

How to secure a digital-first airline

Effective security incident management helps Scandinavian Airlines (SAS) deliver a service customers can trust

Job to be done

Strengthen cyber security incident management to respond faster to threats

Solutions to do it

- ServiceNow® Security Operations Professional – Security Incident Response
- ServiceNow® IT Service Management

What we did

Consolidated six separate systems into one

Protecting critical national infrastructure

Scandinavian Airlines – commonly known as SAS – is one of the world’s largest airlines. Headquartered in Sweden, the business carries more than 28 million passengers a year who trust it implicitly with all their personal data. It has four million loyalty members and operates in 34 countries. It is a critical piece of Scandinavia’s transport infrastructure. The modern business is global, digital – and a highly attractive target to cybercriminals.

“ We’re a digital-first airline. Cyber security is foundational for our business.

Thomas Widen
Head of Cyber Security and Compliance
SAS

Digitizing an integrated workflow

Almost everything about the modern airline business is digital: the ticketing, meal planning, navigation systems, safety process. Digital touchpoints help make for a slick, seamless, global operation. SAS needs integration with logistics, financial payments, regulators, and more, to create an operational ecosystem. With data comes data risk. Airlines are a prime target for cybercriminals, whether they are looking to steal air miles or customers’ financial data, disrupting operations, or holding the business to ransom. Passengers are placing significant trust in their airline.

Integrated:

350+

systems as part of the SAS digital ecosystem

Now takes:

<60

seconds to register a cyber threat

And:

<10

minutes to contain the threat

Taking control and building visibility

Historically, SAS had outsourced much of its IT function. This decision delivered efficiency savings; the challenge for SAS was to strengthen the control and insight needed to navigate an increasingly digital business. By bringing certain management functionality in-house it would be better able to “drive its own destiny”, according to Thomas Widen, Head of Cyber Security and Compliance at SAS: “Safety has always been a priority for airlines. Today, that includes cyber security.” SAS’ main priority is keeping its passengers and their data safe.

“ ServiceNow establishes a unified source for cyber security incidents. Consolidation means we’re much faster to respond and resolve.

Thomas Widen
Head of Cyber Security
and Compliance
SAS

Management of the threat lifecycle

ServiceNow is central to the airline’s security posture. Security Operations Professional – Security Incident Response allows SAS to manage the lifecycle of security threats. SAS can now understand the nature of security incidents, spot trends, and deal with bottlenecks. For the first time, SAS has control of its own dashboards and reporting. It uses the performance monitoring capabilities to report KPIs like availability on all SAS business-critical systems. Threats are identified within one minute, contained in less than ten minutes, and analyzed within the hour.

Achieving further clarity

Today, SAS – recently ranked number one in the Internet Foundations Report – is more efficient and proactive in the way it deals with and hunts down cyber threats. For example, SAS now runs competitions for office workers to identify and report phishing scams. And many manual tasks are now automated; Thomas’ team are more productive. ServiceNow is an example of SAS’ future IT strategy: cloud-based solutions, SaaS, integrated workflows, and in-house visibility. Discussions are underway around the use of ServiceNow across HR, finance, and further IT projects including developing biometric access for ground staff working in sub-zero temperatures (where it is too cold to remove gloves and key in a passcode).

Now you know how work can work better.