concourse labs

The CIO Handbook to Security as Code

Introduction

Companies everywhere are moving to cloud. But they struggle to ensure their security, to comply with regulatory standards, and to protect themselves and their customers from data breach or disruption. Yet the pressure to migrate to cloud continues unabated, and with little tolerance for slowing innovation to get control of cloud risk.

The fundamental flaw is that traditional cybersecurity architectures and models break down when applied to public cloud. Most cloud breaches stem from misconfiguration of cloud services, not attacks on the underlying infrastructure. However, existing cybersecurity tools are not designed to prevent, detect, and correct cloud misconfiguration comprehensively across build time and runtime environments, and at the pace at which cloud applications are delivered or changed. As a result, businesses are either blocked from capturing the full benefits of public cloud or they accept the unknown risks of migration. Neither is sustainable.

An innovative approach is needed—one that:

- Automates security and compliance across the entire cloud application lifecycle
- Prevents breaches before they happen, giving developers real-time assessments of their code, and immediately identifies drift and attack in the cloud
- Protects all cloud environments, including IaaS, PaaS, and SaaS
- Provides enterprise-wide visibility and control, while empowering developers, operators and security professionals with always up-to-date risk, remediation, and compliance guidance

The answer is Security as Code.

Security As Code

When defining Security as Code, it may be helpful to clarify that it is not a product you purchase or a finite set of features or capabilities you build. Instead, it is a novel approach or paradigm to security and risk management. It is uniquely suited to address the new challenges posed by cloud application delivery and operation. Enterprises typically refer to security as code adoption by saying, “we are on a path to security as code,” much like how they refer to their journey toward zero trust.

As the name implies, Security as Code encompasses the creation, enforcement, remediation, and lifecycle of security, as code. It is predicated on the notion that security should be viewed as an integral part of the software development lifecycle (SDLC) and treated like other forms of code. This way, cloud security and risk controls can be created, enforced, and managed at the same speed and scale that automation has made possible for the delivery of cloud infrastructure services.

At its core, the key principles of Security as Code are:

1

Treat security and compliance as first-class citizens

Create, model, apply, and manage security and compliance controls as code.

2

Automate policy enforcement & federate risk remediation

Automate enforcement, delegate remediation to developers and orchestrate findings across security and IT ecosystems.

3

Continuously validate cloud security and compliance

Check and enforce policy continuously and automatically, at every stage of the cloud application lifecycle.

"When adopting Agile and DevOps, many organizations struggle to fulfill security and compliance requirements while maintaining continuous delivery workflows. I&O leaders must continuously enforce and improve compliance using automation across databases, application code, infrastructure and OSS."

Gartner®, "Innovation Insight for Continuous Compliance Automation",
Daniel Betts, Manjunath Bhat, Hassan Ennaciri, Chris Saunderson, refreshed February 11 2022.

Technology Considerations

Security as Code is enabled by several emerging cloud technologies and best practices. And while technical maturity will vary from organization to organization, understanding these, and how they fit in, will help ensure success as organizations embark on their Security as Code journey.

Automation

The fact that almost everything in cloud is an API provides a strong basis for automation of security and risk management. Automation is the only way security and risk teams can keep pace with development and ensure controls are consistently and correctly enforced.

Policy as Code

Policy is becoming the de facto standard for defining and ensuring safe cloud usage. Policy as code is the instantiation of security and compliance standards as code, enabling them to be built, operated, audited, and managed as first-class citizens. It is core to a Security as Code framework.

Infrastructure as Code

Tools like Terraform and CloudFormation are key to an enterprise's ability to automate and scale applications in the cloud. When misused, these tools propagate risks and breaches at unprecedented speed and scale. The only practical way to control and manage this risk is through Security as Code.

Cloud Native Application Protection Platforms

Vendors are rapidly amalgamating disparate tools to form what analysts are terming Cloud Native Application Protect Platforms (CNAPP). However, realizing CNAPP's promise of gaining visibility and control over cloud risk requires a comprehensive system that covers the entire cloud application lifecycle, from development through runtime. Most CNAPP tools are in their infancy, and few are architected with this capability.

"Implement an integrated security approach that covers the entire life cycle of cloud-native applications, starting in development and extending into production."

Gartner®, "Innovation Insight for Cloud-Native Application Protection Platforms", Neil MacDonald, Charlie Winckless, Aug 25, 2021.

Organizational Readiness

Adopting a Security as Code approach is not just about technology. The continued evolution of how organizations are rethinking security and risk management involves:

- **Shifting security left**
- **Federating certain security and risk management tasks to personnel outside security teams**
- **Embracing automation across the entire security lifecycle**

Security operations must move from a reactive to a preventative posture. Security as Code is key to successfully shifting left. It requires that enterprise standards be defined and developed independently of application code and inserted early in the software development lifecycle. This way, standards can be adapted and applied independently of application delivery cycles and processes.

The reality, however, is that developers far outnumber security practitioners, and developers use automated tooling to push more code to cloud more rapidly than ever. Only by inserting automated testing within the development pipeline can security teams prevent breach. This automated shift-left testing empowers developers to instantly validate their code and remediate non-compliance immediately. All while simultaneously giving security and risk teams complete visibility and control early in the development process.

Security as Code is a departure from the more traditional, siloed approach to security and risk management and point solutions that create gaps and add complexity and cost. This requires a culture shift where teams actively collaborate and share their requirements. Cloud is a team sport. And as it becomes the operating system on which businesses run, effectively managing security and risk must become everyone's responsibility.

"Security needs to adopt and support a mindset where security starts at the very beginning of service creation and throughout the DevOps processes, and is continuous, automated and improves with each subsequent iteration."

Gartner®, "Implementing Security Into the DevSecOps Toolchain", Mark Horvath, Neil MacDonald, refreshed March 4, 2021

Enable Safe Innovation & Reduce Risk

Rapidly Innovate Safely

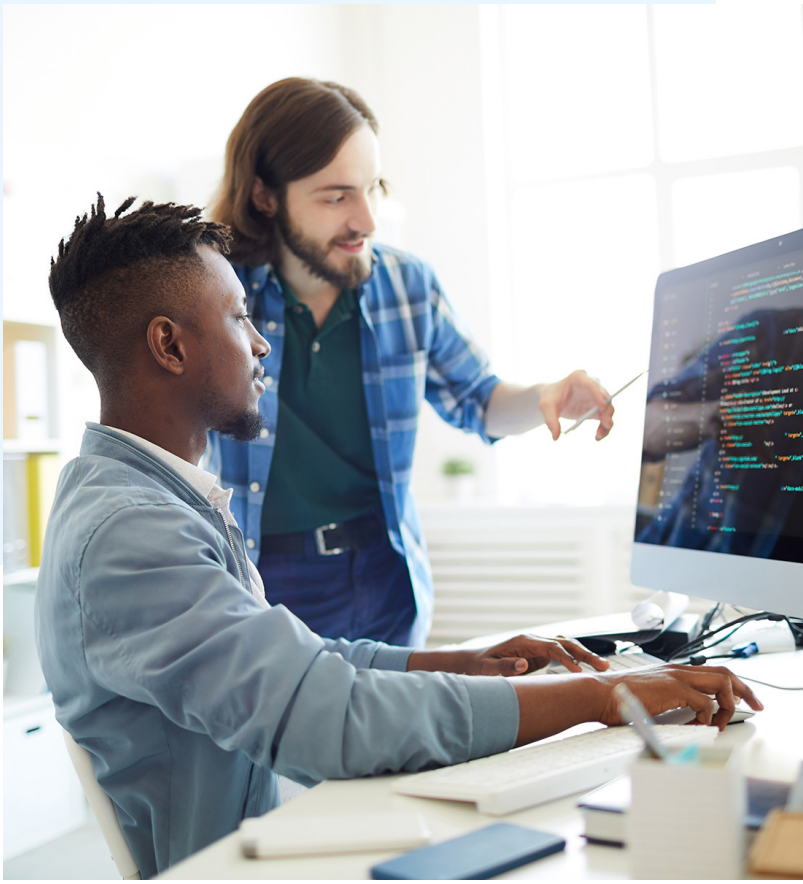
Security as Code enables companies to safely move applications to cloud without slowing down. It empowers developers to deliver secure cloud applications rapidly, without the burden and friction of outdated security practices. Developers instantly confirm their code is compliant and automate the remediation process when it fails. All within the toolchains they use today. Automation helps offset the ongoing skills shortage and enables organizations to achieve their cloud migration goals without increasing the current size of their security teams.

Increase Security and Reduce Risk

The more organizations work in cloud, the more resources they configure. Configuration can change throughout the cloud application lifecycle. Security as Code reduces risk by inserting automated guardrails, to validate configuration, at every stage of the software supply chain – from source code management repos and CI/CD pipelines through production. Because Security as Code is a distributed architecture, it provides the visibility and control that developers, operators and security professionals need, with always up-to-date risk, remediation, and compliance guidance.

Bridge the Gap Between Security and Development

To effectively manage cloud risk, organizations must break down the walls between security and development teams. Security as Code establishes a common framework for collaboration and nurtures a culture of security across the organization. More importantly, Security as Code enables both teams to focus on what they are highly skilled at and measured against. Developers focus on designing core features and functions and application uptime. While security and risk teams focus on developing standards that protect against breach and disruption.



One Company's Security As Code Journey

A large, publicly traded financial services firm embarked on an aggressive infrastructure transformation program that served as the catalyst for its migration to public cloud. As part of this, the company established a modern delivery program for building dynamic agile infrastructure and dynamic applications, redesigning monolithic applications, and deploying them as microservices in the cloud.

The company experienced numerous security and risk management challenges at the onset:

"People were used to doing things a certain way and they just continued trying to do things in that way when we moved to cloud. People thought we could just bring existing processes forward and it just didn't work," said the organization's VP of Technology Strategy.

Given that cloud poses a number of new risks, one of the firm's early goals was to move from a purely reactive to a preventative posture where risks are identified within development, before they are deployed. "No matter how you configure a NAS device running in your data center there is no command you can give to say that I am going to make this thing world accessible. There are just too many layers between that device and the outside world. In Amazon it is just one S3 bucket misconfiguration and your data is out there in the world."

Using a Security as Code approach, the firm decided to address security and compliance in its cloud delivery pipeline. Using infrastructure as code to configure and provision their cloud services, the organization began implementing automated policy checks within CI/CD. After about nine months, they determined that it was critical to shift further left, and check for cloud misconfigurations as developers commit and merge infrastructure as code within source code management tools like Bitbucket and GitLab.

Now, after more than a year into their Security as Code journey, the company can count on every developer across its 40+ cloud application teams to automatically validate their infrastructure as code against the latest security and compliance controls. And that the firm can rapidly and safely deploy applications without disrupting developers and give security teams complete visibility and control of cloud risk early in the application lifecycle.

"We would have had to increase our security staffing budget by $5,000,000 to cope with our cloud migration plans," had they not chosen Concourse.

Three Keys To Successful Implementation

Concourse Labs co-founder Don Duet first implemented a Security as Code program while he was leading the technology division at Goldman Sachs. He has also advised other large cloud-forward enterprises in doing so.

Don's three keys to achieving a robust, scalable, and agile Security as Code program are:

Establish Security as Code Governance

The first key necessitates a focus on ownership and accountability. It also places emphasis on having an internal structure for governing roles, responsibilities, and permissions, such as who can author policy as code and for which parts of the cloud estate. Many companies make the fatal mistake of jumping into technology implementation and skipping this step. Avoid falling into that trap.

Design and Manage Policy as Code

The second key involves the design and management of control objectives that solve discrete use cases. Write policy content with sufficient detail to meet demanding enterprise control standards. Remove ambiguity and failure associated with policy as code by versioning and tracking every change, maintaining a full audit trail of what was done, why it was done and by whom.

Apply Controls Comprehensively Across Cloud Lifecycle

The third and final key entails enforcing automated security and compliance guardrails at every stage of the cloud application lifecycle. Identify risks early in development to prevent non-compliant code from being deployed. Continuously detect drift and attacks in runtime - without agents and without disrupting developers. At the same time, give Security teams complete oversight into cloud risk early in the application lifecycle.

Pioneering Security As Code

At Concourse Labs, we offer the only Security as Code platform that enables organizations to systemically reduce and manage their cloud risk through automation. We pioneered Security as Code and are at the forefront of solving the most fundamental cloud risk challenges at enterprise scale.

Concourse Labs

Delivers complete visibility and control across the entire application lifecycle from development through runtime, with one comprehensive policy architecture.

Makes it easy to automate even the most sophisticated enterprise standards, with the most advanced and richest set of policy authoring and testing tools available.

Increases productivity of security teams via Risk Surfaces™, by ensuring automated policies are appropriately applied and tuned, escalating and remediating resulting risks based on geography, functional area, business, regulatory regime, and lifecycle stage.

Provides the only solution for managing and auditing policy as code across its full lifecycle, similar to how Git manages source code.

Protects applications on all major cloud providers and ensures compliance on platform-as-a-service (PaaS) and software-as-a-service (SaaS) APIs, including your digital supply chains.

concourse labs

With Concourse, companies are now, for the first time, empowered to achieve the same level of automation for governing the security and compliance of public cloud usage that they have with the development and delivery of the cloud itself.

Want to learn more?

Watch our 30-minute webinar