LEGIT SECURITY

Request a Demo

SOLUTION BRIEF

Legit Secret Scanning

The push for rapid software innovation and delivery understandably leads to developers taking shortcuts to meet their objectives, which often includes using secrets in code, including privileged credentials, passwords, access tokens, API keys, PII, and more to expedite testing and delivery. But the risk of those secrets being exposed leaves the organization open to breaches, compliance violations, and other threats.

12

live secrets, on average, are submitted per 100 code repositories every week.

The Unique Challenge of Secrets

Secrets in code and other developer assets are not only a critical security risk, they're also challenging to find and remediate.

Secrets are prolific

As many as 12 secrets are submitted for every 100 code repositories every week, potentially leading to 100s of thousands of secrets in a typical SDLC.

Secrets are pervasive

Once a secret is entered into code it's typically downloaded to every developer endpoint, leading to thousands of copies.

Secrets are persistent

Secrets entered into the Git history or build artifacts stay there indefinitely and most developers are unaware of their presence, with secrets building up for years.

Legit Security Secret Scanning

Legit Secret Scanning integrates with your existing SDLC infrastructure and delivers automated discovery and scanning across all development assets and history, returning critical results within minutes of deployment. The platform not only scans for secrets like credentials, passwords, and API Keys, it also can scan for PII and other confidential data like credit cards and social security numbers. Legit Secret Scanning includes:

- Automated discovery in minutes
- Continuously learning engine
- Easy-to-use interface
- Centralized management
- API integration to existing tools
- Broader detection across the SDLC
- Deeper context for faster remediation
- Enterprise speed and scalability
- Detailed reporting for compliance
- Automated preventative guardrails

The Legit Difference

Best-in-class secrets scanning

Unlike open-source tools, Legit has a continually learning engine with a low rate of missed detections to find all secrets in your SDLC, while the platform delivers extensive context and prioritization capabilities to limit the impact of false positives.

Visibility and coverage

Legit discovers and scans developer assets beyond source code to cover your entire environment and protect your data. It delivers holistic visibility into where secrets exist, the scope of the problem, missing coverage, and remediation progress over time.

Better for remediation

Legit delivers deep context about secrets in your code, relevant details to prioritize, and recommended remediation steps. We can help quickly reduce enormous backlogs of detected secrets using superior alert and ticking management.

Enterprise scalability and performance

Legit uses low level optimization techniques to meet scaling requirements of the largest organizations, with the ability to scan thousands of repositories within minutes of deployment.

Risk correlation

Legit can correlate your secrets risk with your SDLC attack surface and help you respond faster to exposure incidents or prioritize smarter your remediation efforts.

According to IBM's 2023 Data Breach Report, compromised credentials is one of the two most common initial attack vectors, with an average cost of USD 4.62 million. Additionally, these breaches took the longest to resolve. It took an average of 328 days (nearly 11 months) to identify and contain data breaches resulting from stolen or compromised credentials.

Legit Secret Scanning in Action

Stop the bleeding and clear your secrets backlog faster.

Challenge

Organizations may have tens of thousands of secrets embedded throughout their SDLC, with more being added on a daily or weekly basis, creating an ever-expanding attack surface and continually falling farther behind.

Legit Solution

Legit allows you to quickly build automated security guardrails that can dynamically detect when attempts are made new secrets are entered into the SDLC and prevent them from being submitted.

Additional Benefit

Legit's platform gives you the context necessary to understand, prioritize and remediate your backlog faster, with the tracking you need to understand and demonstrate your application security posture over time.

Eliminate your security and compliance blind spots

Challenge

Traditional processes for identifying secrets in the SDLC are limited in scope, lack the right tools, or depend on inefficient, manual processes, leading to missed detections and failed audits.

Legit Solution

Legit scans beyond the source code, looking at artifacts, build logs and other attack surfaces, using a constantly learning detection engine to ensure that secrets don't go undetected.

Additional Benefit

Legit uses deeper context and flexible policy customization to establish an accurate baseline, and leverages better alert/ticket management to deliver faster triage and remediation capabilities.

Replace open-source, home grown, or point products with a best-in-class enterprise-grade solution

Challenge

Open-source and/or partially implemented point solutions are ineffective at consistently detecting secrets across the entire SDLC, leading to missed detections, poor visibility and creating unnecessary operational overhead.

Solution

Legit detects more secrets across a greater area of the developer environment, protecting against missed detections, delivering better visibility across the entire SDLC, and lowering operating overhead.

Additional Benefit

Legit's enterprise capabilities include the ability to correlate secrets in the developer environment with additional SDLC risk to more accurately understand their potential impact and prioritize remediation.

Learn More About Legit Security

Visit our website and Request a Demo

LEGIT SECURITY

About Legit Security

Legit Security provides application security posture management platform that secures application delivery from code to cloud and protects an organization's software supply chain from attacks. The platform's unified application security control plane and automated SDLC discovery and analysis capabilities provide visibility and security control over rapidly changing environments and prioritize security issues based on context and business criticality to improve security team efficiency and effectiveness.