Non-human identities security for a cloud native stack

The first holistic platform that offers unmatched protection and lets you discover a new level of non-human identities security

What is non-human identities security and management in a cloud-native stack?

Securing and managing non-human identities has become crucial to cybersecurity as businesses increasingly adopt cloud-native architectures. Although vaults have gained popularity as a secure way to store non-human identities, managing non-human identities involves more than just storage. With API keys, access tokens, and other sensitive programmatic passwords used to access critical systems and resources in the cloud, the consequences of these falling into the wrong hands is catastrophic.

To ensure that doesn't happen, Entro offers an exclusive non-human identities security platform for organizations with a cloud-native stack that enables you to discover, monitor and manage every single secret in your organization from the time it's created to the time it's retired. Non-human identities scanning is a reactive approach to security. Entro, on the other hand, implements proactive measures to secure your non-human identities, such as real-time non-human identities discovery, monitoring, anomaly detection, and controlled access. We ensure that authentication and authorization of access to various cloud resources and services are done securely to maintain a robust security posture.

> "Using Entro helped my team gain total visibility to all the non-human identities across our different AWS accounts, code repositories and collaboration tools. Now that we have that visibility, we can easily manage them."

Avishai Avivi
CISO | Safe Breach

What should you expect?

- Non-human identities Inventory. Know how many non-human identities you have and where they are by discovering non-human identities across all vaults, clouds, code, CICD, emails, and collaboration solutions, and assess risk severity with actionable context.
- Visualize and reduce non-human identities attack surface. Understand which application is using what secret to access what cloud service, and more vital non-human identities data, such as creation time, non-human identities privileges, rotation date, owner, risks and more.
- Continuously monitors your non-human identities for any threat. Leverage an anomaly detection system that track activities for odd non-human identities behaviors, detects risks, and offers remediation recommendations.
- Detect Dark Web leakage with early alerts and swift remediation mechanisms.
- Detect misconfigurations in vaults and other secret stores to accelerate secret posture management and remediation and fixing of compliance reports.
- Stay secure with least privilege access implementation by eliminating excessive privileges.

Non-human identities security for a cloud native stack

The first holistic platform that offers unmatched protection and lets you discover a new level of non-human identities security

Our approach to non-human identities security and management includes mechanisms for detecting, safeguarding, and enriching non-human identities with context across all channels, including vaults, source code, chat, wikis, logs, and third-party vendor tools. We also provide a central management hub for non-human identities by integrating with vaults, and all places where non-human identities can be stored or exposed, which makes it easy to discover, audit, and control access to sensitive information. One of the key features of our offering is advanced analytics and context-aware insights.

After discovering all your non-human identities, Entro will visualize a map of which application is using what secret to access what cloud service, and more vital non-human identities data, such as creation time, non-human identities privileges, rotation date, owner and more. For real-time threat detection, we utilize machine learning algorithms that, in turn, help identify anomalies, misuse, and unusual patterns of non-human identities behavior. With this functionality, you can quickly detect security breaches and take proactive measures to safeguard your non-human identities.

How does the non-human identities Security and management service work for me?

The recent report titled 'Hiding in Plain Sight', shed light on how mismanagement of non-human identities can translate to a staggering annual cost of $1.2 million to companies. We want to ensure this does not happen to you.

Our exclusive non-human identities security platform caters to organizations with a cloud-native stack. Keeping in mind the growing need for businesses to securely and efficiently manage their non-human identities, Entro was developed to provide a safe and reliable way to discover, monitor, manage, and collaborate around sensitive non-human identities, including API keys, cloud access tokens, passwords, and more.

Our solution offers a centralized platform where non-human identities can be managed, ensuring only authorized personnel can access and transmit them across various cloud resources and services. This helps enterprises control their non-human identities and ensure that only authorized personnel can access them.

We have incorporated advanced access control measures into our solution to ensure maximum security for the non-human identities stored in the vaults. Our system leverages role-based access control and auditing and monitoring functionalities that track all activities performed on the non-human identities. With that, we are able to supply a non-human identities inventory, classify and enrich each secret, continuously monitor non-human identities for any abnormal behavior and detect vaults misconfiguration to keep the

Non-human identities security for a cloud native stack

The first holistic platform that offers unmatched protection and lets you discover a new level of non-human identities security

organization safe and secure against non-human identities targeted attacks.

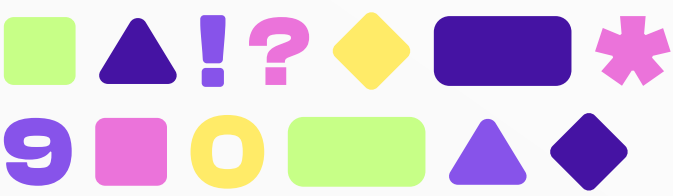
Moreover, our non-human identities security and management platform caters to diverse customer needs and requirements. The user-friendly interface of our platform enables non-technical workers and security professionals to manage and secure their non-human identities effortlessly. At the same time, IT teams and technical employees can benefit from the advanced features and integration capabilities that allow for the customization of workflows and seamless integration with existing systems.

How can enterprises keep up with today's cyber threats? By getting ahead of them

As the threat of cybercrime becomes more sophisticated, enterprises must adopt a proactive stance to protect their non-human identities keys. Today, the age-old traditional security measures are no longer adequate to combat the ever-evolving cyber threat landscape. To deal with it, enterprises must take a proactive approach to implementing cutting-edge cybersecurity solutions to mitigate the risks posed by cybercriminals. This includes utilizing advanced discovery and access control mechanisms, classifying and enriching with context each secret and access token, and monitoring features to secure sensitive data.

Implementing an effective non-human identities security and management solution is one of the most critical decisions organizations can make to stay ahead of today's cyber threats. If the solution comes with all the above features — all the better. And that's where Entro steps in to provide the ultimate non-human identities security solution. It integrates with vaults to offer a centralized location to protect and manage all non-human identities, such as passwords, API keys, and other sensitive data, securely and organized. And it also offers the ability to rotate non-human identities, preventing attackers from using stolen non-human identities to gain unauthorized access.

Moreover, organizations often lack knowledge of the total number of non-human identities they possess, and where are they, and traditional tools like vaults and scanners cannot provide them with this critical information. Only Entro has the capability to scan and identify all active non-human identities in your organization, providing you with a clear picture of the exact number of non-human identities you possess. This is the first and essential step towards protecting your non-human identities, as having a comprehensive understanding of the extent of your non-human identities' landscape is crucial for effective non-human identities management and security.



Non-human identities security for a cloud native stack

The first holistic platform that offers unmatched protection and lets you discover a new level of non-human identities security

A highly functional non-human identities security and management solution like this can have numerous benefits. It will lead to enhanced security, reduce the risk of data breaches through centralized management, and support compliance with regulatory frameworks in your region.

Moreover, with Entro, you can enforce access controls that ensure only authorized personnel are accessing the non-human identities, thus reducing the risk of insider threats.

Why Entro?

Entro's non-human identities security and management solution stands out from the crowd for various reasons. With a focus on cloud-native architecture and a team of experienced cybersecurity experts, Entro offers a comprehensive and tailored solution to meet the needs of enterprises. Instead of relying on a reactive approach of using non-human identities scanners, Entro integrates with vaults, code, cloud, and collaboration tools to provide a centralized location to secure and manage non-human identities and ensures you know how many non-human identities you have, where they are, who is using them, what cloud services they can access and what risks are associated with them.

It also offers other advanced security features such as dark web leakage detection and granular access controls, thus enabling businesses to maintain a robust security posture and protect against data breaches.