THINSCALE

IATA, PCI DSS & Travel Agencies

Why unmanaged personal devices create compliance risk for distributed travel agencies

Executive Summary

The travel industry has undergone a fundamental shift toward distributed working models. Homeworking agents, independent contractors, and franchise networks are now central to how many travel agencies operate.

At the same time, IATA-accredited agencies and those operating within the BSP framework face increasing pressure to maintain strict compliance over how payment data and booking systems are accessed.

This creates a critical challenge:

How can travel agencies maintain IATA and PCI DSS compliance when agents are working remotely on devices the organisation does not fully control?

Many agencies today operate using one of two models:

- → Agents using personal devices (BYOD)
- → Company-issued laptops to support remote work

While both approaches enable flexibility, neither was designed with modern compliance requirements in mind.

As a result, agencies are often operating with:

- → Limited visibility over endpoint security
- → Gaps in compliance enforcement
- → Increasing operational and device-related costs

This whitepaper explores:

- → The growing complexity of IATA and PCI DSS compliance in distributed travel environments
- → The risks introduced by unmanaged or partially controlled endpoints
- → Why traditional approaches fall short
- → A more scalable approach to secure, compliant working

01. The Changing Operating Model of Travel Agencies

Across the travel industry, companies have adopted:

- → Homeworking agent networks
- → Franchise and host agency models
- → Independent contractor ecosystems

These models enable:

- → Rapid scaling
- → Reduced overhead
- → Increased agent flexibility

But they also introduce a fundamental shift:

The computer (endpoint) is no longer controlled by the organisation.

Today, many agencies operate with:

- → Agents using personal devices
- → Or centrally issued laptops supporting remote work

Both models introduce new challenges when it comes to security, control, and compliance.

02. PCI DSS in the Travel Industry

Travel agencies routinely handle:

- → Cardholder data
- → Personal traveller information
- → Booking systems and payment platforms

For any agency that accepts, processes, or transmits card payments, PCI DSS is a core requirement.

PCI DSS requires organisations to:

- → Protect cardholder data
- → Maintain secure systems and networks
- → Enforce strict access controls
- → Monitor and log access to sensitive systems
- → Demonstrate compliance through audit and evidence

In traditional office environments, these requirements are easier to enforce. In distributed environments, they become significantly more complex.

03. IATA Compliance

For many travel agencies, compliance extends beyond PCI DSS.

Agencies that are IATA-accredited or operate within the Billing and Settlement Plan (BSP) framework must meet additional expectations around financial control, operational integrity, and data protection.

IATA accreditation enables agencies to:

- → Issue airline tickets
- → Access global distribution systems (GDS)
- → Participate in BSP settlement processes

With this access comes increased responsibility.

The Link between IATA and PCI DSS Compliance

IATA has reinforced the importance of PCI DSS across the travel sector, particularly for agencies handling card payments.

Where cardholder data is involved, agencies are expected to:

- → Maintain PCI DSS compliance
- → Ensure secure handling of payment data
- → Demonstrate appropriate controls during audits or reviews

Failure to meet these expectations can lead to:

- → Financial penalties
- → Increased scrutiny or audit requirements
- → Restrictions on payment processing
- → Potential impact on accreditation status

The Challenge for distributed models

Traditional compliance models assumed:

- → Centralised offices
- → Corporate-controlled devices
- → Clearly defined IT environments

Modern travel agencies operate very differently, with:

- → Homeworking agents
- → Independent contractors
- → Distributed networks

The responsibility for compliance remains centralised, but the execution is distributed.

> **Agencies remain accountable for compliance, even when they do not fully control the devices being used.**
>
> **David Coombes**, CTO, ThinScale

04. The Compliance Gap: Distributed Agents and Uncontrolled Devices

This shift creates a significant compliance gap.

Key Risks

Unmanaged Personal Devices (BYOD)

- → No consistent security baseline
- → Unknown patching and update status
- → Increased exposure to malware or compromise

Limited Visibility and Auditability

- → Difficulty tracking user activity
- → Gaps in logging and monitoring
- → Challenges proving compliance

Inconsistent Access Controls

- → Access from multiple locations and devices
- → Difficulty enforcing policy uniformly

Expanded Attack Surface

- → Each device represents a potential entry point

These risks directly impact an organisation's ability to:

- → Protect cardholder data
- → Demonstrate PCI DSS compliance
- → Meet IATA expectations

05. The Cost and Complexity of Company Issued Devices

To address BYOD risks, many agencies issue laptops to agents.

While this improves control, it introduces new challenges:

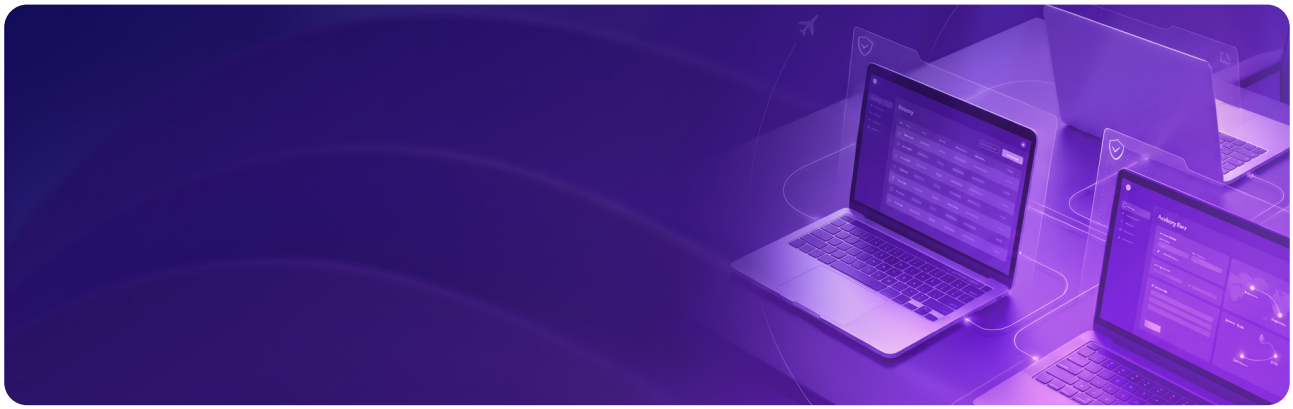
Operational Burden

- → Procurement and provisioning
- → Shipping and logistics
- → Ongoing support and maintenance
- → Device lifecycle management

Financial Impact

- → Upfront hardware costs
- → Replacement and refresh cycles
- → Support overhead

For growing, distributed agencies, this model becomes difficult to scale efficiently.



06. Why Traditional Approaches Fall Short

Common approaches to endpoint security include:

Mobile Device Management (MDM)

- → Requires control over the device
- → Often unsuitable for personal devices

Virtual Desktop Infrastructure (VDI)

- → High cost and complexity
- → Performance and usability concerns

Point Solutions

- → Limited scope
- → Do not fully address compliance requirements

In most cases, organisations are forced to choose between:

- → Control and cost
- → Or flexibility and risk

07. A More Scalable Approach to Compliance

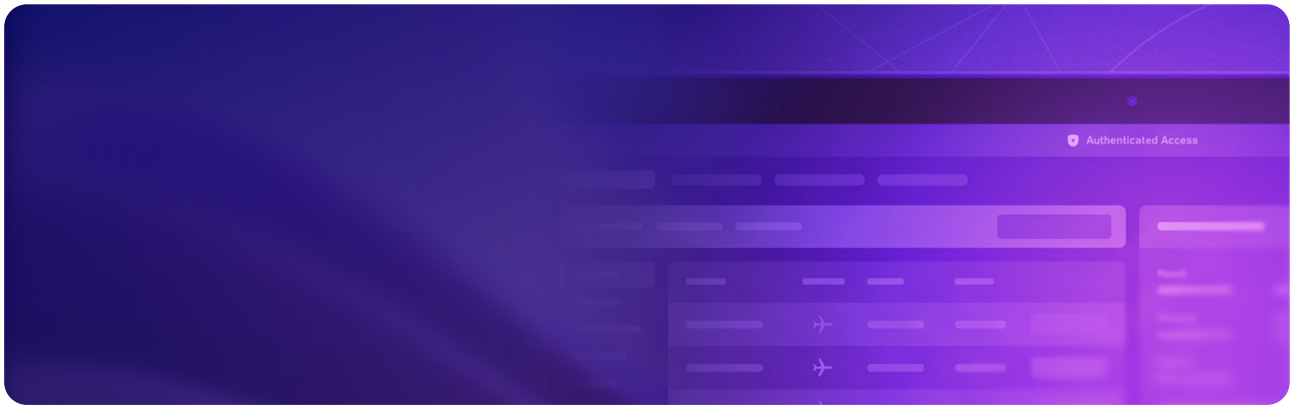
To support modern travel-agency models, a different approach is required.

Rather than attempting to control every device, organisations can:

> **Control the work environment where sensitive activity takes place.**

This approach enables:

- → Secure, isolated access to systems
- → Consistent enforcement of policies
- → Full visibility and auditability
- → Independence from device ownership



08. Enabling Secure and Compliant Distributed Working

A modern compliance model should provide:

Secure Workspaces

- → Isolated environments for handling sensitive data
- → Protection against data leakage

Centralised Policy Enforcement

- → Consistent controls across all users
- → Reduced reliance on endpoint configuration

Audit and Visibility Reporting

- → Monitoring of user activity
- → Evidence for compliance requirements

Controlled Access Across Distributed Environments

- → Secure, isolated access from personal and corporate devices
- → Reduced dependency on device ownership

09. Business Impact for Travel Agencies

Adopting a more effective compliance model delivers:

Reduced Risk

- → Improved alignment with IATA expectations
- → Stronger PCI DSS posture

Lower Costs

- → Reduced reliance on company-issued devices
- → Simplified IT operations

Improved Scalability

- → Support for growing distributed agent networks

Better Agent Experience

- → Flexibility without compromising security

10. Who Needs To Worry About This?

Many agencies operate under a few assumptions:

- → We use 3rd party solutions to process payments so we do not need PCI DSS compliance
- → We have a written PCI DSS process in place already, so we are fine

The reality is:

- → Using a third-party payment provider does not by itself eliminate PCI DSS responsibilities. Agencies that store, process, or transmit cardholder data must still validate PCI DSS compliance using the method that fits their merchant setup, which may be self-assessment or a QSA-led assessment.
- → For IATA-accredited travel agents, PCI DSS compliance is not optional. You must submit evidence of compliance through IATA's process. Simply having a written process or describing your controls is not enough; you must meet the required PCI DSS validation standard.

Failure to maintain the required PCI DSS compliance can result in IATA requiring corrective action and, in serious or repeated cases, can jeopardise your IATA accreditation

Conclusion

The travel industry's shift toward distributed working has created a new compliance challenge.

Agencies must now balance:

→ Flexibility and growth

→ With security, control, and regulatory responsibility

Traditional approaches, whether unmanaged BYOD or fully managed devices, are no longer sufficient on their own.

To meet both **PCI DSS requirements** and **IATA expectations**, travel agencies need a model that:

→ Extends control beyond the traditional office

→ Enables secure access from any device

→ Provides consistent, auditable compliance

Next Step

Assess your current risk exposure to:

→ Identify gaps in your compliance model

→ Explore a more scalable approach to secure, distributed working

→ Justify the appropriate scope and controls for your SAQ or PCI approach.

Assess your current risk exposure

Connect ThinScale with your IT provider

CLICK HERE

Disclaimer: ThinScale helps travel agencies be compliant with their Endpoint requirements under PCI DSS. Recommendations should be evaluated within the context of each organisation's specific and overall environment.

Contact us

learn more **thinscale.com**