VMware Aria Guardrails

Govern your clouds with end-to-end policy enforcement at scale

Teams that can benefit from VMware Aria Guardrails

- Cloud operations
- Platform operations
- FinOps
- Security
- Architecture
- Application (site reliability engineers and developers)

Native public cloud has enabled organizations to accelerate operational velocity with faster deployment of software services. However, organizations must also ensure operations are secure, spend is regulated, and performance is optimized with the vast number of accounts and services spread across multi-cloud environments. Lack of expertise on cloud best practices and manually defining and tracking enforcement of organization-level policies using several disparate tools often lead to inconsistent implementation of operational standards across environments, elevating cloud security risks. Such processes don't allow cloud best practices to scale in growing environments.

Cloud teams need a smarter approach to manage and enforce policies across cloud environments that enables faster software releases without violating organizational boundaries.

Introducing VMware Aria Guardrails

VMware Aria Guardrails™ is a multi-cloud governance service that enables organizations to scale end-to-end policy enforcement across clouds and Kubernetes. Cloud teams can consistently enforce standards that help regulate cost, reduce risks, and optimize performance across clouds, Kubernetes and hosts. The service combines preventative and detective techniques that make it possible to repeatedly create accounts with predefined policies that mirror organizational controls, continuously monitor configuration drift, and automate policy enforcement. Cloud teams can avoid manual approaches and leverage infrastructure-as-code (IaC) templates to define the desired policy configuration and deliver compliant accounts using landing zones. The service also provides a unified view of policy violations and configuration drifts, across policy engines and clouds, in context to a graph-based cloud inventory and offers automated actions to resolve compliance issues. Using one extensible platform, cloud teams can create and maintain compliant public cloud and Kubernetes environments while application teams can continue to build modern apps faster and more securely.

Techniques to strengthen governance

- Policy management and enforcement for public clouds, including Amazon Web Services (AWS) and Microsoft Azure
- Centralized visibility of policy violations across multi-cloud environments and various tools
- Built-in industry standards and compliance frameworks to continuously improve security posture
- Visibility into entitlements to understand and manage permissions granted for a resource
- Understanding of overall risk by viewing policy violations in context with connected cloud objects
- Automated configuration management and vulnerability scanning for hosts
- Automated workflows that make it easy to operationalize governance programs

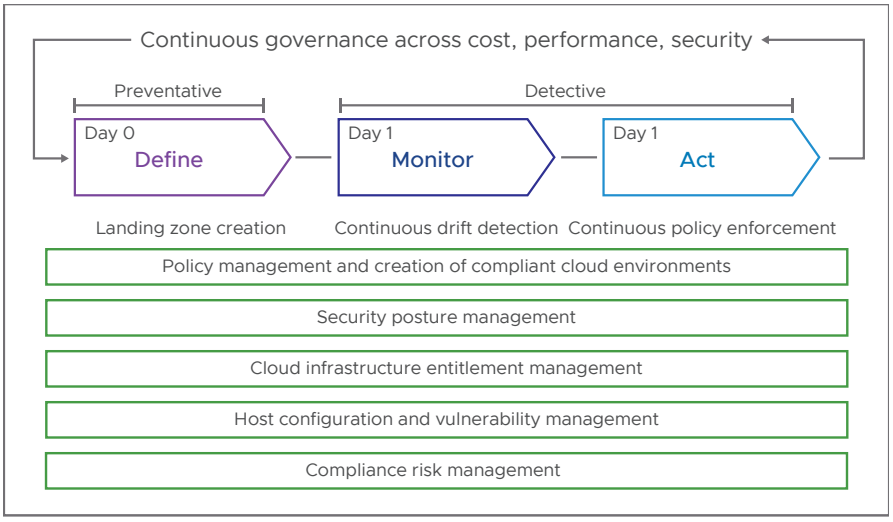

Figure 1: VMware Aria Guardrails enables end-to-end policy enforcement by automating preventative and detective governance techniques in a single service.

End-to-end policy enforcement

VMware Aria Guardrails delivers a preventative mechanism with the ability to define policies in IaC templates and automate provisioning of multi-account environments, which helps enforce Day 0 policies consistently. Post-deployment, the service takes advantage of event-based detection to monitor drift. Cloud teams can either choose to correct drift manually or leverage continuous enforcement functionality to speed up issue resolution and ensure policies are automatically enforced across environments. With this approach, VMware Aria Guardrails provides a mechanism to continuously implement compliance best practices, starting from creation of cloud accounts until as long as post-deployment changes in the cloud asset configurations occur.

The VMware Aria Graph™ datastore enables the continuous detection of policy violations by leveraging cloud asset data, APIs and change events to model the entire multi-cloud environment in a single place. Utilizing this data layer, the service applies predefined compliance benchmarks as well as organization-specific custom rules to detect violations.

This model enables operations and application teams to quickly visualize changes in configurations and connected cloud assets, as well as historical changes to better understand the blast radius for a risky configuration. As objects, data and relationships change, the service continues to update the datastore and detect new violations. Advanced rules allow for risk correlation due to resource relationships and entitlements with configuration errors and threat activity.

Application teams get actionable alerts and can remediate policy violations through the cloud console, auto-remediation, or the application of policy checks within a continuous integration/continuous deployment (CI/CD) pipeline.

Benefits

- Governance at scale – Leverage landing zones as well as built-in and custom policy templates to automate provisioning of compliant accounts for scale. Automate drift remediation to continuously enforce compliance and maintain operational standards across growing cloud environments.

Resources

Visit the VMware Aria Guardrails product page for more information.

- Compliance visibility with inventory context – Gain a unified view of noncompliant cloud resources and policy violations. Correlate violations with a graph-based cloud inventory and entitlements for deeper context.
- Efficient, automated workflows – Suppress noise and deliver meaningful alerts to the right teams to streamline governance operations in muti-account environments.
- In-depth coverage – Monitor compliance risk for more than 350 resource types, using more than 20 out-of-the-box best practices and industry benchmarks, and more than 1,200 rules.

Use cases

- Policy management and enforcement – Provision compliant accounts for multiple developer teams at scale by defining cost, security and operational policies in IaC templates for a hierarchy of accounts. Maintain compliance by correcting configuration drift automatically.
- Security posture management – Leverage event-driven detection, advanced rules to scan Kubernetes connections with external cloud services, and auto-remediation to mitigate policy violations post-deployment.
- Cloud infrastructure entitlement management – Gain bidirectional visibility into principals and their entitlements to cloud resources to identify sensitive access conditions.
- Host configuration and vulnerability management – Automate configuration management, improve compliance, and manage vulnerabilities for hosts.
- Compliance risk management – Benchmark compliance across clouds, Kubernetes and hosts with predefined industry standards and regulatory frameworks.

Key integrations

- Cloud providers and services – Secure the cloud control plane with support for more than 100 infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) solutions in AWS, Azure, and Google Cloud environments.
- Inbound integrations – Ingest security vulnerabilities and threats from multiple tools to improve understanding of security posture. Inbound integrations include Amazon GuardDuty, Microsoft Defender for Cloud, Amazon Inspector, and Google Cloud Security Command Center.
- Outbound integrations – Send notifications and integrate with existing workflows to speed up security response. Outbound integrations include email, Jira Cloud, Slack, Splunk, Amazon SQS, and webhook to use Microsoft Teams, PagerDuty, and more.

Get started

To test-drive VMware Aria Guardrails, sign up for VMware Aria Hub™ Free Tier or talk to an expert today. VMware Aria Hub Free Tier provides access to cloud policy templates, configuration drift monitoring, and Center for Internet Security (CIS) violation data for two public cloud accounts of your choice and a Kubernetes cluster.