buckets.

If that happens, the customer is afterwards responsible for maintaining the privacy, security, integrity, and right-of-use of all documents within those buckets.

8.2.3. *Code signing*

The platform code is GIT-versioned and deployed, at regular intervals, towards the customer’s platform version using custom code and infrastructure orchestration systems in place generated by the Development Team behind Rungutan.

Besides ensuring that specific version of the code gets released at specific intervals, the Development Team will generate for the user a “Code Signing Policy” which will be used in order to actually perform the **Code Signing Process for AWS Lambda**.

Code Signing is used to ensure code integrity through **AWS Signer** which is a service that allows the Development Team to create digitally signed code packages for all functions and layers that the platform needs.

8.2.4. *Database encryption at rest*

The database behind **Rungutan for Organizations** is **AWS DynamoDB** which is a key-value and document database that delivers single-digit millisecond performance at any scale. It is a fully managed, multi-region, multi-active, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second.

Besides its immense scaling capabilities, DynamoDB was used because it allows encrypting all data at rest through AWS KMS, the same way it was done for AWS S3 object storage.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 21 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

Upon customer's request, the AWS KMS key used for DynamoDB can be shared with the customer and a logic of globally replicated tables can be generated so that the customer can contain a live copy of the data at any given time.

If that happens, the customer is afterwards responsible for maintaining the privacy, security, integrity, and right-of-use of all data within those DynamoDB tables.

8.2.5. *Row-level encryption*

Besides encrypting data at rest, **Rungutan for Organizations** also makes use of AWS KMS to encrypt the data at the columnar level for sensitive aspects of the platform.

The following information is currently considered sensitive and encrypted at the column level:

- Values of secret management properties
- All workflow steps within test cases

Since DynamoDB does not store any user data < AWS Cognito is used for that >, there is nothing to encrypt.

8.3. **Monitoring**

8.3.1. *API-level performance monitoring*

To ensure proper SLA for all APIs which encompass the **Rungutan for Organizations** platform, the following services are deployed and configured within the same AWS account:

- **Sentry** -> an open-source stack of on-premises Sentry was created by the Development Team behind Rungutan and is available on GitHub in the **Rungutan/sentry-fargate-cf-stack** repository
- **AWS CloudWatch** -> used to detect anomalous behavior in your environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep the platform running smoothly
- **AWS X-Ray** -> provides an end-to-end view of requests as they travel through the application, and shows a map of the application's underlying components

All API level performance metrics are analyzed in the form of thresholds as well as patterns and provide a complete overview towards the platform’s health.

8.3.2. Web platform page load

The web platform page load is being handled by Sentry as well through the integrated JavaScript engine mechanisms which send encrypted data with monitoring stats towards the internally deployed Sentry platform to track and ensure high SLA for the user.

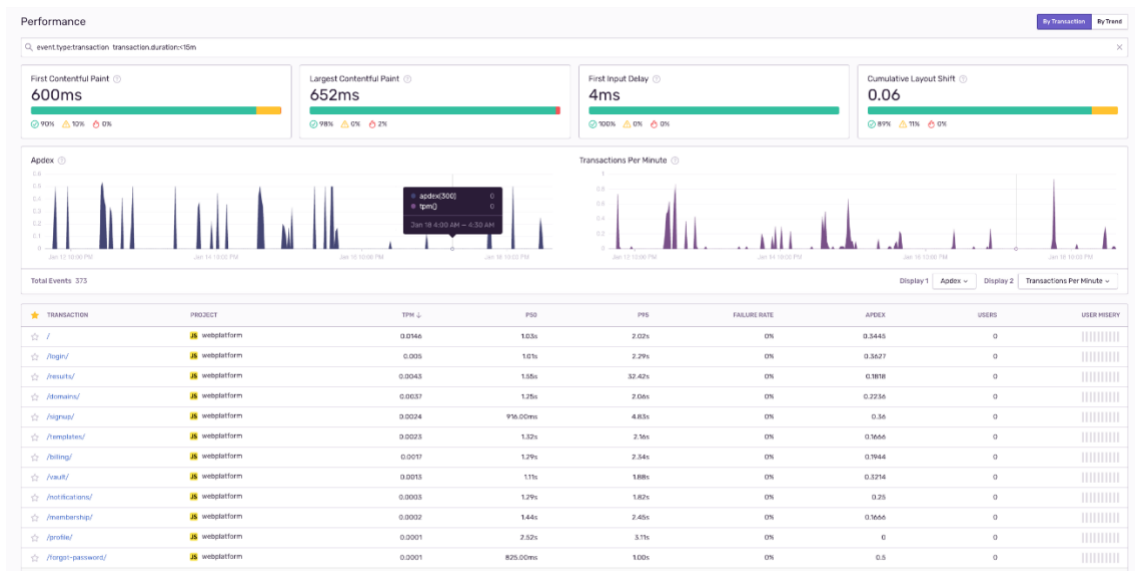


Figure 7 - Web platform performance monitoring with Sentry of page load

<https://rungutan.com/blog/sentry-fargate-cf-stack/>

8.3.3. Exception handling

Exception handling is being targeted currently through Sentry as it has been integrated at the code level to ensure that any exceptions or error messages are being handled immediately and effectively.

THIS DOCUMENT CONTAINS INFORMATION THAT IS CONFIDENTIAL AND PROPRIETARY TO SC NETBEARS TEAM SRL. NEITHER THIS DOCUMENT NOR THE INFORMATION THEREIN MAY BE REPRODUCED, USED OR DISTRIBUTED TO OR FOR THE BENEFIT OF ANY OTHER PARTY OTHER THAN SC NETBEARS TEAM SRL WITHOUT THE PRIOR WRITTEN CONSENT OF SC NETBEARS TEAM SRL.

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 23 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

9. Testimonials

One of the case studies that illustrate the power of *Rungutan for Organizations* is the one that was created in partnership with an EU-based Fintech platform called [Pago](#).

9.1. Before using Rungutan

Before using Rungutan, Pago had some problems with their API calls in regard to their caching mechanism. Don't get us wrong, they knew what they were doing, and they were using caching as much as possible, but because they didn't have a tool to actually measure and understand which and what components needed to be cached, it wasn't optimum at all.

Furthermore, scaling experiments were pretty hard to do. Generating and consistently sustaining live traffic from multiple IPs in order to induce scaling mechanisms was pretty hard to do using the current tools on the market.

9.2. After using Rungutan

Just three days into their trial and they've already started tweaking their infrastructure as now they had valuable information which created actionable insights.

After a few days of tweaking and testing, not only was Pago able to fix all of their API caching problems, but using the *Rungutan for Organizations* stress testing logic, they were able to optimize their auto-scaling mechanisms, helping them save money on ensuring that they always have exactly the amount of infrastructure power that they need.

The initial loading of the app experience has also improved considerably, simply because Pago now loads 62% faster than before! The code optimizations and the backend caching problems could not have been identified without a load testing platform as good and easy to use as Rungutan is.

<https://rungutan.com/blog/startup-fintech-increase-throughput-load-testing/>

rungutan	Document Type and Number: WP-RUNGUTAN-EF-001		
	Document Author: Marius Mitrofan	Effective Date: Last date of signature	Page 24 of 24
RUNGUTAN FOR ORGANIZATIONS – White Paper on Enterprise Features			

“We had been searching for a while for a service which we could rely upon to replicate & test our user flows and I can say for certain that finding Rungutan has helped us step up our load testing to banana levels. All this through a clear UI & API while having close to no limits on the testing power, who does not want that? Add to this the stellar support from the Rungutan team and you get yourself a service you can rely upon during the hardest as well as calmest waters.”

< Alex-Gala Popescu, Co-Founder Pago >

10. Final notes

Our long-term vision is to create through **Rungutan for Organizations** a business environment where top-notch resources can be affordable as well, for anyone who is willing to not compromise the quality of their work.

By creating Rungutan, we wanted to offer more autonomy to IT professionals by saving them lots of time spent on traditional Load Testing platforms and to bring added value to final clients by reducing their costs, while putting disruptive technology to good use.