LEGIT

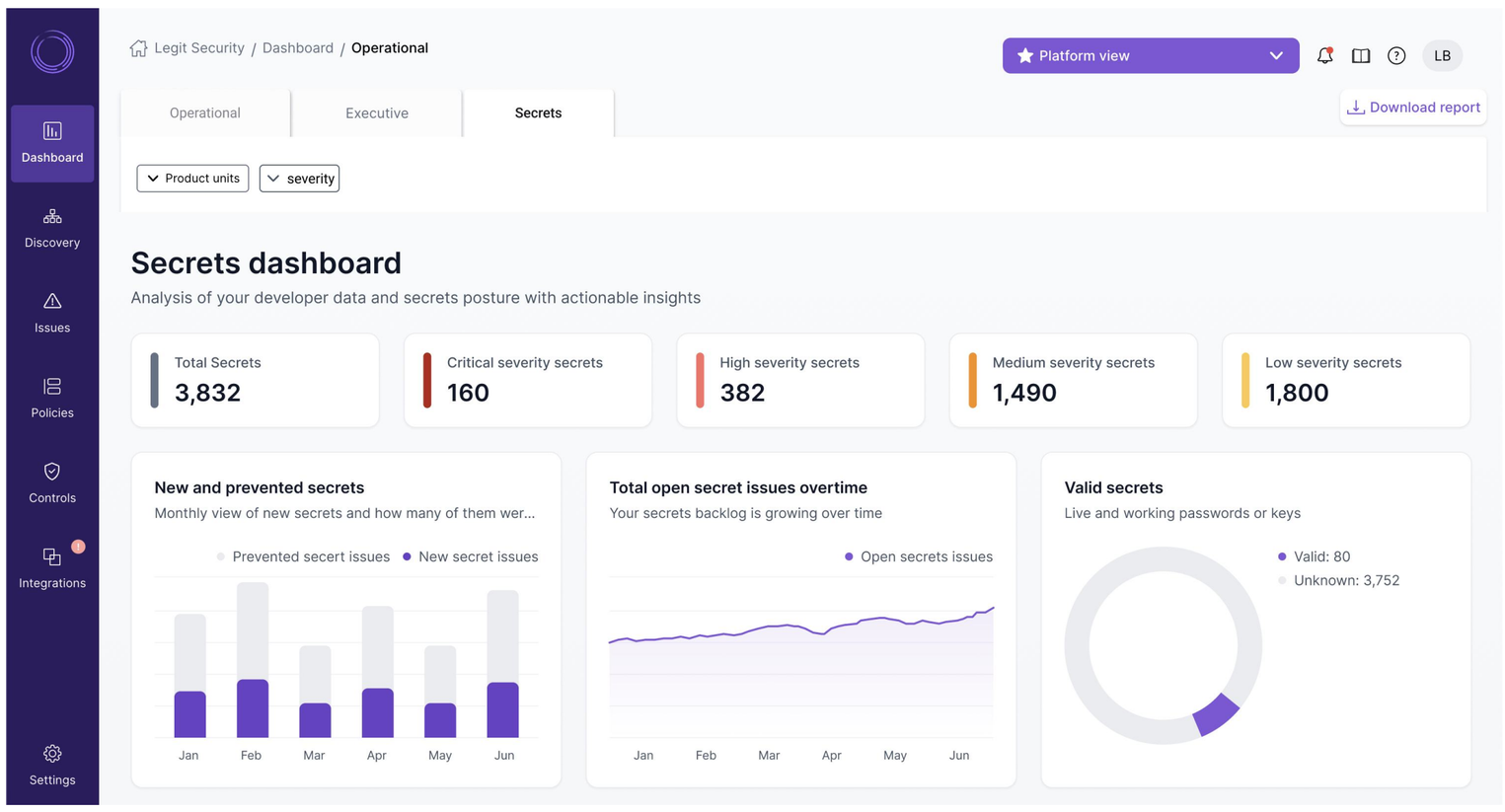
SOLUTION BRIEF

Legit Secrets Detection & Prevention

Find and secure all secrets, not just in source code, with AI-powered, enterprise-grade secrets scanning

Tackle sprawling secrets before attackers do

Secrets are leaking everywhere across developer environments. Sensitive, business-critical secrets – cloud keys, API tokens, configuration files, PII, and more – are routinely hardcoded into source code, stored in logs in plaintext, and reused and reshared across cloud services, productivity tools, and messaging apps. Making matters worse, threat actors are shifting left – just like DevOps – to take advantage of these sprawling secrets estates, and legacy secrets scanners can't keep pace.



Key Features

- 100% SDLC discovery & visibility – beyond source code
- AI-powered accuracy to reduce noise
- Continuous, automated secrets scanning
- Active prevention with pre-built policies & guardrails
- Enterprise scalability & performance
- Context to prioritize remediation
- Centralized management and orchestration

There is a solution – and one that doesn't involve the headaches associated with open-source secrets scanners. To discover and protect secrets wherever they reside – and scale to the largest development environments – Legit delivers AI-powered, enterprise-grade secrets detection and prevention.

Key Challenges in Protecting Secrets

- Secrets are everywhere – well beyond source code
- Secrets open the door to supply chain attacks
- Secrets may live in history and shadow assets forever
- Secrets scanning is burdened with noise and false positives

Find every secret, everywhere

Connect and uncover every secret throughout your developer environment, from source code to Git history to build logs to shared workspaces – and more.

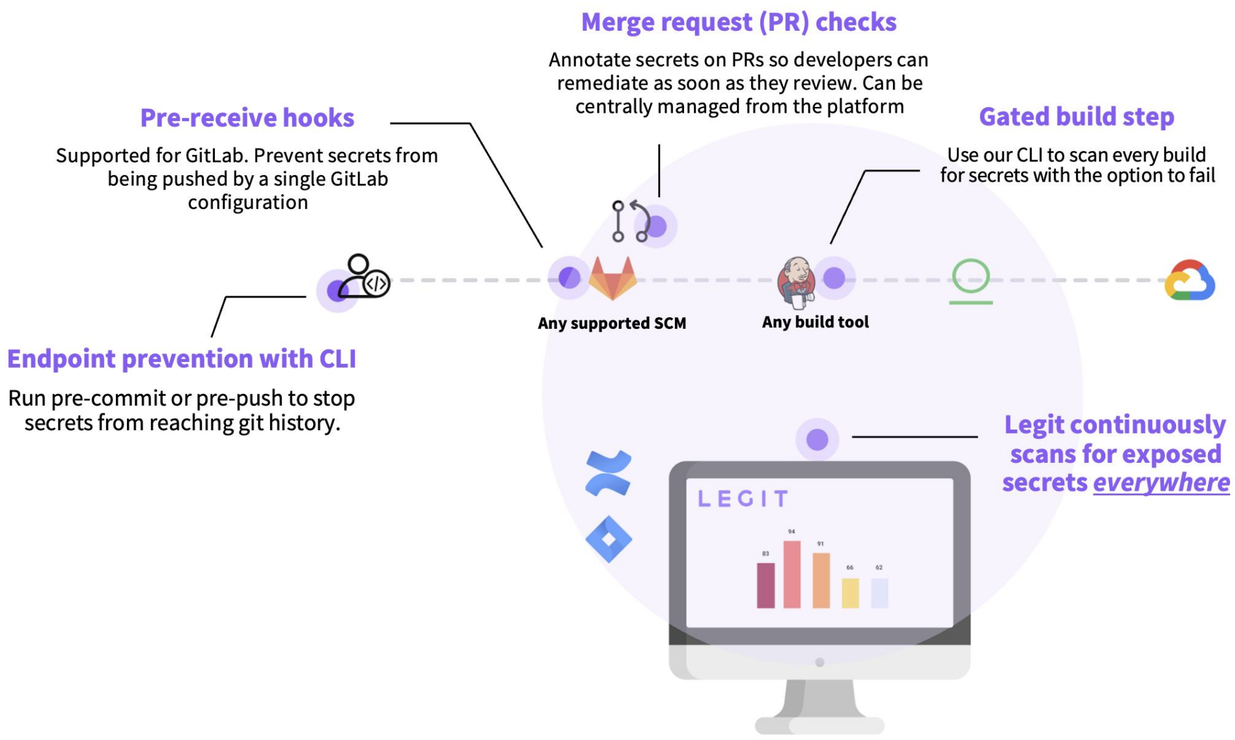
AI-powered accuracy and noise reduction

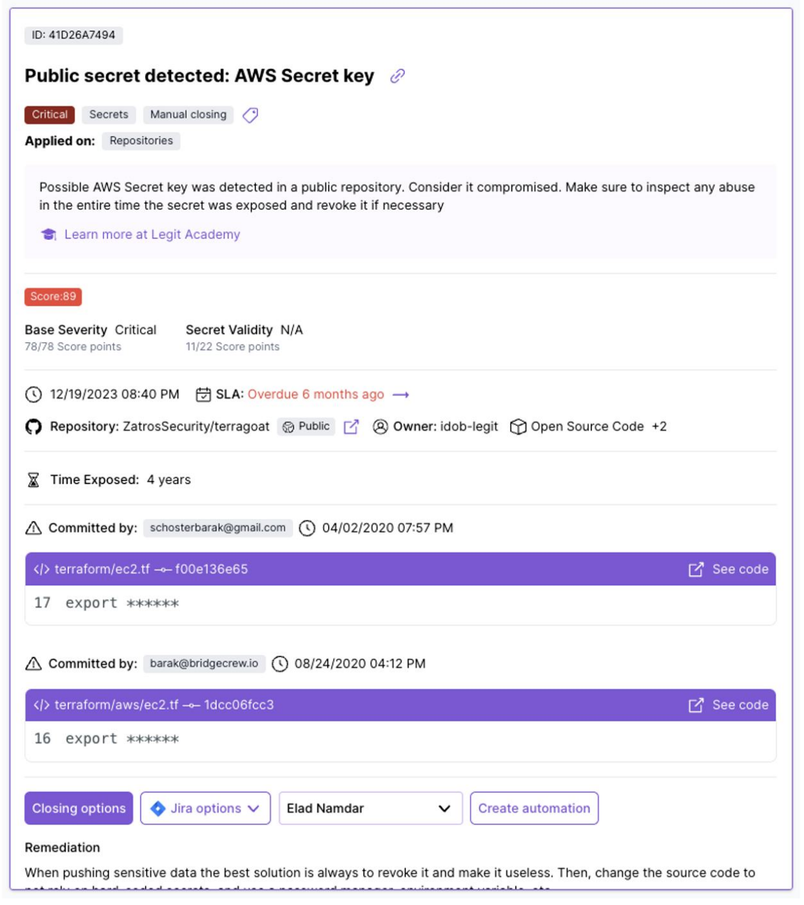
Overcome the noise associated with secrets scanning with AI-powered accuracy to reduce false positives that burn valuable development resources.

Remediate and prevent automatically

Automation and orchestration enable you to immediately fix any existing secrets and enact policies to prevent risk of future secrets.

Legit Next-Gen Secrets Security





Key Capabilities

- **100% SDLC discovery & visibility.** Beyond source code, Legit discovers secrets everywhere – Git history, build logs, shared workspaces (e.g., Confluence, Jira) and more.
- **AI-powered accuracy to reduce noise.** Unlike open-source tools, Legit's AI-powered engine is continually learning to deliver a low rate of missed detections and false positives.
- **Continuous, automated secrets scanning.** Legit continually scans your environment to discover any new secrets, including those in "shadow" assets.
- **Active prevention with pre-built policies & guardrails.** Stop the bleeding with automated guardrails that can actively prevent new secrets from entering the developer environment.
- **Enterprise scalability & performance.** Legit secrets scanning was built to support the largest and most complex development organizations.
- **Context to prioritize remediation.** Legit delivers deep context about secrets, relevant details to prioritize, and recommended remediation to quickly reduce backlogs of detected secrets.
- **Centralized management & orchestration.** Legit enables you to centrally manage secrets discovery and prevention for distributed teams to drive consistent, comprehensive security.

Business Benefits

- **Unearth exposed secrets beyond source code.** Discover developer assets beyond source code to cover your entire environment and protect your data.
- **Follow secrets to their source.** Trace them back to their original source for fast resolution.
- **Slash your MTTR and eliminate false positives.** Stop triaging irrelevant alerts, slash your mean-time-to-remediate (MTTR), and eliminate false positives by 86% with Legit's advanced, AI-powered detection and noise reduction.
- **Rapidly remediate.** Prioritize fixes based on risk to the business and stop wasting your developers' time with low-priority issues.
- **Pre-empt new secrets exposures.** Prevent insecure secrets from leaking and avoid immutable Git history by pre-receiving and pre-pushing your hooks and commits without burdensome controls slowing down dev teams.

Get more details on Legit Secrets Detection & Prevention. Contact us to get more information or Request a demo.

Learn More About Legit Security

Visit our website and Book a Demo

LEGIT

About Legit Security

Legit is a new way to manage your application security posture for security, product, and compliance teams. With Legit, enterprises get a cleaner, easier way to manage and scale application security and address risks from code to cloud. Built for the modern SDLC, Legit tackles the most challenging problems facing security teams, including GenAI usage, proliferation of secrets, and an uncontrolled dev environment. Fast to implement and easy to use, Legit lets security teams protect their software factory from end to end, gives developers guardrails that let them do their best work safely, and delivers metrics that prove the security program's success. This new approach means teams can control risk across the business – and prove it.