

# A Complete Hardcoded Secrets Solution

SOLUTION BRIEF

## Eliminate Existing and Prevent New Hardcoded Secrets

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

With a hardcoded secret, attackers don't need exploit code to gain unauthorized access to applications. Once attackers uncover a username and password, they can easily move laterally across development pipelines or target downstream customers by tampering with code. In addition, the same hardcoded secret is often used across multiple applications. With the elevated privileges granted to most developer accounts, the exposure of a hardcoded secret could be catastrophic.

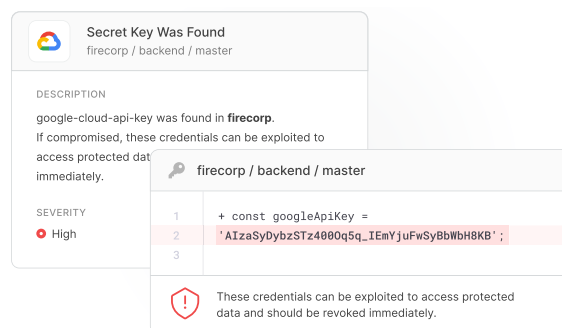
Cycode helps find and fix hardcoded secrets, prevents new hardcoded secrets from being introduced, and reduces the risk of exposure by immediately scanning leaked code for hardcoded secrets.

## Comprehensive Hardcoded Secret Scanning

The challenge when scanning for secrets is that they come in a wide variety of formats—API keys, encryption keys, tokens, passwords, database connection strings, custom secrets, and other high entropy strings. They also live in diverse locations such as source code, build logs,

IaC templates, Kubernetes clusters, version histories, and even Slack channels.

Cycode offers robust, continuous hardcoded secret detection that identifies any type of hardcoded secret anywhere in the SDLC. This includes scanning Source Control Management (SCM) tools; delivery pipelines; public and private repositories; Kubernetes resources; public and shared Slack channels including attachments; and containers stored in container registries like DockerHub, JFrog Artifactory, Amazon ECR, and Google Container Registry. Cycode's hardcoded secrets scanning also leverages multiple detection methods—scenario and pattern matching, high entropy string detection, and more—to provide unmatched detection.



**Secret Key Was Found**  
firecorp / backend / master

**DESCRIPTION**  
google-cloud-api-key was found in **firecorp**. If compromised, these credentials can be exploited to access protected data immediately.

**SEVERITY**  
High

```
1 + const googleApiKey =  
2 'AIzaSyDybzSTz4000q5q_IEmYjuFwSyBbWbH8KB';  
3
```

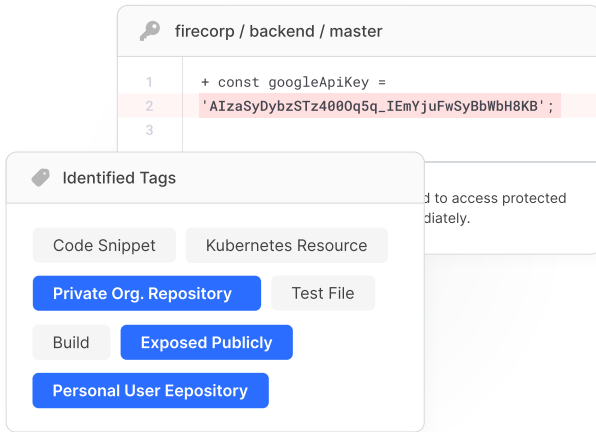
These credentials can be exploited to access protected data and should be revoked immediately.

## Prioritized Remediation

Development teams often have hundreds or thousands of hardcoded secrets across their SDLCs. Cycode helps users assess risk so that the most critical issues are remediated first.

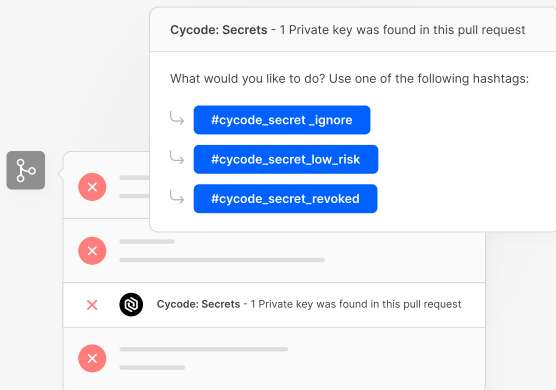
Cycode prioritizes hardcoded secrets based on the type of exposure (publicly or in a private asset) and the location of the secret. Furthermore, when Cycode finds leaked

code, it is immediately scanned for hardcoded secrets.



## Developer Friendly Workflows

Cycode offers a CLI tool and integrates hardcoded secrets scanning into developer workflows via pre-commit and pull request scanning to prevent new hardcoded secrets. Before every pull request, developers' code is scanned, and any hardcoded secrets are flagged for remediation. Moreover, Cycode's policies can block a pull or merge request when a secret is detected. This both helps reduce the risk of exposure of a hardcoded secret and helps developers break the habit of hardcoding secrets. Additionally, Cycode can scan for hardcoded secrets during the build process using the CLI.



## Reduced Exposure Risk

The real risk of hardcoded secrets lies in their exposure to the outside world. An exposed hardcoded secret could damage an organization by providing access

to other components in the software supply chain. Exposure usually happens through compromised insiders, malicious insiders, or code leakage. Cycode approaches the problem of hardcoded secrets using complementary security controls to reduce the likelihood that a hardcoded secret causes a damaging breach.



## Security and Governance

Cycode implements consistent security policies like multifactor authentication and least privilege policies to limit attackers' ability to compromise developer accounts.



## Code Leaks and Secrets

Cycode fingerprints proprietary code and scans public code sharing sites to find and remove leaked code. If a code leak is found, it is immediately scanned for hardcoded secrets.



## Anomaly Detection

Hardcoded secrets exposed to malicious insiders can result in difficult-to-detect breaches. Cycode identifies anomalous user behavior such as excessive cloned repositories or new authentication patterns to detect malicious insiders.

## Comprehensive Software Supply Chain Security

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

To protect against both hardcoded secrets and the entire development pipeline, organizations need a complete solution that secures infrastructure at each phase of the SDLC. Cycode is that solution.

 [Learn more at cycode.com](https://www.cycode.com)