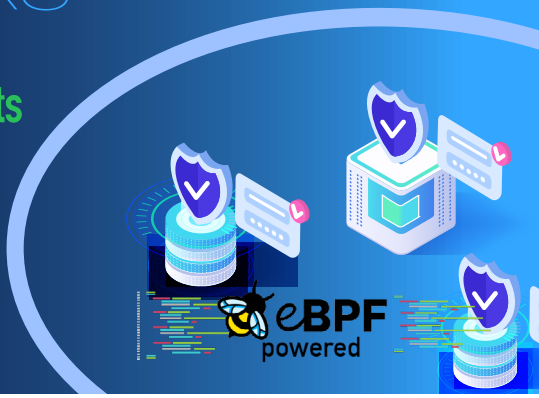
RSAC Innovation Sandbox 2022 FINALIST

SOC 2 COMPLIANT TYPE II

Araali Networks

Prioritized Risk Mitigation for Cloud Environments

Least Privilege for Apps - any Cloud, any Resource



Modern cyber risk management

Digital transformation and the Cloud are significantly changing **risk around customer data.**

- Cybersecurity is mainly about protecting the 4 Ps - PII, PHI, PCI, and IP (intellectual property). All of these are usually part of customer data sitting in production environments.
- Traditionally corporate and production environments were both inside the perimeter. Corporate services are moving to SaaS, and production workloads are transitioning to the Cloud (IaaS), requiring novel ways to implement security.
- The focus has to shift to Prod whereas Cloud is driven by devs.

There are **gaps in the Cloud controls**.

- Cloud security is complex and not well solved. Cloud is optimized for DevOps and speed. Security is still tricky, challenging, and turned off by default (left as a "TODO" in the shared responsibility model).
- Each cloud has its own IAM story. Multi-cloud and hybrid cloud make it even more complex.
- Cloud IAM is applicable only for a small portion of the overall risk and exposure.
- Cloud IAM also has a secret problem (exemplified by the CapitalOne breach), and secrets leaking into GitHub.

Teams are struggling to **prioritize prod risks.**

- High pace of change in both Infra, and complex Apps and Microservices (spaghetti of custom, third-party and opensource apps where provenance is sometimes unknown)
- Appsec struggling with fast paced development needs of prod code changes.
- Vulnerability chasing and appsec (SAST, DAST, IAST) is not scaling.
- Prevent is not working - supply chain, ransomware, phishing, breaches galore.
- Hard to prioritize an unbounded stream of security events with high false positives.

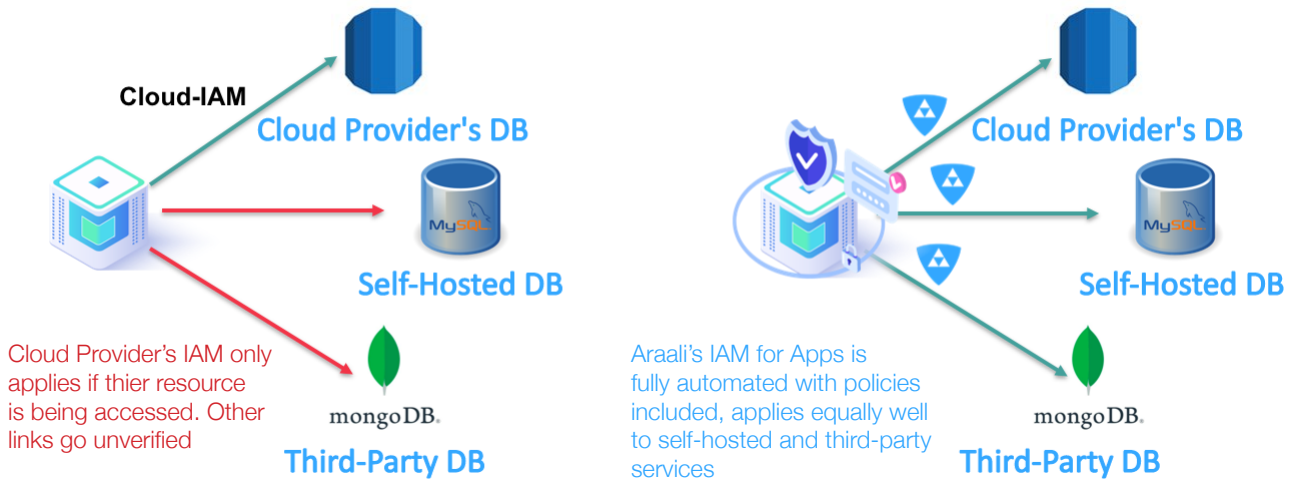


Fig: Cloud IAM is not comprehensive

+1-510-624-9941

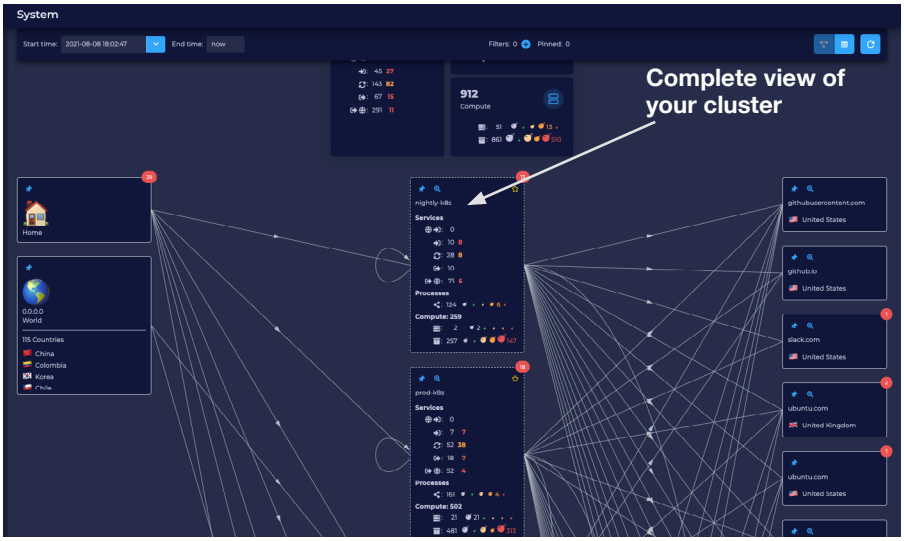
39812 Mission Blvd. Suite 224
Fremont, CA 94539 USA

support@araalinetwork.com

Araali: Least Privilege for Apps - any Cloud, any Resource

Prepare.

- Get a bounded view of all apps and services used in your production.
- This includes all apps - any language and any source (third party, open source).
- This includes all resources - even third party and external to your production environment.
- This includes all clouds.

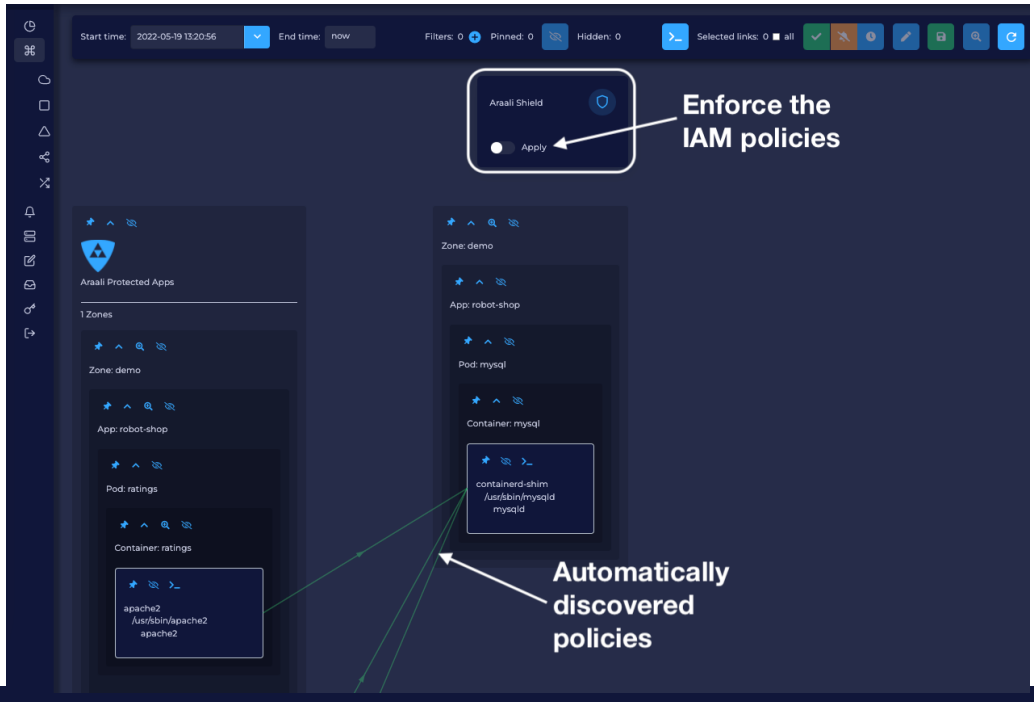


Prioritize.

- Use Insights to identify your “Protect Surface” - crown jewels, critical apps, vulnerabilities, exposed services etc.
- Focus your resources on the “protect surface.” In comparison, the attack surface is an ever-expanding universe, a losing game where you are always running behind/chasing.

Protect.

- Protect apps inside out - only allow identity-based access to critical apps and services.
- Assume compromise - i.e., the overall prod environment is not pristine.
- Monitor egress - breaches happen because there is no good way to control what leaves your prod environment.



+1-510-624-9941
39812 Mission Blvd. Suite 224
Fremont, CA 94539 USA
support@araalinetwork.com

Differentiation

Simple, easy, and secure - all at the same time

Easy Deployment:

- Self serve account signups.
- Single-click install.

Quick Value:

- Instant, continuous, and comprehensive visibility.
- Duality between (a) alert and policy and (b) monitoring and controls.

Performant with Minimal Operational Overhead:

- Highly performant, do no harm operations - powered by eBPF.
- No changes to the environment and no networks to configure.
- Automated least privilege policy discovery and management.

API and Integrations:

- APIs in golang and python as well as command line.
- Logstash integration - i.e., SIEMs like Elastic, Cloudwatch, Azure Sentinel, Google Big Query, Kafka, PagerDuty, Splunk, Datadog, Sumologic, Dynatrace.

Landscape

Cloud has changed the threat model. Cloud providers take care of physical security, infrastructure, even IAM.

What remains as part of the shared responsibility is **configuring the IAM for least privilege.**

CSPM offers to flag the cloud configuration if it is not adhering to security best practices. No matter how much effort is spent in appsec and dev stage, **continuous monitoring and security** is the **essential security function** that will never go away.

By machine generating and automating least privilege zero trust grade policies as part of CWPP, Araali covers most of the checks in CSPM.

+1-510-624-9941

39812 Mission Blvd. Suite 224
Fremont, CA 94539 USA

support@araalinetwork.com