GitGuardian Launches Comprehensive Non-Human Identities Security Strategy

By bringing order to fragmented secrets ecosystems, GitGuardian secures the lifecycles of Non-Human Identities across environments.

PARIS, FRANCE, December 10, 2024 /EINPresswire.com/ -- GitGuardian, the end-to-end Non-Human Identity (NHI) security platform for enterprises, has unveiled its NHI Security strategy, a transformative approach to securing the explosive growth of NHIs and the secrets they depend on. At the core of this strategy is GitGuardian NHI Governance, a solution designed to provide comprehensive visibility and control over the lifecycle of NHIs and their tied secrets. Building on GitGuardian's long-standing leadership in secrets security, this strategy marks a significant leap forward with the launch of integrations across five leading secrets management platforms: HashiCorp Vault, CyberArk Conjur, AWS Secrets Manager, Google Cloud Secrets Manager, and Azure Key Vault.

With Non-Human Identities outnumbering human ones by 50 to 1, enterprises face an unprecedented challenge in securing the rapid expansion of NHIs and their associated secrets—API keys, credentials, access tokens, and more. These secrets are often scattered across codebases, CI/CD pipelines, and productivity tools, creating security blind spots and operational inefficiencies. GitGuardian is responding with an innovative NHI Security strategy explicitly designed to tackle this growing risk.

"Secrets and non-human Identities are now the backbone of modern digital infrastructures, but securing them has become a nightmare for enterprises," said Eric Fourrier, CEO of GitGuardian. "Through our NHI Security strategy, we're urging enterprises to step up and regain control of their secrets. We're giving them a clear, actionable path forward: a way to discover and secure their NHIs at scale while reducing risk and complexity."
The Vision Behind GitGuardian NHI Governance
GitGuardian NHI Governance introduces a comprehensive framework to address these challenges head-on. By unifying governance across platforms and automating key processes, the strategy is designed to provide organizations with:

 Complete Visibility: Centralized tracking of where secrets are stored, how they are used, their permissions, and which NHIs they are associated with.
 Proactive Posture Management: Detection of stale, overprivileged, or compromised secrets, with prioritized workflows for remediation.

- Lifecycle Automation: Seamless enforcement of security policies, from onboarding to secrets rotation, ensuring consistent best practices across teams.

Looking beyond tools and integrations, GitGuardian NHI Governance is designed to establish a vision for long-term resilience. "Our commitment is to empower security and development teams with actionable insights, robust governance, and scalable solutions. This new NHI Governance module is a natural extension of our deep expertise in secrets security. It not only helps organizations remediate leaked secrets but also strengthens overall NHI management and hygiene," said Eric Fourrier.

Tackling Vault Sprawl with Multi-Vault Integrations

Secrets managers are critical to secrets security, providing centralized storage, automated rotation, and access control. However, enterprises suffer from vault sprawl—the use of multiple secrets managers across teams—which often leads to fragmented secrets management and introduces blind spots.

As a foundational component of its NHI Security strategy, GitGuardian has launched integrations with the industry's leading vaults HashiCorp Vault, CyberArk Conjur, AWS Secrets Manager, Google Cloud Secrets Manager, and Azure Key Vault.

These integrations tackle enterprises' challenges of secrets management while complementing existing vault functionalities:

1. Unified Secrets Visibility: Create a comprehensive inventory of secrets stored across multiple vaults, providing teams with a centralized view for managing and auditing secrets.
2. Vault Sprawl Mitigation: Address inefficiencies caused by using multiple secrets management tools by consolidating and streamlining vault operations.
3. Cross-Vault Incident Resolution: Link secret incidents directly to the affected vault entries, allowing quicker and more accurate remediation.
4. Secrets Lifecycle Auditing: Automate the identification of stale, compromised, or overprivileged secrets to prioritize security risks and enforce rotation policies.
5. Efficient Vault Migrations: Simplify the migration of secrets to preferred vaults, eliminate underused systems to reduce redundancies, purge outdated secrets, and cut costs.
6. Streamlined Onboarding and Policy Enforcement: Standardize secrets management practices across teams by integrating GitGuardian's Governance with existing vault policies.

"While vaults play a key role in secrets management, they aren't sufficient to address the full spectrum of secrets security challenges," added Eric Fourrier. "Our integrations take those platforms to the next level, ensuring enterprises can centralize their secrets management, reduce risks, and save on operational costs."

Looking Ahead

GitGuardian continuously enhances its offerings to help enterprises secure NHIs and their secrets at scale, and stay ahead of emerging threats. Future developments will include advanced automation, advanced NHI hygiene analytics, and enhanced incident response tools, further solidifying GitGuardian's position as a leader in NHI security.

GitGuardian's multi-vault integrations are available now. To learn more about how GitGuardian is redefining NHI and secrets security, visit GitGuardian's website or contact the sales team.

Additional resources
GitGuardian - NHI Security solution page - https://www.gitguardian.com/nhi-security
GitGuardian - NHI Security strategy announcement blog post - http://blog.gitguardian.com/nhi-security/
GitGuardian - Multi-vault integrations launch blog post - http://blog.gitguardian.com/secrets-managers-integrations/

About GitGuardian
GitGuardian is the end-to-end NHI Security leader. GitGuardian helps organizations take control of their NHI security by discovering all their secrets, prioritizing and remediating leaks at scale, protecting non-human identities, and reducing breach exposure.
Widely adopted by developer communities, GitGuardian is used by over 600 thousand developers and leading companies, including Snowflake, Orange, Iress, Mirantis, Maven Wave, ING, BASF, and Bouygues Telecom. To learn more about GitGuardian, visit https://www.gitguardian.com.

Holly Hagerman
Connect Marketing
+1 801-373-7888
email us here
