

# A Complete Hardcoded Secrets Solution

SOLUTION BRIEF

## Eliminate Existing and Prevent New Hardcoded Secrets

Hard coding secrets in source code has become increasingly common as more applications leverage dependencies and Infrastructure as Code, which need to authenticate services. Unfortunately, the practice of embedding usernames, passwords, tokens, API keys, and other secrets into code increases organizations' security risk and has been the source of numerous headline-grabbing software supply chain attacks in recent years.

Hardcoded secrets are attractive targets because they expose access to valuable resources, and attackers don't need exploit code to gain unauthorized access to vulnerable applications. Furthermore, once attackers uncover a username or password, they can easily move laterally across an organization's software development pipeline, shifting left into source code or right into production environments and even targeting customers further downstream by tampering with code. In addition, the same hardcoded secret is often used across multiple applications. Since many of these developer accounts are granted elevated privileges, the exposure of a hardcoded secret could be catastrophic.

Ultimately, the risk of hardcoded secrets stems from three types of exposure:

- + Compromised insiders
- + Malicious insiders
- + Code leakage

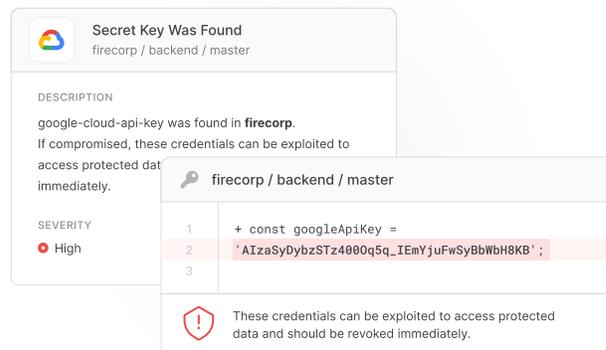
A complete hardcoded secrets solution must include comprehensive scanning, address the ways secrets are exposed, provide remediation assistance, and offer

enforcement mechanisms that prevent the practice of using hardcoded secrets from persisting. Cyclope helps find and fix hardcoded secrets, prevents new hardcoded secrets from being introduced, and reduces the risk of exposure of hardcoded secrets, all of which reduce the overall risk of a breach.

## Comprehensive Hardcoded Secret Scanning

Developers and security professionals often struggle to identify all the hardcoded secrets in their environment. Hardcoded secrets must first be identified in order to be eliminated. The challenge, however, is that secrets come in a wide variety of formats—API keys, encryption keys, tokens, passwords, database connection strings, custom secrets, and other high entropy strings. They can also live in a number of potential locations such as source code, build logs, Infrastructure as Code templates, Kubernetes clusters, version histories, and more.

Because of the diversity of secrets and the difficulty in finding them, a hardcoded scanning tool must be both versatile and comprehensive to deliver the required depth and breadth of scanning.



The screenshot displays a security alert titled "Secret Key Was Found" for the file path "firecorp / backend / master". The description states: "google-cloud-api-key was found in firecorp. If compromised, these credentials can be exploited to access protected data immediately." The severity is marked as "High". A code snippet is shown with the following lines:

```
1 + const googleApiKey =  
2 'AIzaSyDybzSTz400q5q_IEmYjuFwSyBbWbH8KB';  
3
```

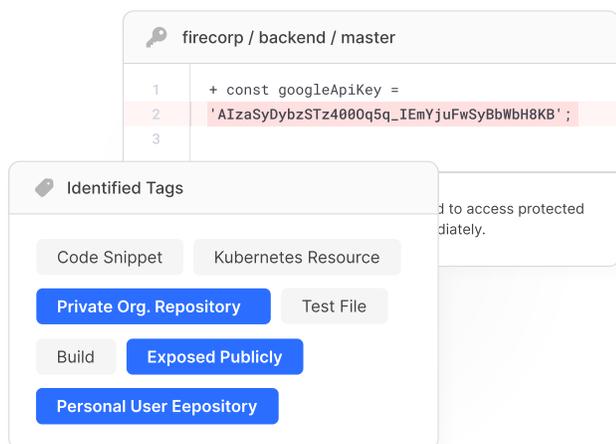
A red warning icon and text at the bottom of the alert state: "These credentials can be exploited to access protected data and should be revoked immediately."

Cycode offers robust, continuous hardcoded secret detection that identifies any type of hardcoded secret anywhere in the software development life cycle (SDLC). This includes scanning Source Control Management (SCM) tools, delivery pipelines, public and private repositories, Kubernetes resources, and more. Cycode's hardcoded secrets scanning also leverages multiple detection methods—including scenario and pattern matching, high entropy string detection, and more—to provide unmatched detection.

## Prioritized Remediation

It's common for development teams to have hundreds or even thousands of hardcoded secrets spread across their software development pipelines. Due to sheer volume and the time required to apply a fix, it is impossible for developers to address all secrets at once. With numbers this big, prioritizing the remediation of the most critical hardcoded secrets is essential to rapidly reducing risk. Without prioritization, developers could spend their time fixing hardcoded secrets that have little chance of being exposed while leaving critical ones vulnerable to discovery.

After scanning the entire SDLC, Cycode prioritizes hardcoded secrets based on the type of exposure (publicly exposed or in a private asset) and the location of the secret (for example, a production application, personal developer repository, Kubernetes resource, CI/CD log, code snippet, test file, and more).



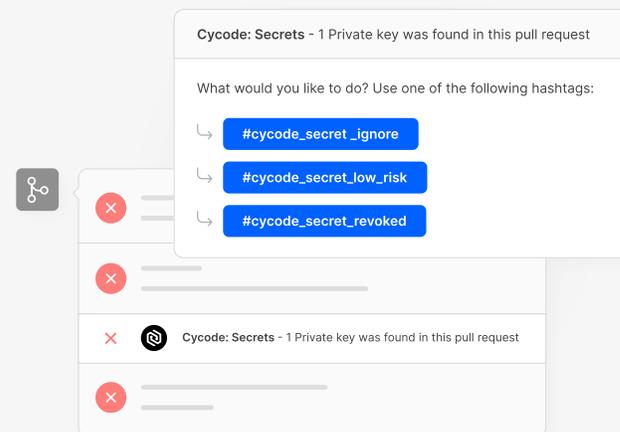
This allows users to easily assess the risk so that the most critical issues can be remediated first.

Cycode also identifies which results are likely to be false positives and can be safely ignored, which saves developers precious time. Cycode's Knowledge Graph further helps prioritize the remediation of hardcoded secrets by providing context like knowing whether a hardcoded secret is associated with a code leak or is in a repository that has been pushed to production. Prioritized remediation helps organizations fix their riskiest secrets first to reduce their exposure as quickly as possible.

## Developer Friendly Workflows

Though finding and eliminating existing hardcoded secrets is an essential first step, organizations also need to prevent hardcoded secrets from being introduced into their codebase. Integrating scanning directly into developer workflows ensures new code is free from hardcoded secrets that might otherwise lead to a breach, thus significantly reducing an organization's risk.

Cycode has integrated hardcoded secrets scanning directly into developer workflows via pre-commit and pull request scanning. Before every pull or merge request, developers' code is scanned, and any hardcoded secrets are flagged for remediation. Moreover, Cycode can be configured to block a pull or merge request when a secret is detected. This not only helps shield the main branch from exposure to hardcoded secrets, but helps developers break the habit of hardcoding secrets in their code. By scanning early in the SDLC, Cycode prevents the problem from even occurring.



## Reduced Exposure Risk

The real risk of hardcoded secrets lies in their exposure to the outside world. Once uncovered by an attacker, a hardcoded secret could result in serious damage to an organization as it can provide access to other components of the software supply chain. Exposure usually happens through compromised insiders, malicious insiders, and code leakage. Because the risk is so great, implementing complementary security controls that address these areas is one of the best ways to prevent exposure.

Cycode approaches the problem of hardcoded secrets from multiple angles to reduce the chance that hardcoded secrets will result in a damaging breach. This includes security and governance, code leakage detection, and anomaly detection.



### Security and Governance

Cycode implements consistent security policies across all tooling, including strong authentication and least privilege

policies. Together these policies limit attackers' ability to compromise developer accounts and limit access to code such that attackers must compromise the right account, which has access to the code that contains hardcoded secrets.



### Code Leakage Detection

Cycode reduces the risk of a code leak that could expose hardcoded secrets. By fingerprinting proprietary code and

proactively searching public code sharing sites for it, Cycode finds and removes leaked code as soon as possible. This minimizes the chances that a code leak with hardcoded secrets is discovered by hackers.



### Anomaly Detection

Hardcoded secrets exposed to malicious insiders can result in difficult-to-detect breaches. Cycode identifies anomalous

and suspicious user behavior such as excessive cloned repositories, new authentication patterns, and more to detect potentially malicious insiders in any environment.

## Comprehensive Software Supply Chain Security

Cycode helps customers find and fix hardcoded secrets, prevent new hardcoded secrets from being introduced, and reduce the risk of exposure of hardcoded secrets. This multifaceted approach to hardcoded secrets is proven to help organizations reduce the risk of a breach.

While preventing hardcoded secrets is critical, it is only one step in protecting the software supply chain. To truly reduce risk, organizations need a comprehensive solution that covers the entire SDLC. Cycode is the only end-to-end software supply chain (SSC) 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 enable complete visibility and hardened security posture through consistent governance and security policies. 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.

To further reduce the risk of breaches, Cycode provides a series of scanning engines that look for issues that go beyond hardcoded secrets by scanning for IaC misconfigurations, code leaks, and more. Cycode's patented 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.

Protecting against hardcoded secrets is one step in securing the software supply chain. To protect the entire development pipeline, organizations need a complete solution that secures infrastructure at each phase 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](https://www.cycode.com)