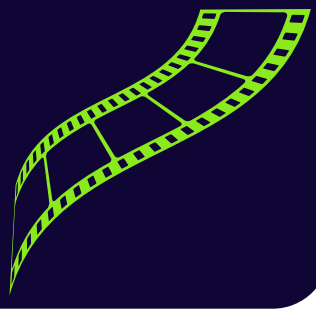
CASE STUDY

Securing An Entertainment Enterprise with Lifecycle Management

At a glance

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 integrates with more third-party vendors, the security team is confident that Entro will remain a key component of their security strategy.

Moving forward, the company has a greater confidence in their security and compliance standings, and are leveraging Entro's lifecycle management to save time and ensure optimal efficiency.



BACKGROUND

As a leading entertainment platform, this company is at the forefront of digital media innovation. Given the continuously expanding infrastructure and diverse array of third-party integrations, the company's cybersecurity team, faced an escalating challenge: managing and securing non-human identities (NHIs) —including API keys and service accounts for automation scripts. These identities are essential to their system operations but, if not properly secured, represent a significant vulnerability.

THE CHALLENGE

As the platform scaled, the number of non-human identities multiplied, leading to a number of cybersecurity risks:

- **Increased Exposure to Breaches:** With so many keys, tokens, and service accounts in play, the risk of credentials being exposed or misused was growing. They struggled to track where each secret was being used, which made auditing and securing these identities increasingly difficult.
- **Lack of Automation and Governance:** Limited visibility and control over the lifecycle of non-human identities. Secrets were being rotated manually, and the auditing process was time-consuming, inconsistent, and prone to human error.
- **Regulatory Compliance:** As a streaming service operating in multiple regions,they had to comply with a growing number of data protection regulations. Ensuring that secrets and non-human identities were handled in compliance with industry standards was an ongoing challenge.

"Managing non-human identities was a constant headache. The sheer volume of service accounts, API keys, and automation scripts we had to secure was overwhelming," says the Head of Cybersecurity "We knew that if we didn't get a handle on this, we would face serious security and compliance risks."

entro.security
Boston | Tel Aviv
support@entro.security

CASE STUDY

Securing An Entertainment Enterprise with Lifecycle Management

THE SOLUTION:

The Company turned to Entro Security, a leader in managing and securing non-human identities and secrets. Entro's platform offered a comprehensive solution that not only simplified the management of non-human identities but also helped enforce policies that ensured these identities were securely managed throughout their lifecycle.
The key features of Entro's solution that benefited them:

1

Visibility and Governance

Entro helped us understand where secrets were used, who had access to them, and what actions were being performed. With an integrated audit trail they could now easily trace and monitor the use of non-human identities, simplifying compliance with regulatory standards.

2

Streamlined Secrets Management

Entro's platform simplified the rotation and lifecycle management of non-human identities, significantly reducing the risk of human error. All our secrets, whether used by applications, APIs, or microservices, are now securely stored, rotated, and monitored in real-time.

3

Least Privilege Security

The platform enforced least-privilege access policies, ensuring that service accounts and automation scripts had only the minimum level of access required to perform their tasks. Entro's dynamic policy engine allowed for granular control over permissions and access rights.

4

Scalability and Flexibility

As The Company continued to scale, Entro's solution easily adapted to their growing infrastructure, supporting new integrations and expanding service accounts without compromising security.

CASE STUDY

Securing An Entertainment Enterprise with Lifecycle Management

THE RESULTS

1. **Reduced Secrets Exposure**
   Automating the rotation of secrets and monitoring their use dramatically reduced the risk of exposed or compromised credentials.

2. **Increased Operational Efficiency**
   The time spent on manual processes was reduced by 70%. This allowed the security team to focus on higher-priority initiatives.

3. **Enhanced Compliance Posture**
   With Entro's robust audit and reporting features, the Company was able to maintain full compliance with data protection regulations.

4. **Greater Confidence in Security**
   With Entro's solution in place, they now knew that non-human identities were secured, tracked, and managed in a way that minimized exposure and mitigated risk.

"Before Entro, managing non-human identities felt like a constant battle. Now, it's just part of our normal workflow. We have the tools to monitor, govern, and secure our non-human identities without interrupting our operations. Entro has been a critical partner in enabling us to scale securely and with confidence."

CONCLUSION

As the company continues to scale and integrate with more vendors and services, ensuring the security of sensitive data and non-human identities becomes even more critical.
By adopting Entro Security, this company has strengthened its defenses against data leaks, improved compliance, and empowered its development teams to work with greater confidence. With Entro's automated secrets detection, real-time alerts, and robust integrations, they are poised to continue its leadership in the travel industry—while maintaining the highest standards of cybersecurity.

entro