
accenture
Cybersecurity in Aviation:
Mitigating Risk,
Maximizing Growth

Contents

03 **Executive Summary**

05 **Soaring into the digital future**

07 **When opportunity increases risk**

08 **Innovation and cybersecurity challenges**

09 **Risk-proofing the future**

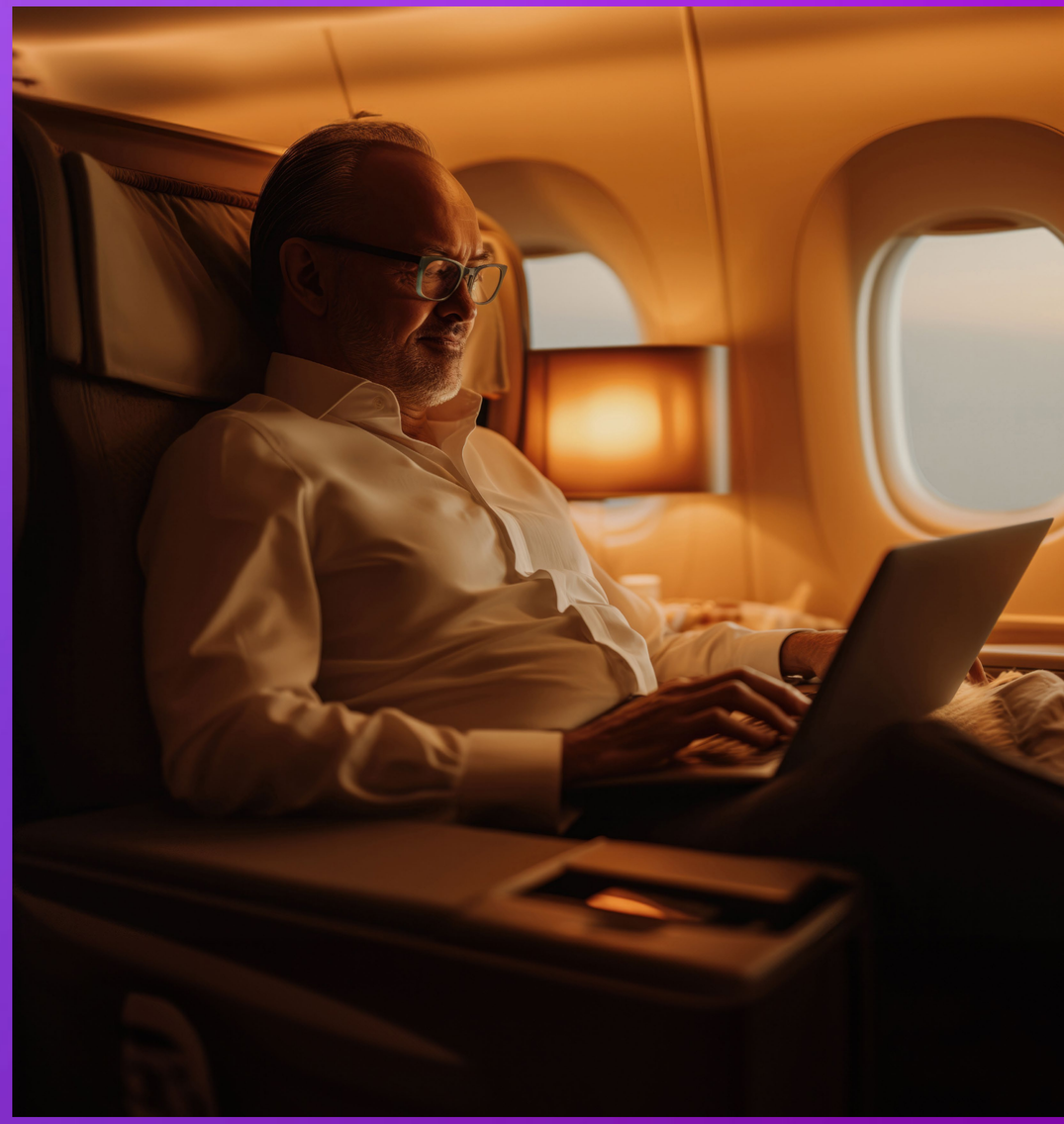
Step 1 Strategize: Embed cybersecurity into core strategies and establish shared accountability across people and organizations

Step 2 Modernize: Modernize and adapt security measures to match the speed of business innovations

Step 3 Re-imagine: Harness AI for proactive and adaptive defenses

13 **Getting started**

14 **About the research**



Executive summary

The aviation industry is at a pivotal moment of transformation: technology-driven growth opportunities and glaring security vulnerabilities are colliding. Airlines and airports are rapidly adopting AI, cloud platforms and hyper-personalized services to redefine travel experiences and create new revenue streams. United Airlines flights, for example, are becoming marketplaces with targeted advertisements on seat-back screens.[1] Saudia Airlines is using chatbots powered by generative AI (gen AI) to redefine how travelers plan, book and manage trips through a conversational interface.[2] Our recent survey of 300 leaders (including 250 CXOs) from the aviation sector showed confidence is soaring—92% of aviation leaders believe their digital offerings rival top online retailers, and 70% expect new business model revenues to grow within six months. But this rapid transformation carries a serious risk.

Passengers expect seamless digital experiences, but trust and safety are non-negotiable. A staggering 83% of airline consumers say they would lose faith in a brand after a data breach.[3] Yet cybersecurity readiness across the aviation industry remains dangerously inadequate. Only 21% of airlines have robust cybersecurity frameworks, and industry benchmarks for information security controls and best practices are far below optimal levels, leaving critical systems vulnerable to attack.

As airlines and airports expand their digital ecosystems, they rely increasingly on interconnected systems, third-party services and real-time data sharing—essential for growth, but also fertile ground for cyber risks. Cyber threats are escalating at an alarming rate. GPS spoofing incidents—where false signals mislead navigation systems—have skyrocketed from just a few dozen per day in February 2024 to over 1,100 per day by August 2024.[4]

While airlines are investing billions in digital innovation, security is often an afterthought—treated as a compliance exercise rather than a strategic priority. The disconnect is undeniable. CEOs acknowledge the potential hazards, yet 83% admit their cybersecurity efforts are driven primarily by compliance, not proactive risk management.[5] Threat detection ranks among the lowest capabilities in the National Institute of Standards and Technology (NIST) framework, and nearly 50% of airlines operate with outdated information security systems.[6] Further compounding the issue, 83% of Heads of Security lack representation on board committees, reflecting a leadership blind spot that leaves critical operations exposed.[7] This lack of visibility leaves decision-makers blind to emerging threats, further widening the security gap.

The stakes are too high to ignore. Without embedding cybersecurity as a foundational pillar of digital transformation, airlines and airports risk catastrophic data breaches, ransomware attacks and operational disruptions that could derail their ambitions. What's more, innovation and growth cannot survive without safety and trust. Now is the time for aviation CEOs and boards to take decisive action to close the cybersecurity posture gap, ensuring progress isn't overshadowed by preventable risks. The future of aviation depends on it.





To achieve this, aviation company leaders need to take three distinctive steps:

1. Strategize: Organizations must embed cybersecurity into their core strategy, treating it as a fundamental pillar of safety and operational resilience rather than a separate IT concern. This requires integrating security measures into every layer of airline and airport operations—including flight systems, air traffic management, maintenance and passenger services—while ensuring compliance with evolving regulations.

2. Modernize: Cybersecurity must be adaptive, resilient and seamlessly integrated into every facet of the industry. This requires modernizing legacy systems, embedding security into next-generation aviation technologies and adopting dynamic frameworks that evolve alongside advancements in aircraft systems, air traffic management and passenger services.

3. Re-imagine: Gen AI has the potential to revolutionize cybersecurity in aviation by enabling proactive and adaptive threat defenses across airline and airport operations. It can analyze vast aviation datasets—including flight telemetry, passenger data and air traffic communications—to detect anomalies, predict cyber threats and automate response measures in real time.

By embracing these steps, aviation companies will set the stage for a future where security and innovation go hand in hand. Those leading the charge will not only mitigate cyber risks but will also gain a competitive advantage —by improving passenger confidence, enhancing operational efficiency and driving sustained growth and resilience.

Soaring into the digital future

The aviation industry is fundamentally reimagining the air travel ecosystem, striving to enhance convenience, sustainability and resilience in response to a rapidly evolving global landscape. At the heart of this transformation lies technology, serving as both a catalyst and enabler, redefining the passenger experience while addressing complex operational challenges. Nearly three-quarters of aviation industry leaders we surveyed (72%) believe their technology investments are at least meeting requirements for innovation and competitive advantage.

With customer acquisition, operations and other costs set to rise and competition intensifying, airlines are rethinking their traditional models to maximize efficiency and create new revenue streams.

Advanced technologies like artificial intelligence (AI), extended reality and cloud-based platforms are allowing airlines to deliver personalized passenger experiences, streamline operations and drive revenue growth through innovative partnerships and business models. From integrating retail into flights and airports to leveraging data-driven insights for tailored offers, the aviation sector is evolving into a dynamic ecosystem where commerce and travel converge. In fact, 92% of aviation leaders surveyed believe the digital experiences they offer are at least as good as those from online retailers. Seventy percent expect to see revenues from new business models increase in the next six months.

70% **of executives expect to see revenues from new business models increase in the next six months.**



Examples include:

Redefining the passenger journey

From curated recommendations to dynamic pricing, AI is reshaping how passengers interact with airlines. Airlines are leveraging gen AI to transform trip planning, booking and personalized experiences, with 82% still in early stages and 15% scaling chatbot capabilities. Saudia, for example, is launching a gen AI-powered platform to streamline travel planning through a conversational interface.[8]

> United Airlines is making waves with its own approach to personalization. By tapping into passenger data like preferred destinations and travel classes, the airline now delivers tailored seat-back advertisements. This innovation isn't limited to marketing—it's transforming flights into opportunities for curated retail experiences. Partnerships with luxury brands, targeted loyalty offers and duty-free shopping experiences onboard are turning flights into vibrant marketplaces.[9]

Personalization in the cloud

Cloud-based platforms are driving aviation's digital transformation, enabling seamless operations and personalized passenger experiences. With open, modular designs, airlines can integrate third-party services, streamline bookings and unify ancillary offerings for greater efficiency and customer satisfaction. Partnering with tech firms, airlines use real-time data to optimize revenue strategies and stay competitive. While only 19% have adopted cloud-based platforms, 77% are in the early stages of adoption, highlighting the industry's shift toward cloud-driven innovation.

> Riyadh Air has created the world's first fully cloud-based airline. The airline ensured its digital core is future-proof and scalable through cloud-only infrastructure, enhanced cybersecurity and AI-driven operations, provided through a partnership with Accenture. This strong, collaboration-based digital foundation will allow Riyadh Air to rapidly expand, supporting its goal of operating over 100 destinations by 2030.[10] AI-facilitated personalization includes options like last-minute fast track opt-ins should a guest be running late. Passengers can also seamlessly book hotels, lounges, taxis, or even concerts or football tickets when booking flights, ensuring everything needed for their full travel itinerary is completed instantaneously and solely on the Riyadh Air shopping cart. [11]

Smart airports

Shifting from B2B to consumer-focused models, smart airports—Airport 4.0—deliver personalized, flexible journeys from booking to arrival. Smart technologies like IoT, big data, blockchain and cloud computing improve efficiency and passenger experiences. Real-time data helps airports collaborate seamlessly with stakeholders for smarter decisions and resource allocation. AI-powered video analytics, adopted by 15% of airports in our survey, enhance surveillance, monitor passenger flow and predict congestion. Eighty-one percent of airports are piloting or ideating such uses and are on their way to data-driven operations.



When opportunity increases risk

The rapid tech revolution is propelling airlines and airports into uncharted territory, bringing with it new opportunities and significant risks. Managing modern technology architectures, navigating multiple digital ecosystems and countering an ever-shifting cyber threat landscape have exposed airlines to increased vulnerabilities. While new business models focus on enhancing customer trust through improved travel experiences, the evolving cyber threat landscape jeopardizes this very foundation. Our research, including a survey of over 18,000 respondents, shows a staggering 83% of airline consumers say they would lose faith in a brand after a data breach.

Most airlines and airports still have legacy technologies in their architecture, making integrating new technologies like cloud, gen AI and extended reality a tedious and difficult task. Any gap in the integration increases the attack surface area for threat actors to exploit. Moreover, when adopting new technologies, companies often prioritize speed over security. Neglecting early security integration increases risks and prolongs remediation efforts. A reactive approach also accumulates technical debt, leading to costs far greater than if security had been embedded from the start.

Consider these alarming trends:

- Cyberattacks in the aviation industry surged by 24% in the first half of 2023.[12]
- GPS spoofing incidents jumped from a few dozen daily in February 2024 to over 1,100 by August 2024.[13]
- Ransomware mentions targeting aviation on the dark web more than doubled in 2023,[14] with 61% of UK[15] and 55% of US aviation[16] cyber leaders reporting ransomware attacks in the past year.
- Sharing data (38.01%) and selling data (34.39%) emerged as the most common dark web activities related to data theft involving aviation in 2023.[17]

Aviation industry as a target

> A vulnerability in an Asian airline's software led to a massive data breach, exposing 6.5 terabytes of data including the personal details of flight crews. The breach stemmed from a misconfigured Amazon Web Services bucket. Safety detectives found 23 million files, including sensitive flight charts, navigation data and plain-text passwords.[18]

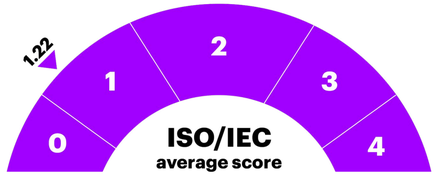
Innovation and cybersecurity challenges

As airlines soar into a future powered by cutting-edge technologies and transformative innovations, they face a stark reality: innovation without robust protection is a recipe for disaster. Shockingly, only 21% of airline companies have established a mature cybersecurity framework. Similarly, only 20% of airports have a comprehensive framework in place for cybersecurity, leaving the majority vulnerable to escalating threats. Security benchmarks reveal critical gaps, with airlines scoring a mere 1.22 (out of 4) and 1.28 (out of 4) on the International Organization for Standardization/ International Electrotechnical Commission (ISO/ IEC) and NIST frameworks respectively—far below optimal levels. The deep dive into benchmark results and our work with industry experts highlight three major hurdles:

- Cybersecurity is often viewed as a technical or compliance-driven function, not a business risk. For most airports and airlines, cybersecurity is not a board level agenda. In fact, 83% of travel industry CEOs say that compliance drives their cybersecurity strategy.[19] Moreover, our additional survey of 12 airlines shows that in eight out of 10 cases, the "Head of Security" is not part of a board committee.[20]
- Due to the rapidly evolving threat landscape, airlines and airports also struggle to detect threats in time to avert disruption. This lag can disrupt operations, compromise passenger safety and expose sensitive data, leading to financial losses and erosion of customer trust. In the NIST framework, detection scored the lowest on the assessment (0.97 out of 4) with the implementation rate of detection practices scoring 0-5% out of 100%.
- Inadequate security controls for technology and data poses a third major concern. A lack of security measures leads to blind spots that threat actors can exploit to take unauthorized control of systems or cause data loss. Nearly one in two airlines has neither implemented nor updated an Information Security Management System.[21] In fact, only 39% of airline, travel and transport companies have a continuous mechanism for real time threat detection across IT and OT systems.[22]

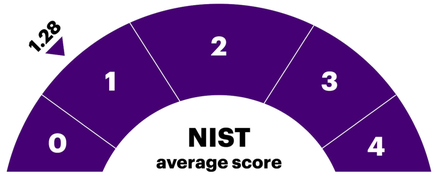
Figure 1: ISO and NIST Benchmark

The ISO/IEC 27002:2002 provides the detailed best practices and control objectives related to key cybersecurity aspects. Airlines scored just 1.22 while the (Commercial) Banking industry scores an average 3.15, using the same conditions.



Controls	Score
Organizational controls	1.16
People controls	1.46
Physical controls	1.36
Technological controls	1.21

The 5 functions of the NIST CSF v1.1 provide a comprehensive view of the lifecycle for managing cybersecurity risk over time.



Controls	Score
Identify	1.37
Protect	1.35
Detect	0.97
Respond	1.21
Recover	1.09

Source: Aviation Benchmark study

Risk-proofing the future

To overcome these challenges that increase vulnerability, airlines and airports need to take three steps to enhance their cybersecurity posture.



Step 1
Strategize

Embed cybersecurity into core strategies and establish shared accountability across people and organizations

Without a clear understanding and quantification of the risk environment, effective mitigation becomes nearly impossible. CEOs and boards must consider cyber complexities when first designing their strategies. When leaders recognize the importance of cyber risk management as a business enabler and understand its benefits, they are more likely to implement effective practices from the outset. Cybersecurity should be seen not just as a compliance issue but as a crucial business necessity and a competitive advantage.

Actions to take:

1. **Integrate cybersecurity into the business strategy from the outset.** Senior leadership should endorse and champion a risk assessment framework to guide business decisions and tech investments. In today's environment, aviation companies also need advisory strategies to monitor and address cyber and supply chain risks, especially those arising from geopolitical tensions.

2. **Instil a culture of shared accountability across the C-suite.** Accountability within leadership teams includes incentives and consequences based on specific roles. CFO and COOs, for example, must govern the playbook and process for determining and reporting the financial impact of cybersecurity incidents. This requires insights from other leaders in the organization. Business heads understand transaction volumes and business loss impacts. IT leaders know the interdependencies of applications, infrastructure and processes. The CHRO should lead efforts to recruit and upskill cybersecurity talent in a competitive market and work with the CISO and other leaders to strengthen security awareness. This helps address the human risk factor in cybersecurity.

3. **Incorporate third-party vendors into your strategy.** Acknowledge the crucial role of the supply chain and prioritize collaborations with vendors that demonstrate robust cyber resilience. Develop and enforce tailored policies and controls for third parties, and actively involve them in joint cyber crisis assessments, preparations and simulations. For a comprehensive view of cyber risk factors involving third and fourth-party vendors, establish a supply chain cyber risk management program that utilizes multiple data sources such as government threat intelligence data and automated analysis.

4. **Review cyber risk assessments throughout the lifetime of all critical strategic initiatives.** Integrating continuous cyber risk management is essential when launching new products, expanding services, making acquisitions, or establishing operations in new locations. A proactive approach helps quantify and address potential cybersecurity vulnerabilities in business strategies. Leaders should establish clear metrics and require comprehensive reporting on how, when and where security measures were integrated, including identified risks and implemented solutions throughout the strategic planning, execution and the entire lifecycle of any business initiative.

Step 2
Modernize

Modernize and adapt security measures to match the speed of business innovations

Modernizing security to keep pace with business innovation requires continuously updating security measures to protect emerging technologies and new processes. As businesses evolve, security programs must adapt at the same pace to prevent vulnerabilities, ensuring that innovation is both secure and sustainable.

Actions to take:

1. **Introduce security by design in innovation and operation.** The aviation industry must embed security into every stage of digital transformation, ensuring new innovations are secure by design while addressing vulnerabilities in legacy systems. Security cannot be an afterthought—it must evolve alongside business growth, extending beyond traditional IT functions to enhance overall resilience. CEOs must move beyond compliance-driven cybersecurity and integrate it into operational resilience. This means assessing security effectiveness across flight operations, passenger services and maintenance, conducting regular risk evaluations and embedding cybersecurity into crisis management. Cross-functional collaboration between business, IT and security teams is critical to aligning cybersecurity investments with operational risks. True resilience requires a strategic, business-wide approach that safeguards both innovation and critical operations.

2. **Implement Zero Trust architecture.** A Zero Trust approach treats every access attempt as potentially unauthorized, irrespective of the user's identity or network location. A good starting point for adopting Zero Trust is Secure Access Service Edge (SASE). As organizations embrace digital transformation and transition security to the cloud, SASE integrates networking and security into a unified cloud service. This consolidation reduces complexity, boosts agility and secures multi-cloud SD-WAN architectures.

3. **Modernize Identity and Access Management.** Airlines must implement modern identity management solutions and move away from legacy solutions more than five years old. To mitigate the risk of password leaks and sharing, they should implement passwordless authentication. Passwordless solutions enhance security by eliminating the risks associated with password theft and misuse, ensuring that only verified users can access sensitive systems and data.

4. **Secure Cyber-physical systems (CPS).** CPS, like electronic flight control systems, RFID tagging in bagging and Smart Grid systems at airports, create value, and disruptions can halt production or cause mission failures. Increased connectivity expands the attack surface, making these systems targets for ransomware and malware. Organizations must identify and secure all CPS, and regularly test them for vulnerabilities.

5. **Implement key security principles to secure tech and data.** Airlines need to apply key security principles to safeguard their data and technology.

These principles include:

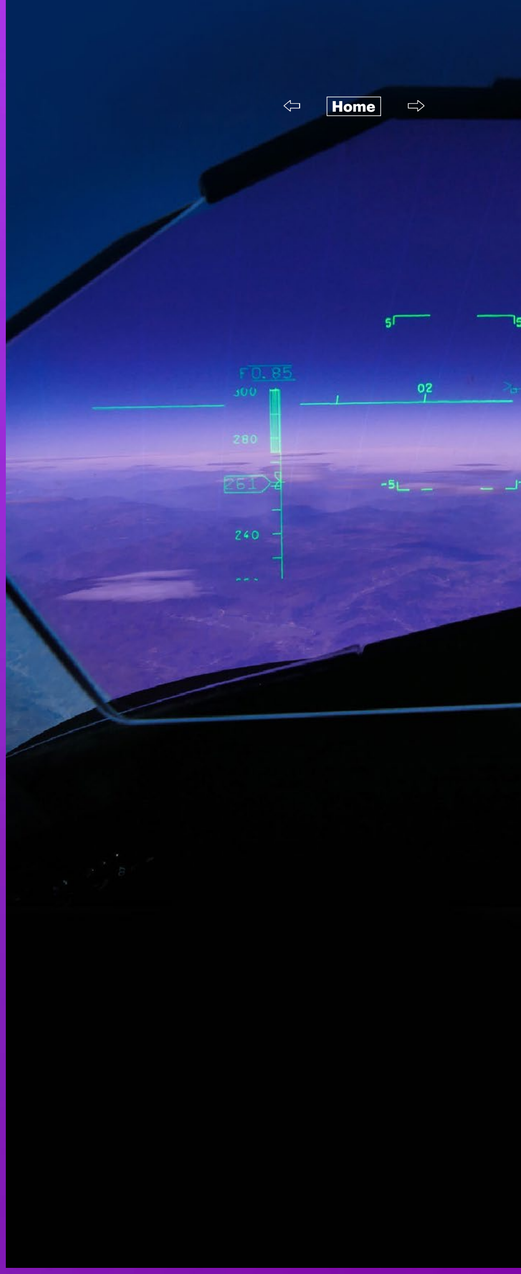
Regular patching and updating
Update software regularly and apply patches promptly to protect against known vulnerabilities and reduce the risk of security breaches.

Defense in depth
Implement multiple security measures to protect company assets. If one line of defense is compromised, additional layers provide backup to stop threats along the way.

Data governance and encryptions
Adhere to relevant legal, regulatory and industry standards to protect and store data. Encrypt sensitive data both at rest and in transit to protect it from unauthorized access.

Segregation of duties
Identify critical functions of key processes and disperse them to more than one individual or department to mitigate the risk of fraud or other unethical behaviors.

6. **Prepare for emerging technology like Quantum.** Aviation companies must partner with the right security experts to safeguard emerging technologies like quantum computing, space security and human-AI interfaces as they evolve. While quantum computers capable of breaking current encryption don't yet exist, adversaries are already stealing sensitive data, intending to decrypt it later. Achieving crypto agility—swiftly adapting encryption methods and replacing compromised keys—without disrupting critical infrastructure is essential.





Partnering to protect against cyberattacks

One of the largest international airports in the Middle East partnered with Accenture to transform its security approach and protect the airport from cyber-attacks. Through a managed services approach, the airport is building an integrated operating model tightly coupled with business, security operations and third-party suppliers to help bolster the security environment.

The airport plans for annual assessments of its partners' security capabilities and technological maturity to ensure its cybersecurity stays ahead of evolving threats.

Case Study

A leading international airport in the Middle East Airport partnered with Accenture to deploy a Managed Cyber Defense model to enrich its detection and response capabilities as well as improve insider threat monitoring. The result is full visibility into the airport's IT and OT environments, driving faster threat response.

Step 3
Re-imagine

Harness AI for proactive and adaptive defenses

To bolster cyber resilience in airlines and airports, it's crucial to improve visibility across the attack surface for more effective vulnerability detection. Simplifying security layers and leveraging AI will better equip airlines to defend against today's sophisticated threats.

Actions to take:

1. **Implement AI Firewalls.** An AI firewall represents the evolution of next-generation firewalls (NGFWs), leveraging intelligent detection technologies to better identify advanced and emerging threats. Unlike traditional NGFWs, which rely on static rule databases and struggle to address sophisticated threat variants, AI firewalls use intelligent detection engines to train threat detection models using vast datasets. These models are continuously refined with real-time traffic data, significantly boosting their ability to detect and mitigate advanced threats.

   With AI models proliferating and threat actors using AI to create sophisticated cyber-attacks, AI firewalls customized to fit organizational policies provide a strong first line of defense, securing interactions, preventing data leakage and blocking malicious or unauthorized uses. For example, Accenture introduced a gen AI security diagnostic tool designed to identify vulnerabilities in data lakes and detect unauthorized foundational models. The tool provides protection against prompt injection attacks by employing a mechanism similar to an AI firewall, ensuring robust security for foundational models. [23]

2. **Adopt AI enabled security tools.** As AI-powered threats grow increasingly sophisticated, traditional security measures are proving insufficient. To stay ahead, organizations must embrace AI-driven defense technologies and use automated tools for actions like red teaming and penetration testing for proactive threat assessment. Industry leaders and hyperscalers are already deploying advanced AI-based security solutions. Accenture's security teams, for instance, are leveraging AI assistants that can better aggregate and analyze threat intelligence, ultimately enabling significantly improved risk correlation.

3. **Leverage AI to automate and augment.** The aviation industry continues to grapple with talent shortages, especially in security expertise. To mitigate this challenge, aviation companies must leverage generative AI to automate manual security processes, boosting efficiency and strengthening overall security operations. Our analysis reveals that 71% of tasks performed by information security analysts can be either automated (28%) or augmented (43%) using generative AI. This approach not only increases efficiency but also elevates a company's security posture. [24]



Getting started

As the aviation industry soars to greater heights, it must also elevate its cybersecurity defenses. By embedding cybersecurity into business strategies, reinventing cyber-resilience and modernizing security practices, aviation companies can protect their innovations and ensure a secure, sustainable future for air travel. The challenge is clear: fortify defenses to keep the future of aviation on course. Only those who rise to this challenge will truly succeed.

Start your journey of secure innovation by asking these crucial questions to identify vulnerabilities and drive action.

Questions every aviation company should ask:

Strategize

- Does the cyber protection strategy cover every element of innovation?
- Does our organization understand and manage third-party cyber risks to build business continuity?

Modernize

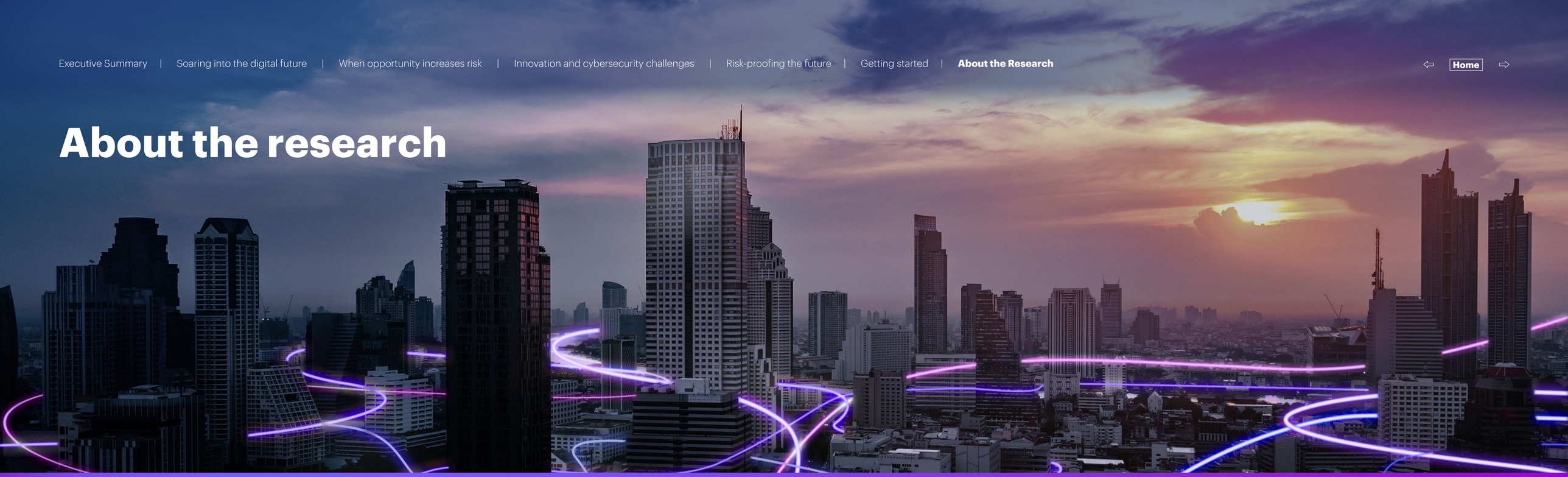
- Is our cybersecurity program sufficiently mature and agile to effectively address modern-day threats?
- Does business consider cyber resilience as a continuous journey or a one-time sprint?
- Is your security partner well equipped to identify and detect future sophisticated cyber threats?

Re-imagine

- Is our organization leveraging AI to scale security through automation?
- Has our organization identified use-cases to implement AI to address security skill gaps?



About the research



1. Charting Aviation's path to reinvention

Accenture Research surveyed 300 leaders (including 250 CXOs) from the aviation sector to gauge their views about a number of critical business topics including cost pressures, business models, technology, talent, sustainability and customers.

2. The Information Security Forum (ISF) Benchmark Tool

The ISF Benchmark tool has the following key characteristics that allowed us to get an outside view on how the airline industry is scoring on average on cybersecurity.

Peer Group
Selecting the airline industry in the tool gave us a global view over a period of 10 years, including a total of 16 airlines.

Industry Best Practices
Out of several frameworks the ISF supports, we selected

NIST (National Institute of Standards and Technology) Cybersecurity Framework

ISO/IEC 27002, is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

3. Average Benchmark Score

The ISF average benchmark score provided valuable insight on how the airline industry is measuring up against globally-recognized cybersecurity standards.

References

1. United Airlines starts serving passengers personalized ads on seat-back screens CNBC
2. Saudia Unveils Cutting-Edge AI-Powered Innovations in “LEAP” | Saudia Airlines
3. Pulse of Change Consumer Survey | Accenture
4. Electronic Warfare Spooks Airlines, Pilots and Air-Safety Officials | WSJ
5. The Cyber Resilient CEO | Accenture
6. Aviation Sector Analysis | Accenture
7. Aviation Sector Analysis | Accenture
8. Saudia Unveils Cutting-Edge AI-Powered Innovations in “LEAP” | Saudia Airlines
9. United Airlines starts serving passengers personalized ads on seat-back screens | CNBC
10. Riyadh Air collaborates with Accenture to build core technology capabilities | Riyadh Air
11. Riyadh Air unveils world-class digital channels designed to transform the travel industry with hyper-personalization | Riyadh Air
12. Aviation Cybersecurity National Governance | ICAO
13. Electronic Warfare Spooks Airlines, Pilots and Air-Safety Officials | WSJ
14. SOCRadar’s 2024 Aviation Industry Threat Landscape Report | SoC Radar
15. Escalating Ransomware and Phishing Threats Demand Reinforced Cyber Defences for Aviation | Bridewell
16. US Cybersecurity in Aviation: 2024 | Bridewell
17. SOCRadar’s 2024 Aviation Industry Threat Landscape Report | SoC Radar
18. Pegasus Airline breach sees 6.5TB of data left in unsecured AWS bucket | TechMonitor
19. The Cyber Resilient CEO | Accenture
20. Aviation Sector Analysis | Accenture
21. Aviation Sector Analysis | Accenture
22. Digital Core Survey | Accenture
23. Accenture Launches New Suite of Gen AI Focused Security Services
24. Accenture Research Analysis | Accenture



Authors



Ahmed Etman
Middle East Cybersecurity Lead, Accenture



Dr. Radwane Saad
Middle East Cybersecurity Strategy Lead, Accenture



Yusof Seedat
Global Cybersecurity Research Lead, Accenture



Manav Saxena
Cybersecurity Market Unit Research Lead, Accenture

Contributors

Subject Matter Experts



Abedalqader Nasrallah



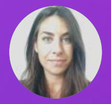
Dr. Ahmed Baswaid



Chiara Celli



Jennifer Graham

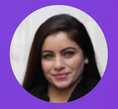


Jessica Smits



Yusra Zvavi

Research Team



Carla Issa



Gargi Chakrabarty



Meredith Trimble

Marketing Lead



Theodore Halabi

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent- and innovation-led company with approximately 801,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology and leadership in cloud, data and AI with unmatched industry experience, functional expertise and global delivery capability. Our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Song, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients reinvent and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities.

Visit us at **www.accenture.com**

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data-science-led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value and deliver on the power of technology and human ingenuity.

For more information, visit Accenture Research on **www.accenture.com/research**