SOLUTION BRIEF

Strengthening AppSec with Dedicated Secrets Security

Exposed secrets such as API keys, tokens, credentials, and certificates that grant direct access to critical systems have become a primary attack vector for data breaches. Organizations have a critical responsibility to prevent these highly sensitive assets from being inadvertently exposed or misused within their software development lifecycle.

Traditional AppSec tools, while crucial for identifying vulnerabilities in custom code and dependencies, often lack the necessary capabilities to proactively identify and address these risks. Integrating the detection and remediation of secrets into comprehensive AppSec strategies, prevents these high risk credentials from entering your codebase, protecting the entire software supply chain from critical blind spots.

Comprehensive, platform agnostic supply chain defense

Combining Mend.io with GitGuardian delivers a comprehensive, platform-agnostic security solution for modern software supply chains. This joint solution protects against vulnerabilities in open-source components, custom code, containers, emerging AI components, including hardcoded credentials and exposed secrets found across each of these layers, regardless of your chosen platform.

Joint solution advantages

Prevent breaches with precision secret detection. GitGuardian provides 482 specialized detectors with unmatched accuracy for comprehensive secrets detection, dramatically reducing false positives.

Universal security across the SDLC. Works across all major SCMs and poly-repo environments, eliminating vendor lock-in and providing unified security wherever your code lives.

Comprehensive coverage for modern threats. Mend.io provides deep SAST and SCA scanning with actionable reachability analysis, to prioritize exploitable vulnerabilities. We also offer container security and pioneering AI component security.

Strategic investment for holistic protection. Fill vital security gaps and maximize ROI. A comprehensive and future proof security posture strategy that tackles open source, custom code, container, AI specific threats, and especially exposed credentials..

Outmatching competitors' supply chain protection

Together, Mend.io and GitGuardian effectively secure the modern software supply chain against evolving threats. Their combined strength delivers specialized, deep coverage for supply chain risks, particularly in secrets detection and remediation, along with platform-agnostic flexibility that offerings like GitHub Advanced Security can't match.

Mend.io + GitGuardian vs. GitHub Advanced Security

	Mend.io & GitGuardian	GHAS
Specialized Secrets Detection	482+ specialized detectors, fewer false positives, deep remediation.	General scanning, more false positives, less specialized remediation.
Incident Management & Remediation Features	Grouping, timelines, automated scoring & remediation, automated playbooks, deep secrets manager integration, and robust feedback.	Lacks advanced incident management, prioritization, automated remediation workflows. Limited integration vaults.
Platform Agnostic & Poly-Repo Support	All major SCMs and poly-repo environments, no vendor locking.	Limited to GitHub; lacks diverse SCM support.
Comprehensive Security Layers	Optimized SCA & SAST with Reachability analysis, automated fixes. Dedicated Container Security with Kubernetes scanning, in-container secret detection. Pioneering AI security with coverage for both AI components and AI behavioral risks	Standard and less efficient SCA & SAST Limited Container Security: Dependency scanning, relies on 3rd parties. AI for scanning only. No dedicated AI model security.
Reduce Risk & Improved Efficiency	Covers open-source, custom code, Containers, AI, and exposed credentials. Lower false positives, automated workflows.	Limited to GitHub; lacks diverse SCM support.

Visit us online!

Mend.io

GitGuardian.com

Mend.io