cycode

Infrastructure as Code Security

SOLUTION BRIEF

Detect & Prevent Misconfigurations With Every Pull Request

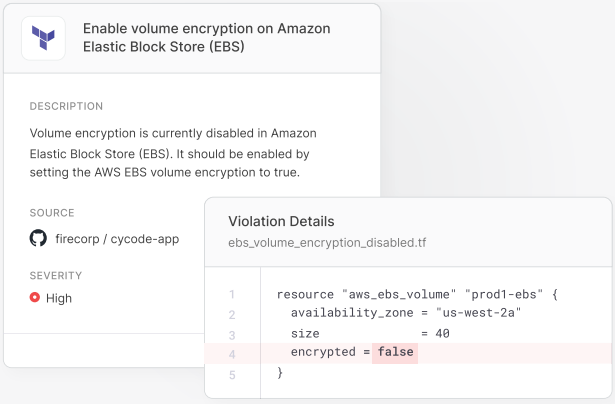
In the not too distant past, if developers needed a server, they worked with their IT administrators to procure and rack-and-stack it. With the advent of cloud computing and the embrace of microservice-based architectures, deployment complexity increased to the point that automated orchestration became necessary. Through this process developers gained the ability to spin up infrastructure like VMs, S3 buckets, and other assets at will, usually as part of an automated infrastructure as code (IaC) process. Instead of telling an IT admin what type of resource is needed, developers simply define the asset they want using tools like Terraform or CloudFormation — and build that asset as needed in the cloud. Among the many benefits of this approach are speed, elasticity, and repeatability; all of which are fundamental characteristics of today's cloud native applications.

However, the IaC approach is not without its drawbacks. If there are misconfigurations in IaC — whether because the developer lacked experience writing IaC code, they used a vulnerable component, or forgot to consider security, like publicly exposing a database holding sensitive, unencrypted data — then those problems end up being built into the infrastructure at the push of a button or as part of a fully automated process. Each time the infrastructure is built it will have the same vulnerabilities or misconfigurations, essentially automating holes into the build process for hackers to exploit when the application is in production. Application security (AppSec) teams need a way to detect and fix these problems without impacting developer efficiency.

Cycode enables infrastructure as code security by identifying misconfigurations and fixing them directly within developer workflows, ensuring configurations are secure and adhere to best practices.

Find IaC Misconfigurations

Virtually all companies running cloud applications have experienced misconfigurations at some point, these misconfigurations often expose companies to the potential for a breach. In fact, according to Gartner, "through 2022, at least 95 percent of cloud security failures will be the customer's fault."

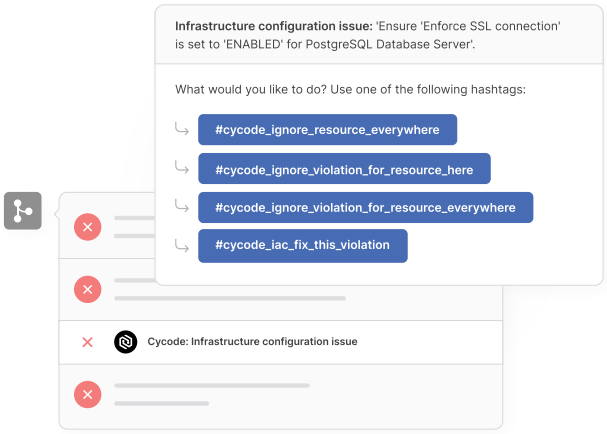


Cycode helps developers easily find and fix misconfigurations in IaC code such as Kubernetes, Terraform, CloudFormation, and Azure Resource Manager (ARM). It scans IaC at relevant points throughout the SDLC, leveraging built-in rules to recognize hundreds of security issues like publicly accessible storage buckets, critical data that is not encrypted at rest, weak password policies and non-rotated encryption keys.

Embed Scanning In Developer Workflows

Many organizations struggle to introduce effective security controls in the development process, where every change has the potential to introduce a vulnerability or misconfiguration, without disrupting the innovation pipeline. Cycode helps organizations detect and fix IaC issues before they reach production by automating IaC scanning with every pull request. These scans protect the main branch by testing new commits for misconfigurations and adherence to industry IaC best practices like NIST and CIS or custom build rules. IaC policy violations are presented to developers along with remediation advice, all within the pull request itself to ensure dev teams keep IaC secure and compliant with minimal disruption.

With out of the box integrations into common DevOps tools, Cycode fits easily into any workflow: ticketing systems, email, messaging platforms, ChatOps, or build something new with the no-code workflow engine.



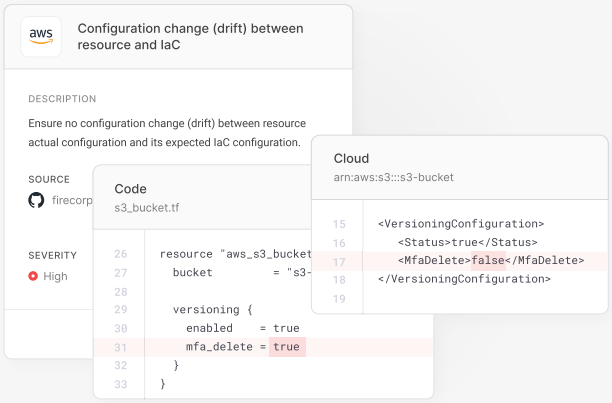
Automate Remediation

Development teams are not always fully versed in security practices, the security architecture and nuances of the broader runtime environment. Moreover, many organizations lack the resources to maintain security staff dedicated to supporting developers. To avoid delayed fixes and confusion around the right way to fix IaC misconfigurations, Cycode can generate pull requests containing the exact code fix needed to correctly remediate the specific problem detected in the IaC. This ensures that your infrastructure remains in line with best practices; problems are fixed efficiently, correctly, and completely; and your developers are not burdened by cumbersome security processes or backlogs.

Identify Configuration Drift

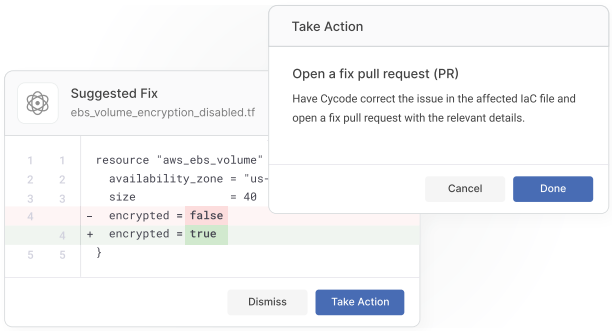
In theory the infrastructure assets in your dev, test, and production environments should be identical; after all, they were created by the same IaC code. In practice, configurations are constantly changing due to things like support tickets, regular maintenance or ad hoc fixes. Many of these changes are implemented by operators directly through the cloud console, and the resulting changes to production infrastructure aren't reflected in IaC; a situation known as drift. Depending on the nature of the changes, drift may result in the introduction of misconfigurations that could be exploited by bad actors. While drift is typically an unintended byproduct of ad hoc changes, it can also be the result of intentionally malicious activity such as that of a compromised insider. In this situation drift can pose a serious risk to organizations because hackers can adjust critical configurations like network access or encryption settings.

Cycode helps users easily identify when IaC configurations are out of sync with the configuration of the runtime environment, and sends alerts to designated DevOps and AppSec teams so these environments can be realigned to the organization's IaC.



Complete Software Supply Chain Security

Cycode helps customers find and fix misconfigurations and security risks in infrastructure as code as part of existing development workflows, and prevent drift so that runtime configurations remain consistent with the IaC. This approach of securing infrastructure in automated workflows before it is deployed and keeping it secure by preventing drift is proven to help organizations reduce the risk of a breach.



Securing infrastructure as code against misconfigurations and drift is a necessary step toward securing your software supply chain but only addresses one dimension of risk. Software supply chain attack surfaces are so vast and interconnected that organizations need a comprehensive solution that covers the entire SDLC. Cycode is the only end-to-end software supply chain security solution that provides visibility, security, and integrity across all phases of the SDLC.

Cycode integrates with all software delivery pipeline tools and infrastructure providers to implement consistent governance and security policies, harden security posture, and provide visibility across the entire SDLC. Pre-built integrations are easily deployed. With just a few simple clicks, organizations are able to realize immediate value and maximize their agility as new tools are added to the SDLC.

The Cycode platform includes a collection of scanning engines that identify other important dimensions of software supply chain risk such as hardcoded secrets, code leaks, and more. Cycode's Knowledge Graph tracks code integrity, user activity, and events across the SDLC to find anomalies and prevent code tampering so that organizations can be sure their supply chain is completely covered.

To protect the entire development pipeline, organizations need a complete solution that secures across all phases of the SDLC. Cycode is that solution.

Cycode is a complete software supply chain security solution that provides visibility, security, and integrity across all phases of the SDLC. Cycode integrates with DevOps tools and infrastructure providers, hardens their security postures by implementing consistent governance, and reduces the risk of breaches with a series of scanning engines that look for issues like hardcoded secrets, infrastructure as code misconfigurations, code leaks and more. Cycode's knowledge graph tracks code integrity, user activity, and events across the SDLC to prioritize risk, find anomalies, and prevent code tampering.

More solution briefs at Cycode.com