IDC

July 2026
InfoBrief
Sponsored by Jamf

From Gate to Galley to Ground

Rethinking Frontline Endpoints in Asia/Pacific Aviation

Stephanie Krishnan
Associate Vice President,
IDC Insights

Table of contents

Click any title to navigate directly to that page.

Executive summary: The execution gap

85% experienced a material endpoint incident in the past 12 months.

17% can roll out a critical update across the estate within 24 hours.

35% rank third-party access a top risk, with no matched investment.

The frontline endpoint is operational infrastructure.

Aviation's work has moved off the desk and onto tablets, smartphones, and ruggedized handhelds, across the gate, the galley, the ramp, and the hangar. The estate is converging on a tight set of execution-focused priorities, including **resilience, shared-device productivity, and identity,** but execution lags ambition. The organizations that pull ahead will run endpoints as operational infrastructure, held to a consistent operational standard that fits each device platform rather than flattening it.

What you'll find in this InfoBrief

The state of the estate
Converging, not consolidating: a deliberately mixed estate built role by role.

The operational gap
Incidents are near-universal and land first on turnaround and boarding.

The execution gap
Rollout speed and inconsistent enforcement throttle every other investment.

Country lenses
How priorities differ across ANZ, Japan, Korea, ASEAN, and Rest of AP.

The operational and technology pressure is consistent: The capacity to manage it varies considerably

In frontline aviation, a technology failure and an operational failure are the same event, and management cannot afford to treat them separately.

Top challenges

next 2 to 3 years

34%
On-time performance and turnaround pressure

33%
Workforce productivity and skills gaps

31%
Rising operating cost and margin pressure

Technology priorities

next 12 to 24 months

41%
Operational resilience and business continuity

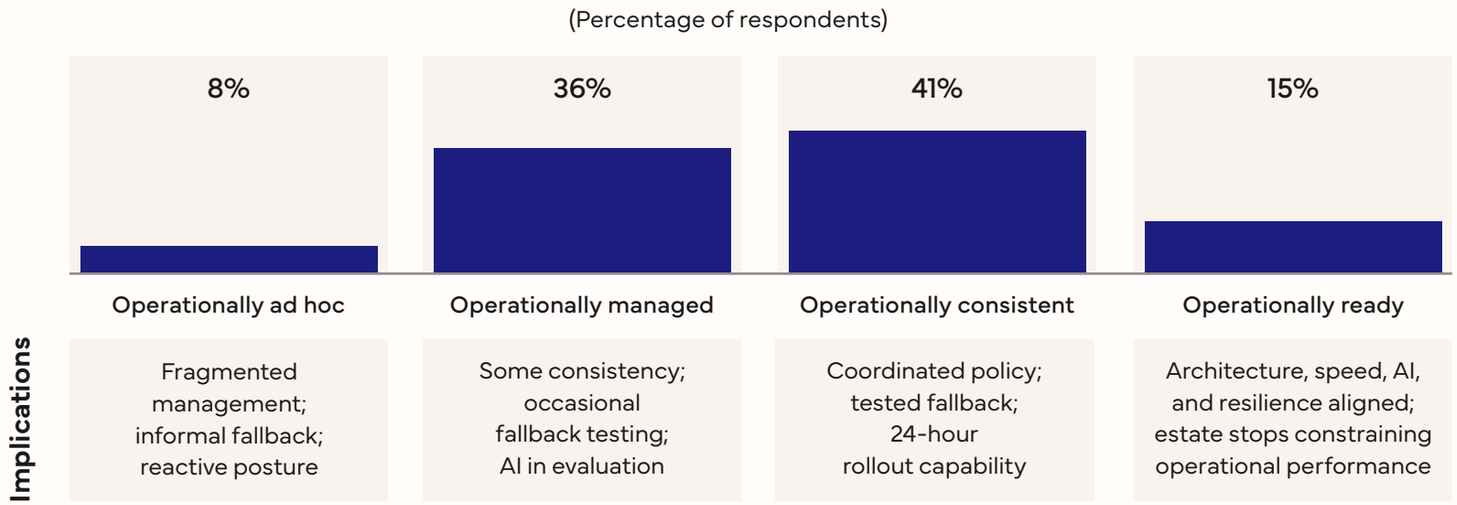
36%
Shared-device processes across shifts

35%
Identity and access for frontline staff

Figure 1

Operational readiness

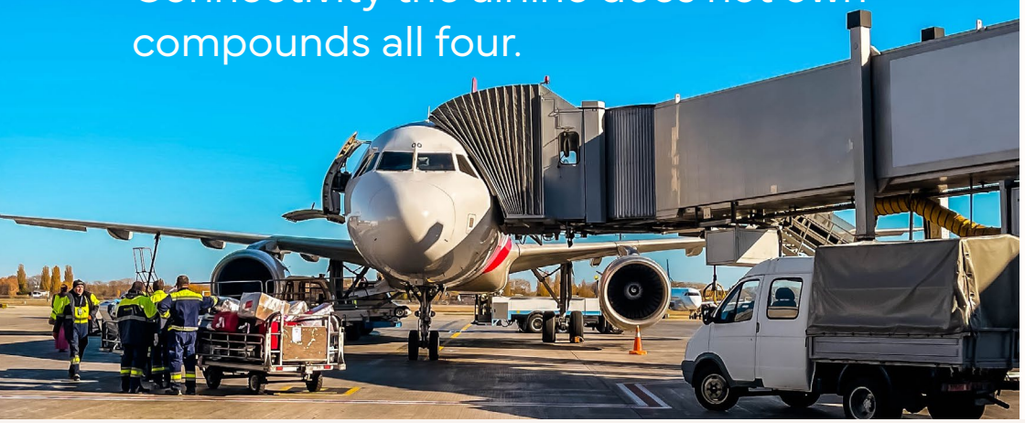
Operational readiness is scored across four dimensions: management architecture, rollout speed, AI adoption, and fallback resilience. The average Asia/Pacific aviation organization sits at the top of Stage 2, just short of operational consistency.



When business performance and technology priorities align, delayed IT operation shows up directly in operational performance, indicating a need to close the gap between IT investment decisions and operational performance accountability.

What aviation needs from frontline endpoints

The four demands do not sit in isolation. Gaps in visibility **undermine trust;** slow rollout speed **compounds continuity failures.** In a connected frontline estate, the weakest demand determines **device estate resilience.** Connectivity the airline does not own compounds all four.



Endpoints are not tools. They are operational infrastructure, judged against four operating demands.

Continuity

41% of Asia/Pacific aviation leaders rank resilience their top technology priority, yet 30% operate without tested fallback, leaving continuity dependent on improvisation at the point of failure. 34% rank offline resilience a top capability.

Speed

Only 17% of Asia/Pacific aviation organizations can roll out a critical update across the full estate within 24 hours, leaving the majority exposed for days after a risk is identified.

Security

For Asia/Pacific aviation, identity (37%) and third-party access (35%) are the top cybersecurity risks, placing the greatest exposure at the boundaries the estate does not directly control.

Visibility

Device health visibility is the second most critical endpoint capability yet carries the widest enforcement gap in the estate, leaving organizations blind to failure before it becomes disruption.

Aviation regulatory requirements from DHS/TSA, FAA, and NIST now extend to frontline mobile estates. Compliance runs through all four demands. Organizations that address it proactively carry less exposure.

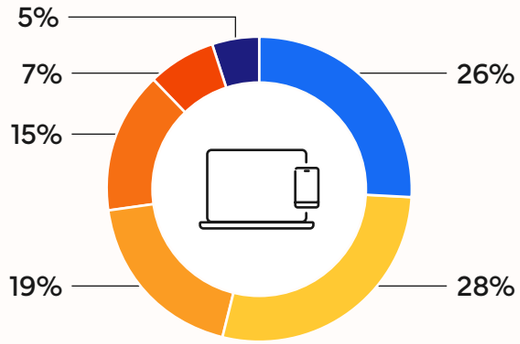
The estate is converging but not consolidating

Many Asia/Pacific aviation organizations have hybrid device estates, with roles dictating device choices.

Figure 2

Estate composition

(Percentage of respondents)



- Apple-first above-wing, other below
- Mostly rugged Android in operational areas
- Mostly Apple across most frontline roles
- Mixed Apple and Android, no single standard
- Mixed mobile and Windows endpoints
- Limited use of frontline mobile devices

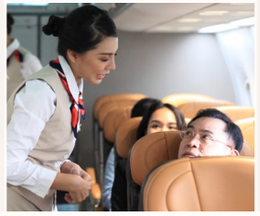
What the composition shows

Pilot and EFB

The cockpit is the most binary role in the estate. Over half of organizations run zero iOS in pilot and EFB deployments, yet a significant share run exclusively iOS. The operating context demands a full commitment either way.

Cabin crew

Cabin crew sit alongside the cockpit above the wing and are also split between iOS/Android. Their devices carry the most varied use cases, including inflight payment and roaming connectivity, requiring tools to fit the workflow.



Gate and check-in

Gate and check-in is the most mixed role in the estate, with adoption spread evenly across the range and no concentration at either end. The challenge here is consistency across a deliberately varied fleet.

Baggage, ramp, and dispatch

Ground operations show no dominant adoption pattern. iOS runs alongside rugged Android and Windows handhelds because the role and the operating environment determine device selection.

Maintenance, engineering, and inspection

Maintenance and inspection were reported as the most critical operational priorities for mobile devices, with the most distributed device mix. No platform dominates because no single device fits every task. The management challenge is delivering consistent outcomes across a deliberately varied fleet.

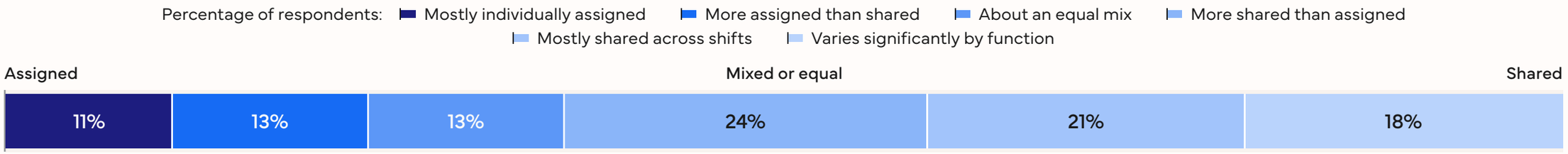
Whichever composition an organization runs, the requirement is the same: a **consistent security and operational outcome** across the estate, delivered through **management that fits** each platform rather than flattening it.

Aviation runs on shared devices, and the pattern is structural

The frontline is built around devices that pass between people, shifts, and locations, and that pattern is structural, requiring policy, identity, and recovery procedures that align with it.

Figure 3

How are frontline devices assigned and used?



Shared estates lean on three capabilities

43% Remote lock, wipe, or recovery

42% Device health and compliance visibility

36% Rapid reset for the next user

Most Asia/Pacific organizations run estates where devices pass between people, shifts, and operational areas. Shared devices place a disproportionate weight on three capabilities: **rapid reset** between users, **role-based access** at sign-in, and **identity that travels with the user** rather than the device.

Source: IDC *Asia/Pacific Aviation Endpoint and Resilience Study, 2026* (n = 150)

What's hardest day-to-day and what it costs

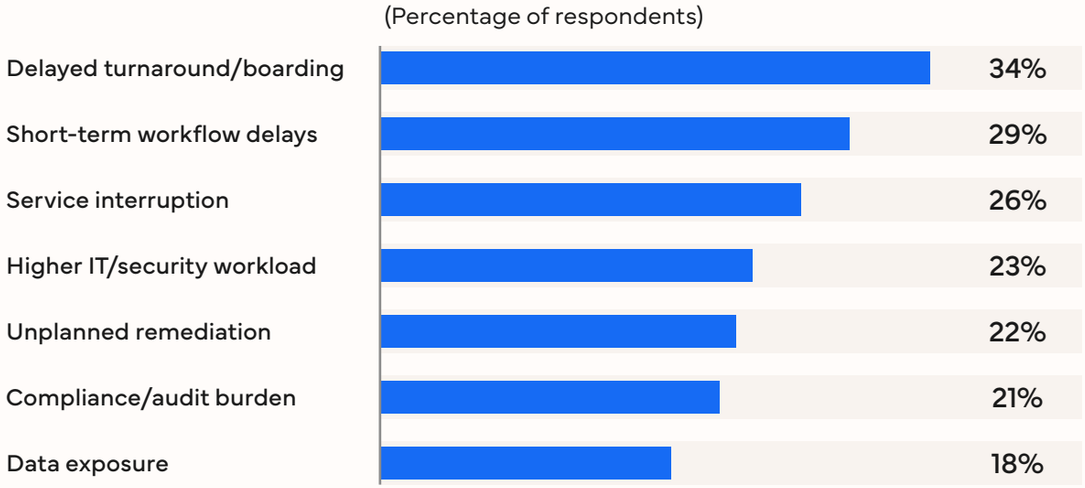
The endpoint estate is producing material operational consequences in nearly every aviation organization in the region.

Endpoint-related delays carry real operational cost. The FAA estimates airline operating costs at approximately $100.76 per block minute, compounded by remedial expenses when disruption reaches passengers.

85% of APAC aviation organizations experienced material endpoint-related operational incidents in the past 12 months.

Figure 4

Where the operational impact lands



Connectivity is a shared responsibility. While tarmac networks, gate infrastructure, and 5G roaming are beyond an airline's control, they still face the **operational and cost impacts of frontline device usage.** Device-level policy enforcement is the only consistent point of control.

Where is device management hard?

36% Keeping OS and apps current without disruption

35% Remote troubleshooting

32% Tracking device health and compliance

31% Shared-device handoffs

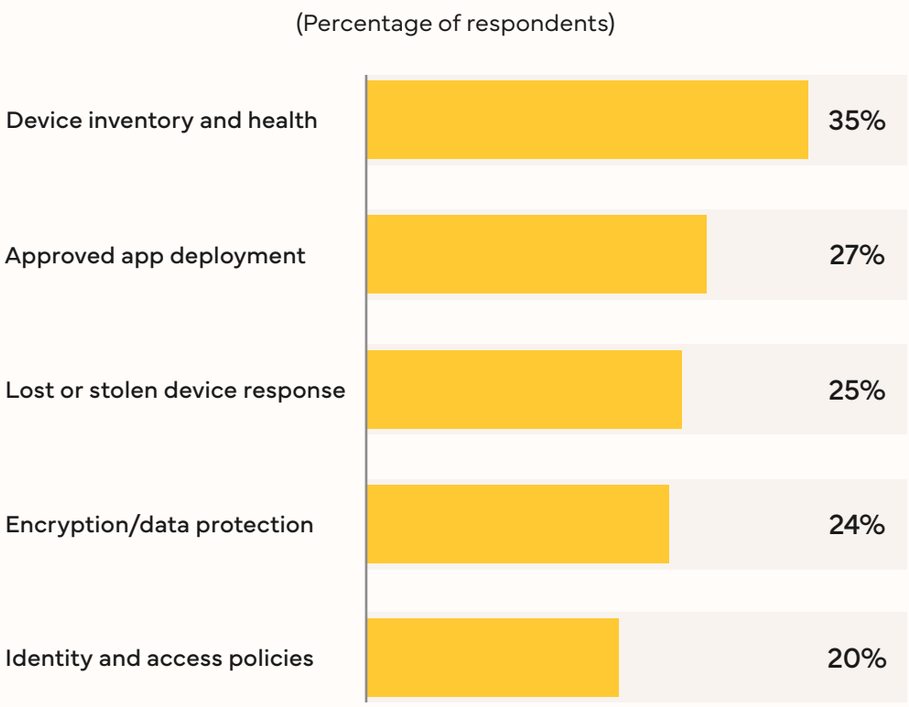
31% limited connectivity in frontline environments

Sources: (1) IDC *APJ Agentic AI Survey 2025*, ASEAN (n = 200), (2) IDC *Future Enterprise Resiliency & Spending Survey 2026 Wave 1*, ASEAN (n = 51)
Source: IDC *Asia/Pacific Aviation Endpoint and Resilience Study, 2026* (n = 150)

The attack surface is not shrinking because enforcement is inconsistent

Figure 5

Security enforcement gap: Inconsistent or no formal standard



Most organizations manage the frontline estate in fragments, and inconsistent enforcement creates both operational and security exposure.

6%

of Asia/Pacific aviation organizations run a single management model across the frontline estate, making **estate-wide consistency the exception rather than the norm.**

31%

of passenger airlines run **two or more platforms under a coordinated central policy,** the most structured approach in a sector where the estate is rarely uniform.

29%

of aviation services providers use **different tools and policies by device type** or function, reflecting the most varied management footprint in the estate.

Inconsistent enforcement is a regulatory liability. DHS, TSA, FAA, and NIST mandates now extend to mobile endpoints and EFBs; pilots carry a personal, non-delegable obligation to self-certify device compliance before every flight. Managing by exception is a direct regulatory infraction.

From exposure to action: Risk versus matched investment

The frontline is built around devices that pass between people, shifts, and locations, and that pattern is structural, requiring policy, identity, and recovery procedures that align with it.

Third party/partner access without investment in management has operational consequences.

Table 1

Security risk area today	Risk %	Matched investment priority	Invest %
Identity and access for frontline users	37%	Stronger access controls and authentication	40%
Third-party or partner access	35%	*No matched investment priority*	—
Frontline smartphones and tablets	31%	Faster OS and application updates	41%
Public networks/external connectivity	31%	Better protection on public/untrusted networks	30%
Legacy operational systems that are hard to patch	27%	Consistent policy enforcement across locations	32%
Shared devices across shifts or flights	26%	Better audit and reporting readiness	30%

Third-party and partner access is the clearest gap between where threats enter the estate and where budgets are directed. In Asia/Pacific aviation, that boundary includes ground handlers, MRO partners, and airport ecosystems. An unmanaged entry point is not a vendor problem; it is an ownership problem.

Source: IDC *Asia/Pacific Aviation Endpoint and Resilience Study, 2026* (n = 150)

When the system goes down: Resilience and remaining gaps

Progress on resilience is real but uneven. What gets reported looks strong; however, what is tested under pressure reveals the gaps.

Progress on key operational outcomes by Asia/Pacific aviation organizations

47%
Cybersecurity posture

47%
Compliance and audit readiness

24%
Incident recovery time

23%
Endpoint/app visibility

Four resilience requirements

Visibility
Determine that an incident has occurred, assess its scope, and establish which systems, devices, and users are affected before response can begin.

Containment
Isolate the affected segment of the estate to prevent lateral spread across devices, functions, or partner connections.

Continuity
Maintain operational workflows through a tested fallback. An untested workaround is an assumption, not a continuity plan.

Recovery
Return the estate to a verified baseline, with confirmed device health and policy enforcement, not just restored connectivity.

Strong resilience programs reduce the number of security incidents the recovery arc absorbs. Proactive controls, patch currency, app vetting, and phishing protection do that work before the incident, not after.

Aviation has invested in resilience posture. Incident recovery time and endpoint visibility, the two capabilities that determine whether an operation survives a disruption, remain the least developed in the estate.

Source: IDC *Asia/Pacific Aviation Endpoint and Resilience Study, 2026* (n = 150)

Change needs to keep up with operational tempo

The time between intent and execution on the front line needs to be hours, not days.

Organizations that roll out in days rather than hours are carrying compliance debt as well as operational risk.

Figure 6

Rollout speed: A critical update, full estate

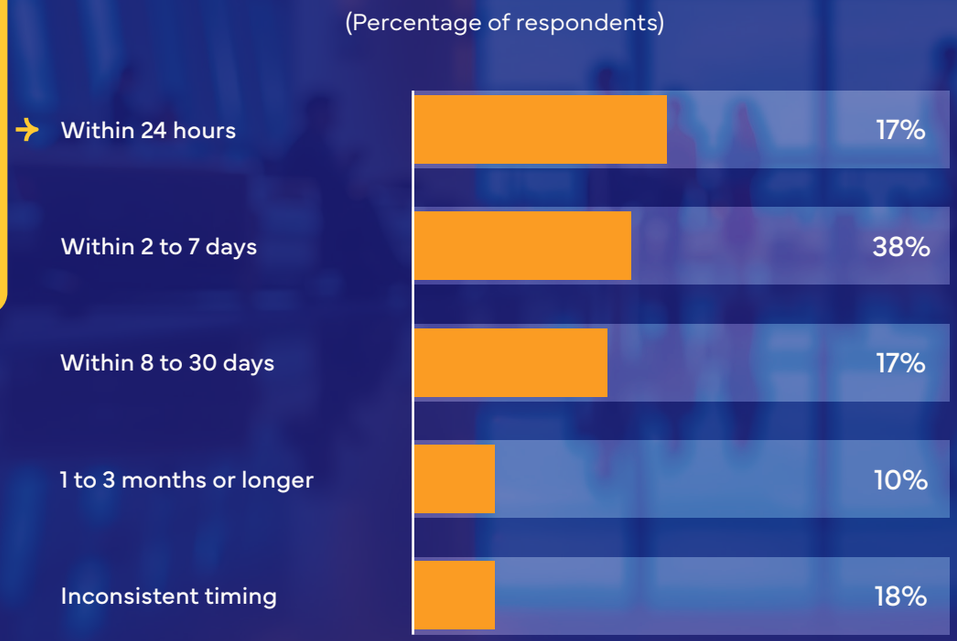
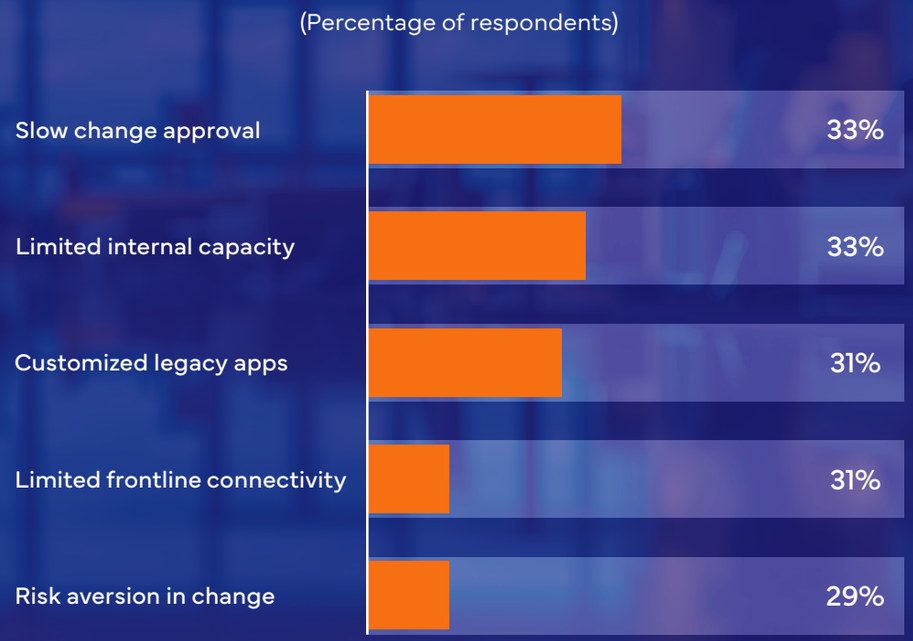


Figure 7

Constraints are people and process, not technology



Every security fix, policy update, and AI-enabled workflow is only as fast as the slowest change-approval process. The constraints that prevent it are organizational: approval cycles, internal capacity, and risk aversion. Modernization is challenged by change management.

Operational modernization and AI adoption are not parallel tracks. The estate that cannot update in 24 hours also cannot run AI at scale. Leaders who fix the foundation first are the ones who move from pilot to production.

Where leaders want to modernize first

The modernization agenda has moved from infrastructure to operations. The three workflows that leaders prioritize first are the ones closest to the customer and the operational outcome.

38%
Airport or terminal operations

37%
Turnaround coordination

36%
Incident response and service recovery

AI ambition is real

Where is Asia/Pacific aviation with regards to AI?

53%
pilot or evaluation only

15%
in production at meaningful scale

AI ambition is not the problem. Production is. Until the estate can move at operational tempo, AI remains a capability organizations are evaluating, not operating.

Source: IDC *Asia/Pacific Aviation Endpoint and Resilience Study, 2026* (n = 150)

Country-level lenses on a regional pattern

A common structural challenge is producing distinct national responses across investment, execution, and security.

Table 2

Region	Top 2 investment priorities	Top 3 hardest aspects today	Highest security exposure
Japan	**Device and workflow modernization** Endpoint security and policy enforcement	**Mixed Apple, Android, and Windows estates** **Remote troubleshooting at scale** Identity and access management	**Third-party or partner access** Identity and access for frontline users
South Korea	**Identity and access for frontline users** Shared-device management and automation	**OS and app patching without disruption** **Device health and inventory tracking** Mixed Apple, Android, and Windows estates	**Frontline smartphones and tablets** Identity and access for frontline users
ANZ	**Connectivity and network reliability** Device and workflow modernization	**OS and app patching without disruption** **Identity and access management** Device health and inventory tracking	**Identity and access for frontline users** Email, collaboration, and user-driven threats
ASEAN	**Data integration and observability** Shared-device management and automation	**OS and app patching without disruption** **Device replacement after loss or damage** Public network protection	**Third-party or partner access** Identity and access for frontline users
Rest of AP	**Operational app modernization** Business continuity and resilience tools	**Shared-device handoffs between shifts** **Remote troubleshooting at scale** Device health and inventory tracking	**Public networks or external connectivity** Operational applications on mobile devices or tablets

Across all five markets, investment priorities, execution gaps, and security exposure point to the same structural problem: The frontline estate has extended beyond the boundaries of the governance model managing it. Partner networks, shared infrastructure, and external access are now operational dependencies, not peripheral risks.

Source: IDC *Asia/Pacific Aviation Endpoint and Resilience Study, 2026* (n = 150), *Country segments* (n = 30)

From endpoint estate to operational infrastructure

Three conversations need to happen for Asia/Pacific aviation in the next 12 months.

For the CIO

- **Reframe:** From "we manage endpoints" to "we run operational infrastructure."
- The conversation is with the COO and CFO, not with vendors. The frontline estate now sits alongside ground equipment, scheduling, and fuel planning in operational consequences and requires addressing regulatory and governance requirements.

In 12 months:

- Endpoint performance is reported in operational dashboards, not IT dashboards. The estate is held to a consistent operational outcome, regardless of platform. Rollout speed is measured in hours, not days.

For operations

- **Reframe:** From "IT supports our work" to "IT is part of our work."
- The conversation is between operations and IT, built around a shared scorecard that most aviation organizations do not have today. Operations owns the recovery-time target and funds the visibility and rollout speed behind it. There are clear financial costs to endpoint- and connectivity-related delays.

In 12 months:

- Operational resilience targets include endpoint recovery time. Change windows are agreed in advance, not negotiated during incidents. Above-wing and below-wing operations report against the same operational outcomes.

For security

- **Reframe:** From "we protect endpoints" to "we close the gap between exposure and response."
- The conversation is about who owns the speed of response, not who owns the threat. The patching paradox, top operational pain, top investment priority, and slowest execution is resolved by bringing operations into change approval and ensuring device compliance requirements are addressed above and below the wing.

In 12 months:

- Critical updates reach the entire estate within 24 hours. Third-party access has a named budget owner. Identity travels with the user, not the device.

These conversations reflect the **same structural gap,** requiring decision coordination between IT and operations. Asia/Pacific aviation organizations must establish **joint accountability for the device estate** at the level where **on-time performance, recovery time, and partner governance** are clearly managed. The endpoint is not an IT asset with operational consequences. It is an operational asset that requires IT to run.

Study demographics

n = 150 frontline endpoint and security decision-makers across Asia/Pacific aviation

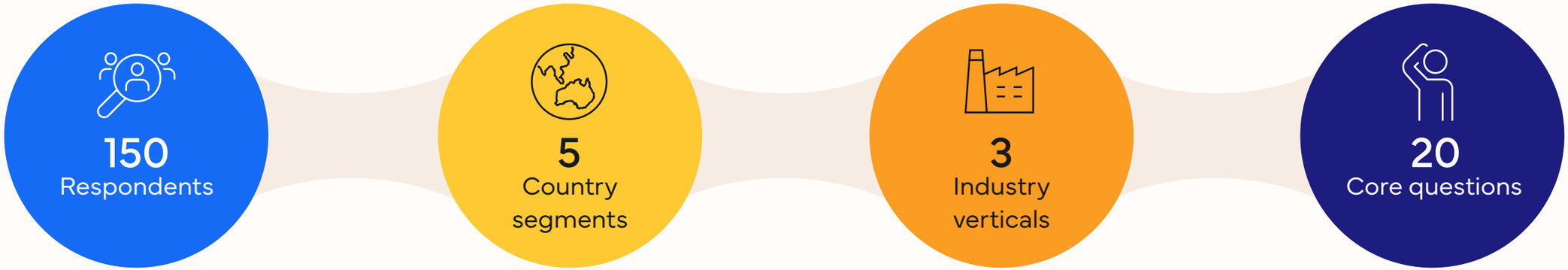


Figure 8

Country distribution

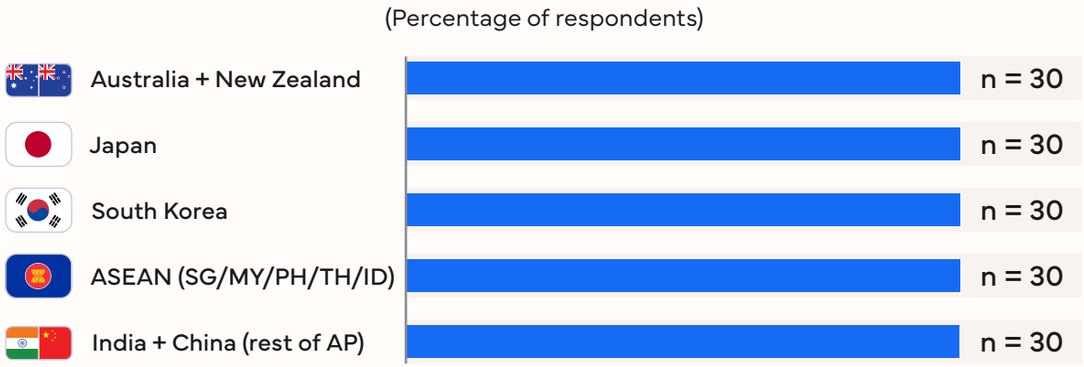
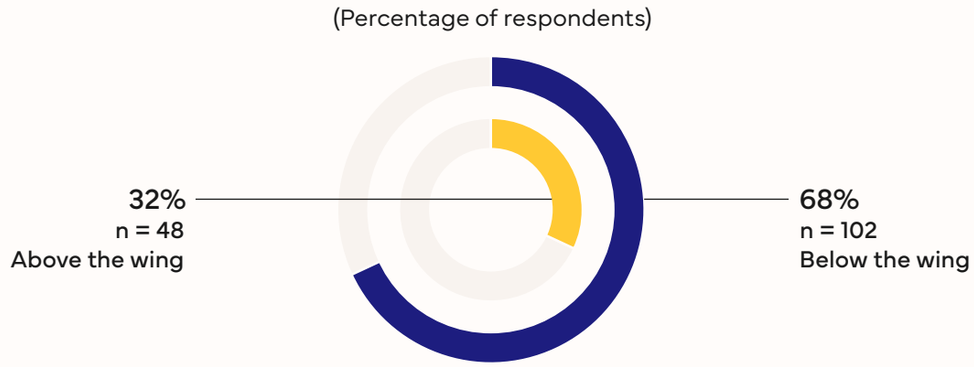


Figure 9

Above vs Below the Wing



Source: IDC *Asia/Pacific Aviation Endpoint and Resilience Study, 2026* (n = 150)

About the IDC analyst

Stephanie Krishnan

Associate Vice President, IDC Insights

Stephanie Krishnan is Associate Vice President at IDC, responsible for shaping research across manufacturing, supply chain, and retail, with particular focus on Asia/Pacific and worldwide supply chain strategies. She covers transportation, warehousing, logistics, global trade, warehouse and inventory management, and integrated supply chain execution, alongside emerging themes such as agentic AI, physical AI, cybersecurity, and sustainability.

More about Stephanie Krishnan →

Message from the sponsor

jamf

Aviation operations depend on mobile technology to keep crews informed, compliant and ready across time zones, aircraft types and constantly shifting connectivity. Managing those devices at scale introduces real challenges: maintaining security and compliance across international routes, controlling data usage, minimizing downtime when every grounded minute carries operational cost, and ensuring devices are ready without requiring hands-on IT support.

Aviation IT teams need solutions that address the full device lifecycle, from zero-touch provisioning and automated policy enforcement to seamless role-based access, threat prevention and shared device workflows between flights. The goal is simple: devices that are secure, compliant and always ready, whether below or above wing.

Named a Leader in the IDC MarketScape: Worldwide Unified Endpoint Management Software for Apple Devices 2025–2026, Jamf gives airlines more than mobile device management. They get a reliable way to keep crews connected, operations moving, and devices secure and compliant, no matter where they are in the world.

Learn More

IDC Custom Solutions

IDC Custom Solutions produced this publication.
The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC.com | IDC on LinkedIn | IDC Blog

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA