GitGuardian

Protecting Non-Human Identities (NHIs) and Secrets: Your Path to Regulatory Compliance

Non-Human Identities (NHIs)—such as service accounts, APIs, and machine credentials—are integral to modern IT operations. However, their increasing number and often broad access privileges introduce significant security challenges.

If compromised, these powerful identities can provide malicious actors with unfettered access to sensitive data, critical systems, and even the ability to escalate privileges and move laterally within the network. The potential for significant data breaches, operational disruptions, and severe financial and reputational damage dramatically increases with each unmanaged or poorly secured NHI.

The scale of this challenge is staggering: Machine identities now outnumber human identities by as much as 144:1, with 23.8 million secret occurrences detected on GitHub.com in the last year alone. Nearly half of all exposed secrets are found outside of source code, embedded across various systems, tools, and workflows.

Recognizing this, leading cybersecurity frameworks and regulations have established controls to ensure the secure management of NHIs and their associated secrets.

GitGuardian

Regulatory & Framework Controls Addressing NHI Secrets

Framework / Regulation	Relevant Controls & Requirements	Key Focus Areas	Non-Conformity Consequences	How GitGuardian Addresses This
ISO/IEC 27001:2022 Global · All industries	**Annex A 5.15:** Access Control **Annex A 5.16:** Identity Management **Annex A 5.17:** Authentication information **Annex A 5.18:** Access Rights	Mandates full lifecycle management of identities, encompassing both human and non-human entities. Emphasizes approval, registration, and administration processes.	No statutory fines. As a certification standard, non-compliance results in the loss of certification and a significant contractual or commercial impact.	GitGuardian provides **comprehensive NHI lifecycle management** through its NHI Governance solution, supporting automated discovery, inventory, and administration of non-human identities across multiple secrets managers (HashiCorp Vault, CyberArk Conjur, AWS Secrets Manager, Google Cloud Secret Manager, Azure Key Vault, Delinea Secret Server). The platform implements **access controls, authentication information management**, and access rights governance aligned with ISO 27001 requirements. GitGuardian's self-hosted solution includes **FIPS 140-3 approved cryptographic modules** and Chainguard-hardened container images for enhanced security compliance.
NIST CSF 2.0 (National Institute of Standards and Technology Cybersecurity Framework) United States · Government · Technology	Identity Management, Authentication, and Access Control (PR. AC-1 to PR.AC-6) CSF 2.0 introduces the "Govern" function, highlighting the importance of aligning cybersecurity with organizational risk management, including policies and responsibilities for managing NHIs	Advocates for the identification and management of all identities, including NHIs, ensuring they are authenticated and authorized appropriately.	No statutory fines. As a voluntary framework, regulators may reference it, but any penalties are derived from sector-specific laws, not the CSF itself.	GitGuardian's NHI Governance solution directly addresses NIST CSF 2.0 requirements through **comprehensive identity management capabilities**. The platform provides **automated identification and inventory** of NHIs across infrastructure, implements authentication and authorization controls, and aligns with organizational risk management through policy-based governance. GitGuardian Scout (ggscout) safely collects NHI metadata using HMSL hashing to maintain security while enabling governance, supporting the **«Govern» function** emphasis in CSF 2.0.
CIS Controls v8 (Center for Internet Security) Global · All industries	**Control 5:** Account Management **Control 6:** Access Control Management	Recommends inventorying all accounts, including service accounts, and implementing access controls to manage NHIs effectively, removing unnecessary credentials, and monitoring usage of NHIs.	No fines. As a best-practice framework, its impact is felt in audits, assurance, and contractual agreements.	GitGuardian provides **automated discovery and continuous inventory** of all NHIs across across secrets managers and infrastructure sources (GitLab CI, Kubernetes clusters). The platform implements **access control management** by identifying **duplicated secrets, weak credentials, and unused accounts for removal.** GitGuardian's **monitoring capabilities track NHI usage patterns** and provide insights for effective access control management, directly supporting CIS Controls v8 requirements.
SOC 2 (System and Organization Controls 2) United States · Technology · SaaS · Cloud computing	**CC 6.2** - Controls Access Credentials to Protected Assets **CC6.2** - Removes Access to Protected Assets **CC6.2** - Reviews Appropriateness of Access Credentials	Requires organizations to implement controls ensuring NHIs have appropriate access, are monitored, and do not compromise system integrity.	No statutory fines. A failed or qualified report carries commercial and contractual impact, including lost business and the requirement for a re-audit.	GitGuardian itself maintains SOC 2 Type II compliance since 2022, demonstrating its own adherence to these controls. For customers, GitGuardian provides the technical controls required for SOC 2 compliance including **credential access management** through **secrets detection across 500+ credential types, automated removal** of inappropriate access through incident remediation workflows, and **continuous review capabilities** through its governance platform. The platform's **comprehensive logging, monitoring, and audit capabilities** support SOC 2 compliance requirements.

GitGuardian

GDPR (General Data Protection Regulation) European Union Any organization processing data of EU residents	**Article 32:** Security of Processing	Requires organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes managing NHIs that process personal data.	Upper tier fines up to €20M or 4% of annual worldwide turnover (whichever is higher), depending on gravity and nature of infringement.	GitGuardian offers **GDPR-compliant SaaS solutions** with data processing and retention within the EU for European customers. The platform implements **industry-standard encryption (TLS1.2, AES-256-CBC)** for data at rest and in transit, maintains **comprehensive logging and monitoring systems**, and provides **incident response capabilities.** GitGuardian's secrets detection and NHI governance capabilities help ensure that NHIs processing personal data are **properly secured and monitored**, supporting GDPR Article 32 security of processing requirements.
OWASP NHI Top 10 (2025) (Open Worldwide Application Security Project) Global All industries using NHIs	**NHI1** – Improper Offboarding **NHI2** – Secret Leakage **NHI3** – Vulnerable Third-Party NHI **NHI8** – Environment Isolation **NHI9** – NHI Reuse **NHI10** – Human Use of NHI	Advises the use of dedicated secret management tools, avoidance of hardcoded secrets, and implementation of ephemeral credentials to mitigate risks associated with NHIs.	No fines. As a security guidance framework, non-adherence increases risk and can be used as evidence of negligence under applicable laws.	GitGuardian's security policies are directly informed by the **OWASP Top 10 for NHIs**. The platform addresses: **NHI1** through lifecycle management and offboarding workflows; **NHI2 via 350+ specific secret detectors** and continuous monitoring; NHI3 through third-party integration monitoring; NHI8 via environment categorization (prod, staging, dev, testing); **NHI9** by identifying reused and duplicated secrets; and NHI10 through monitoring and access controls. GitGuardian provides **comprehensive coverage** across **code repositories, CI/CD pipelines, and infrastructure** to prevent hardcoded secrets and support dedicated secret management tools
SOX (Sarbanes-Oxley Act) United States Publicy traded companies	**Section 404** - Management Assessment of Internal Controls	Regular user access reviews are mandated to ensure only authorized personnel (human and non-human) have access to critical financial systems. Segregation of duties also applies, ensuring no single identity (human or non-human) has excessive control over financial processes.	No fixed schedule of SOX fines for control weaknesses. Actions by the SEC or PCAOB are determined on a case-by-case basis. Willful executive miscertification can carry severe civil or criminal penalties, with practical impacts including restatements, enforcement actions, and multi-million dollar penalties.	GitGuardian enables **regular access reviews** through **automated discovery and continuous monitoring** of NHI permissions across financial systems. The platform provides detailed audit trails through **comprehensive logging** and API access for audit purposes. GitGuardian identifies **over-privileged identities** and supports **segregation of duties** by mapping NHI relationships, access patterns, and usage contexts. The platform's incident management and remediation tracking capabilities support **SOX Section 404** internal control assessment requirements.
PCI DSS v4.0 (Payment Card Industry Data Security Standard) Global Organizations that process, store, or transmit cardholder data	**3.5**: Cryptographic keys must be securely managed **7.1:** Access rights should be limited to the minimum necessary (least privilege) **7.2.5 & 8.1.4:** Access rights must be periodically reviewed, and unnecessary accounts must be removed **8.2.2:** Each non-human entity must have a unique ID to ensure accountability **8.3.5:** Authentication credentials must be securely managed and rotated regularly **8.5:** Credentials must be transmitted using strong cryptography **8.6:** Strong authentication methods must be implemented, avoiding hard-coded passwords **8.6.1:** Hard-coded passwords in code or scripts are prohibited **10.2.1:** Activities of non-human accounts must be logged and monitored **10.4.1:** Non-human accounts must not have conflicting responsibilities (segregation of duties)	Highlights the need for strict management of NHIs, including service accounts and APIs. Emphasizes role-based access control, secure authentication, credential management, and monitoring.	While not a law, card brands and acquirers can levy fines for non-compliance, typically ranging from $5,000–$100,000 per month. Additional consequences can include further assessments after a breach and possible termination of processing privileges.	GitGuardian directly addresses PCI DSS 4.0 requirements through: **automated detection of hard-coded passwords/credentials (8.6.1) via 350+ specific detectors; secure credential management with rotation capabilities** through secrets manager integrations (8.3.5); **least privilege enforcement** through permission analysis and over-privileged identity detection (7.1); **continuous monitoring and logging of NHI activities** (10.2.1); unique identification of each NHI through comprehensive inventory **(8.2.2)**; regular **access reviews** with automated discovery of unnecessary accounts (7.2.5, 8.1.4); and strong cryptography for credential transmission using TLS1.2 and AES-256-CBC encryption (8.5).

DORA (Digital Operational Resilience Act) European Union Financial entities	**Article 20:** Identity Management	Mandates unique identification and access controls for users and systems in the financial sector. DORA emphasizes governance, incident response, and resilience testing, all of which should encompass the management and security of non-human identities.	DORA empowers EU national competent authorities to impose administrative penalties. Public guidance commonly cites daily fines of up to ~1% of average daily worldwide turnover for up to 6 months, or lump-sum penalties of up to 2% of annual worldwide turnover.	GitGuardian's **comprehensive NHI governance platform** supports DORA Article 20 compliance by **providing unique identification and access controls** for all NHIs in financial sector environments. The platform includes incident response capabilities through automated detection and remediation workflows, **continuous monitoring** for operational resilience testing, and governance frameworks specifically designed for regulatory compliance. GitGuardian Bridge enables secure connections to self-hosted financial services while maintaining compliance requirements, and the platform's **multi-vault integrations** support the operational resilience mandates of DORA.

High-Profile Breach Examples: When NHI Controls Fail

The following real-world incidents demonstrate the severe consequences of inadequate NHI and secrets management, directly violating the regulatory controls outlined above:

GDPR Article 32 Violations

Meta Platforms Ireland (2023) - €1.2 billion fine

- Violation: Continued data transfers without adequate safeguards for EU users' personal data

- NHI Control Failures: Inadequate technical measures for protecting data processed by automated systems

- Impact: Record GDPR fine demonstrating the critical importance of implementing proper security controls for systems processing personal data

British Airways (2018) - €22 million GDPR fine

Violation: Magecart code injection compromising 380,000 booking transactions

NHI Control Failures: Failed to implement adequate security measures for web applications and associated service accounts

ISO 27001 Connection: Proper implementation of Annex A controls (5.15-5.18) for access control and authentication could have prevented this incident

Tesla (2023) - Potential €3.3 billion GDPR exposure

Violation: Two former employees misappropriated nearly 100GB of confidential data affecting 75,000 individuals

NHI Control Failures: Failed ISO 27001 Annex A 5.16 (Identity Management) and 5.18 (Access Rights) - inadequate employee offboarding procedures for system access

OWASP NHI Connection: Direct violation of NHI1 (Improper Offboarding) - failure to revoke access permissions upon employee termination

GitGuardian

PCI DSS Control Violations

British Airways (2018) - Additional PCI DSS penalties

Violation: Same Magecart attack compromised payment card data

NHI Control Failures: Violated PCI DSS 8.6.1 (hard-coded password prohibition) and 8.3.5 (secure credential management)

Impact: GDPR fine plus additional card network assessment

Target (2013) - $292 million total costs

Violation: 40 million credit card numbers and 70 million customer records compromised

NHI Control Failures: Weak network segmentation and inadequate access controls

CIS Controls Connection: Failures in Controls 1 (Asset Inventory), 4 (Secure Configuration), and 6 (Access Control Management)

PCI DSS Impact: $67M (Visa) + $19M (Mastercard) + $18.5M state settlements

Heartland Payment Systems (2009) - $145+ million

Violation: SQL injection attack compromising 100+ million cards

NHI Control Failures: Inadequate application security and credential management

Impact: $60M (Visa) + $41M (Mastercard) + exclusion from processing networks for 14 months

SOC 2 Control Deficiencies

Equifax (2017) - $575 million settlement

Violation: Unpatched Apache Struts vulnerability and expired monitoring certificates exposed 147 million records

SOC 2 Control Failures:
CC7 (System Operations) - inadequate detection/monitoring
CC8 (Change Management) - failure in timely patching
CC6 (Logical Access Controls) - insufficient data segmentation

ISO 27001 Connection: Failed to implement proper supplier relationship management and risk assessment controls

Capital One (2019) - $80 million OCC penalty

Violation: Inadequate cloud migration risk assessment and governance

SOC 2 Control Failures:
CC3 (Risk Assessment) - failed to establish effective risk processes
CC4 (Monitoring of Controls) - inadequate control monitoring
CC8 (Change Management) - poor cloud migration controls

PCI DSS Impact: $67M (Visa) + $19M (Mastercard) + $18.5M state settlements

Snowflake Breach (May 2024) - - Multiple customer data exfiltration

Violation: Credential theft via infostealer malware affecting service accounts.

NHI Failure: Exploitation of static, long-lived credentials and lack of MFA on service accounts.

Regulatory Tie-ins: Violates PCI DSS 8.6 (Strong Authentication) and SOC 2 CC6.2 (Access Controls).

Impact: Multiple high-profile customer data exfiltrations with ransom demands.

GitGuardian

OWASP NHI Top 10 Violations

MGM Resorts & Caesars Entertainment (2023)

Violation: Simultaneous breaches caused by a single threat actor, Scattered Spider, exploiting social engineering and weak access controls.

NHI Control Failures: OWASP NHI Top 10: Direct violation of NHI10 (Human Use of NHI), as the hackers used social engineering to trick human employees into giving them access to non-human credentials.

PCI DSS: Violations of 8.6 (strong authentication) due to the bypassing of multi-factor authentication (MFA).

CIS Controls: Failure in Control 6 (Access Control Management) by not preventing unauthorized access.

Impact: MGM Resorts suffered a major operational disruption, with systems like slot machines and digital room keys taken offline, leading to an estimated $100 million in losses. Caesars reportedly paid a $15 million ransom. The attacks highlight how a failure in NHI management can lead to both severe data breaches and crippling business disruptions.

Uber (2022) - Complete network compromise

Violation: Hardcoded credentials in PowerShell scripts provided admin access to the Privileged Access Management system

OWASP NHI Failures:
NHI2 (Secret Leakage) - hardcoded credentials in scripts
NHI10 (Human Use of NHI) - inadequate segregation between human and machine credentials

Impact: Complete access to AWS, GCP, Google Drive, Slack workspace, and internal systems

Microsoft (2022) - 38 terabytes of data exposed

Violation: Access token exposed in public GitHub repository for over two years

OWASP NHI Failures:
NHI2 (Secret Leakage) - long-lived secrets in public repositories
NHI8 (Environment Isolation) - insufficient controls on credential scope

Impact: Massive data exposure highlighting risks of long-lived secrets in NHI management

SOX Section 404 Violations

Wells Fargo (2022) - $22 million OSHA penalty

Violation: Retaliation against a whistleblower reporting financial control violations

Control Failures: Inadequate internal controls and segregation of duties

Impact: Demonstrates severe penalties for SOX-related control failures

Kraft Heinz (2021) - $62 million SEC settlement

Violation: Long-running accounting improprieties, including false expense reports

Control Failures: Inadequate access controls and approval processes for financial systems

SOX 404 Connection: Failed management assessment of internal controls

GitGuardian

CIS Controls Violations

Home Depot (2014) - $200+ million total costs

Violation: Malware on point-of-sale systems exposing 56 million credit card numbers

CIS Control Failures:
Control 7 (Continuous Vulnerability Management)
Control 10 (Malware Defenses)

Impact: $17.5M state settlements plus significant bank reimbursements

Marriott (2018) - $23.8 million GDPR fine

Violation: 339 million guest records exposed over four years

CIS Control Failures:
Control 3 (Data Protection)
Control 8 (Audit Log Management)
Control 13 (Network Monitoring)

Impact: Breach went undetected for years due to inadequate monitoring controls

Cloudflare Breach (November 2023) - Inventory gaps and missed rotations

Violation: Four missed credential rotations in the Atlassian environment following a previous Okta compromise.

NHI Failure: Improper Offboarding (NHI1) and Credential Reuse (NHI9) across environments.

Regulatory Tie-ins: Failed ISO 27001 A 5.16 (Identity Management) and CIS Controls 5 & 6 (Account & Access Control).

Impact: Attackers maintained persistence despite a strong security posture, accessing internal systems

Why This Matters

- **Proliferation of NHIs:** Machine identities now outnumber human identities by a significant margin of 100:1, increasing the attack surface.
- **High-Profile Breaches:** As demonstrated above, mismanagement of NHIs has led to significant security incidents with multi-million dollar penalties, emphasizing the need for stringent controls.
- **Regulatory Scrutiny:** Non-compliance with the aforementioned frameworks can result in severe penalties and reputational damage, with fines ranging from millions to billions of dollars.
- **Operational Resilience:** Proper NHI management helps prevent disruptions and ensures the integrity of automated processes, as evidenced by the business disruptions suffered by companies like Heartland Payment Systems.

How GitGuardian Helps

GitGuardian empowers organizations to comply with today's toughest NHI and secrets governance requirements. It provides deep, real-time visibility into where machine identities exist, how their credentials are used, and whether they've been exposed. By mapping the full lifecycle of secrets—from creation to revocation—and correlating them with usage patterns, GitGuardian enables teams to detect zombie credentials, enforce rotation policies, and benchmark their hygiene against OWASP Top 10. With built-in policy enforcement and integrations across secrets managers, IAM cloud providers, cloud infrastructure tools, and more, GitGuardian offers a unified layer of control for securing machine identities at scale.

For a deeper dive into how the GitGuardian platform can assist in aligning with these frameworks, please reach out for a personalized demo.

Book a **tailored consultation**

Take a self-guided tour to see how NHI Governance can secure your environment

GitGuardian

Sources

Meta Platforms Ireland (2023) - €1.2 billion fine
Irish DPC decision
EDPB binding decision summary

British Airways (2018) - €22 million GDPR fine
ICO penalty coverage
Media recap

Tesla (2023) - Potential €3.3 billion GDPR exposure
Reuters
TechCrunch

British Airways (2018) - Additional PCI DSS penalties
ICO decision

Target (2013) - $292 million total costs
$18.5M multistate AG settlement
Target–Visa settlement (up to $67M)
Target CEO notice (contemporaneous)

Heartland Payment Systems (2009) - $145+ million
BankInfoSecurity (Visa/Mastercard assessments)
Privacy Rights breach profile

Equifax (2017) - $575 million settlement
Source

Capital One (2019) - $80 million OCC penalty
Source

MGM Resorts & Caesars Entertainment (2023)
Sources

Uber (2022) - Complete network compromise
GitGuardian analysis

Microsoft (2022) - 38 terabytes of data exposed
GitGuardian write-up

Wells Fargo (2022) - $22 million OSHA penalty
DOL/OSHA press release

Kraft Heinz (2021) - $62 million SEC settlement
SEC press release
Company statement

Home Depot (2014) - $200+ million total costs
Reuters coverage
NY AG press
Company disclosure (breach findings)

Marriott (2018) - $23.8 million GDPR fine
Company statement on ICO outcome

Cloudflare Breach (November 2023) - Inventory gaps and missed rotations
Cloudflare official incident report