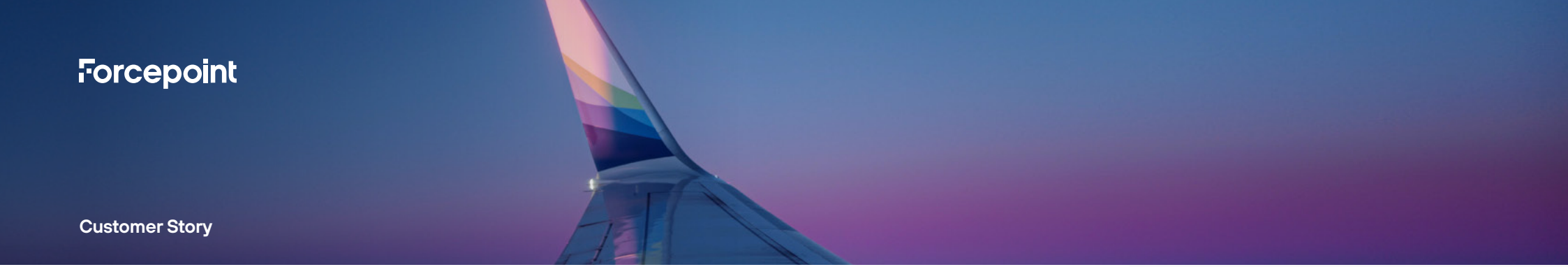


Forcepoint

Customer Story

Global Aviation Leader Flying High with Data Security Everywhere

A global aviation leader with over a century of history operates across the United States, the United Kingdom and Mexico. Leading its IT security efforts is the Vice President of IT, who oversees a compact yet highly skilled team. With three CISSP-certified engineers, the VP of IT describes the team as "small but mighty," emphasizing their expertise and passion for security. "I'm just really fortunate to have the team I have," they shared.

Despite the team's modest size, their responsibilities are vast, encompassing compliance and security across the organization's footprint in global operations. From managing firewalls to navigating data challenges, the team safeguards the organization's assets in an increasingly complex digital world.

Global aviation cybersecurity compliance frameworks are thorough, tackling security risks from various perspectives to ensure comprehensive protection. For example, ICAO's (International Civil Aviation Organization) strategy ensures global cooperation and incident management, crucial for mitigating cyber threats across borders. Another example is EASA Part-IS (European Union Aviation Safety Agency), which mandates robust security management systems, ensuring airlines and aviation stakeholders proactively manage cybersecurity risks that could impact safety.

CUSTOMER PROFILE:

A global aerospace company specializing in propulsion systems, aircraft structures, and MRO services for commercial, business, and defense aviation sectors.

INDUSTRY:

Aerospace Industry

HEADQUARTERS:

United States

PRODUCT:

- Forcepoint Data Loss Prevention (DLP)
- Forcepoint Cloud Web Security
- Forcepoint Email Security

Optimizing IT Security with Forcepoint DLP

To address their unique IT security needs, the team relies on Forcepoint DLP, which has become a cornerstone of their security strategy. The VP of IT highlights the tool's ability to identify and protect critical data with unparalleled accuracy.

The ability to remotely access and manage security tools has made Forcepoint's solution an indispensable asset in their operations. By simplifying processes and providing robust functionality, Forcepoint helps the IT team to work more efficiently while maintaining a strong security posture.

As a global aviation leader, this customer relies on a suite of IT security solutions, including:

→ **DLP:** A foundation for identifying, protecting and managing sensitive data, DLP has become increasingly effective in detecting and securing information across multiple channels. The VP of IT described it as 'awesome because I can do discoveries; I can find things.' The enhanced accuracy leveraging Forcepoint DLP can be found in several applications:

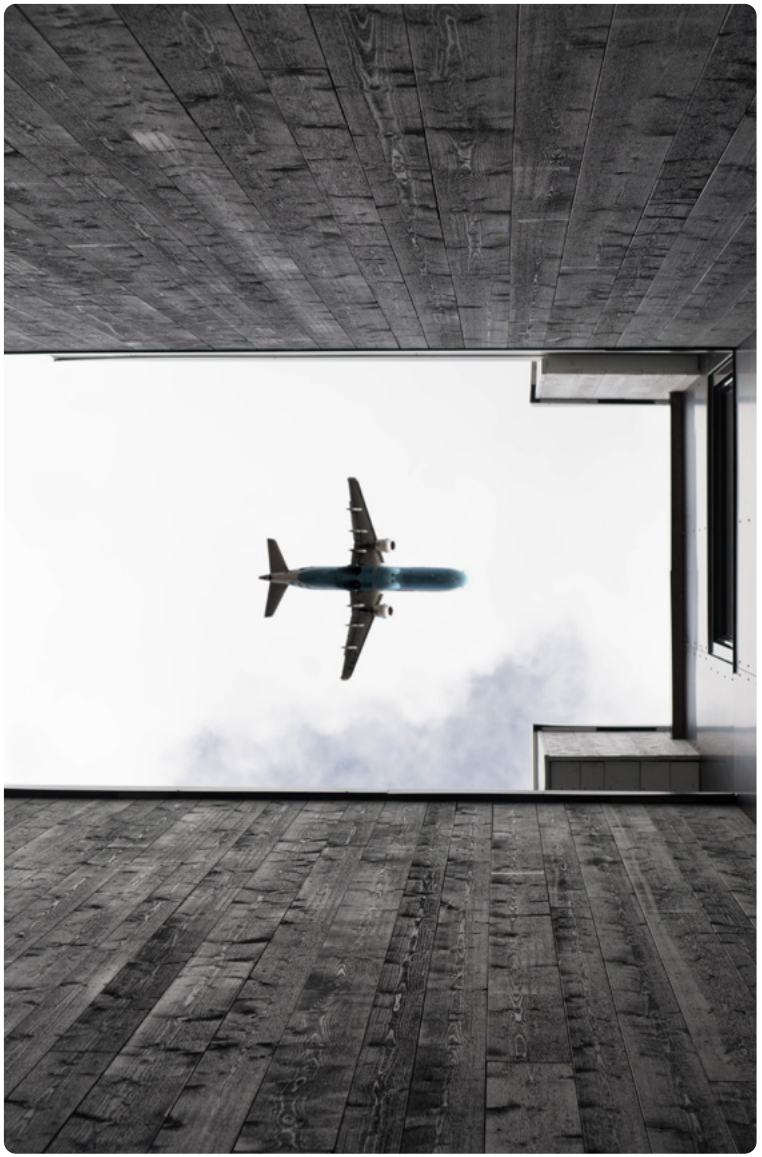
- **Unified Policy Management Across All Channels:** Industry-leading DLP allows a single policy to be enforced across endpoints, SaaS applications, email and web. This unified approach reduces complexity, ensures consistent data protection and simplifies compliance mandates by reducing security gaps and streamlines compliance audit readiness.
- **Precise Data Classification:** AI-powered data classification ensures highly accurate identification of sensitive data, enabling precise DLP enforcement that reduces false positives. Forcepoint uses a multi-layered strategy incorporating NLP, fingerprinting, file type detection, regex, compliance keywords, metadata tags and more to identify and protect data across environments.
- **Risk-Adaptive Protection:** By monitoring user activity and assessing risk, this dynamic solution tailors enforcement actions to each situation for each user. This adaptive security approach helps prevent data loss without getting in the way of legitimate work.
- **Offline Data Loss Control:** Forcepoint DLP policies remain active even when users are offline or disconnected from the corporate network, providing continuous protection in hybrid and remote work environments. This ensures sensitive data stays secure regardless of connectivity or device location.

- **Email Security Gateway, Web Security Gateway:** These tools **provide seamless and secure access across the organization and** are essential for maintaining data integrity and protecting against cyber threats. By extending the controls of DLP across web and email channels, organizations can ensure sensitive information remains safeguarded, regardless of how it's accessed or shared. This approach allows security policies to be consistently enforced across multiple communication and collaboration platforms, mitigating risks such as unauthorized data transfers, phishing attacks and accidental leaks.

  The global aviation leader's journey underscores the value of intuitive, efficient IT security solutions. The VP of IT applauded Forcepoint's decision to strengthen its email security gateway: **"I think your decision to make [Email Security] stronger is probably one of the best things that Forcepoint's done."**

- **Remote Browser Isolation (RBI)** takes security a step further by embedding a Zero Trust approach into web access. RBI ensures that users interact with web content in a fully isolated environment, preventing malicious threats from ever reaching the endpoint. By assuming that all web interactions could be risky, RBI eliminates the possibility of malware infections from compromised sites while still allowing seamless browsing. This layered security strategy enhances organizational protection by neutralizing web-based threats without disrupting productivity, providing the ultimate safeguard for employees navigating the internet.

The intuitive interfaces are among the standout features of Forcepoint's solutions. In transitioning from a Cisco Umbrella background, they were 'very pleasantly surprised' at the ease of using Forcepoint's solutions. This simplicity has made Forcepoint's tools more accessible and efficient, enabling the team to navigate and manage security tasks seamlessly. The VP of IT shared their experience: **"Everything is right there in tab format... It's also web-based, so we can get to it from anywhere on our mobile phones."** This accessibility has been instrumental for their team, enabling them to resolve issues in real-time, even outside regular business hours. They elaborated, **"If we're out and about on the weekend and someone says, 'Hey, I've got this email locked up,' we can release it from anywhere."** This capability has been helpful in supporting executives working around the clock, enabling the IT team to resolve issues efficiently and effectively.



AI in a Complex IT Landscape

The global aviation leader faces pressing challenges as artificial intelligence (AI) rapidly evolves and reshapes industries. At a recent CISO conference, attended by over 100 IT professionals, the Vice President of IT observed a common concern among participants: balancing the executive push to embrace AI with the need to protect sensitive organizational data. They shared, **"Every CISO in the room... has an executive team that's ready to run headlong into AI. But even Microsoft is not going to protect your data from the models."**

This tension underscores the difficulty of safeguarding data in an AI-driven world. The VP of IT elaborated on the risks: **"The more things that you push out there, the more your company becomes exposed."** As AI models grow more powerful, the task of managing data becomes increasingly important and increasingly complex, especially when dealing with controlled and classified information.

The challenges extend beyond AI itself to the broader issue of data governance. The VP of IT noted, **"The second topic [at the conference] was how in the heck are we gonna manage data? How do you protect it?"** The complexity of unstructured data combined with the limitations of metadata tagging adds another layer of difficulty, as **"meta tags are only as good as the system they're in."**

Despite these challenges, the VP of IT remains hopeful about tools like Forcepoint DLP, which can assist in data discovery and protection. AI integration in cybersecurity requires balancing innovation with protection, especially in data-driven industries. Advanced security solutions from Forcepoint, including DLP, Data Detection and Response (DDR) and Data Security Posture Management (DSPM), help organizations safeguard and classify sensitive data, ensure data governance and protect sensitive data from potential data breaches. Further, Forcepoint's recent acquisition of Getvisibility expands capabilities beyond DLP, strengthening data discovery, classification and security posture management.

Forcepoint leverages advanced AI for highly accurate data classification and precise enforcement. Forcepoint DSPM—featuring its specialized AI Mesh technology—enhances visibility into sensitive data across multiple environments. Integrated with DSPM and DDR, Forcepoint DLP strengthens data security across every channel, delivering a unified approach to protecting data and users everywhere. These capabilities are increasingly vital as cybercriminals integrate generative AI into malicious activities and as more organizations process sensitive data through AI models, heightening risks of data leakage and exfiltration.

Lessons Learned: A Forward-Looking Perspective

As they navigate the challenges of a data-driven world, this global aviation leader and their team continue to adapt and innovate, leveraging robust tools and partnerships to safeguard their operations.

Forcepoint DLP has empowered the organization to enhance its data discovery capabilities with high accuracy across a wide set of regulated data and intellectual property, while streamlining its security processes. They emphasized the solution's effectiveness in managing data and reducing false positives. The tool's robust features have enabled their team to stay ahead of potential threats and protect sensitive information with confidence.

The organization's experience with Forcepoint extends beyond the technology itself. Collaboration and support have played a critical role in their success. Whether troubleshooting technical challenges or optimizing the solution's capabilities, the partnership has contributed to the IT team's ability to safeguard the company's operations.