

The Security-as-Code Innovator for Public Cloud



WHY CONCOURSE LABS

- Increase cloud security review throughput by **30x**
- Reduce security exposure time by **99%**
- Implement cloud security best practices within **minutes**
- Stop the #1 cause of cloud data breach: **misconfiguration**

Prevent Cloud Data Breach Without Slowing Innovation

Most cloud breaches are caused by misconfiguration, not attacks on cloud infrastructure. However, rapidly detecting and remediating security risks continually, across cloud development, delivery, and runtime environments, is exceedingly difficult. Existing CSPM, CWPP and infrastructure-as-code scanning tools are either fragmented – meaning they only cover part of the lifecycle, or they are immature – meaning their security domain and control coverage is extremely limited. All of which leaves organizations highly vulnerable to cloud breach.

A new approach to cloud security is needed. Concourse Labs, the innovator in Security-as-Code, makes it easy to embed security into every stage of the cloud application lifecycle, automatically. Teams can shift security far left, to prevent exposure from vulnerable cloud resources, while protecting against drift and attack at runtime.

With Concourse Labs, organizations can, for the first time, fully automate cloud security reviews and ensure cloud data stores are properly encrypted and key material is secure, know which cloud services are exposed to the public internet, eliminate shadow cloud resources by verifying trusted ones, remove excessive access permissions and weak IAM controls, and much more. All without slowing innovation.

SECURITY-AS-CODE MAKES SHIFT-LEFT SECURITY POSSIBLE

Security-as-Code is the only way organizations can gain comprehensive visibility and control of cloud security and compliance risk, across the full application lifecycle, at cloud speed and scale.

Security-as-Code is the practice of expressing security and cloud control objectives in code to orchestrate and automate their use at cloud scale. It's predicated on the notion that security should be considered an integral part of the software development process and treated like other forms of code. This way, cloud controls can be created, enforced, and managed at the same speed and scale as the cloud infrastructure automation organizations have already achieved.



**WITHOUT
CONCOURSE, WE
COULD NOT HAVE
MOVED MORE
APPLICATIONS TO
CLOUD."**

VP, TECHNOLOGY STRATEGY
FORTUNE 50 FINANCIAL
SERVICES COMPANY

Rapidly detect and remediate cloud risks across the **entire cloud application lifecycle**, with **one policy architecture**, to eliminate security gaps and remove friction.

KEY SECURITY BENEFITS

- Accelerate secure cloud migration
- Reduce the security backlog
- Overcome cloud security skills shortage
- Satisfy regulators and auditors

CONCOURSE PROTECTS AGAINST CRITICAL CLOUD RISKS

- Encryption and key management
- Public internet exposure
- Excessive privileges and weak IAM controls
- Shadow and untrusted resources
- Secrets sharing
- Cloud configuration drift

Cloud-Native Application Protection Platform (CNAPP) for the World's Most Vigilant Organizations

PREVENT DEPLOYING VULNERABLE RESOURCES AND CONTINUOUSLY DETECT RISKS IN RUNTIME

Automatically detect cloud services risks within infrastructure-as-code (IaC) and prevent insecure resources from ever being deployed. Concourse's Security-as-Code architecture validates security within CI/CD pipelines and far left within source code management (SCM) tools, like GitHub and Bitbucket. Developers get instantaneous feedback, directly within their existing tools, as they commit code, or share IaC through merge or pull requests. Empowering them to remediate violations without requiring security teams to intervene. This federated approach to security enforcement and remediation is critical to controlling cloud risk. And while shifting left is essential, Concourse's agentless technology continually evaluates cloud usage to detect drift from security blueprints in runtime.

PRIORITIZE WHAT MATTERS MOST AND ELIMINATE ALERT FATIGUE

Security teams require context to make intelligent decisions. Concourse Labs clearly identifies high-risk vectors that have the greatest potential impact on the business. Reduce mean time to resolution by filtering out the noise and letting everyone, at every level, focus on the violations that matter most. With Concourse Risk Surfaces™, security teams can delegate policy authorship and approval to frontline leaders, enabling them to build context-aware policies to ensure the right controls are enforced to meet the specific needs of their business or function, while maintaining centralized visibility, oversight, and control.

AUTOMATE CLOUD SECURITY WITH THE MOST ADVANCED POLICY SYSTEM

Increase the throughput of cloud security reviews by up to thirty times. Concourse's advanced policy architecture enables teams to express cloud security and compliance requirements as code, to easily instantiate them as gates and guardrails, automate reviews and ensure unambiguous results. Concourse is the only Security-as-Code solution that delivers a single policy architecture that spans the entire cloud application lifecycle – from development through runtime. This significantly increases security, and reduces complexity and cost, by eliminating blind spots that result from a patchwork of products, each with their own policies, control checks, and GUIs. Key to successfully implementing Security-as-Code is the ability to manage codified security controls. Concourse provides the most advanced gitops-style environment for centrally managing and auditing policies, controls and associated permissions.

ABOUT CONCOURSE LABS

Concourse Labs provides the only Security-as-Code platform that empowers organizations to systemically reduce and manage cloud security risk, without slowing innovation. Through a single policy architecture, Concourse embeds security checks at every stage of the cloud application lifecycle, from far left through runtime. Organizations can express cloud security and compliance requirements as code and easily implement them as guardrails, automate reviews and attain unambiguous results. Concourse also eliminates the most common Security-as-Code pitfalls with the most advanced gitops-style environment for managing and auditing policies, controls and associated permissions.

READY FOR A GUIDED TOUR?

Request a demo today at concourselabs.com/demo