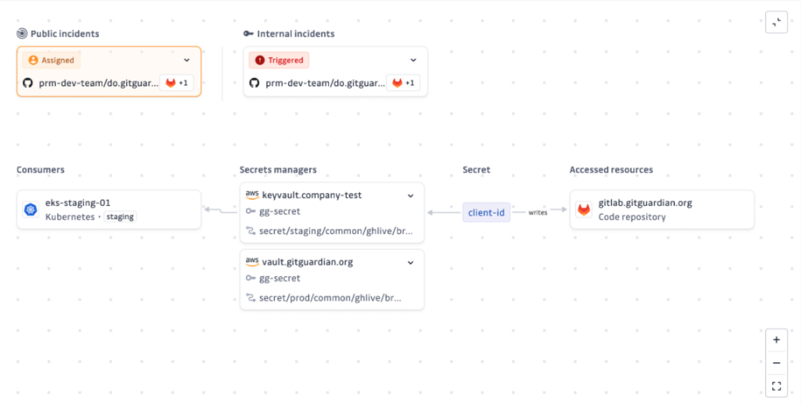
EINPRESSWIRE

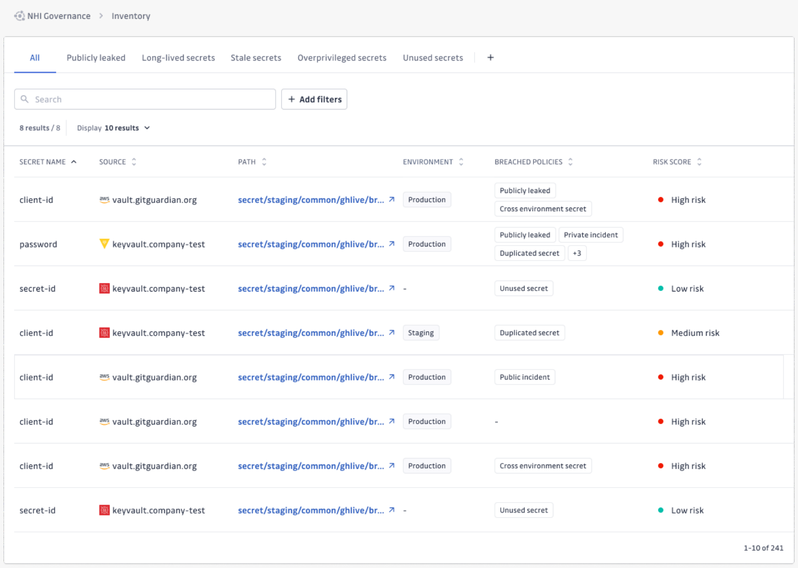
GitGuardian Launches NHI Governance: Bringing Order to the Chaos of Non-Human Identity Security

NHI Governance delivers unified visibility and control over secrets in complex environments, addressing critical security gaps

BOSTON, MA, UNITED STATES, April 15, 2025 /EINPresswire.com/ -- GitGuardian, the leader in secrets security, today announced the launch of NHI Governance. This innovative new product addresses the most critical blind spot in modern cybersecurity: the security and management of Non-Human Identities (NHIs) and their associated secrets. In a landscape where AI agents, no-code automation, and machine-driven tasks rapidly expand, organizations face an explosion of NHIs—now outnumbering human users 100 to 1—creating a vast and increasingly targeted attack surface.



GitGuardian NHI Governance



SECRET NAME	SOURCE	PATH	ENVIRONMENT	BREACHED POLICIES	RISK SCORE
client-id	vault.gitguardian.org	secret/staging/common/ghlive/br... ↗	Production	Publicly leaked Cross environment secret	● High risk
password	keyvault.company-test	secret/staging/common/ghlive/br... ↗	Production	Publicly leaked Private incident Duplicated secret +3	● High risk
secret-id	keyvault.company-test	secret/staging/common/ghlive/br... ↗	-	Unused secret	● Low risk
client-id	keyvault.company-test	secret/staging/common/ghlive/br... ↗	Staging	Duplicated secret	● Medium risk
client-id	vault.gitguardian.org	secret/staging/common/ghlive/br... ↗	Production	Public incident	● High risk
client-id	vault.gitguardian.org	secret/staging/common/ghlive/br... ↗	Production	-	● High risk
client-id	vault.gitguardian.org	secret/staging/common/ghlive/br... ↗	Production	Cross environment secret	● High risk
secret-id	keyvault.company-test	secret/staging/common/ghlive/br... ↗	-	Unused secret	● Low risk

GitGuardian NHI Governance inventory

"The surge of non-human identities driven by automation, APIs, and cloud-native architectures is redefining enterprise security priorities," said Katie Norton, Research Manager, DevSecOps and Software Supply Chain Security at IDC. "Fragmented secrets management is leaving organizations vulnerable to credential-based attacks that exploit inconsistencies and gaps across tools and environments. IDC research found that nearly one in five organizations experienced a software supply chain attack in 2024, underscoring the urgent need for more unified and scalable approaches to securing non-human access."

With NHI Governance, GitGuardian extends its proven expertise in secrets security to provide enterprises a comprehensive solution for addressing the identity and access management challenges that security and IAM teams increasingly face.

Moreover, Don Tait, Senior Analyst from Omdia, says, "With more and more business processes being automated by generative AI (GenAI) and utilizing AI agents, NHI growth is likely to accelerate and further increase the threat landscape. It is important to recognize NHI as a vital link in the cybersecurity threat chain.”

Solving the "Vault Sprawl" Crisis

Security professionals have long struggled with fragmented secrets management, commonly known as "vault sprawl," where critical credentials become scattered across multiple, often disparate secrets management platforms. With the average enterprise maintaining 5+ distinct secrets managers, this fragmentation — compounded by poor developer practices like provisioning overprivileged and long-lived secrets, creates security silos and operational complexity. Organizations cannot effectively track, secure, and enforce policies consistently, significantly increasing breach risk.

GitGuardian NHI Governance solves these challenges with a discovery-first approach that automates visibility across the entire tech stack:

- Unified secrets inventory – Provides a single source of truth for all non-human identities and secrets, eliminating silos and enabling real-time tracking across all integrated vaults and other sources.
- Cross-vault integration – Connects with major secrets managers like HashiCorp Vault, CyberArk Conjur, AWS Secrets Manager, Google Cloud Secrets Manager, Azure Key Vault, Akeyless, and Delinea, ensuring full visibility across fragmented vault environments.
- Consistent policy enforcement – Enables uniform security policies across all vaults, reducing inconsistencies caused by different teams managing secrets with varying security standards.
- Cross-vault incident resolution – Links security incidents directly to relevant vault entries, eliminating the need for manual investigation across disparate systems and accelerating incident response.
- Vault migration assistance – Facilitates secure consolidation of secrets by detecting duplicate, orphaned, or stale credentials, optimizing their storage, and streamlining migrations to fewer, more secure vaults.
- Enhanced context for vaulted secrets – Leverages vault metadata to provide deep insights into secret paths, lease durations, and access permissions, aiding in risk prioritization.

Creating Enterprise-Wide Secrets Governance

Unlike competitors who rely on manual integrations and lack full visibility into secrets, GitGuardian's approach provides a more complete and scalable solution. NHI Governance goes beyond traditional solutions that merely detect secrets by providing full lifecycle management, ensuring NHIs and their secrets are:

- Created securely with least-privilege principles
- Monitored continuously for suspicious access patterns
- Rotated according to compliance requirements
- Revoked immediately when compromised or no longer needed

This end-to-end approach helps organizations enforce zero trust principles, eliminate long-lived credentials, and prevent overprivileged access, addressing the exact tactics used in recent high-profile supply chain attacks.

"Without proper governance of Non-Human Identities, organizations are flying blind when it comes to managing their most privileged access points," added Eric Fourrier. "GitGuardian brings structure and security to this previously chaotic space, giving security leaders the tools to implement consistent policies, automate critical security processes, and significantly reduce their attack surface. We are uniquely positioned to address secrets sprawl at its root, offering a solution that bridges the gap between secrets discovery, management, and identity governance."

Key Benefits of NHI Governance:

- Centralized secrets inventory – Complete visibility and control over all NHI secrets across cloud and on-premises environments.
- Automated lifecycle management – Streamline the entire lifecycle of NHI secrets, from creation to rotation and revocation.
- Actionable context & insights – Map NHIs to their associated secrets, permissions, and usage patterns, identifying excessive privileges and potential attack paths.
- Improved security posture – Identify policy breaks and bad practices such as overprivileged NHIs or long-lived secrets, reducing your overall attack surface.
- Streamlined incident remediation – Accelerate remediation of compromised secrets by integrating directly with secrets managers.

Leading the Future of NHI Security

With attackers increasingly targeting NHIs as their primary entry point, organizations need more than just detection—they need complete security and lifecycle management. GitGuardian is leading this evolution, providing a comprehensive NHI Security platform that integrates both Secrets Security and NHI Governance to protect the most critical access points in modern infrastructure.

Availability

GitGuardian NHI Governance is generally available. Security and IAM leaders can request a personalized walkthrough at www.gitguardian.com/nhi-governance.

About GitGuardian

GitGuardian is an end-to-end NHI Security platform that empowers software-driven organizations to secure their Non-Human Identities (NHIs) and comply with industry standards. With attackers increasingly targeting NHIs, such as service accounts and applications, GitGuardian integrates Secrets Security and NHI Governance. This dual approach enables the detection of compromised secrets across your dev environments while also managing non-human identities and their secrets' lifecycles. The platform is the world's most installed GitHub application and supports over 450+ types of secrets, offers public monitoring for leaked data, and deploys honeytokens for added defense. Trusted by over 600,000 developers, GitGuardian is the choice of leading organizations like Snowflake, ING, BASF, and Bouygues Telecom for robust secrets protection.

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