EPAM Syndicate

Rule Engine

October 2025

Client & Market Fit

Problem & Solution Fit

PROBLEM

An enterprise needs to be sure that the environments used for production or development purposes are compliant with legal, industry-related, corporate, and customer-specific requirements, standards and best practices. There is also a need to make sure that the infrastructures are cost-effective and properly optimized.

Finding proper tools, performing checks in different directions, analyzing the findings and immediate reaction to them, proper remediation planning and ensuring continuous compliance can be a challenging task.

These challenges are specifically faced by:

- **Existing businesses** that need inventory and assessment for their legacy infrastructure and planned updates
- **New businesses** that need to make sure that their processes and infrastructure match the standards, are effective and safe

TARGET MARKET

SOLUTION

EPAM Syndicate Rule Engine allows checking and assessing virtual infrastructures in AWS, Azure, GCP infrastructures and Kubernetes clusters against different types of standards, requirements and rulesets.

By default, the solution covers hundreds of security, compliance, utilization and cost effectiveness rules, which match world known standards like GDPR, PCI DSS, CIS Benchmark, and a bunch of others.

The core of the EPAM Syndicate Rule Engine is a mechanism that scans a specified account to find resources that are not compliant with the applied rule set.

The result of a scan is a list of vulnerabilities and metadata of the scan that can be used to generate 20+ analytics reports (delivered as emails) for different organization levels: Chief, Department, Project, Operational.

Value Proposition & Differentiation

VALUE

EPAM Syndicate Rule Engine is a cloud infrastructure assessment solution. It allows checking and assessing virtual infrastructures in AWS, Azure, GCP, infrastructures against different types of standards, requirements and rulesets.

By default, as a cloud rule engine, it covers hundreds of security, compliance, utilization and cost effectiveness rules, which cover world known standards like GDPR, PCI DSS, CIS Benchmark, and a bunch of others.

As a result, it ensures customer solution's fit to corporate, legal, and industry requirements, with high effectiveness, as well as minimized human effort and error possibility.

KEY DIFFERENTIATORS

All-in-One Checks

A single tool to assess against different types of standards and requirements (Security and FinOps out of the box)

Easy to Admin

Easy to configure, manage and review the tool performance

Quick Setup & Launch

The solution is offered in preconfigured state covering major part of customers needs in assessment. Just run and scan
(up to 30 minutes to configure)

Full Cycle Support

Configure the product on your own or we can do it for you

Rich & Customizable Rules Library

Includes numerous rule sets for security and FinOps out of the box (constantly updated), and allows own rules creation and managing the set of the rules to be applied.

+ Small cost for underlying AWS infra

Strategic & Tech Availability

Scalability & Usability

QUICK SETUP

- 30 minutes to start
- Self-service or Support-assisted configuration

RULES MANAGEMENT

- Regular rules review
- Custom rules (own or assisted creation)

CONVENIENT CONFIGURATION

- Multi-tenant
- Cross-cloud
- Platform agnostic

SCAN RESULTS PROCESSING

- **Detailed data for analytics** – the scan results are returned as metadata that can be processed by selected tools.
- **Scan data analytics** – the scan results can be analyzed and transformed into over 20 reports facing different types of users.
- **Data obfuscation** – the possibility to cover the details of the vulnerable resources during the processing, without exposing the vulnerabilities to third-party tools.

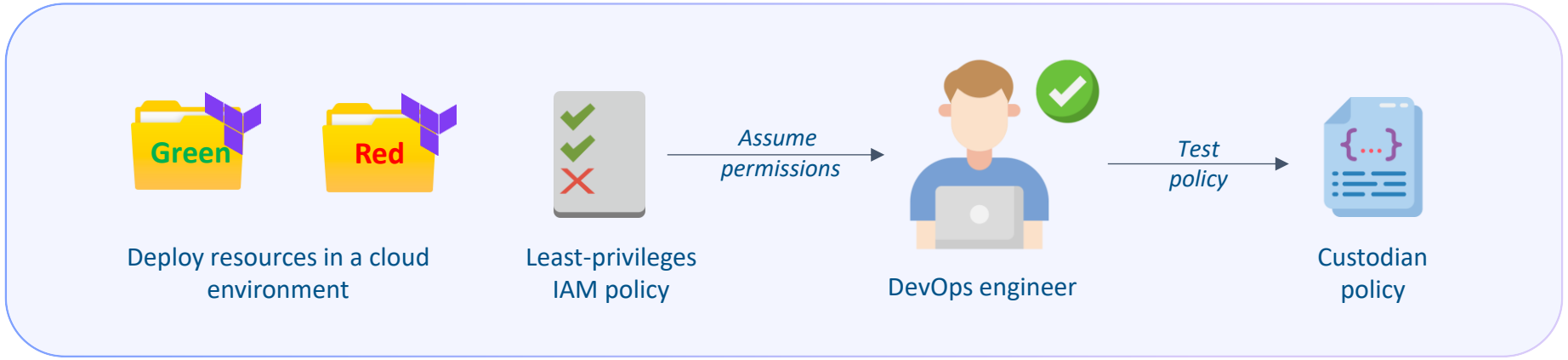
Tech Health & Debt: Quality Assurance

Throughout the SRE product development, the team was facing and resolving a set of challenges, which resulted into building a reliable and easy to maintain product

Problem 1: Absence of quality assurance

Implemented solution:

- Create *red* and *green* Terraform templates per policy
- Create a file with minimal permissions required to run a policy
- Have it manually tested in test environment



Manual testing process

Tech Health & Debt: Quality Assurance

Problem 2: Manual testing of each Terraform template for the full ruleset extremely slow

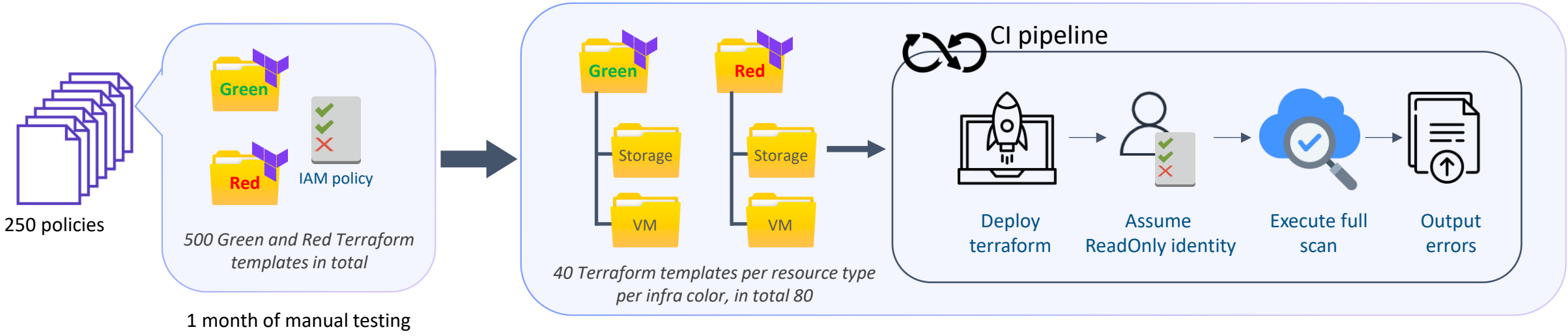
It takes about 1 month for one DevOps engineer to test

Solution:

- Aggregate templates based on policy resource type (storage, vm, sql, etc)
- Automate testing with CI pipeline

Results:

- Accelerated testing from 1 month to 3-4 hours of automatic tests and 2-3 d. by DevOps engineer
- Covers testing of
  - Custodian policies
  - IAM permissions
  - Cloud API
  - Cloud Custodian core



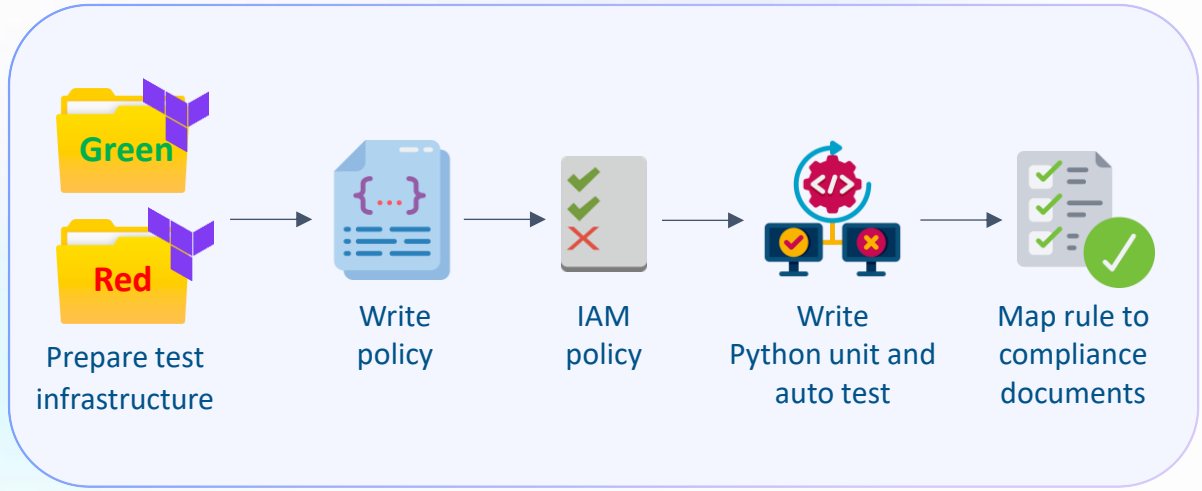
Approximately 3h of pipeline execution, and 2-3 d. of DevOps engineer analysis

Policy as Code Development Lifecycle

1. Create Terraform template
   - 1.1 Create *'red'* terraform infrastructure
   - 1.2 Create *'green'* terraform infrastructure
2. Create a policy
3. Map policy to cloud events
4. Add metadata to a policy (severity, impact, remediation, etc)
5. Write a Python unit test for policy, record infrastructure
6. Add auto-test for policy
7. Create a file with minimal permissions required to run a policy
8. Map policy to regulation documents and MITRE ATT&CK

Cloud Custodian Rulepacks:

- *github.com/epam/ecc-aws-rulepack*
- *github.com/epam/ecc-azure-rulepack*
- *github.com/epam/ecc-gcp-rulepack*
- *github.com/epam/ecc-kubernetes-rulepack*



Monthly Release Cycle

Syndicate Rule Engine is updated on a monthly basis. Each release is described and documented, which typically covers the following:

- New features and important updates
- Improvements
- Issue fixes
- Artifact and component updates
- Rulesets updates
- Changelog References

- SRE CLI. Added resource exception management commands (`sre resource exception describe/add/update/delete`)

ISSUE FIXES

- SRE. Fix issue during releasing ruleset
- SRE. Fix version compatibility for SRE CLI
- SRE. Updating role policies issue

ARTIFACT AND COMPONENT UPDATES

Software Components:

- Syndicate Rule Engine API: 5.14.0
- Syndicate Rule Engine CLI: 5.9.0
- Cloud Custodian: 0.9.46
- Defect Dojo: 2.34.2
- Modular API: 4.3.5
- Modular CLI: 2.3.12
- Modular Service: 3.3.2
- Redis: 7.2.3
- MinIO: RELEASE.2025-05-24T17-08-30Z (1.3.0)
- Mongo: 5.0.28
- Vault: 1.19.5 (1.2.1)

Please follow the steps below to update your system to the new release, version 5.14.0:

1. **List available updates:**
   `sre-init list` - Displays the available updates and helps confirm the version to update.
2. **Execute the following commands to perform update:**
   `sre-init update --same-version --no-backup --no-patch` - Gets new update manager.
   `sre-init update` - Starts the update process to a new version.

For more detailed instructions on the update process, refer to the Update Guide.

RULESETS UPDATES

The table below presents statistics on ruleset changes that occurred during the release.

Rulesets Status	AWS	Azure	GCP	Kubernetes	OpenStack
New	0	3	0	0	0
Updated	18	13	0	0	0
Deprecated	3	0	0	0	0
Non-compatible	15 (↓4)	5	63	0	0
Compatible	567(↑1)	332 (↑3)	230	82	32
Total	**582 (↓3)**	**337**	**293**	**82**	**32**

Competitive Landscape: Open Policy Agent vs Cloud Custodian

	Cloud Custodian	Open Policy Agent (OPA)
Policy language	Simple YAML format	More complex Rego language
Terraform support	+	+ Requires creation of a *tfplan.json* before policy validation
OpenStack support	+ Work in Progress	- Requires middleware that will pass resources description into OpenStack
Kubernetes / OpenShift support	2 modes: Audit and Enforcement	
	In audit mode: can be installed anywhere as a Python3.10 application with a user with ReadOnly permissions In enforcement mode: installs as a Dynamic Admission Controller	Installs as a Dynamic Admission Controller
Kubernetes policy library	81 audit policy	45 audit policies 6 mutation policies
Open Source	CNCF incubating project Highly supported by community. In the last few years, development speed for supporting new platforms has increased.	CNCF graduated project Has enterprise version – Styra, with added support for data sources you already use, without the need to perform any discovery or write and maintain custom data source integrations.
Reporting	• Built-in • Multiple custom EPAM reports	-
Advantages	• Supports multiple platforms • Policies for IaC do not require execution of '*terraform init & plan*' • For audit mode for K8s and clouds scans can be installed anywhere • Custom EPAM tool – Custodian as a Service (CaaS)	• Takes any JSON file as input, not limited by a platform • Integrated with Terraform Cloud
Disadvantages	• Can work only with supported platforms, and their resources, but they're open to contribution	• Requires middleware to pass input to it

Other Similar Solutions

Qualys: cloud-based security and compliance solutions, offering vulnerability management, compliance monitoring, and threat protection for IT systems and web applications**.**

Wiz.io: a cloud security platform that identifies risks and vulnerabilities across multi-cloud and containerized environments, providing actionable insights.

Stacklet.io: a cloud governance platform that helps businesses manage security, compliance, and operational efficiency across their cloud infrastructure.

SRE DIFFERENCIATORS

Similar Solutions

- **Rich and customizable rules library** — Includes numerous rule sets for security and FinOps out of the box, and allows own rules creation and managing the set of the rules to be applied.
- **Quick installation and setup** — needs up to 30 minutes to setup and run the first scan
- **Cost effectiveness** — small bills for used AWS infrastructure.

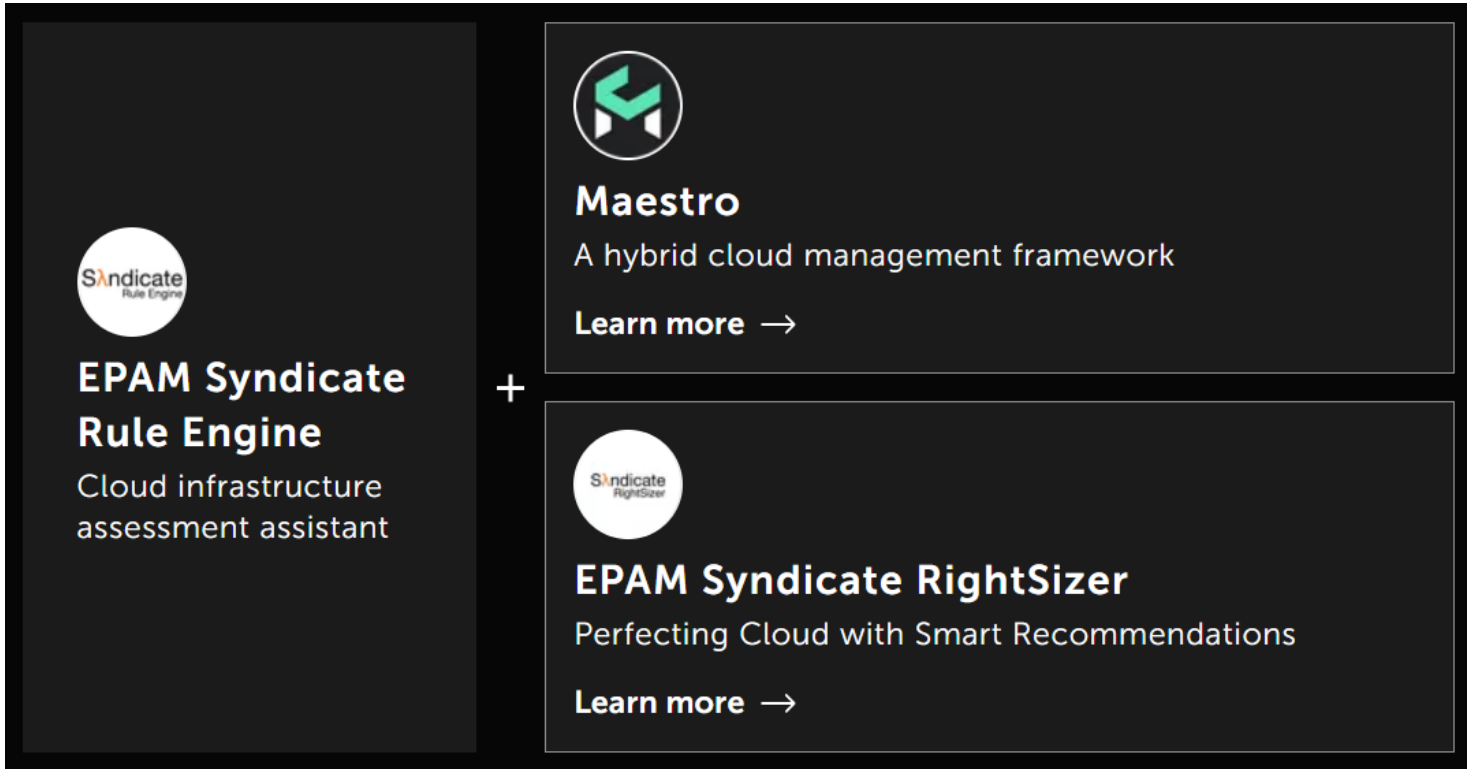
Related AWS Products & Services

Multi cloud security and compliance – being hosted in AWS, Syndicate Rule Engine can be used for compliance check of resources in AWS, Azure, and GCP clouds, as well as within Kubernetes clusters.

Strategic Alignment & Cross-Sell

The SRE is actively delivered not only as a stand-alone solution, but also as a part of complex offerings and combinations

Maestro Cloud Management Platform	As a component enabling detailed and effective infrastructure assessment
Syndicate Education Platform	As a component for automated tasks check
GovTech Offerings	As a component enabling infrastructure security and compliance



GTM & Enablement

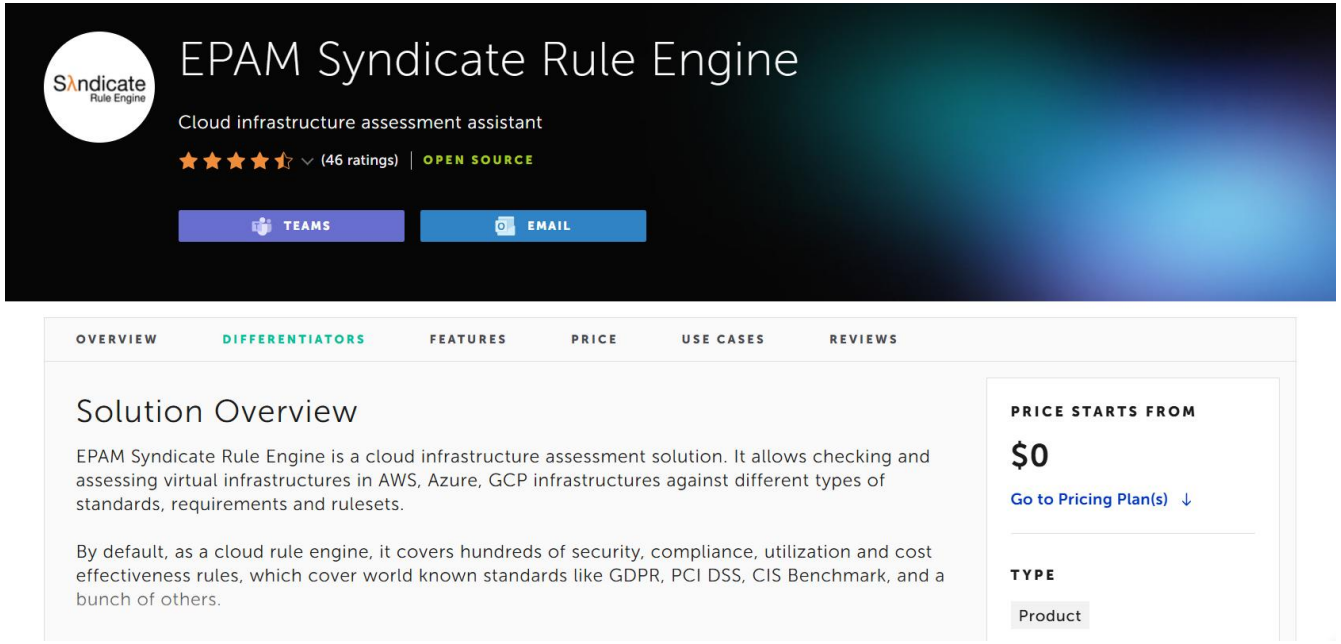
Sales and Marketing Readiness

Product Sales Points

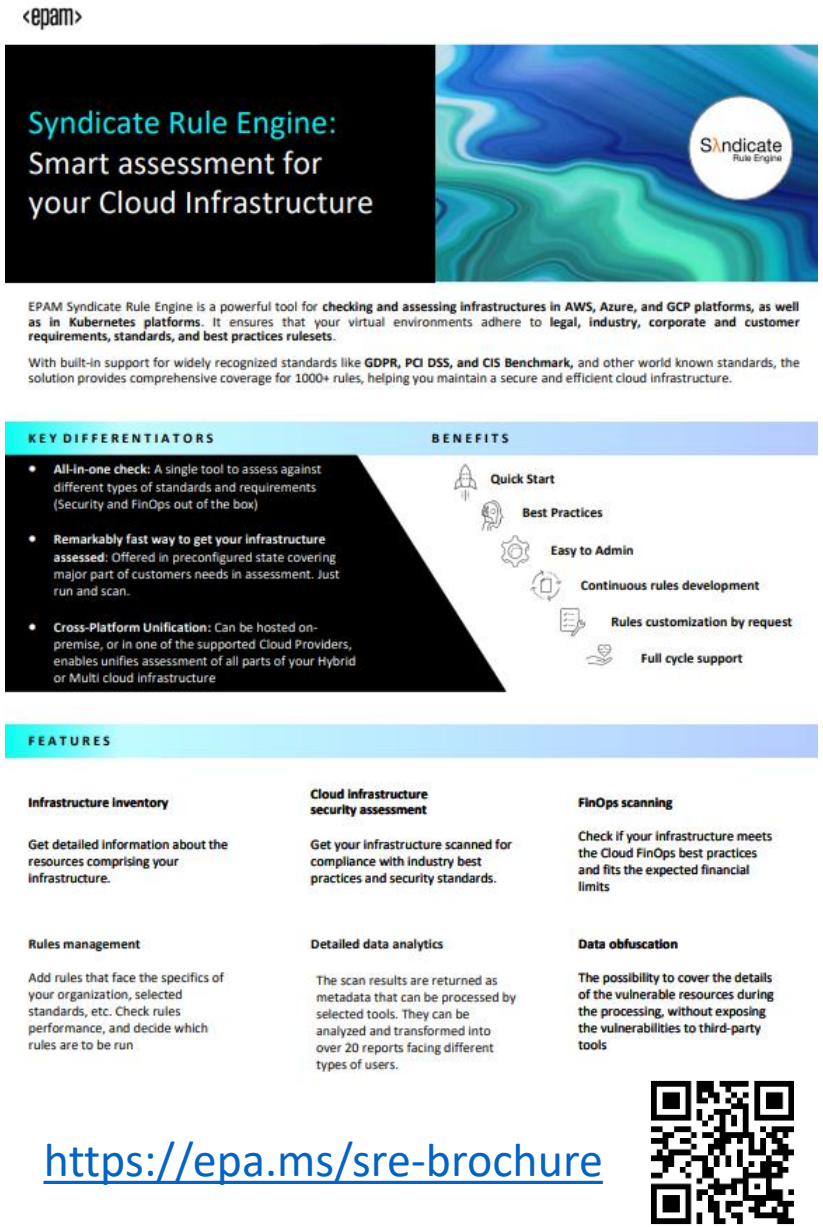
The product available on:

- *AWS Marketplace*
- *EPAM Solutions Hub*

Product on Solutions Hub



Product Brochure



https://epa.ms/sre-brochure

Product Pricing

SAAS Pricing

Monthly plans | Yearly plans (SAVE 10%)

MOST POPULAR

Startup

Access to a tenant in a multi-tenant setup with all the features included

$999/mon

- ✓ Environment Type - Shared
- ✓ Scans amount - 5/mon
- ✓ Tenants - 1

See more ↓

Business

Dedicated instance for you only providing enhanced security and extended management features

$3,990/mon

- ✓ Environment Type - Dedicated
- ✓ Scans amount - Unlimited
- ✓ Tenants - Unlimited

See more ↓

Enterprise

Custom offering composed personally for your organization

Let's talk

- ✓ Environment Type - Dedicated
- ✓ Scans amount - Unlimited
- ✓ Tenants - Unlimited

See more ↓

OnPrem Pricing

Monthly plans | Yearly plans (SAVE 10%)

Open Source

Feel free to deploy the service on your own and be secured with no charges

Free

Basic Security

Best match for Startups who do not have a dedicated Security Expert

$3,000/mon

- ✓ Professional service hours - 24
- ✓ Minimum commitment month - 3

MOST POPULAR

Standard Security

Option to have a reliable security support of the software

$6,400/mon

- ✓ Professional service hours - 64
- ✓ Minimum commitment month - 3

Zero Tolerance Security

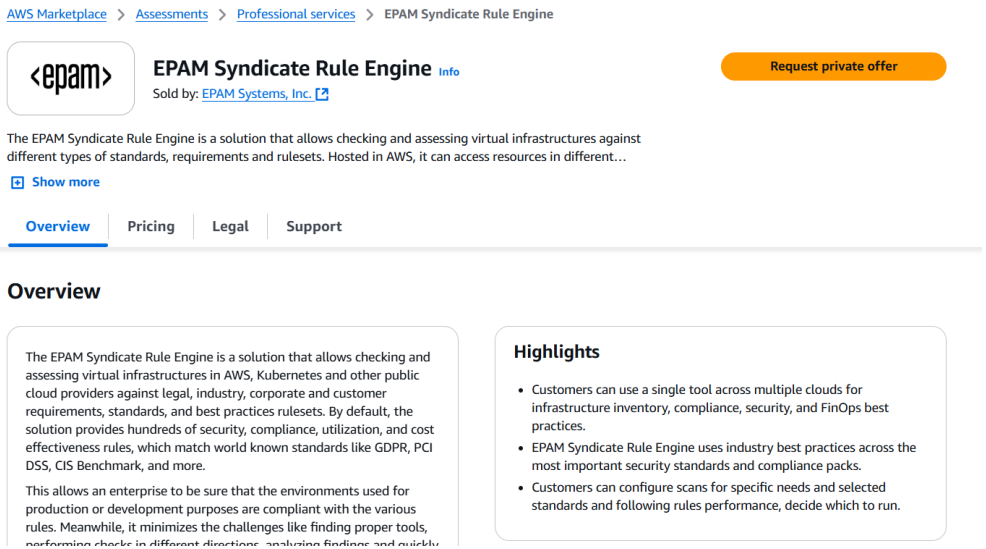
Minimize possible loses related to data leaks and infrastructure backdoors of your critical software components

$14,000/mon

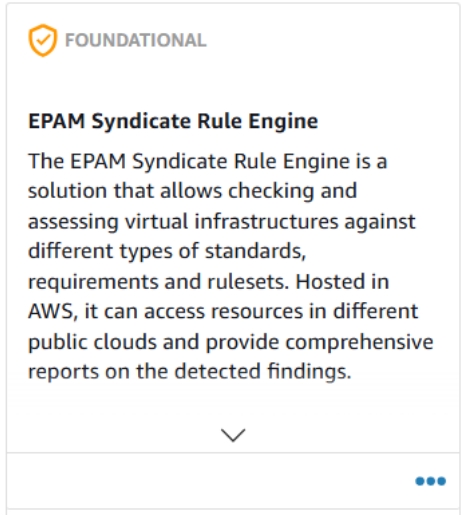
- ✓ Professional service hours - 160
- ✓ Minimum commitment month - 3

Partnership Potential

SRE on AWS Marketplace:

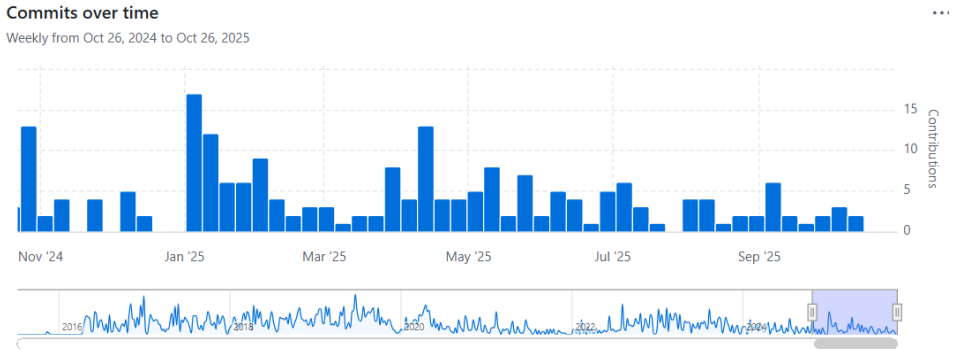


SRE on AWS Solution Finder:



EPAM AMONG TOP CONTRIBUTORS TO CUSTODIAN OPEN SOURCE

https://github.com/cloud-custodian/cloud-custodian



Want to know more?

Reach out to SupportSyndicateTeam@epam.com

to get more details or a demo