concourse™ LABS

A comprehensive approach to securing cloud workloads and data — now integrated with Google Cloud Platform™

Rapidly amplify your Google Cloud investment with automated, preventative, and detective controls for complete risk posture management out of the box.

Prevent the #1 cause of cloud data breaches

In the cloud, misconfigurations are the most prevalent threat to cloud security.[1] Misconfiguration can be caused by failure to change default settings or configuration drift, where changes to various components are made outside of approved processes and pipelines without consistency and auditing.[2] Cyber criminals are actively hunting for the easiest way to steal data, passwords, financial information, and other exploitable business and personal data. Misconfigured cloud infrastructure and assets create the vulnerabilities that attackers use to access your systems and data.

Save on security and compliance costs

The cost of containing and mitigating security breaches and possible regulatory fines impacts your bottom line. Research shows that it can be 30X more costly to resolve security vulnerabilities in the monitor phase than the pre-build phase.[3] And GDPR violations for security defects carry fines of up to 4% of global revenue.[4] In contrast, firms that build security into their daily work spend 50% less staff time addressing security issues.[5]

Increase company performance

Manual pre-deployment security reviews and reactive fire drills after a breach sap developer productivity — and morale. Automating security into existing development workflows reduces security risks and increases developer productivity. High-performing organizations can recognize 200X more frequent code deployments, 2,555X faster lead times, 24X faster recovery times, and a 3X lower change failure rate.[5]

Shift left with Security-as Code

Implement effective, scalable, and auditable cloud security in days.

Traditional cybersecurity approaches simply can't meet the rapidly evolving security requirements of modern cloud environments. Just 10% of IT leaders say they can detect, contain, and resolve cyber threats within one hour, making it no surprise that 77% report they struggle to identify what tools they need to achieve their security objectives.[6]

That's why Concourse Labs pioneered the concept of Security-as-Code — the most effective way to secure cloud applications and data. Security-as-Code formalizes security and control objectives into a set of automated rules and logic. With thousands of out-of-the-box policy checks, based on industry standards and best practice, and our no-code approach to developing your own policy, it is easy to implement security standards without being a cloud expert or writing code.

Centralized policy management and automation across any environment means you can write policy once and apply it anywhere. And it's all available in a fast-to-results, easy-to-use cloud-based software platform that protects development pipelines, provides immediate visibility to misconfigurations, and monitors cloud security compliance in real time.

Concourse Labs enables you to apply business context and maintain granular control of policy deployment by geography, environment, business unit, application workload, or regulatory requirement. With Concourse Labs, you can transform security visibility from opaque to transparent — giving developers real-time, where-they-work insight into policy compliance requirements so they can write better infrastructure-as-code, unconstrained by manual security reviews and rework.

Integrated with Google Cloud Platform security

Concourse Labs preventative controls are now integrated with Google Cloud Platform (GCP), helping you to quickly and confidently understand, improve, and manage your cloud security posture.

Automate risk-based security assessment of GCP services

Concourse Labs Connector for Google Cloud Security Command Center

Concourse Labs Connector for Google Cloud Security Command Center (SCC) collects and integrates policy violation and remediation data into SCC to provide a unified view of the security posture of all Google Cloud assets. Concourse automatically validates security and compliance at every stage of the cloud application lifecycle, so you can prevent a data breach before it happens and immediately respond to drift in runtime.

Close configuration security gaps with preventative controls

Google Cloud Blueprint-Based Policy Collections

Concourse Labs provides out-of-the-box, curated policy collections aligned to Google security foundations blueprints and can provide policies over Google-provided Terraform modules. Concourse Labs translates GCP blueprints and complex enterprise standards into automatable policy that automatically enforces blueprints within the development lifecycle and gives developers just-in-time remediation guidelines.

Explore the best approach for securing cloud workloads and data

Concourse Labs can help you reduce risks in the cloud while accelerating cloud migration and new development of compliant and secure workloads and data. You can explore, launch, and manage Concourse Labs solutions on GCP in just a few clicks using Google Cloud Marketplace.

[1] Elgan M, Why Are Cloud Misconfigurations Still a Major Issue? Security Intelligence, Nov. 1, 2022.
[2] Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Advisory, Weak Security Controls and Practices Routinely Exploited for Initial Access, Dec. 8, 2022.
[3] Connelly M, Bartol N, Weinberg C, et al., Accelerate Cloud Migration with Security Automation, Boston Consulting Group, Feb. 14, 2023.
[4] European Union's General Data Protection Regulation (GDPR), What are the GDPR Fines?, accessed March 2023.
[5] Puppet + DevOps Research and Assessment (DORA), 2016 State of DevOps Report, 2016.
[6] Muncaster P, Just 10% of Firms Can Resolve Cloud Threats in an Hour, InfoSecurity Group, March 2023.