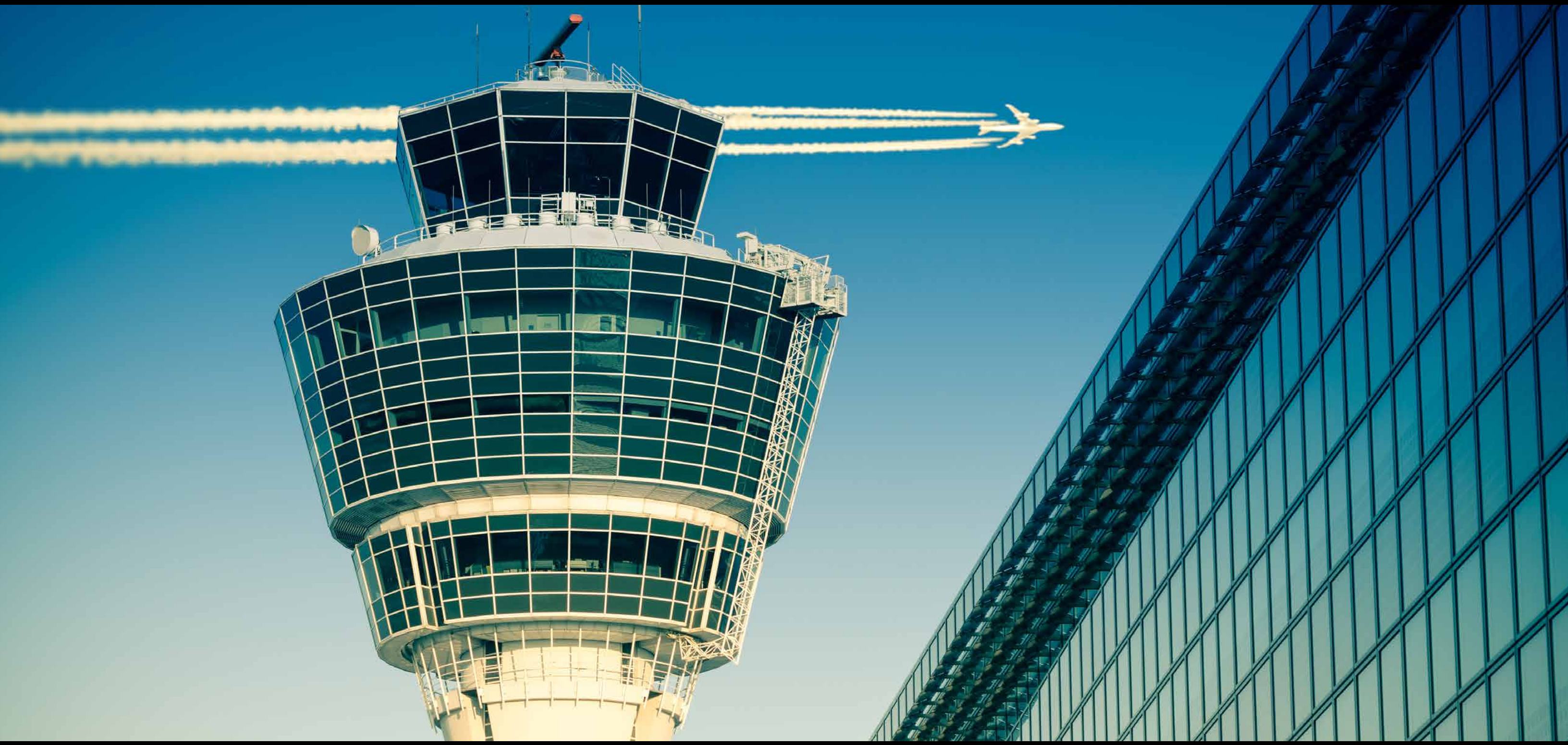
SpyCloud



Case Study

EUROCONTROL Strengthens Security and Cyber Awareness for the European Aviation Industry with SpyCloud

Overview

The European Organisation for the Safety of Air Navigation, or EUROCONTROL, is an intergovernmental organisation working to achieve safe and seamless air traffic management across Europe. EUROCONTROL's member states, comprehensive agreement states, and stakeholders, including navigation service providers, civil and military airspace users, and airports, work in a joint effort to make aviation in Europe safer, more efficient, more cost effective, and with a minimal environmental impact.

Challenge

When EUROCONTROL created its European Air Traffic Management Computer Emergency Response Team (EATM-CERT), the team was charged with seeking opportunities to enhance the organisation's security posture and increase cybersecurity awareness.

Solution

After an evaluation of services, the team selected SpyCloud Employee ATO Prevention as the first tool in its cybersecurity framework because they saw protecting users against account takeover (ATO) and ransomware as a high-impact opportunity.

Result

EUROCONTROL protects its 2,000 employees and 1 million constituent accounts on 130 domains from ATO that can lead to ransomware attacks, increases cybersecurity awareness, and provides enormous value to their security program with SpyCloud.

SpyCloud

Protecting the European Aviation Industry Against ATO and Ransomware

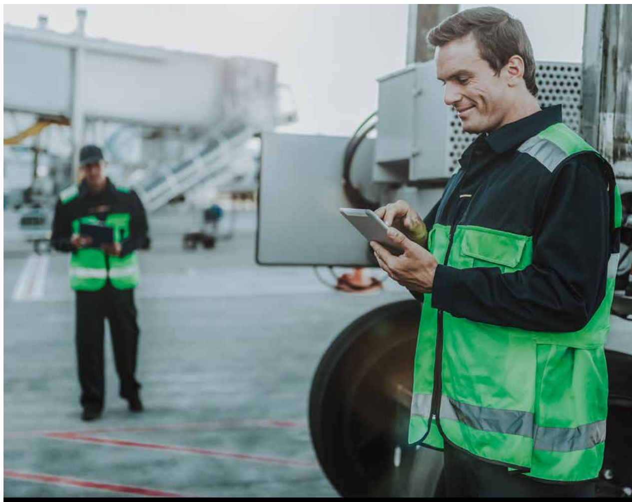
EUROCONTROL fulfills the European Union's commitment to "One European Sky" as an intergovernmental agency that supports aviation in Europe by delivering technical excellence and civil-military expertise across the full spectrum of air traffic management. The organisation consists of 41 member states, two comprehensive agreement states, and aviation stakeholders, including navigation service providers, civil and military airspace users, and airports. The agency's mission is to support operations, research, and innovation for the aviation industry across the continent.

When the European Air Traffic Management Computer Emergency Response Team (EATM-CERT) was created within EUROCONTROL in 2017, the team sought security solutions that would make a quick impact on the community by enhancing the organisation's security framework and also promoting cybersecurity awareness with their constituents. A key criteria for potential solutions was automation, since the team was new and had limited resources available to manage new programs.

"We are there to help the community and provide something that is adding value," said Patrick Mana, Cyber Security Program Manager and EATM-CERT Manager for EUROCONTROL. "We sought out new services that would make a difference to help our community of member states and stakeholders."

The team initiated the lengthy public procurement process in which services were evaluated in an open, fair and transparent manner, with considerations during testing including whether the service was useful, impactful, and cost and resource efficient.

One of the security challenges facing the aviation industry is "big game hunting," where cybercriminals target large, high-value organisations with ransomware. Aviation stakeholders, especially airlines and airports, manage a lot of personally identifiable information (PII) for passengers, which is an intriguing target for criminals as information that can be monetised.



> "We sought out new services that would make a difference to help our community of member states and stakeholders."

- Patrick Mana,
EATM-CERT & Cyber Security Program Manager

SpyCloud

“Aviation tends to be an attractive target for cybercriminals and state-sponsored groups because it is a critical infrastructure sector for a country, and for a lot of countries they are very much dependent on aviation. It can be an important element of the economy, as well as a source of national pride. For aviation, it’s really important to be protected because we are a target for hackers with enhanced capabilities for attacks,” Patrick explained.

SpyCloud Employee ATO Prevention was selected as the first value-added service for EUROCONTROL’s EATM-CERT program because it would make an immediate, high impact on the organisation by protecting accounts from account takeover and ransomware using insights from data recaptured from the criminal underground.

Previously, a national cybersecurity centre would alert EUROCONTROL of any breach notices and the team would handle that on a case-by-case basis as a result of an outside alert. Now with SpyCloud, EUROCONTROL proactively monitors and manages its employee and constituents’ user accounts to ensure compromised credentials aren’t being used within internal systems. SpyCloud Employee ATO Prevention protects 2,000 EUROCONTROL employee accounts and approximately 1 million constituent accounts from 130 domains against ATO and ransomware.

Additionally, SpyCloud created a feature to provide account views and dashboards for each individual constituent using the service. The EUROCONTROL EATM-CERT team was able to implement and manage the solution quickly and with ease, with the scalability to accommodate new constituents.

EUROCONTROL’s mission to achieve safe air space in Europe aligns well with SpyCloud’s mission to make the internet a safer place. While EUROCONTROL uses SpyCloud to protect against ATO and ransomware, another benefit of the solution is that it helps bring awareness to everyone’s responsibility to protect their credentials and identity.

> “Aviation tends to be an attractive target for cybercriminals and state-sponsored groups because it is a critical infrastructure sector for a country, and for a lot of countries they are very much dependent on aviation.”
>
> - Patrick Mana,
> EATM-CERT & Cyber Security Program Manager

"As we move toward digitalisation, people tend to be naive about digital assets. For example, they will protect their passport, but not their credentials. We're trying to convey the message that credentials are as important as your passport. It helps people understand the world we're living in and to behave in a more responsible way."

Offering SpyCloud Employee ATO Prevention to its constituents helps EUROCONTROL provide critical value-added services and strengthen its reputation. The agency's success is evidenced in the addition of new constituents over time.

Protecting a Million Accounts from ATO and Ransomware

With EUROCONTROL supporting all aspects of aviation in Europe, SpyCloud's Employee ATO Prevention protects the accounts for all EUROCONTROL constituents, including airlines, airports, and civil and military airspace users. While EUROCONTROL protects 2,000 of its own employees, the SpyCloud solution extends to its constituents, protecting approximately 1 million accounts from 130 domains from ATO. Since 2018, EUROCONTROL has been able to identify more than 300,000 vulnerable accounts and prevent potential ATO attacks.

Further, protecting against ransomware attacks in a critical infrastructure sector such as aviation is paramount to ensure the safety of employees, passengers, military personnel, and all those involved in the European airspace. EUROCONTROL is able to use insights on malware-infected users from SpyCloud to help constituents prevent attacks that can have serious consequences.

"We recently helped an aviation stakeholder identify that they had compromised systems," Patrick said. "Our ability to identify infected users was really beneficial because their cyber capabilities didn't detect that their system was subject to a cyber attack. It's via the information of the compromised account from EUROCONTROL that they further investigated and they found out that their system was attacked."

Since 2018, EUROCONTROL has been able to identify more than 300,000 vulnerable accounts and prevent potential ATO attacks.

SpyCloud

Bringing Value and Awareness to All Constituents

Working with SpyCloud allows EUROCONTROL to not only address security challenges, but also bring awareness to the value of security solutions by making it personal. For example, during the test phase, SpyCloud was able to show EUROCONTROL board members their personal exposure on the criminal underground. This information helped the organisation see the value and importance of investing in this type of solution.

"The biggest benefit of working with SpyCloud is raising awareness, really opening everyone's eyes and making a big difference with something tangible to individuals, including senior management. The beauty of it is showing that all staff in the organisation have a responsibility. Everyone is a door to enter the organisation, and each of us is a guardian of that door. It's not the business of just the IT security team. It's everyone's duty to behave in a way that will contribute to enhancing the level of resilience of the organisation. Because they are aware, they are careful and they are mindful about their responsibility with regard to their credentials," Patrick said.

Strengthening Security For Every Constituent Through Automation and Efficiency

EUROCONTROL is able to offer SpyCloud services to all of its constituents, many of which may not be able to procure such a service themselves due to challenges with the procurement process, financial constraints, or competing priorities.

"We help the community because the more companies that are aware of this kind of service and the benefits, the more they will be open to other cyber investments. It's a dynamic that we're creating to enhance the level of cyber culture," Patrick said.

With SpyCloud, EUROCONTROL and its constituents can automate activities, responses, and analysis so the teams can be more efficient and focus on other value-added projects.

"Having a certain level of automation is important because it allows us to conduct analysis that derives indicators and signals on a dashboard. It's super flexible, efficient and easy, so it gives our team the opportunity to spend time on other priorities rather than manual tasks related to monitoring for and remediating compromised credentials," Patrick said.

Bolstering Penetration Testing Capabilities with Recaptured Data

Password hygiene is critical for the organisations supported by EUROCONTROL. Many workers in the aviation industry are passionate about flying, and key phrases, aeroplane types or company names tend to show up in passwords, which is to be expected based on human behaviour. EUROCONTROL not only uses SpyCloud data to produce rainbow tables for penetration testing (pen testing), but it also plans to strengthen its overall password security and pen testing by developing an artificial intelligence/machine learning (AI/ML) application to identify aviation-related passwords based on SpyCloud's dataset.

"For an AI/ML tool to work, you have to train a model and for that you need a data set," Patrick said. "Since our users are interested in aviation, they may use passwords with aviation terms in them. That's where the SpyCloud service is really useful because most of the time, the passwords that have leaked can be cracked and therefore we can enrich our AI model with already known aviation-related passwords."

SpyCloud

Support Regulatory Compliance Preparedness

When industry and government regulations have significant impacts for noncompliance, having a strong security framework is critical to ensure requirements are being met. For example, a EUROCONTROL constituent may find that they aren't as prepared to meet regulatory requirements like GDPR, but having access to solutions such as SpyCloud Employee ATO Prevention through EUROCONTROL can strengthen their ability to comply.

"While there's no regulation in place that requires organisations to investigate whether credentials are exposed, the SpyCloud solution can be part of your arsenal to demonstrate that you're able to comply with the regulation. GDPR is tough and not everybody understands all the consequences of that immediately, so it may take a while to address the overall issue and the challenges around that regulation," Patrick said.

About SpyCloud

SpyCloud transforms recaptured data to protect businesses from cyberattacks. Its products leverage a proprietary engine that collects, curates, enriches and analyzes data from the criminal underground, driving action so enterprises can proactively prevent account takeover and ransomware, and protect their business and consumers from online fraud. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to over 150 cybersecurity experts who aim to make the internet a safer place.

Enterprise Protection

Prevent account takeover that can lead to ransomware.

Learn More

Consumer Protection

Combat account takeover and online fraud.

Learn More

Investigations

Unmask criminals attempting to harm your business.

Learn More

Data Partnerships

Enhance your solution with SpyCloud's data.

Learn More