LEGIT

SOLUTION BRIEF

Legit Platform Overview

ASPM and Secrets Detection & Prevention

A comprehensive platform to protect your most critical assets: applications and the software factories that produce them

Building a sustainable, scalable AppSec program

Application security is a long-standing challenge, but detecting vulnerabilities is not the problem. The real obstacle lies in operationalizing results to understand where business risk is the greatest, speeding remediation of high-priority issues, and preventing future risks.

In addition, CISOs and their teams need evidence to demonstrate success of their AppSec programs to the Board, customers, and partners. And, they need to ensure policies are monitored and enforced across disparate development teams.

Legit Platform

- Application Security Posture Management (ASPM)
- Secrets Detection & Prevention

Key Features

- Automate AppSec risk prioritization & remediation
- Get a real-time view of your software factory, applications & risk
- Leverage AI-powered secrets detection & prevention
- Use control mapping and custom frameworks to assess and report
- Implement secure-by-design developer guardrails
- Grow with enterprise scalability and performance
- Benefit from centralized management and orchestration

Operationalizing AppSec

Getting ahead of these challenges starts with new thinking that centers on building an AppSec program rather than simply adding more point tools. To operationalize an AppSec program, CISOs and their teams must have:

- **Complete visibility into assets and risk:** a complete view of applications developed, vulnerabilities that exist, and all assets and risk within the software factory.
- **Consistent policy enforcement:** guardrails and policies to ensure application security is applied as intended across complex, diverse development teams.
- **Security that doesn't slow delivery:** consistent policies, reduced noise from security tools, and automated workflows for remediation make it faster to make the fixes required.

Protect your dev environment & apps from end to end

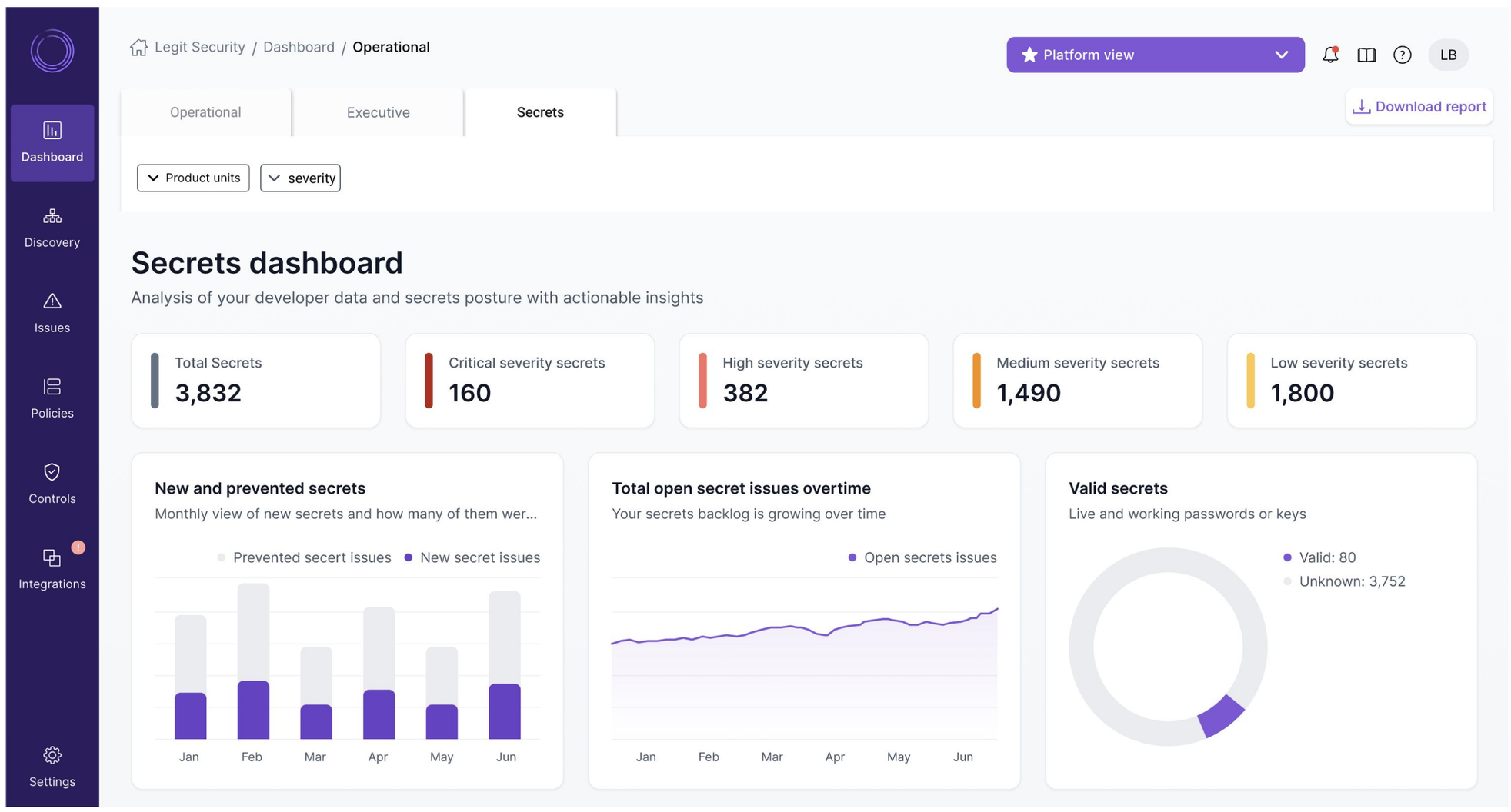
Stop worrying about what you're missing – from GenAI code to secrets – and understand the holistic risk across your entire software factory and attack surface. Make sense of findings from multiple AppSec tools to confidently prioritize and fix highest-risk issues fast.

Automate security & remediation for your CI/CD pipelines

Implement in no time to lighten the load on your security teams by consolidating findings from multiple tools and setting boundaries that let developers work their own way safely. Create processes that engage developers to get cleaner code the first time and use complete context to prioritize fixes.

Prove the success of your security program

Test your policies, ensure they're being enforced, and show the value of your hard work. Collaborate and hold everyone accountable with data. Use metrics to communicate more clearly about risk and progress with developers, product teams, and executives.



Benefits With Legit

With the Legit ASPM and Secrets Detection & Prevention platform at the core of your application security program, you'll be able to:

- **Reduce business risk** by fully protecting both the applications and the development environment that accelerate growth.
- **Improve operational efficiency and reduce noise** by aligning security and development around remediation of issues creating the greatest business risk.
- **Streamline compliance** by making it easy to provide real-time evidence to auditors – without painful manual work.

Legit is the leader in mitigating application business risk by providing visibility and protection for both the entire software factory and the applications it produces. Legit shows a unified risk posture across code, cloud, and the software factory infrastructure by combining all data into a clear and actionable view and providing the tools to remediate risk.

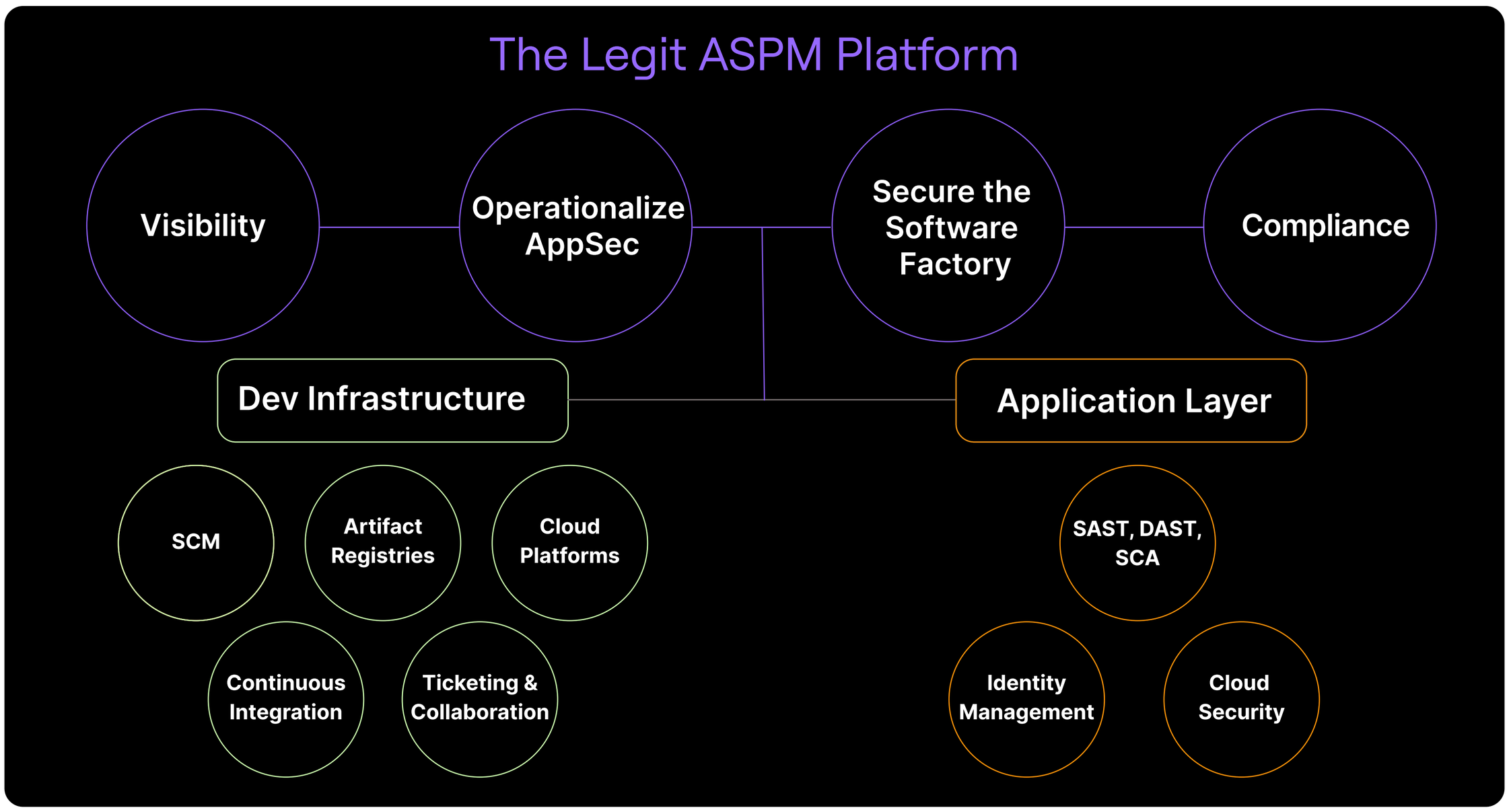
Legit's unmatched ability to discover and visualize the entire software factory attack surface, including secrets; correlate and streamline AppSec vulnerability data from siloed scanning tools; accelerate prioritized remediation; and support compliance make us the legit foundation of AppSec programs.

Mission

Our mission is to instill full confidence in the security of the applications our customers build and rely on to drive business growth.

Vision

Our vision is a world where building secure software is simple and assured.



Key Capabilities of the Legit Platform

Visibility

Do you have complete and real-time visibility of your software factory and application attack surface?

- **Get a real-time view:** benefit from an automated view of the entire software factory and apps, including shadow assets.
- **Identify supply chain risk:** visualize tools and dependencies that create security concerns.
- **Manage GenAI usage:** pinpoint when, where, and how developers are using GenAI and code assistants.

Secure the Software Factory

Can you ensure your complete development environment is always secure?

- **Secrets detection & prevention:** identify and remediate secrets exposure everywhere it exists; prevent future exposure.
- **SDLC visibility:** discover and visualize all aspects of your software factory, including assets, dependencies, misconfigurations, and shadow IT.
- **Supply chain security:** shore up security gaps that provide gateways for attackers to breach an app and damage downstream partners.

Operational AppSec

Can you secure your entire SDLC – from code to cloud to infrastructure, enact guardrails, and enforce policy?

- **Automate risk prioritization:** correlate, dedupe, and prioritize vulnerabilities across the SDLC; automate triage and remediation.
- **Reduce noise:** apply AI to reduce false positives and eliminate noise.
- **Orchestrate remediation:** integrate with developer tools and workflows to streamline remediation.

Compliance

Do you have metrics & evidence to prove the success of your security program?

- **Control mapping:** align your AppSec program with regulations and standards, such as PCI DSS, CISA, ISO 27001, and SSDF, among others.
- **Custom frameworks:** combine regulations and standards with your own policies to create custom frameworks and assess current AppSec posture.
- **Automated monitoring:** continuously monitor for non-compliance, and deliver metrics and evidence.

Get more details on ASPM and 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.