WHITE PAPER

Stacklet

Governance as Code

The Guardrails for Cloud at Scale

Executive Summary

To meet their digital transformation imperatives, organization leaders continue to leverage more cloud services.

To gain and sustain their competitive advantage, today's businesses need to leverage the cloud and empower developers to write applications more quickly and effectively.

However, for many organizations, a lack of effective governance capabilities represents a big inhibitor to cloud adoption.

For businesses that move forward without effective governance, these expanding cloud implementations can present significant financial, legal, and brand risks.

In this white paper, we examine why cloud governance as code is emerging as a foundational requirement for organizations running business-critical services in cloud environments.

We'll highlight how governance as code champions automated management of the complex cloud ecosystem via a human-readable, declarative, high-level language. Infrastructure and security engineering teams can adopt governance as code to enforce policies in an agile, flexible and efficient manner while reducing developer friction.

86%

of respondents agree cloud governance tends to be a pivotal inhibitor to cloud adoption[1]

[1] Stacklet, *State of Cloud Governance*, Insights from Q4-2021 survey of 700+ IT professionals and developers

What is Cloud Governance?

Cloud governance is a framework that's focused on ensuring cloud deployments are operating securely and properly. To achieve these objectives, effective cloud governance must encompass the effective application of policies, procedures, and tools.

For enterprises running business-critical services in the cloud, governance must be comprehensive—supporting effective security, continued compliance, cost efficiency, and optimized operations. In addition, it is vital that governance capabilities span not just a single implementation, or even all deployments within a single cloud provider, but all cloud deployments across all providers—ensuring they are all operating optimally and securely. Without these capabilities, teams struggle with manual, labor-intensive, and inefficient workflows and efforts, and, as a result, cloud migrations and cloud-based development can be significantly slowed.

Dimensions of Cloud Governance

In order to manage cloud governance effectively, there are many different responsibilities that have to be addressed. Capabilities for managing security, compliance, operations, and cost represent the foundation of a well-managed cloud governance framework. Without these capabilities, development teams will be mired in complex, labor-intensive workflows and review cycles that stifle developer speed and productivity.

To be effective, teams need to establish governance that spans these areas:

Security. Cyber attacks are a constant threat, and criminals' tactics continue to evolve. Teams need to ensure strong controls are in place, and kept current to meet these evolving threats.

Compliance. Compliance mandates are changing constantly. So too are cloud implementations. Teams need to be able to gain the visibility and control required to ensure compliance with standards and mandates like NIST Cyber Security Framework (CSF), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and CIS benchmarks.

Cost. Without effective governance, costs for cloud services can quickly spiral out of control. Teams need to be able to constantly ensure available resources are being utilized, and, if excess resources are identified, ensure they are deprovisioned immediately.

Operations. Within cloud environments, it is vital that end users always receive responsive, reliable service. Teams need to be able to institute the redundancy and adaptability required to ensure that optimized service levels are delivered at all times.

99%

of cloud security failures will be the cloud user's fault[2]

$40M

USD average cost of non-compliance[3]

70%

average savings from policies that schedule service access[4]

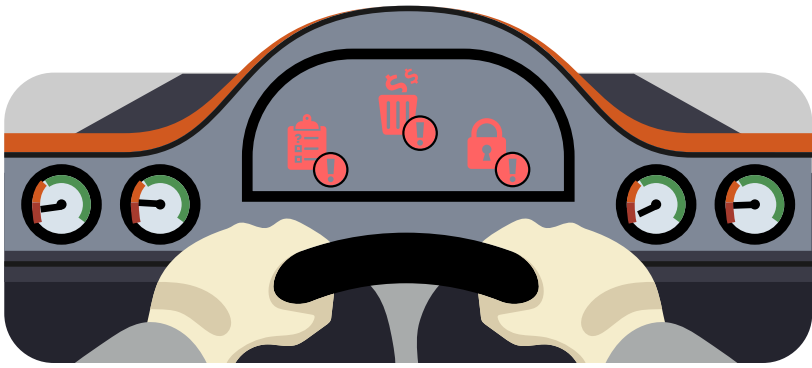
[2]Gartner, *Is the Cloud Secure?*, Kasey Panetta, October 10, 2019
[3]Spin, *The Financial Impact of Non-Compliance on Businesses*, Anastasia, June 28, 2020
[4]Gartner, *How to Manage and Optimize Costs of Public Cloud IAAS and PAAS*, March 23, 2020, Analysts: Marco Meinardi, Traverse Clayton, ID: G00465208

The Perils of Ineffective Cloud Governance

Without effective, nimble cloud governance capabilities, the burgeoning complexity of cloud environments can be difficult to manage, leaving the business exposed to the potential for a range of penalties:

Security risk. Much has been written about the security risks of moving to the cloud, and for good reason. Compared to traditional on-premises environments, securing data and services in the cloud represents a very different paradigm, and many organizations struggle in navigating this transition. In fact, through 2025, Gartner analysts estimate that 99% of cloud security failures will be the customer's fault—not the cloud provider's. Further, in the same report, analysts estimate that 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data.[6]

Non-compliance penalties. For modern enterprises, compliance represents an increasingly vital imperative. Particularly any time personally identifiable data is stored in a cloud environment, organizations need to ensure compliance with a range of increasingly stringent privacy and security mandates—and failure to comply is an ever more costly proposition. On average, non-compliant organizations incur penalties in excess of $14M a year, and costs can run as high as $40M.[7]



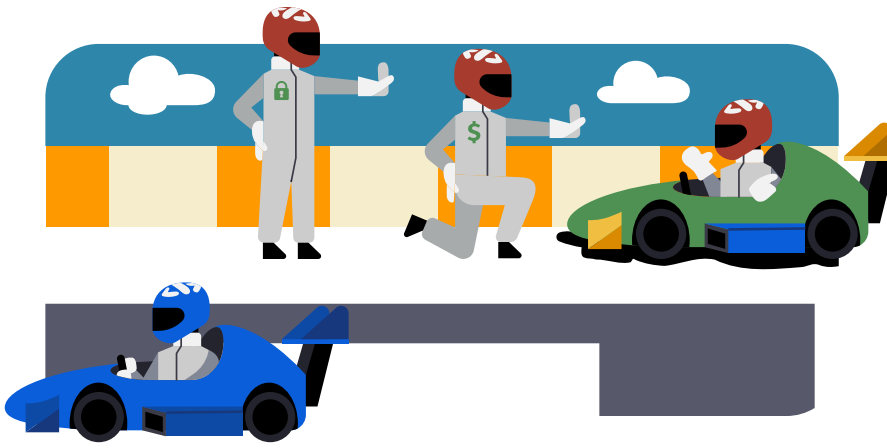
Wasted money. While the cloud offers a range of benefits compared to legacy, on-premises infrastructure, without proper governance, cloud costs can quickly spiral out of control. In fact, Gartner analysts report that in the next few years, 60% of organizations will encounter cost overruns in public clouds.[8] Opportunities to optimize cost efficiency are plentiful. For example, simply scheduling development instances to operate during business hours rather than 24 hours a day, teams can reduce costs by 70%.[9] However, it takes effective, efficient governance to institute these controls.

Poor performance. Within cloud environments, teams can leverage a broad assortment of agile, dynamic technologies. While these modern environments present a range of opportunities for developers, they also pose a number of challenges for operations teams. In containerized, dynamic, and highly automated cloud environments, resources and workloads are in virtually constant motion. With all this change, it can be difficult for operations teams to track performance and spot potential or actual performance issues—before it's too late.

[6] Gartner, *Is the Cloud Secure?*
[7] Ponemon Institute LLC, sponsored by Globalscape, *The True Cost of Compliance with Data Protection Regulations*, December 2017
[8] Gartner, *6 Ways Cloud Migration Costs Go Off the Rails*, Meghan Rimol, July 7, 2021
[9] Gartner, *How to Manage and Optimize Costs of Public Cloud IaaS and PaaS*

The Challenge: Establishing Strong Governance Without Hindering Development Velocity

For some time, digital transformation imperatives have been important, and they've only grown more urgent in recent months. Given that, enabling developers to gain maximum flexibility in how they leverage cloud resources is a must-have requirement for business success. It is absolutely vital to enable these teams to maximize agility and velocity in the cloud so they can deliver the innovative products and services that propel successful digital businesses. The challenge is that meeting this demand for flexibility and agility has to be balanced with risk. Without effective controls, organizations can be exposed to cost overruns, security breaches, and non-compliance penalties.



> *Software developers are like kids in a candy store when it comes to selecting and configuring all of the public cloud services they want to use for creating their applications. This makes governance hard and the number one challenge that delays cloud adoption and deployment.*
>
> Torsten Volk, Managing Research Director, EMA

Once business services are running in the cloud, governance is critical. However, cloud services present a fundamentally different paradigm for governance. In years past, organizations could establish manual governance controls that could be applied across an organization's computing estate. While these processes were slow and required manual tasks and approvals, teams were able to make these approaches work. That's because, for the most part, on-premises environments were relatively static and homogeneous, which meant it was far simpler to establish and enforce uniform policies.

Within cloud environments, all that changes, however. As cloud providers continue to innovate and expand service offerings at an increasingly rapid rate, development and operations teams are presented with a wide range of tools, configuration options, platforms, and technologies. As outlined above, development teams need to be afforded maximum flexibility in capitalizing on these innovations.

Teams need to balance risk with developer flexibility and productivity. While this proliferation of options in the cloud offers unprecedented flexibility, it also ushers in unprecedented complexity, posing significant implications for teams across the organization:

> *Governance is incredibly important, but it's difficult to achieve at scale. If teams try to manage it in a central, unified fashion, policies won't be optimized for the specific requirements of a given application, workload, or service. On the other hand, if teams try to adapt policies to each specific use case, governance quickly grows so complex it becomes too costly and too difficult to manage.*
>
> David Linthicum, Chief Cloud Strategy Officer, Deloitte

Cloud engineering. These teams struggle to gain the visibility and unified control they need to monitor, manage, and optimize the performance of cloud-based services. Within a given cloud provider's suite of offerings, a number of different APIs and tools may be available. Similarly, completely different APIs are employed in other cloud provider's environments. Because there are no standard APIs across services and providers, teams struggle with complex, manual handoffs and integrations.

Security engineering. These teams find it increasingly difficult to understand threats and take proactive steps needed to ensure constant safeguards against breaches and cyber attacks across an increasing number of cloud services and technologies.

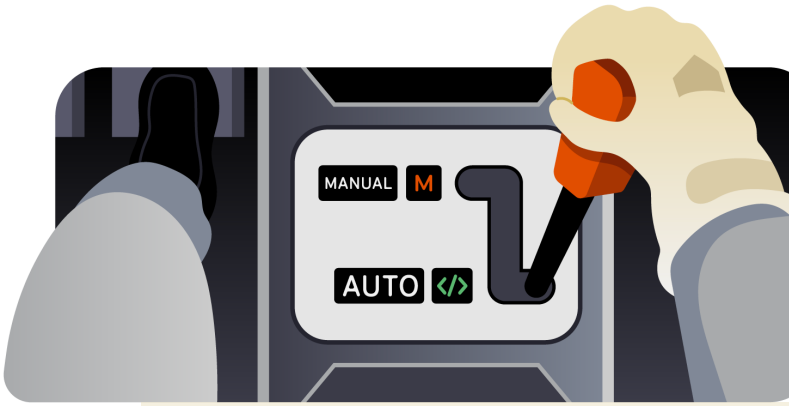
Compliance and risk management. These teams have to contend with constantly changing cloud environments and ever-evolving mandates and policies, making it difficult to ensure businesses aren't exposed to fines and other penalties associated with non-compliance.

Financial operations. Lacking comprehensive control and visibility over multi-cloud environments, these teams can't proactively manage costs—and too often find out about wasted expenditures and high costs of under-utilized resources after the fact. With self-service access to so many configurations and resources, it can be difficult to control developers' and other users' actions, and it can be hard to get them to follow up in a timely manner when requests are made or issues arise.

Mitigating the risks outlined above poses a number of challenges for many teams. For example, when surveyed about managing multi-cloud environments, "maintaining security, policy, and compliance" was by far the top-rated challenge, one that respondents found the most "challenging, frustrating, or difficult."

Given all these challenges, the reality is that, in many organizations, teams are forced to choose between mitigating risk or promoting developer productivity—because they lack the ability to meet both of these objectives. Ultimately, these shortcomings represent an increasingly significant barrier to cloud adoption—not to mention business success.

Cloud Governance as Code: A Paradigm Shift



For all the reasons previously outlined, teams are being compelled to take a new approach to cloud governance. For many, this means embracing the concept of cloud governance as code.

Through cloud services, cloud providers began offering infrastructure as code, which offered a way to dynamically provision and deprovision cloud resources in order to maximize agility and flexibility. In much the same way, cloud governance as code represents a way to dynamically apply policies in fast-changing cloud environments.

This approach enables organizations to use code to manage and automate various aspects of governance, including cost, operations, security, and compliance. Through automation, teams can reduce their maintenance burden, while increasing their cross-environment visibility and control. By shifting to a governance as a code model, teams can establish real-time policy enforcement across all clouds, employing capabilities for detection, notification, and remediation.

When compared to policy as code, governance as code represents a superset of capabilities. Through policy as code, teams can set policies and generate alerts. By contrast, governance as code offers these capabilities, plus it also includes the ability to enforce policies and take corrective action when policies are breached or in danger of doing so.

With governance as code capabilities, teams can now give development teams maximum flexibility for innovation, while at the same time instituting the guardrails that ensure effective governance. With effective solutions, teams can apply governance in a comprehensive, holistic fashion, enforcing policies around security, compliance, cost, and operations. Further, by enabling governance to be employed in a dynamic fashion, it allows them to not just institute controls required once but to keep up with the pace of change within their organization and with cloud service innovation.

> *Statistics show lack of compliance is a costly issue for today's enterprises. When incidents of non-compliance arise, it can be difficult to remediate issues and get back on track. With cloud governance as code, teams can breathe easy. Governance as code enables policies to be enforced as part of the technology lifecycle, and to automate policy implementation and remediation.*
>
> David Linthicum, Chief Cloud Strategy Officer, Deloitte

[10] ZDNet, *Cloud Computing in the Real World: The Challenges and Opportunities of Multicloud*, Charles McLellan, April 29, 2021

Cloud Governance as Code: Four Key Principles

Policies Defined via a Simple, Declarative Language

Much has been written about the security risks of moving to the cloud, and for good reason. To maximize the power and flexibility of cloud governance as code, teams need to be able to define policies via a simple, declarative language. In effect, a declarative language takes the approach of instructing what should be done, rather than how it should be done.

In this way, teams should be able to express any policy their organization may require. Further, by employing an understandable, consistent language, it is easier for different teams and individuals to get started and to collaborate and gain alignment on key objectives and approaches. Different stakeholders—including developers, cloud engineers, financial operations staff, security teams, and more—can contribute to the establishment and ongoing refinement of policies.

Finally, it is also critical that this language is independent of any specific programming languages that developers may use for applications, and can be applied not only across multiple applications but multiple clouds.

Policies are Deployed via Git with CI/CD

Inherently, it is vital that governance as code keep pace with dynamic cloud environments. Therefore, it is essential that policies are deployed in a manner consistent with continuous integration/continuous delivery (CI/CD) approaches. This includes deployment via Git, a leading open-source version control system. Through this approach, teams can apply policies in a manner consistent with their software development and delivery lifecycles.

By codifying governance in this way, controls can be enforced as part of the CI/CD process—and enable teams to avoid complex manual processes, managing tickets, and so on. Further, this approach means, just as application code, governance code can be traced through various state changes, rolled back if needed, and so on.

Real-Time Automated Enforcement

True governance means more than just alerting. In addition to issuing notifications, governance as code empowers action. Policy violations are effectively communicated as needed within the organization and remediation is automated. Governance as code enables enforcement of workflows and actions that are required, whether that means notifications, escalation, or automated remediation.

Continuous Collaboration and Communication

Cloud governance as code encourages collaboration and establishes agility by design. Through this approach, development, operation, security, and finance teams can gain visibility into policies, and they can collaborate more effectively on policy definition and enforcement. Teams can quickly and efficiently modify policies and create new policies, and changes can be implemented in much the same way teams modify application code or underlying infrastructure in today's agile, DevOps environments. As a result, teams can work to continuously improve development velocity, strengthen security, meet regulatory requirements, and optimize cloud spending.

The Benefits of Cloud Governance as Code

Through cloud governance as code, teams can apply policies in an agile, flexible, and efficient manner. With these capabilities, cloud and security engineering teams can realize the following advantages:

Strengthen security. With governance as code capabilities, security teams can more effectively and flexibly establish strong security policies, more consistently enforce those policies, and respond rapidly if those policies are in danger of being breached. In this way, teams can more effectively safeguard against the constant threat of cyber attacks.

Address ever-changing compliance requirements. With these capabilities, teams can establish persistent compliance with evolving requirements and mandates, including the General Data Protection Regulation (GDPR), NIST CSF, PCI DSS, HIPAA, and more.

Reduce operational overhead and developer friction. Through cloud governance as code approaches, teams can establish governance within the framework of agile CI/CD workflows, so controls can be implemented while minimizing administrative effort and development hurdles.

Control costs. With cloud governance as code, teams can automatically identify, right-size, and deprovision unnecessary resources. As a result, in spite of the proliferation of cloud instances, and the infinite permutations of technologies and tools that can be employed, teams can nevertheless ensure constant adherence with best practices for resource allocation and utilization.

Governance as Code in Practice: Introducing Cloud Custodian

Cloud Custodian is at the forefront of the movement to cloud governance as code. Cloud Custodian is an open source project that allows cloud and security engineering teams to enforce governance as code, similar to the way infrastructure is managed as code. Further, the project enables teams to work with a common language across all major cloud providers. Cloud Custodian helps teams enforce a fleet of policies that control cloud costs, avoid potential breaches, and meet regulatory requirements across an ever-increasing number of cloud services and providers. With the solution, these teams can manage costs and stay secure, while maximizing developer flexibility and productivity.

Now a member of the Cloud Native Computing Foundation (CNCF), Cloud Custodian has been adopted by thousands of organizations across multiple industries. Cloud Custodian features these core capabilities:

Simple, domain-specific language for policies. Cloud Custodian simplifies the complexity of policy authorship, enabling teams to write policies using the simple YAML language. Each policy is assigned to a specific resource type and consists of a vocabulary of actions and filters that can run in different modes. At the most basic level, each policy must have a name and resource specified. Through this approach, teams can easily create thousands of policies.

```
- name: aws-cloudwatch-log-group-no-retention
  resource: aws.log-group
  description: |
 This policy will identify AWS CloudWatch Log Groups which have no retention
period set, and enable retention. Setting a log group retention period helps save
on costs by removing old logs and helps you meet organization data retention
standards.
  filters:
    - or:
      - "retentionInDays": absent
      - "retentionInDays": null
  actions:
    - type: retention
      days: 90
```

Stateless rules engine. With the solution, these teams can manage costs and stay secure, while maximizing developer flexibility and productivity. The project enables teams to do policy definition and enforcement, with metrics, structured outputs, and detailed reporting for cloud infrastructure.

Multi-cloud support. Cloud Custodian features integrations with multiple cloud environments and platforms, including Amazon Web Services (AWS), Kubernetes, Microsoft Azure, OpenStack, and Google Cloud Platform (GCP). The project supports over 280 resources across these environments. In addition, the project integrates tightly with serverless runtimes to enable real-time remediation and response, while minimizing operational overhead.

Thriving open source community. Cloud Custodian's community is large and diverse. The project has been deployed in some of the largest, most sophisticated cloud environments, and across a wide range of industries. The major cloud providers have made a large number of contributions to the project. Because of the project's capabilities and diverse community, Cloud Custodian has become the industry standard for multi-cloud governance.

Creators and Maintainers

Cloud Custodian

300+ Contributors

1,600+ Chat Participants

10M+ Monthly Downloads

Case Study: Subscription-Based Streaming Service Provider

Business need: Break down fears that slow down innovation in the cloud

For a growing global video streaming service provider with more than 60 million paid subscribers, it was a key business imperative to stay at the forefront of innovation. The organization needed to keep pace with evolving markets, technologies, and consumer demands in a highly competitive market. In order to provide the development and product organizations with maximum latitude to solve consumer problems, the organization grew heavily reliant on a range of cloud services. At the same time, it was critical that the security team could ensure that digital assets and customer data remained secure at all times. However, the security team didn't want to add controls that slowed down innovation. Instead, they wanted to build trust with development teams and eliminate the fears that slow down innovation.

Cloud Custodian provided automated guardrails at scale

To contend with these competing demands, the team leveraged Cloud Custodian. With this open-source project, the team established scalable guardrails that fostered strong adherence to policies. At the same time, they've been able to give development teams maximum flexibility, so they can leverage the services and models that work best for them.

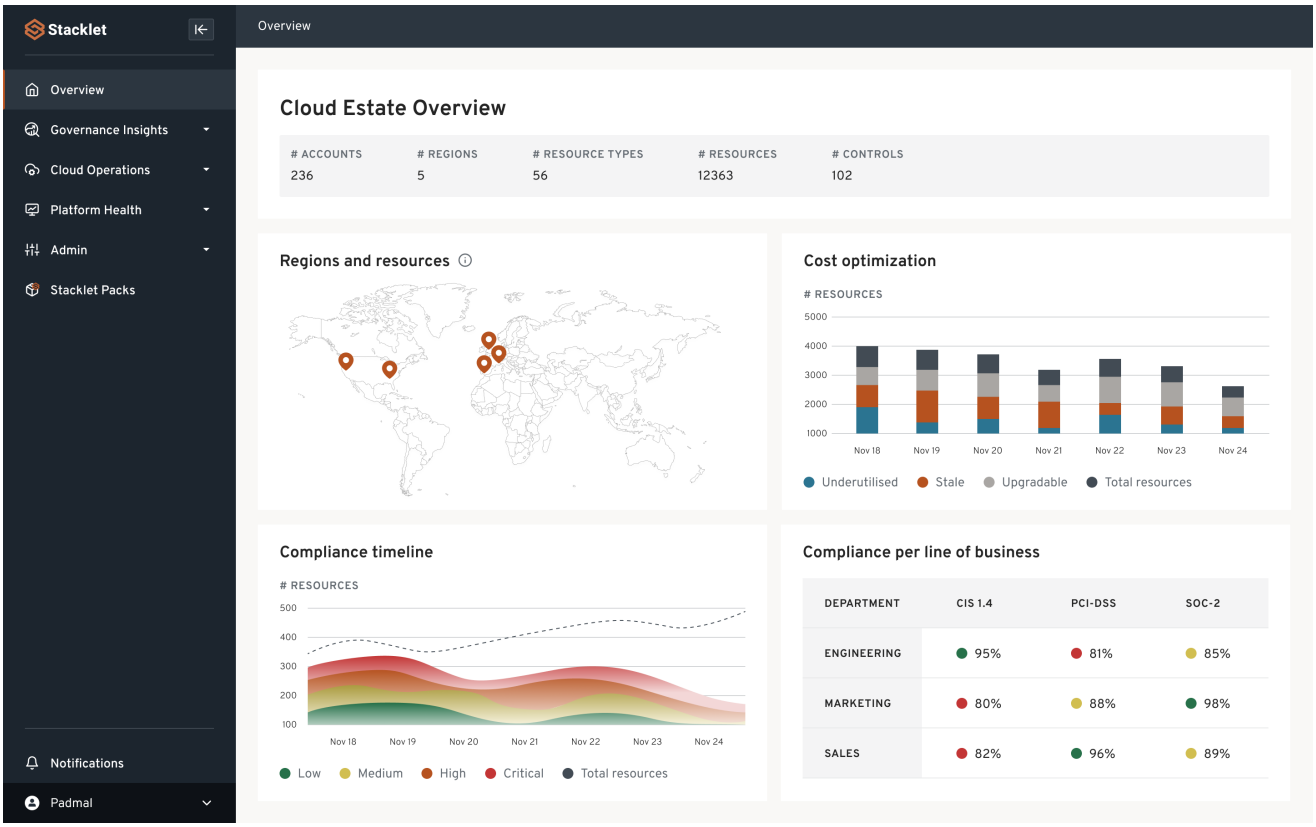
Cloud Custodian enables the team to consolidate multiple tools, scripts, and remediation processes into a single, flexible solution. Now, security engineers build a simple YAML file that defines policies and actions, and Cloud Custodian executes those policies across a multi-region and multi-account cloud environment.

In this way, the organization can rapidly scale and innovate while maximizing security and the customer experience.

> *"With Cloud Custodian, we have provided our development teams and business with the right amount of guardrails. As a result, we can scale faster and respond to our customer needs with confidence.*
>
> CISO at Subscription-Based Streaming Service Provider

Stacklet Platform:
Extending Cloud Custodian with Intelligent Management Capabilities

Stacklet was founded by the creator and lead maintainer of Cloud Custodian, an open-source cloud-native security and governance project. Stacklet Platform is a governance as code solution that accelerates cloud adoption with intelligent guardrails for security, compliance, cost, and operations. Stacklet Platform empowers cloud and security engineering teams to codify, automate, visualize, and collaborate on policies using a standard, easy-to-use, declarative language. Stacklet Platform extends the Cloud Custodian open source project with intelligent management capabilities, including governance insights, real-time asset inventory, out-of-the-box policy packs, and advanced communications. With these capabilities, the solution can help businesses innovate securely, efficiently, and scalably in the cloud.



Stacklet Platform extends Cloud Custodian by providing additional capabilities to meet the needs of complex, large-scale multi-account and multi-cloud environments

> *Stacklet accelerates our move to the governance as code model. The solution empowers our security teams to establish automation and scale real-time, continuous evaluation and enforcement of our governance policies.*

Large Financial Analytics Company

Stacklet Extends Cloud Custodian with Intelligent Capabilities

		
Standard Policy Language	✓	✓
Automated Remediation	✓	✓
Multi-Cloud Support	✓	✓
Management Console		✓
Governance Insights		✓
Real-time Asset Inventory		✓
Integrated GitOps		✓
Policy Packs		✓
Intelligent Communication		✓

About Stacklet

Stacklet was founded by the creators and lead maintainers of Cloud Custodian, an open-source cloud governance project used by thousands of well-known global brands today. Stacklet provides a cloud governance as code platform that optimizes how Global 2000 companies manage security, asset visibility, operations, and cost in the cloud.

To learn more, visit https://stacklet.io/

To request a demo of Stacklet Platform or Cloud Custodian, please visit https://stacklet.io/get-demo-stacklet

Stacklet