FIREEYE™

SOLUTION BRIEF

Augmented Policy Governance for Cloud Security

Scenario for consideration
Policy governance automation is not difficult. But automating policy governance with nothing but true least-privilege policy rules is difficult.

Creating true least-privilege policies at any reasonable scale is especially difficult.

The creation of true least-privilege policies is difficult because it requires both in-depth knowledge of specialized security controls and in-depth understanding of the deployment environment—the expected behaviors of and relationships between various entities (such as application services, systems, users) governed by a given set of controls.

Actual network policies are rarely created by those who possess deep knowledge of both least privilege security and the deployment environment.

Feeding artificial intelligence with data from cloud provider APIs automatically gives machines contextual information about environment behavior to generate better least-privilege security policies at any scale.

Augmenting policy governance with machine intelligence
Each cloud provider offers their own form of granular, API-driven controls for least-privilege policy governance. While these security controls may be granular by design, their actual configuration is often wide open. Whether out of convenience, ignorance or even malicious intent, critical security controls are commonly misconfigured, even when automation tooling is used to provision them.

Cloud providers also offer various features and services which enable ephemeral and hyper-scale deployments. Mature deployment automation technologies are widely used for to automate the deployment of security controls in tandem with the resources they control. Unfortunately, these security controls are commonly misconfigured and rarely (if ever) audited, to ensure granular configuration with least-privilege access rules.

Organizations want to preserve their efficient DevOps deployment workflows that rely on version-controlled, orchestrated deployments of infrastructure as code and ephemeral infrastructure. At the same time, organizations need their SecOps teams to do more than bridge the visibility gap. There is a real and urgent need for better oversight and tighter governance at enterprise scale.

Organizations need intelligent automation that can augment existing deployment automation workflows with better, more granular policies to reduce costs while stopping internal and external threats.

Core problems
Over the past decade, deployment automation technologies have significantly outpaced security automation technologies in terms of adoption, features and maturity. This trend created a common situation in medium to large enterprises where multiple (distributed) DevOps teams independently managed their own deployments using their own choice of mature deployment automation solutions such as Ansible, Chef,

CloudFormation, Puppet, Salt, Terraform or one of many other tools used for orchestrated deployments of VMs, containers and other workloads via provider APIs. At the same time, the central security team lost visibility into—and governance over—the behavior of distributed DevOps assets. There seems to be little chance of the security team using its own (new) tooling to take over DevOps governance any time soon.

SecOps teams struggle to integrate with DevOps automation tooling. Deployment automation technologies can efficiently develop ways to create or reproduce any given deployment, but they do not provide useful visibility into the behavior of governed assets. Governance without visibility is trusting without verifying.

SecOps must find some way to overcome this deficit, because in many organizations developers control most of the security policies which govern cloud assets. The self-service multi-tenancy model enabled by cloud technologies has resulted in significant improvements to deployment efficiency and consistency, but organizations have learned the cost of putting security decisions in insecure hands. Many organizations now acknowledge that they need better policy guardrails for self-service multi-tenancy to remain viable in the long-term.

If SecOps manages to find a technical way to bridge the visibility gap and gain the context required to build true least-privilege security policies, several challenges would still remain. If maintaining context requires any significant human effort, it would not be scalable or sustainable in large cloud environments. At the same time, the control of production assets cannot be surrendered to machines alone. Balance must be established between forms of automation and groups of technology users. .

Solution requirements

Governance solutions must provide visibility into the configuration and behavior of governed assets, such that the performance of governance activities may be analyzed and improved over time. To improve governance, the real challenge is not policy governance automation, but determining the ideal set of least-privilege security policies which should be enforced via automation.

Since mature deployment automation technologies are already commonly used throughout many organizations, an governance solution should focus on automating the creation of better governance policies and be capable of creating ideal policy recommendations without deploying any changes outside of standard deployment automation pipelines.

The main role of the governance solution is to augment (not replace) existing governance controls with better policy inputs. Creating better governance policies requires deep visibility into the full context of a given set of assets. Machine learning can feed on context to model the behavior of assets over time. The more context, the more complete the model, the better the policy outputs. Therefore, as a prerequisite to augmenting governance with intelligent policies, a governance solution should automate the process of collecting, processing and correlating the different layers of context used to model and understand asset behavior.

The ideal solution would use artificial intelligence (AI) (machine learning) technologies to automate the process of deriving deep asset context from cloud provider APIs. It would use the asset's full context as the basis for learning the asset's ideal set of least-privilege governance policies. These AI-created policies would then be used to augment existing governance processes and tooling. The solution should enable the export of policy recommendations into a native format which can be used to either update some version-controlled infrastructure-as-code repository or to update the security policies associated with a given deployment using an existing deployment automation tool.

The Cloudvisory solution

Cloudvisory governance delivers cloud-native governance of governance policies through direct communication with cloud provider APIs. Without relying on workload-based agents, Cloudvisory completely automates the collection, processing and primary analysis of security events from workloads and cloud services across multiple cloud accounts and cloud providers. Cloudvisory detects changes to asset inventory and security configurations in real time, allowing users to customize response actions (e.g. alert, rollback, remediate) for detected policy violations.

Cloudvisory provides stepping stones on the journey to least-privilege policy governance, allowing organizations to bridge the visibility gap and achieve continuous compliance assurance as they improve their governance practices. Cloudvisory governance also feeds on the deep context provided by visibility and compliance capabilities, using an asset's cloud, historical, security and system context to automatically model the asset's behavior.

Cloudvisory governance uses machine learning to automate the difficult and expensive tasks associated with formulating least-privilege policies based on the needs of governed assets. While Cloudvisory provides a complete policy orchestration engine to enforce network microsegmentation and other least-privilege security policies, it also allows users to choose preferred tools for governance and orchestration. Cloudvisory governance is powerful enough to support large multi-cloud deployments using nothing but true least-privilege governance policies. And it is flexible enough that users can augment existing governance processes with better governance policies.

Why Cloudvisory?
Cloudvisory can efficiently solve complex cloud challenges at enterprise scale.

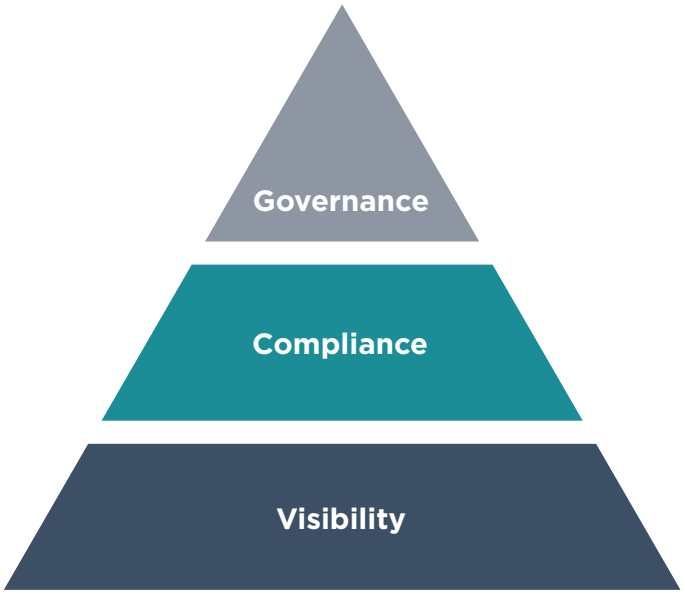
Competing products may make grandiose claims, but only offer are disjointed results for narrow issues. Many alternatives only support public cloud providers such as Kubernetes and OpenStack. So-called "multi-cloud solutions" are often agent-based and endpoint-reliant (operating systems), which are not cloud native and (at minimum) lack cloud context.

The most difficult problems are systemic in nature and those problems require comprehensive solutions. Cloudvisory is the only comprehensive solution for cloud-native, multi-cloud governance. Only Cloudvisory provides support for agentless governance across public and private cloud environments, such as AWS, Azure, Google Cloud, Kubernetes and OpenStack.

Even a comprehensive technical solution may be insufficient. Any technical solution must work in harmony with the people and processes that implement it. Cloudvisory allows organizations and business units to implement governance policies according to their unique requirements and practices.

Cloudvisory allows you to keep your existing automation tooling and let an intelligent machine augment security policy governance for your organization.

Better together
Cloudvisory governance builds upon Cloudvisory visibility and Cloudvisory compliance to deliver intelligent, cloud-native governance for complex and dynamic multi-cloud environments. Cloudvisory machine learning algorithms learn from the deep context provided by Cloudvisory visibility and compliance, incorporating as much information as possible from the cloud, historical, security and system context associated with a given asset. Greater context yields more accurate governance policies, and the artificial intelligence built into Cloudvisory helps organizations achieve more accurate governance policies with less time and effort.



Continuous Compliance Assurance for Cloud Security

Minding the Visibility Gap for Cloud Security

Supported Cloud Service Providers

- Azure
- AWS
- Google Cloud
- Kubernetes
- OpenStack

Supported Operating Systems

- CentOS
- Redhat
- Ubuntu Linux

Gartner Cool Vendor 2018

Cloudvisory named Gartner Cool Vendor in Cloud Security 2018.

CIO APPLICATIONS TOP 25 AMAZON SOLUTION PROVIDERS-2017

Cloudvisory recognized by CIO Applications in top 25 Amazon Solution Providers.

AICPA SOC aicpa.org/soc4so

Cloudvisory-SaaS independently SOC2 certified.

To learn more about Cloudvisory, visit: **www.FireEye.com/cloudvisory**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™