CASE STUDY

Securing A Travel Enterprise Across Clouds and Infrastructures

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 plans to extend the platform's coverage to other parts of its infrastructure, and leverage Entro's auditing and reporting features to ensure that its security practices are continually refined, keeping them ahead of evolving threats and compliance requirements.

THE CHALLENGE

A leader in the travel industry aggregates a massive amount of data from various third-party service providers, including airlines, hotels, rental cars, and vacation packages. Their vast infrastructure involves thousands of integrations and systems that rely heavily on Non-Human Identities to connect with external vendors and internal services. As they expanded their operations and integrated with new third-party services, the number of these identities skyrocketed. This meant more access points to secure, and more opportunities for potential breaches if not properly managed. Simultaneously, sensitive information—like API keys and access tokens—were often shared in tools like Jira, Confluence, GitHub, Slack, AWS, and Okta, posing a significant security risk. Additionally, mismanaged secrets could lead to data leaks, violate compliance regulations (like GDPR and PCI-DSS), and even open the door to unauthorized access.

THE SOLUTION: ENTRO SECURITY'S AUTOMATED SECRETS DETECTION

The security leaders turned to Entro Security to address these challenges. Entro provides automated, real-time detection of secrets across their tools and infrastructure. Key features included:

- **Comprehensive Secrets Detection:** Entro scans repositories, communication channels, and internal documents to detect sensitive information, such as API keys or passwords, across platforms like GitHub and Slack.
- **Real-Time Alerts & Automated Remediation:** Upon detecting a secret, Entro immediately alerts the security team and offers automatic remediation steps, such as key rotation or token revocation.
- **Seamless Integration:** Entro integrates with Kayak's existing tools—GitHub, Jira, Confluence, and Slack—ensuring that security is embedded without disrupting workflows.

entro

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

CASE STUDY

Securing A Travel Enterprise Across Clouds and Infrastructures

BENEFITS

1

Reduced Secrets Exposure

Entro's automation caught exposed API keys and passwords, preventing leaks in public repositories or Slack channels.

2

Faster Incident Response

Real-time alerts and automated fixes reduced response times, minimizing the impact of potential breaches.

3

Stronger Compliance

With better control over secrets, the enterprise could easily meet regulatory requirements like **GDPR** and **PCI-DSS.**

4

Developer Confidence

Developers felt reassured knowing that sensitive data would be flagged and managed automatically.

"We're very happy with the way Entro has detected the secrets in GitHub, Slack, Jira, and Confluence. It's made our lives easier by providing us with automated, real-time alerts for any sensitive information that might accidentally slip through the cracks. Not only has it improved our security posture, but it has also helped us establish a proactive culture where security is embedded in our workflow, instead of being an afterthought."

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