Windows Application Management:
The Unquantified Risk in Your Organization

How unmanaged applications became one of the most overlooked cyber vulnerabilities in enterprise business.

A board-level guide to closing the door on the unmanaged and unowned application in your business.

juriba

From the Desk of the CEO

In every enterprise, there are invisible roles, quiet responsibilities that never make it onto a job description yet hold extraordinary influence over business resilience. One of those roles is the **Functional Application Owner**. They exist in every function, HR, Finance, Legal, Operations, and often unknowingly hold responsibility for the systems that store our data, connect our customers, and protect our brand.

This didn't happen through negligence; it evolved through progress. As applications multiplied, ownership spread organically across the business, faster than governance, training, or visibility could keep up.

Today, that legacy has become one of the largest unseen risks facing enterprises. The people who 'own' critical applications often have no idea they're accountable for their security, patching, or compliance. And that gap, between ownership and awareness, is where exposure lives.

At Juriba, we've lived this challenge. Before founding Juriba, as responsible for Desktop Infrastructure across EMEA at JPMorgan Chase, I saw firsthand the sleepless nights and operational strain that came from managing thousands of applications with limited visibility and fragmented accountability. That experience shaped our mission: to build practical solutions made for enterprise IT people, by ex-enterprise IT people.

Our Windows Application Management portfolio: **App Readiness and App Owner**, gives organizations a structured way to see, secure, and simplify their entire application landscape, managed and unmanaged, owned and unowned.

This paper isn't about fear; it's about foresight. The enterprises that act now will protect more than their data — they'll protect their people, their customers, and their credibility, whilst driving efficiencies via automation.

Because visibility isn't just an IT goal anymore — it's a leadership responsibility.

Barry Angell
Chief Executive Officer,
Juriba

The Unquantified Risk in Your Organisation

Every enterprise carries a hidden cyber risk, one that isn't born from bad actors or broken code, but from **invisible ownership.**

The Hidden Owners

Across every organization, hundreds of business users have quietly become Functional Application Owners, individuals who approve updates, test compatibility, or manage access to critical tools.

The Training Gap

Most were never trained for this responsibility, and many may not even know they have it.

The Result

A people-driven vulnerability: unmanaged applications, untracked patching, and unquantified exposure. **IBM estimate a single data breach on average costs Enterprises $4.4m[2]**

Many of those applications sit outside IT's direct control. What was once a smart business practice, when applications were fewer and patches less frequent, has evolved into a structural weakness of **functional ownership without visibility or control**.

[1] According to Ponemon Institute as reported by ServiceNow (2024)

[2] According to IBM Cost of a data breach 2025 | IBM

How We Got Here: When Good Practice Becomes a Hidden Risk

Originally, distributing application ownership across business functions made sense. It aligned accountability with expertise. The people using the tools were best placed to understand their value and manage change. For a long time, that worked.

But **the world has changed**. Applications now update weekly, integrate deeply, and connect to countless external systems. Security, compliance, and patch velocity have become constant moving targets, and the model that once empowered agility now exposes risk.

Why Re-centralizing Isn't the Answer

Some might argue, 'just give it back to IT.' But that's neither practical, effective, nor affordable.

35%
Budget Increase Required

According to Gartner (2024)[1], enterprise IT budgets would need to increase by more than 35% to absorb full ownership of all business-managed applications. An impossible lift when most CIOs are already expected to reduce operational cost by 5–10% annually.

75%
Time on Routine Tasks

Juriba's 'State of the Windows Application Packaging Nation'[2] survey found that today 75% of Windows applications packaging took from 1-4 weeks from initial service request to "ready to deploy"

1,000+
Unique Windows Applications

The same survey found 50% of organizations manage over 1,000 unique Windows applications with over 30% of those managing >2,000. This figure is forecasted only to increase given the explosion in applications and patches.

82%
Struggle to keep Apps Updated

Additional of organizations who responded to our Windows Application Packaging Nation survey, 82% of organizations surveyed struggle to keep up their Windows applications updated within 3 months

Re-centralizing ownership would only deepen that imbalance. Adding headcount, delaying delivery, and reversing years of digital empowerment..

The answer isn't to undo progress; it's to modernize control.

[1] According to Gartner IT Key Metrics Data 2024
[2] According to Bob Kelly's findings on the State of the Windows App Packaging Nation Report

The Scale of the Problem

Visibility gaps have become a systemic enterprise challenge. Responses to our *Application State of the Nation survey* suggests an indicative industry estimate of 43% of Enterprise applications are unmanaged [1]; actual exposure will vary by organization, while ISACA (2023)[2] found that 54% of enterprises experienced a security incident linked to poor patch governance or unowned software.

This isn't simply an operational inefficiency; it's a compliance and reputational risk. In sectors with regulatory oversight, such as finance, healthcare, utilities, telcos and public services, missing ownership trails can trigger audit failures and loss of certification.

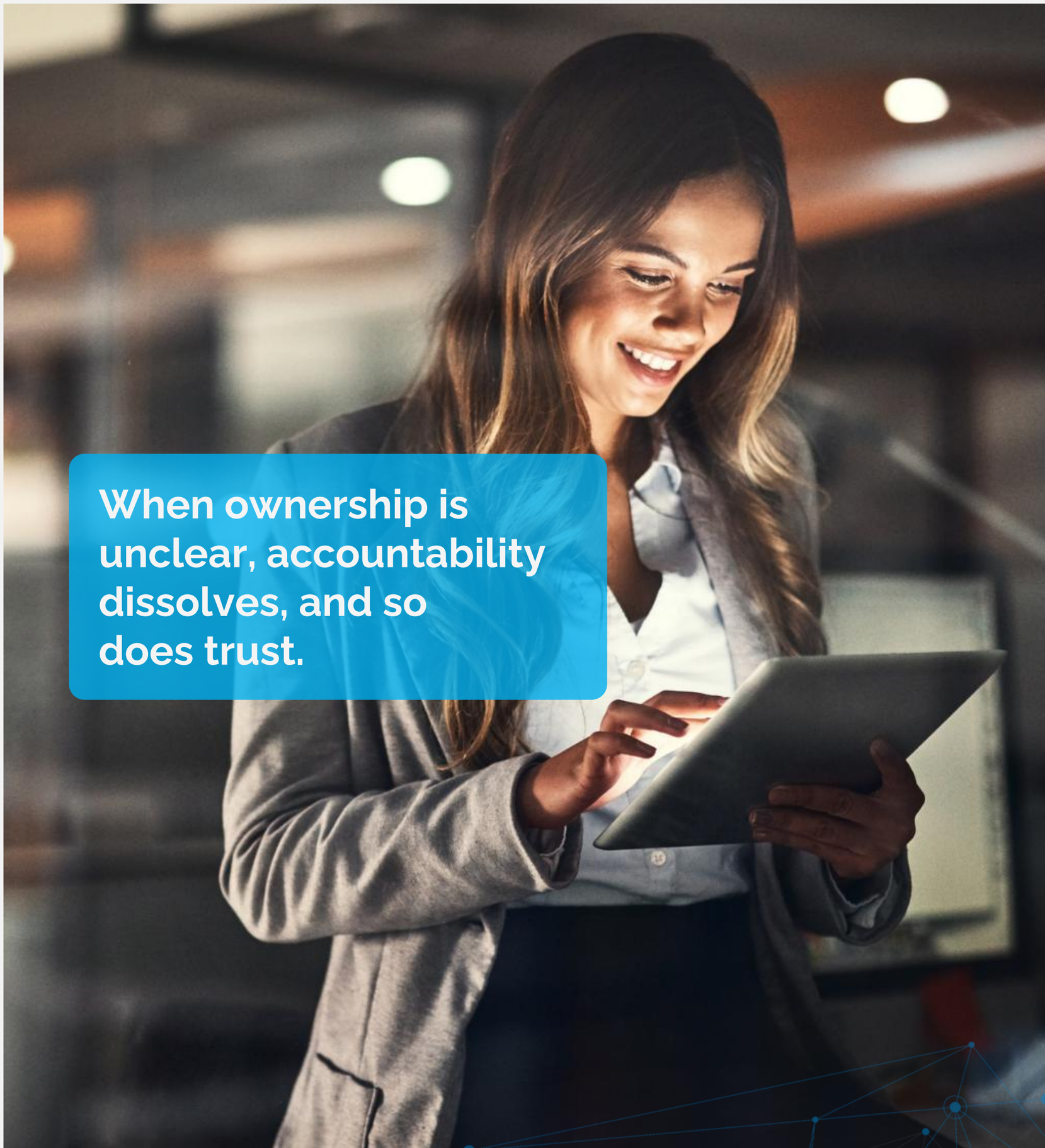
When ownership is unclear, accountability dissolves, and so does trust.

From Untrained to Empowered: The Human Shift

For years, the role of the Functional Application Owner evolved informally, born out of necessity rather than design. Business users took ownership of applications to move faster and meet immediate needs, not realizing they were assuming accountability for updates, testing, and security.

Juriba enables organizations to turn that hidden risk into a managed advantage by combining automation, visibility, and governance.

1. Juriba State of the Windows Application Management Nation Report
2. According to ISACA State of Cybersecurity 2023 | ISACA



With Juriba's App Readiness and App Owner solutions, organisations can:

1 **Automate Operations**

Automate up to 80% of applications, freeing IT teams from manual coordination and repetitive effort.

2 **Accelerate Testing**

Achieve 97% faster application smoke testing through robust package testing.

3 **Reduce Costs**

Reduce application management costs by up to 40%, enabling teams to focus on high-value, complex, and security-critical initiatives.

4 **Rapid Response**

Accelerate IT responsiveness and employee satisfaction with rapid application packaging and testing completed in just 7–15 minutes, available 24/7/365.

5 **Improve Visibility**

Improve visibility and reduce risk associated with unmanaged applications by identifying those lacking ownership, assigning clear responsibility, and receiving alerts when owners fail to respond or leave.

6 **Scale with Confidence**

Scale packaging, testing, and publishing across thousands of applications with consistency and compliance.

7 **AI Intelligence**

Leverage Juriba AI intelligence to remove human error from command-line selection and automate complex steps.

Visibility Is the New Currency of Trust

Application ownership is no longer just an operational issue; it's a measure of organizational resilience. Every unmanaged, unpatched, or unowned application represents not only a security gap but a credibility gap.

Enterprises that bring structure, automation, and shared accountability to their application estate don't just reduce risk; they gain agility, compliance, and confidence across every function.

Juriba's vision is to make readiness a built-in capability, not a reactive chore. When every application is visible, every owner accountable, and every patch assured, via automation or applied human intervention when business need or risk requires, your organization isn't just compliant; it's confident.

Next Steps – lets talk

To learn more about how Juriba can help your organization achieve full application visibility, readiness, and control, please contact us: or download our Windows Application Management Risk Qualification Survey to help you size and understand the risk in your enterprise today.

Visit our Application Management site

Why not...

Complete the Application Management Risk Assessment to Qualify the Risk in your Organization

Read Juriba's 2025 State Of The Windows Application Packaging Nation Report

Take the Application Management Risk Calculator to evaluate coverage and compliance

Or contact us to

Take a Product Tour

Request a Personal demo

Speak to the team to find out more

Built for IT People, by IT People.

Helping large organizations manage Digital Workplaces at scale

Juriba helps you manage your Windows applications and devices easily and at scale. Together, we reduce risk and costs while driving IT transformations so you can deliver business outcomes faster.

Visit: www.juriba.com

Juriba Limited

83 Victoria Street
London, SW1H 0HW
United Kingdom

UK: +44 20 7873 2225
www.juriba.com