Delinea | **GitGuardian**

GitGuardian & Delinea end credential sprawl and compliance gaps with automated NHI lifecycle management

The Challenge

Non-Human Identities (NHIs) come in many different forms. When these identities are not disabled or reassigned after they're no longer needed, they pose significant security and compliance risks. According to Delinea Labs' cybersecurity report, there are currently **46 NHIs for every human identity**. These identities may retain elevated privileges, making them attractive targets for attackers seeking unauthorized access.

Without regular monitoring and timely deactivation, these accounts create blind spots in audit trails and compliance reporting. According to OWASP Non-Human Identities report, **51% of organizations have no formal process to offboard or revoke** long lived API keys. This lack of visibility increases the risk of data breaches, regulatory non-compliance, and insider misuse, particularly if credentials are exposed across your organization (i.e., code repositories, misconfigured systems).

The Solution

The integration of GitGuardian with Secret Server on Delinea Platform allows for the retrieval of rich metadata about each secret, such as creation and rotation timestamps, vault path, associated services or repositories, and number of exposures in code or config files. GitGuardian can then apply heuristics and signals to these secrets and flag ones that are considered high-risk.

Once an identity is flagged as high-risk, depending on the secret's context and type, the IT Admin in Secret Server can rotate, disable, archive, or erase the identity. Once remediation steps are taken, the old identity no longer poses a risk. GitGuardian can then validate and confirm the actions taken with continuous monitoring.

Together, GitGuardian and Delinea empower organizations to gain end-to-end protection against secrets sprawl and credential exposure. This integration reduces the risk of breaches,streamlines compliance, governance, and operational efficiency. In tandem, Gitguardian and Delinea enable organizations to take control of their NHI protection policies through an automated, secure, and compliant approach.

Key Integration Benefits

✔ **NHI Discovery**
Scan codebases, infrastructure, and secrets managers to detect NHIs that are stagnant, over permissioned, or orphaned.

✔ **Prioritized Remediation**
Rotate, disable, or archive, high-risk secrets to ensure timely and policy-driven cleanup without maneuvering between platforms.

✔ **Continuous Monitoring**
Monitor active and dormant secrets with Secret Server, so new NHIs or exposure events are detected in near real-time, reducing the risk for exploitation.

✔ **Audit and Compliance**
Log all detection, remediation, and lifecycle actions in Secret Server's audit trail, preserving historical records for compliance frameworks, while ensuring even disabled or archived secrets remain traceable for future audits.

Click here to learn how Delinea and GitGuardian address the challenges of NHIs in our joint blog post.

Delinea + GitGuardian
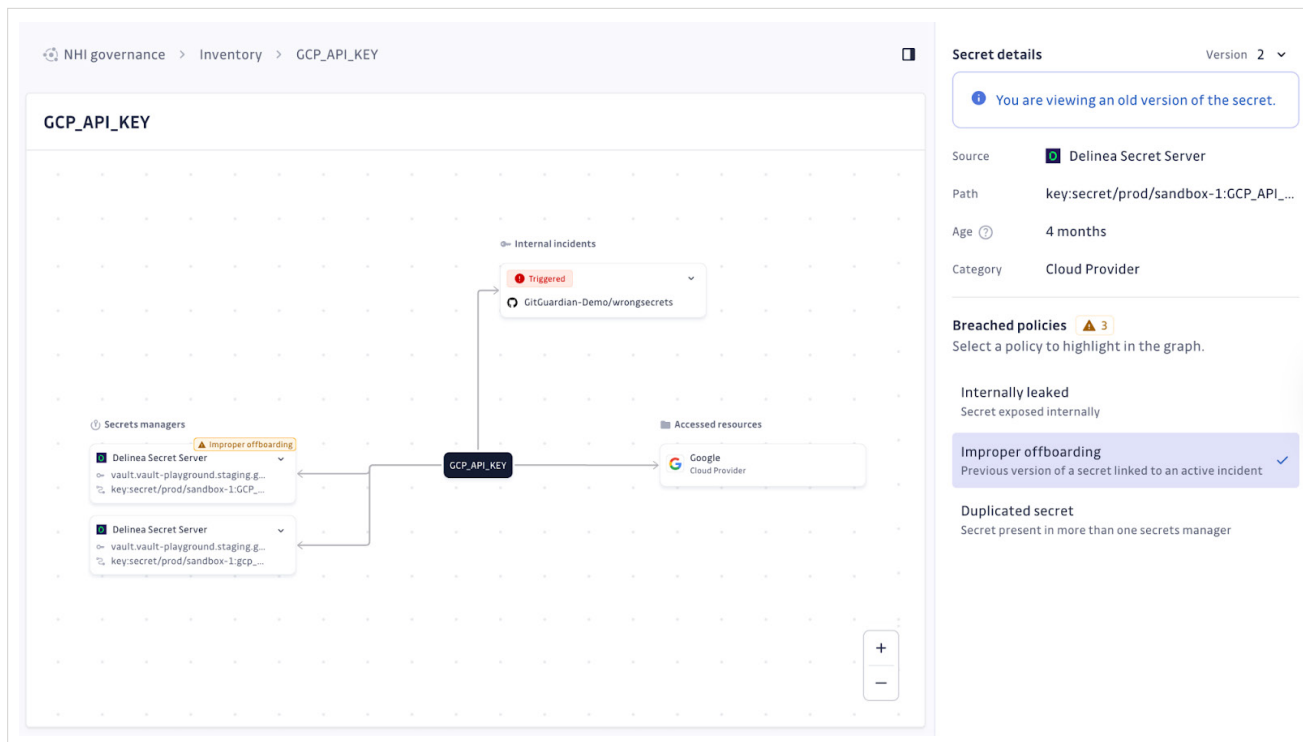
Delinea

Delinea is a pioneer in securing human and machine identities through intelligent, centralized authorization, empowering organizations to seamlessly govern their interactions across the modern enterprise. Leveraging AI-powered intelligence, Delinea's leading cloud-native Identity Security Platform applies context throughout the entire identity lifecycle – across cloud and traditional infrastructure, data, SaaS applications, and AI. It is the only platform that enables you to discover all identities – including workforce, IT administrator, developers, and machines – assign appropriate access levels, detect irregularities, and respond to threats in real-time. With deployment in weeks, not months, 90% fewer resources to manage than the nearest competitor, and a 99.995% uptime, Delinea delivers robust security and operational efficiency without compromise. Learn more about Delinea on **Delinea.com**, **LinkedIn**, **X**, and **YouTube**.

GitGuardian

GitGuardian is an end-to-end NHI and Secrets Security platform that empowers software-driven organizations to secure their Non-Human Identities (NHIs) and comply with industry standards. With attackers are 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 500+ 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. Learn more about GitGuardian at **gitguardian.com**.