CASE STUDY

Providing Full Visibility of the Non-Human Identities at a Growing Tech Company

At a glance

As the Company expanded its services, so did the complexity of its cloud-based infrastructure. The company's cybersecurity technology relied heavily on non-human identities—such as API keys, CWTs, and service accounts for automation scripts—that were necessary to power its tools and integrations. This experience with Entro Security underscored the importance of automation in modern cybersecurity efforts. As non-human identities continue to proliferate and as the company grows, the security team is confident that Entro will remain a key component of their security strategy.

THE CHALLENGE

As a cybersecurity technology company's infrastructure became more dynamic and integrated with external services the security team faced several key challenges around managing non-human identities:

Lack of Visibility and Control: The Company's growing number of non-human identities—spanning microservices, cloud platforms, and third-party integrations—created blind spots in their security posture. The team lacked a clear understanding of where and how secrets were being used across different environments, increasing the risk of unauthorized access.

Manual Secrets Management: Secrets such as API keys and service account credentials were manually rotated and stored in different locations across the infrastructure. This inconsistent, ad-hoc approach led to security gaps and compliance risks. The team spent significant time trying to track down outdated or improperly managed secrets, which increased the potential for human error.

Risk of Credential Exposure: With multiple tools and services accessing critical systems, the risk of secrets being exposed—either through code repositories, misconfigured environments, or outdated credentials—was a significant concern. Without a centralized management system, the Company was constantly worried about the potential for a security breach due to improper secrets management.

entro

CASE STUDY

Providing Full Visibility of the Non-Human Identities at a Growing Tech Company

THE SOLUTION:

1

Automated Secrets Rotation and Management

Entro's automated solution eliminated the need for manual secrets rotation, as well as handled the lifecycle management of NHIs, including secure storage, rotation, and access control, with minimal intervention.

2

Unified Visibility and Auditing

Entro's platform gave complete visibility into the use of NHIs across its environment. With real-time auditing and monitoring, the security team could easily track which service accounts or APIs were accessing sensitive systems and data, making it easier to detect anomalies.

3

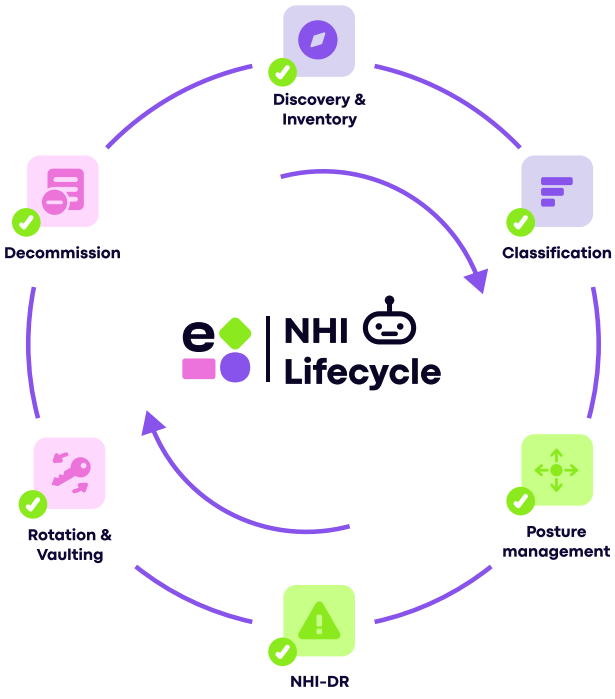
Least-Privilege Access

Adopted a least-privilege approach to NHI's shrinks the attack surface. Entro's dynamic policy engine ensured that service accounts and automation scripts only had the permissions necessary to carry out their functions, minimizing the attack surface.

4

Scalable and Flexible Integration

As the Company's infrastructure continued to grow, Entro's solution scaled seamlessly to accommodate new integrations, cloud environments, and services without compromising security. The flexibility of Entro's platform allowed them to integrate with a wide range of tools while maintaining a consistent and secure approach to secrets management.



entro

CASE STUDY

Providing Full Visibility of the Non-Human Identities at a Growing Tech Company

BENEFITS

1

Reduced Risk of Credential Exposure

Entro's ability to rotate secrets automatically and in real-time removed the reliance on manual processes that were prone to human error.

2

Increased Efficiency and Focus

The automation of secrets rotation and management freed up the team's time, allowing them to focus on higher-priority tasks.

3

Stronger Compliance and Audit Trails

Entro's integrated audit logs and reporting features, allowed for easy compliance with industry regulations and internal security policies

4

Improved Confidence in Security Posture

Implementing Entro's platform enabled a stronger security posture, knowing that all secrets were being managed in a consistent, controlled, and compliant manner.

"Managing non-human identities was one of the hardest challenges we faced as our infrastructure grew. There were too many secrets to track, and we didn't have a unified system to govern them properly. We knew that a simple misconfiguration could expose our entire environment to attack...Entro gave us the tools we needed to manage non-human identities at scale. The automated rotation of secrets and centralized governance was exactly what we were looking for. We could now manage thousands of service accounts and API keys securely and efficiently, without compromising our agility."

CONCLUSION

For this company, Entro Security has been an invaluable partner in securing non-human identities and enhancing their cybersecurity posture. By automating the management and governance of service accounts, API keys, and other secrets, they were able to significantly reduce the risk of credential exposure, increase operational efficiency, and maintain compliance with global security standards. They now can continue to innovate, confident that their infrastructure is protected against the growing threat landscape of credential misuse and unauthorized access.

entro