Key Takeaways

- As cloud environments become decentralized, Policy as Code (PaC) can be leveraged to automate governance across workloads.
- The approaches of PaC include capabilities and industry best practices aligned to specific buyer personas. These personas include: governance-centric, security-centric and developer-centric.
- Solutions may cater to specific domains; however, the general policy engines that fuel PaC can be utilized to create custom policies across all domains within an enterprise.
- Before implementing PaC, it is important to have a General-Purpose Architecture that operates across multiple environments, supports standard APIs and has a declarative policy language.
- To clarify common misconceptions, Policy as Code can and should be leveraged without waiting for Infrastructure as Code deployment and should also be checked consistently throughout the Software Development Lifecycle (SDLC) for optimal use.
- Trace3 Innovation expects as PaC gains popularity, solutions will continue to be marketed in new ways across cross-functional manual processes.

What is it

While Infrastructure as Code (IaC) emerged for automating IT environment modifications, Policy as Code (PaC) specifies enterprise policies for how applications and infrastructure should run, while implementing and testing them across cloud, cloud native, and/or on-prem environment regardless of how it was deployed. The policies are enforced pre-deployment and post-deployment they are monitored for continuous evaluation.

Why It Matters

Cloud capabilities are being adopted and managed not only by IT teams, but throughout the enterprise. This decentralized environment is creating the need to find automated ways to maintain governance, as it can be challenging for teams to manually apply and validate compliance, security, or operation policies in every instance being deployed. For policy enforcement, compliance and governance teams traditionally authored policies in a document and referred to this whenever approving or denying requests from business. Security teams were commonly consulted after a project had been coded, creating unfair tension and unexpected delays when the code had vulnerabilities. These manual processes can be error prone and difficult to scale. PaC allows enterprises to leverage IaC best practices through codifying different policies across the enterprise. Policies can be managed and documented consistently at scale, with automatic policy deployments and updates, as well as thorough testing to discover any violations early in the development process throughout cloud and on-prem environments.

Approaches

PaC is an umbrella term referring to a variety of different policies automated across an enterprise. It is important to note that as PaC buyers are typically focused on finding a solution that meets their unique policies and budgets, the market is differentiating solutions in the following domain categories: governance, security, operations and cost optimizations. Solutions within these domains cater to the buyer persona's needs by offering predesigned policy templates to match domain best practices. For example, a governance PaC solution may have templates provided to align the workflows to SOC standards. This would be appealing to those working in a compliance or governance organization; however, even though these solutions appear to be domain-specific, most PaC solutions incorporate a general-purpose policy engine that can be leveraged to automate custom policies across any domain in the enterprise. The following explains each domain in a bit more depth and how to best begin implementing PaC within an organization.

Governance as Code (GaC) allows enterprises to enact industry regulations and customize internal best practices across cost, availability, security, performance and usage. Within applications and infrastructure, predefined industry compliance standards (PICI-DSS, SOC, GDPR) and internal governance policies are automatically enforced, as well as tested thoroughly for accuracy pre-deployed. Once deployed, these policies are monitored for continuous refinement and recorded for audit trail purposes. Another industry recognized name for this capability is Compliance as Code (CaC).

Security as Code (SaC) creates consistency by allowing security and development teams to codify the enterprise's security policies across multiple environments. SaC can be broken into three forms: conducting specific tests on security policies, scanning architecture against vulnerabilities and creating access policies for monitoring and reviewing authorizations. Other industry names for SaC are: Secure DevOps, Security Automation, Security by Design and Infrastructure as Code Security.

Operational Excellence Policies automate the insights and best practices learned from operations and site reliability engineers (SRE) in order to continuously ensure high availability of services in production environments and improve supporting procedures. The goal is to limit human error and enable consistent response to events that occur. Examples of this would be policies to mandate at least a certain number of services or validation of new configurations.

Cost Optimization Policies are created in order to ensure that development and operation costs are monitored and regulated. Examples of cost optimization policies are tagging resources to cost centers or shutting down development environments outside of business hours.

To help develop these policies, it is important to have complete visibility and a consistent asset inventory, as well as a General-Purpose Architecture that creates a common framework across multiple environments, supports standard APIs and has a declarative policy language. Each solution, regardless of the domain, may have a different approach to the policy as code exercise. Some may implement policies through

authorizations, while others may leverage resource graphs or scan fields in order to develop an understanding of the environment and which policies should be executed. This implementation approach should be evaluated to select the right fit for an organization. Once policies are determined, policies can either be selected in the PaC platform from a prebuilt policy engine, such as Open Policy Agent (OPA), or can be custom built to meet the unique requirements of an enterprise. It is recommended that the policies be consistent across development, deployment and runtime cycles in order to eliminate confusion and inconsistencies. After policies have been vetted, they should be thoroughly tested before implementation. After implementation, the PaC platform will continue to track these policies and provide alerts in case anomalies arise.

Trace3 Innovation's Point of View

The cloud security and governance markets are highly contested and rapidly evolving. As enterprises grow their cloud presence and begin to experience challenges, cloud providers and 3rd party vendors are increasing their governance functionalities. Policy as Code has the potential to enhance governance efficiency but requires changes in people, processes and technology that can be disruptive during early stages of adoption. There are some common misconceptions when it comes to implementing and leveraging Policy as Code. PaC can create and maintain policies regardless of how it was deployed and does not require Infrastructure as Code to be adopted within the cloud environment. In fact, implementing a PaC solution before IaC does not require a heavy lift and allows for centralized policy management sooner in an enterprise's cloud journey. Another misconception is that checking policies pre-deployment will ensure they are carried through seamlessly in runtime; however, the Software Development Lifecycle (SDLC) is dynamic and it is highly advised to check the same policies at every stage of the lifecycle to ensure consistency and avoid any variations in code.

There are different types of buyers within an enterprise, including: governance-centric, security-centric and developer-centric. Each will have their own priorities and motivations for implementing particular PaC use cases. To remain competitive, it is important for vendors to ensure their offerings can reach the right audience and scale as the market grows. To attract buyer personas, some vendors specialize in a particular domain and include these domain industry standard best practices as policy templates for enterprises to easily leverage in their own codes. Vendors are also differentiating in the approach taken to implement the policies. Some vendors, such as Styra, focus on the authorization of certain resources; whereas, Fugue, for example, creates resource graphs to ensure analysis of all available resources in the policies. Security as Code is currently the most recognized form of PaC, with Compliance as Code undergoing a massive explosion in the market. However, even if these solutions claim to specialize in one domain, OPA and other policy languages are designed to be cross-functional and can be leveraged for any type of automated guardrail. Trace3 Innovation expects that as enterprises begin to realize the benefits and PaC gains popularity, solutions will continue to be marketed in new ways across cross-functional manual processes.

Recent Acquisitions in PaC Market (2021-2022):

- Palo Alto Networks acquires Bridgecrew, March 2, 2021
- Sysdig Inc acquires Apolicy.IO Inc., July 20, 2021
- Accurics is acquired by Tenable, October 4, 2021
- Lacework Inc with Soluble, November 11, 2021
- Weaveworks Limited acquires Magalix Corporation, January 26, 2022
- Fugue joins Snyk, February 17, 2022

Trace3 Innovation Perspective:

As Policy as Code enables consistent policy enforcement across an enterprise, Trace3 Innovation recognizes that these acquisitions signal a shift from manual or paper policies to automated governance. While the market continues to mature, we expect PaC's value to expand into additional use case offerings and for PaC engines to continue to be leveraged in new ways. In order to prepare for this shift, organizations will need to acknowledge the shift away from traditional processes and towards a devops mindset. PaC requires organizations to adopt many DevOps methodologies, including: maintaining controls in a central repository, applying version control, and enabling automatic validation. Another important call-out when evaluating a PaC approach is that *most* PaC engines are designed to address policies across an organization. Offerings may be differentiated by user persona and have best practices as policy templates for areas such as security, compliance, governance; however, most industry PaC engines can be leveraged to fit the needs of any organization.

Solutions

**All vendors provided are examples and is not meant to be an exhaustive list. Emerging technologies are subject to significant changes in market share and relative capability.*

Security:

SECBERUS

Secberus is an Enterprise Governance Platform with an embedded Continuous Adaptive Policy Assessment (CAPA) framework at its core. With this approach, you can establish a policy baseline that is risk-driven, adaptable, and scalable. The adaptable policies become the single source of truth for each pillar of governance across clouds and business units.

MAGALIX

Magalix sets out to accelerate the implementation of innovative technologies and products
by powering developers and security teams with the tools for them to codify security and compliance in their software development lifecycle."

Concourse Labs automates cloud governance, protecting enterprise data, controlling risk, and accelerating success in the cloud.

Styra enables enterprises to define, enforce, and validate security across their Kubernetes environments. With a combination of Open Source (Open Policy Agent) and commercial solutions (Declarative Authorization Service), Styra provides compliance guardrails to secure applications and ease compliance. Styra's policy-as-code solution lets DevOps and Security teams mitigate risks, reduce human error, and accelerate app development.

Tigera is a provider of integrated, secure, policy-driven cloud-native networking solutions for enterprises looking for secure application and workload delivery across private, public and hybrid clouds. Tigera is solving the networking and security problems inherent in deploying and enforcing policy in large private, public, and hybrid enterprise clouds.

Prisma Cloud embeds comprehensive security across the software development cycle. The platform identifies vulnerabilities, misconfigurations and compliance violations in IaC templates, container images and git repositories. It offers IaC scanning backed by an open source community, and image analysis backed by years of container expertise and threat research. With centralized visibility and policy controls, engineering teams can secure their full stack without leaving their tools, while security teams can ensure that only secure code is deployed.

Accurics helps companies secure cloud native infrastructure throughout the DevOps lifecycle and eliminate risk posture drift.

Shift Security to the left by Prancer's end-to-end cloud security platform. Prancer's static code analyzer for Infrastructure as Code (IaC) enforces cloud security posture right from the development lifecycle. And our continuous compliance engine scans your cloud in real-time based on Policy as Code.

Compliance:

Stacklet implements governance as code in the same way infrastructure is being managed as code today. It provides development and security engineering teams with an easy to use, standardized language for enforcing governance policies in large scale, dynamic cloud environments.

JupiterOne is a cloud-native security and compliance platform built on a graph data model. It enables users to create and manage their entire security process from policy creation to compliance & certifications and to operating a secure cloud infrastructure while a company quickly grows and evolves. It is a platform that enables security in digital transformation.

NexaStack helps organizations to use and manage multiple different automation frameworks through a single platform. Enterprises can experience centralized Governance of Multiple Public Cloud Providers under one roof for an easier shift towards the multi-cloud environment approach and efficient management of the same through the use of NexaStack as an IAC platform

Chef Compliance helps organizations streamline their ability to stand up and maintain compliant IT infrastructure, whether on premises or in the cloud. Built on technology proven at extreme scale, including Chef InSpec, Chef Compliance leverages certified, curated audit and remediation content to help organizations quickly meet industry standards such as CIS benchmarks and DISA-STIGs. The product offers flexibility to easily apply and track waivers and tune controls to enterprise-specific needs.

Cross-Functional:

Pulumi provides the cloud development model: helping Development and DevOps teams get their code to the cloud quickly and collaboratively. Pulumi provides frameworks and libraries to define, deploy, and manage cloud services -- from serverless to container to virtual machines, using pure code.

Fugue

Fugue, previously known as Luminal, simplifies cloud operations with its software-defined system for orchestrating and enforcing cloud infrastructure at scale. Teams can use Fugue to declare the desired state of cloud infrastructure and policies in a collaborative, human-friendly programming language and automate the provisioning, management and teardown of complex cloud environments, while continuously enforcing infrastructure state and policy compliance.

cycode

Cycode is a source code visibility and protection company. Cycode utilizes its Source Path Intelligence engine to deliver comprehensive visibility into all of an organization's source code and automatically detect and respond to anomalies in access, movement, and usage.

HashiCorp

HashiCorp is an open-source software company. HashiCorp provides open source tools and commercial products that enable developers, operators and security professionals to provision, secure, run and connects distributed application infrastructure.

checkov by bridgecrew

Checkov scans cloud infrastructure configurations to find misconfigurations before they're deployed. Checkov uses a common command line interface to manage and analyze infrastructure as code (IaC) scan results across platforms such as Terraform, CloudFormation, Kubernetes, Helm, ARM Templates and Serverless framework.

env0

env0 provides an automated, collaborative remote-run workflows management for cloud deployments on Terraform, Terragrunt and custom flows. env0 enables users and teams to jointly govern cloud deployments with self-service capabilities.

SPACELIFT

Spacelift is a specialized, Terraform-compatible continuous integration & deployment (CI/CD) platform for infra-as-code.