Forcepoint

Customer Story

Major U.S. Airline Rapidly Deploys Unified Security Solution and Staff Capabilities Soar

One of the world's largest airlines achieves comprehensive data protection with Forcepoint DLP to meet the GDPR deadline, and makes even less-experienced analysts more effective and efficient.

This global U.S. airline faced a confluence of security challenges, any one of which could cause major disruptions to its business or potentially compromise millions of travelers' personal data and safety. The company was racing to become GDPR compliant within the EU deadline. Its staff wrestled with disconnected point products that seriously slowed the identification of growing threats. And a tight worldwide cybersecurity labor market forced it to rely on more junior analysts than it had in the past, creating further inefficiency. Realizing it had to act quickly to upgrade its security, the company partnered with Forcepoint to deploy a holistic data protection solution that could meet these security challenges in one stroke.

CUSTOMER PROFILE:
This Fortune 500 airline operates daily flights in more than 50 countries with 80,000 staff and $40 billion in revenue.

INDUSTRY:
Airline

HQ COUNTRY:
United States

PRODUCT:
Forcepoint DLP Suite: Discover, Endpoint, and Network

The high stakes of storing high-value data

In 2018 alone, cybersecurity breaches at major airlines exposed the personal data of more than 10 million passengers worldwide. Passengers entrust airlines with a wealth of sensitive personal data—names, addresses, dates of birth, state and national identification and passport numbers, and credit card information—making airlines an inviting target for theft. In this highly competitive industry, any breach can create a dent in customer trust and leave an opening for the competition to swoop in.

Perhaps even more unsettling is the danger of having proprietary data, including flight information, flight lists, and flight records, fall into the wrong hands. The potential for terrorist or adversarial nation-state activity makes safeguarding this data a life-or-death necessity.

Yet protecting critical data in this unique, high-stakes environment isn't easy. Globally distributed air carriers need fast, secure access to data to provide the highest level of customer service. This is encouraging industry movement to the cloud, which presents its own problems such as gaining visibility and controlling movement of data. Additionally, the continued reliance on some legacy IT systems can hinder innovation, since upgrades increase the risk of downtime. At best, business slowdowns cause customer service headaches and potentially cost millions in revenue. At worst, they create a risk to passenger and crew safety.

Closing the gaps from the inside and out

When this large U.S. airline first contacted Forcepoint, it wanted to more effectively safeguard its customer and proprietary data from internal and external vulnerabilities. This included its fast-growing cloud infrastructure. With tens of thousands of employees and dozens of locations globally, that alone was a massive challenge. But there was another wrinkle that greatly increased the pressure: meeting the European Union's looming GDPR compliance deadline.

The company's cybersecurity team was spinning its wheels with a stack of point products that focused more on external rather than internal threats, leaving gaps inside the organization where data could fall through the security cracks. To make matters worse, the point products also left cybersecurity staff overwhelmed with alerts—many of them false positives—and unsure how to efficiently and effectively investigate and respond.

As if that wasn't enough, the worldwide talent shortage in cybersecurity meant there were more junior-level employees than in the past, slowing analysis and adding to the indecision. "There's a lack of people resources in the field," explained Justin Truglio, Forcepoint account executive. "When you get an organization as large as this, it's likely you won't have enough people to do what you need."

For these reasons, the carrier needed a comprehensive solution that would safeguard data and supercharge what its staff could do. And it needed that solution up and running, enterprise-wide, ASAP.

Taking a holistic approach and speeding to deployment

"We didn't want to just sell them a piece of software, because we didn't want them to be in the same boat with our solutions as they were with their other applications," said Beasley. "Instead, we built a partnership with the organization to develop a holistic, best-practice data protection program with the full Forcepoint DLP Suite as the foundation."

Speeding installation was the next hurdle. The carrier wanted full-blown deployment for its 80,000 employees as soon as possible. The solution's scalability, made possible by a virtual architecture environment, proved up to the challenge.

Challenges

Sensitive customer and enterprise data, on its network and in the cloud, created a ripe target for hackers or terrorists.

GDPR requirements for data security.

Staff overwhelmed with false positives generated by a stack of point cybersecurity products.

Approach

Implement a holistic data protection program with Forcepoint DLP Suite and staff training.

Blocking threats in record time

Forcepoint DLP provided a certifiably quick time-to-value. One of the top advantages for the organization was the predefined, prebuilt policies that come with Forcepoint DLP. "We do a lot of the heavy lifting up front, which helped them achieve quicker time-to-value and meet the compliance requirements of GDPR," explained Truglio.

In addition, predefined policies empowered the organization to move from audit to block mode more quickly than it would have with Forcepoint competitors. The quick move to automated enforcement, along with the solution's built-in analytics and automated risk ranking, almost immediately made the burden of investigations lighter, since investigators no longer had to look at log minutae to see what was what. "A lot of people who purchase our competitors' DLP systems remain in audit mode and don't actually block anything because of issues they have with false positives," said Truglio. Its ability to key in on the riskiest events, combined with customized policies that were easy to create and deploy, allowed the airline to go into full blocking mode much faster.

Recognizing real risks quicker

Forcepoint's incident risk ranking is the first page analysts see when they access the solution dashboard. Incident risk ranking uses the product's built-in analytics to give the security team a snapshot of the events they need to focus on first. This greatly reduces the time-wasting drill of unnecessary investigations, and helps investigators—even junior analysts—quickly recognize events, act faster, and reach conclusions with a high degree of confidence. The entire staff moved with a speed and efficiency that, compared to previously, could only be measured in hundreds of percent improvement. And meeting GDPR requirements was no longer an issue.

Employees working better in a more secure workplace

The built-in analytics have also helped the organization become more attuned to its people and their interactions with data. Upon deployment, Forcepoint DLP builds a baseline of "normal" behavior at both the organizational and individual levels to identify anomalous activity. It also correlates and groups related incidents and events into meaningful DLP cases instead of looking at them as disparate events. This reduces false positives by providing a fuller contextual picture of employee activity and allows cybersecurity staff to prioritize and respond to the most serious threats. Staff now feel empowered to take action with confidence, able to identify those threats, and swiftly respond. The frustration and indecisiveness has disappeared.

The airline's partnership with Forcepoint has helped it achieve a holistic and meaningful view of its data at rest, in use, and in motion—even across integrated enterprise cloud applications.

"It's great to be a part of it," Beasley said. "There's nothing more fulfilling than a partnership that accomplishes what it sets out to do."

Results

- **Greater visibility** of data at rest, in use, and in motion.
- **Reduction** in false positives.
- **Achieved** GDPR compliance.
- **All staff empowered** to take action with confidence.