entro Labs

2025 State of Non-Human Identities and Secrets in Cybersecurity

A Comprehensive Analysis of Risks, Misconfigurations, and Best Practices for NHI & Secrets Security

Introducing Entro Labs

As a new and evolving approach to cybersecurity, Non-human Identity security has received attention, but compromised NHIs stayed a leading attack vector across industries and verticals.
Entro security is the creator of the only NHI security platform, purpose-built to secure all non-human identities in an organization from inception to rotation. Being the first and only vendor focused on the NHI-Sec space, Entro needed to establish Entro Labs to analyze the NHI space in more depth and gain additional insight.

Entro Labs' stated goals are to:

- Identify NHI risks and insights across multiple markets
- Track the evolution of the NHI security space
- Highlight routine misconfigurations that greatly increase risk
- Investigate research from and with peer research institutions

Entro and Entro Labs were both formed with the single-minded focus of safeguarding NHIs from inception to rotation, thereby keeping the digital assets NHIs interact with portable, accessible, and fully secure. As a result, Entro will publish Entro Labs' findings, allowing visitors of entro.security to leverage these insights and stay a step ahead of bad actors in the NHI security space.

Note: This paper is the first publication of Entro Labs research, highlighting some of the results of Entro Labs' findings. Entro Labs will continue to publish up-to-date findings periodically in order to assist in further development of the industry's understanding of the NHI threatscape.

The Objective

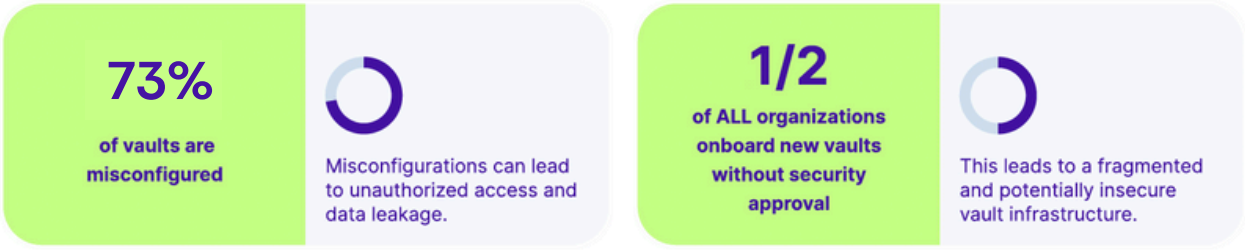
The primary objective of this research is to identify and analyze risks in the NHI security market, highlight concerns affecting modern enterprises worldwide, and identify meaningful steps that can be taken towards resolution. In order to meet this goal, a comprehensive analysis of statistical data sourced from various channels as well as proprietary data sourced by Entro Security has been performed. This study aims to provide actionable insights and highlight key trends in cybersecurity vulnerabilities, threats, and incidents impacting enterprises.

At a Glance

- **There are more NHIs than anticipated in most organizations**
- **Secrets are handled insecurely in most organizations, leading to NHI risk exposure**
- **NHIs are created at will with no regard to securing their lifecycle until retirement**

The Proliferation of Non-Human Identities

The Vault Landscape



There are **at least 5 different vault solutions** in use per organization, including Hashicorp Vault, Azure KeyVault, AWS Secrets Manager, Kubernetes Secrets, and GitHub Secrets. This diversity can complicate management and increase the risk of misconfigurations.

The Risk of Idle, Overused, and Duplicated Secrets

of identified secrets are idle

These are valid secrets that are not currently being used by application workloads, representing an unnecessary risk of exposure and potential misuse.

of secrets are less secure

They are shared across multiple applications, violating the principle of least privilege. This practice increases the risk of a security breach, as a single exposed secret could compromise multiple systems.

of former employee tokens are never revoked

This oversight in de-provisioning is a critical gap in the security posture of organizations and a serious regulation breach.

of environments we've audited

have secrets that have been granted excessive permissions and access authorization than necessary

of all secrets are duplicated & stored in multiple locations

This redundancy increases the risk of exposure and complicates the management of secrets.

Token Management Failures and Exposure Risks

90% of tokens have excessive permissions and access

This oversight creates a major security vulnerability, as these tokens could be exploited by malicious actors.

44% of tokens are exposed in the wild

These exposures are often found in channels like Teams, Jira tickets, Confluence pages, code commits, and more

What It Means

Securing non-human identities and secrets clearly presents significant challenges for a majority of organizations that interact with them. An assessment of the research compiled by Entro Labs helps identify several key challenges faced by the industry:

Complexity of Managing Non-Human Identities

Non-human identities, such as service accounts, API keys, and application tokens are integral to modern IT environments. These identities are often used to facilitate automated processes and inter-application communications. However, managing these identities poses several challenges:

- **Over-Provisioning:** Non-human identities frequently have excessive privileges, increasing the risk of exploitation. Properly scoping and regularly reviewing permissions is critical but often neglected.
- **Visibility and Tracking:** Tracking the usage and lifecycle of non-human identities is complex. Without comprehensive visibility, it's challenging to detect misuse or stale credentials.
- **Lifecycle Management:** Ensuring that non-human identities are deactivated or updated promptly when systems are modified or retired is a persistent issue.

Securing Secrets Across Diverse Environments

Secrets, certificates, service accounts, and tokens are essential for system operations. Protecting these secrets is crucial but remains problematic due to:

Exposure Risks

Dynamic Nature

Encryption & Storage

- **Exposure Risks:** Secrets can be inadvertently exposed through misconfigured repositories, hardcoded in codebases, using communication or collaboration tools, or stored in other insecure storage solutions. This often leads to an increased risk of data breaches followed by active insider threats.
- **Dynamic Nature:** In environments with frequent deployments and changes, secrets must be dynamically managed and rotated. Implementing effective secret management practices that align with rapid development cycles is very challenging.
- **Encryption and Storage:** Securing secrets in storage and during transmission requires robust encryption mechanisms. Ensuring that these mechanisms are implemented correctly and consistently across all systems can be a complex task.

Integrating Secure Architectures

Architectures involving non-human identities and secrets must be designed with security as a top-of-mind concern. Key challenges include:

- **Design Complexity:** Building secure architectures that effectively manage and isolate non-human identities requires careful design to avoid vulnerabilities. This complexity increases with the scale and diversity of systems, secrets, and NHIs involved.
- **Compliance Requirements:** Adhering to compliance standards (such as GDPR, PCI-DSS) while managing non-human identities and secrets requires implementing additional security controls and maintaining detailed audit trails.
- **Automation vs. Security:** Balancing the need for automation with security considerations is critical. Automated systems that manage non-human identities and secrets must be configured to prevent misuse and ensure that security controls are not bypassed.

Threat Detection and Response

The detection of threats related to non-human identities and secrets requires advanced monitoring and response strategies:

- **Anomaly Detection:** Identifying anomalous behavior involving non-human identities can be challenging due to the high volume of legitimate automated transactions.
- **Incident Response:** Rapidly responding to incidents involving secrets or non-human identities demands well-defined processes and tools. Effective incident response requires a deep understanding of how non-human identities interact within the environment.

In conclusion, securing non-human identities and secrets is a multifaceted challenge that requires a combination of robust management practices, sophisticated security technologies, and constant oversight. Addressing these challenges effectively is crucial for protecting sensitive information and maintaining the integrity of IT systems in today's complex and dynamic digital landscape.

Methodology

Research Approach

Entro Labs' employs a mixed-methods approach, integrating quantitative data analysis with qualitative insights derived from industry observations. The quantitative component focuses on statistical analysis of security incidents and vulnerabilities, while the qualitative aspect provides context and interpretation of these findings within the broader cybersecurity landscape.

Data Sources

Proprietary Data: Data collected from Entro's cybersecurity infrastructure, encompassing real-world environments of Entro's customers. This data includes:

- Incident reports
- Threat intelligence feeds
- Vulnerability assessments
- Security event logs

Secondary Data: Publicly available and industry-sourced data from:

- Cybersecurity threat intelligence platforms (e.g., FireEye, CrowdStrike)
- Industry reports (e.g., Verizon Data Breach Investigations Report, Ponemon Institute studies)
- Government and non-governmental organization reports (e.g., European Union Agency for Cybersecurity, U.S. Cybersecurity and Infrastructure Security Agency)

Survey Data: Results from surveys conducted with enterprise IT and security professionals, which include:

- Perceptions of security threats
- Incident response practices
- Security posture and challenges faced

Data Collection Methods

Automated Data Extraction: Entro labs utilizes advanced analytics tools and platforms to aggregate and analyze data from Entro's infrastructure in real-time.
Surveys: Entro Labs distributes structured questionnaires via email, conventions, and online platforms, targeting IT and cybersecurity professionals across diverse industries.
Secondary Data Analysis: Relevant industry reports and studies collected through databases, subscriptions, and partnerships with cybersecurity research firms inform Entro Labs' research.

Data Analysis

Quantitative Analysis

Descriptive Statistics: Descriptive statistics are used for the calculation of basic metrics such as frequency, mean, median, and standard deviation of incidents, vulnerabilities, and threat types.
Trend Analysis: Examination of data over time periods has been performed to identify emerging patterns and shifts in security concerns.
Correlation Analysis: Entro Labs has performed an investigation of relationships between different types of security incidents and organizational factors such as industry sector, company size, and geographic location.

Qualitative Analysis

Thematic Analysis: Identification of recurring themes and concerns in survey responses and incident reports.
Case Studies: In-depth analysis of significant incidents reported by Entro's infrastructure has been performed to further confirm common vulnerabilities and attack vectors.
Expert Interviews: Insights from cybersecurity experts and practitioners has been conducted to contextualize statistical findings and provide expert interpretations.

Ethical Considerations

Data Privacy

All proprietary data is anonymized and aggregated to protect customer confidentiality. Sensitive information is handled in compliance with relevant data protection regulations, including GDPR and CCPA.

Bias Minimization

Efforts are made to ensure that the research findings are objective and representative of the broader cybersecurity landscape. Secondary data sources are critically evaluated for reliability and validity.
When developing research on non-human identities, secrets, and securing architectures, several ethical considerations must be taken into account to ensure that the research is conducted responsibly and that its findings are used appropriately. Here are key ethical considerations for this topic:

Informed Consent

Participant Awareness: When involving human subjects, such as through surveys or interviews, Entro Labs obtains informed consent. Participants are fully aware of the research objectives, how their data will be used, and their rights.
Voluntary Participation: Participation is voluntary, and individuals have the option to withdraw from the study at any time without facing any negative consequences.

Security Implications

Impact of Findings: Entro Labs considers the potential impact of research findings on cybersecurity practices when disclosing research, to ensure that the dissemination of results does not inadvertently aid malicious actors or increase vulnerabilities.
Responsible Disclosure: If research uncovers significant security flaws or vulnerabilities, Entro Labs follows responsible disclosure practices. This involves notifying affected parties before making findings public to allow them to address the issues.

Compliance with Legal and Regulatory Standards

Regulatory Adherence: Entro Labs adheres to relevant data protection regulations, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and industry-specific standards.
Ethical Standards: Entro Labs adheres to ethical standards set by professional organizations and research ethics boards, particularly those related to cybersecurity and data handling.

Impact on Stakeholders

Stakeholder Sensitivity: When disclosing information, Entro Labs considers the potential impact of the research on stakeholders, including organizations, end-users, and the broader community. Entro Labs evaluates research to ensure it does not inadvertently harm or disadvantage any group.
Beneficial Outcomes: Entro Labs aims for research outcomes that contribute positively to the field of cybersecurity and provide practical benefits for improving security practices and protecting sensitive information.

Limitations

Data Bias

Proprietary data may reflect the security concerns specific to Entro's customer base, potentially introducing bias. To mitigate this, secondary data and survey results are used to provide a more comprehensive view.

Data Completeness

The study relies on the availability and accuracy of data from various sources. Some incidents or vulnerabilities may not be fully captured due to reporting delays or incomplete datasets.

Data Drift

As a wide variety of sophisticated tools and technologies are used by Entro as well as other cybersecurity research institutions, data collected from these peer institutions may have its own drift that cannot be accounted for.

Concept Drift

Data collected across multiple sources must also account for changes in the relationship of the input data and model targets used by various sources - for example a vendor that waits for a specific signal to log a message may not log a message in the same way when the signal is received with a modified payload due to a software update. Models that are leveraging these logs to analyze these signals would need to account for this discrepancy.

Reporting and Dissemination

The research findings will be compiled into a detailed report, highlighting key statistics, trends, and insights. The report will be disseminated through:

Entro's web page: Visitors can learn more about these topics on entro.security, as well as view additional content

Industry Conferences: Presentation of findings at relevant cybersecurity conferences and symposiums.

White Papers: Distribution of a white paper summarizing the key results and recommendations to industry stakeholders and the general public.