The Hidden Cost of Incomplete Application Coverage

Every large organization carries a form of invisible risk: created by unowned and unmanaged applications.

These are applications that continue to run on desktops, virtual machines, or cloud environments but sit outside formal packaging, testing, or compliance workflows.

juriba

The Scale of the Problem

According to responses to our *Application State of the Nation survey* **43% of Windows applications in the average enterprise are unmanaged[1], with no clear ownership or governance trail**. These applications often bypass patching, testing, or version control, creating security and compliance blind spots.

Industry data supports this concern. The Ponemon Institute Report 2024[2] found that **nearly 60 % of organizations** that experienced a data breach reported that **the breach was due to a known vulnerability for which a patch was available but had not been applied**.

ISACA's State of Cybersecurity 2023 found that **over half of enterprises experienced incidents were tied to poor patch governance or unowned software** (ISACA, 2023) [3].

.

These unmanaged assets are not just operational inefficiencies. They are hidden liabilities that can breach compliance, inflate support workloads, and delay strategic change.

60%

of breaches stem from known but unpatched vulnerabilities[2]

[1] According to Bob Kelly's findings on the Windows App Management State of the Nation survey. *Actual exposure will vary by organisation*

[2] According to Ponemon Institute survey, as reported by ServiceNow

[3] According to ISACA State of Cybersecurity 2023 | ISACA

When Progress Creates Exposure

The decentralisation of application ownership began as a sensible move. Empowering business units to manage their own tools improved responsiveness and user experience. But over time, agility outpaced control.

Application Owners — users in HR, Finance, or Operations who "own" their applications, often don't realise they are responsible for patching or security. Meanwhile, IT remains accountable for compliance and service continuity but lacks the visibility to enforce governance.

The result is a widening "readiness gap" between what IT manages and what the business runs. This is where risk, delay, and duplication live. However, with business pressures, it's not an easy fix:

.

Estimated Cost to Fix

.

Gartner's 2024[1] IT Operations Budget Guidance suggests that IT budgets would need to grow by over 30% to absorb full ownership of all business-managed applications, while most CTIOs are still expected to cut operating costs by 5–10% annually (Gartner, 2024.)

This structural mismatch means that current working practices and budgets cannot keep up with the scale or velocity of modern application estates

30%

Budget Growth Needed

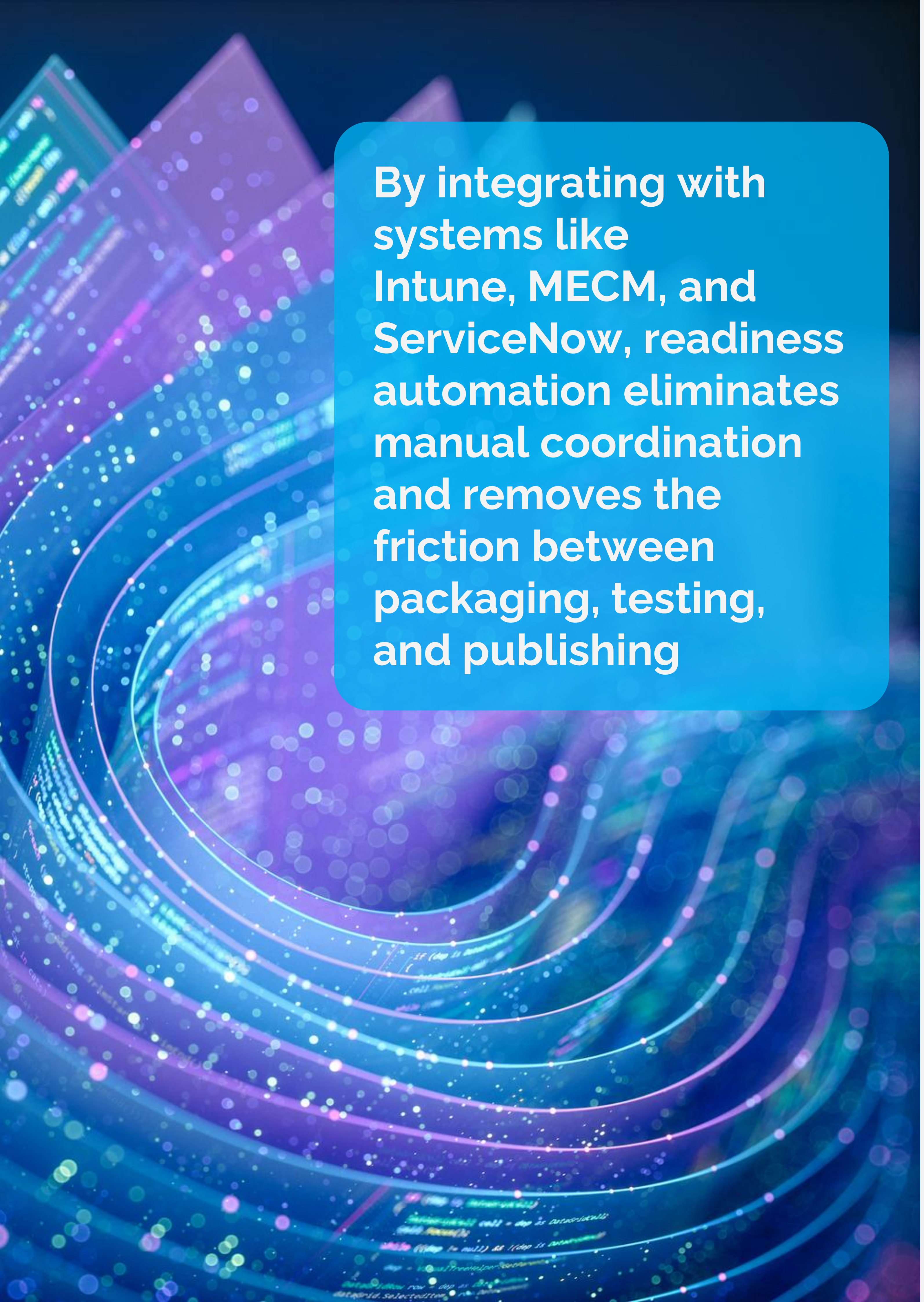
IT budgets would need to grow by over 30% to absorb full ownership of all business-managed applications

5-10%

Expected Cost Cuts

Most CIOs are still expected to cut operating costs annually

[1] According to IT Key Metrics Data 2024: Working with IT Budget and Comparison Tools



By integrating with systems like Intune, MECM, and ServiceNow, readiness automation eliminates manual coordination and removes the friction between packaging, testing, and publishing

A New Approach: Readiness Automation as a Control Layer

Application Readiness Automation introduces a new operating model. Rather than centralising ownership back to IT, automation acts as a control layer that connects and governs distributed processes..

Every application, whether owned by IT or the business, follows the same automated readiness workflow: **discovery, packaging, smoke testing, validation, and deployment.**

.

Automation Provides

Coverage

Applications becomes visibility owned and tracked.

Consistency

Standardised packaging and testing ensures uniform quality.

Confidence

Automated validation and audit trails create compliance assurance.

.

....this isn't change through disruption. It's change through enablement

The Measurable Gains of Change: Speed, Consistency & Control

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**

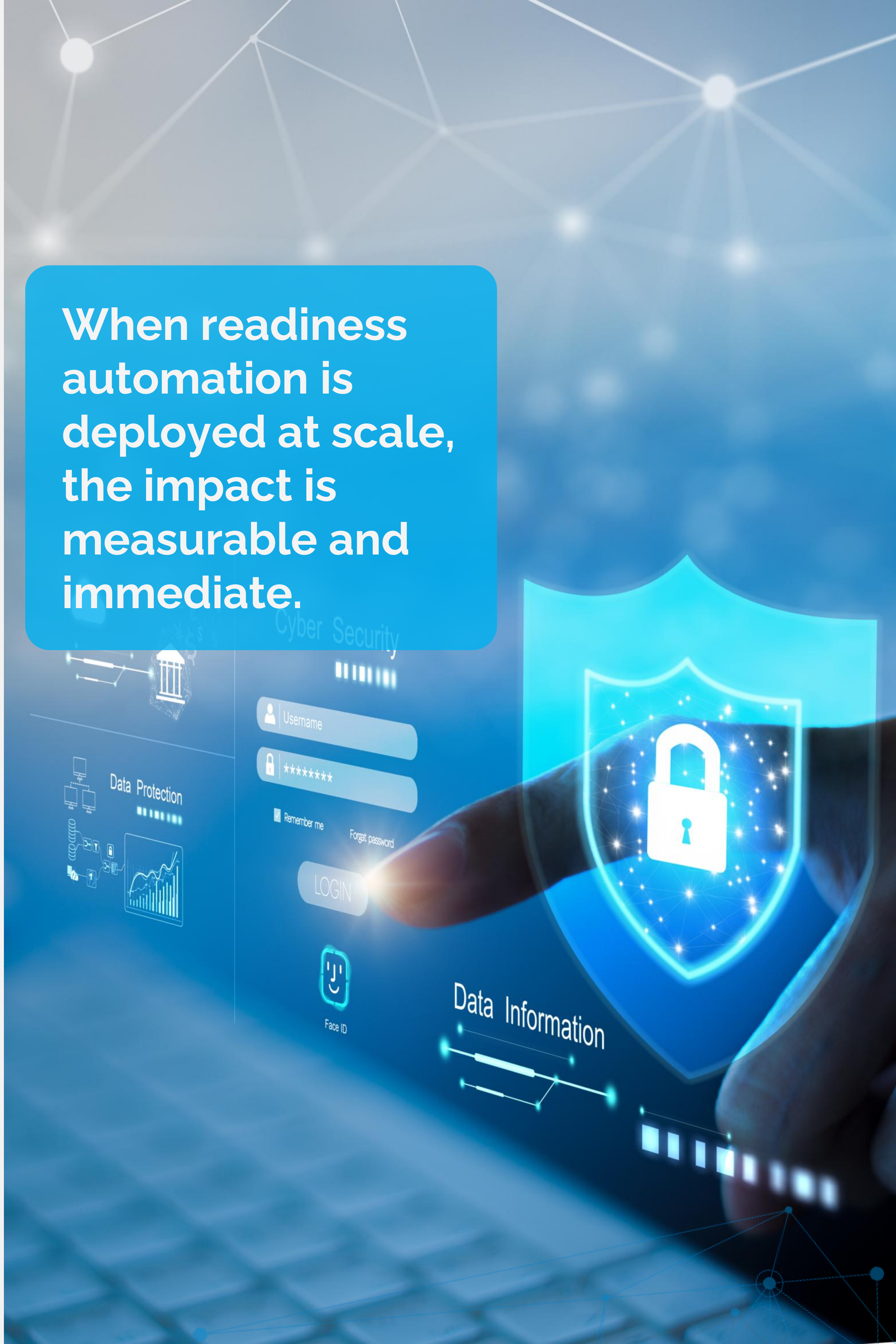
Improve visibility and reduce risk associated with unmanaged applications by identifying those lacking ownership, assigning clear responsibility, and receiving alerts when owners fail to respond or leave.

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 find answers faster and even automate application repackaging tasks.



When readiness automation is deployed at scale, the impact is measurable and immediate.

Customer Outcomes With Application Readiness

With our Application Readiness solutions, our customers have been able to achieve the following business benefits:

Business Case For US Enterprise Defence Contractor

-60%
Av Package Cost

$1634
reduced to
$467

For a typical simple & medium complexity application package (blended rate)

-94%
Creation Cycle

33 Hours
reduced to
2 Hours

For a typical medium complexity (unattended install) application package

+332%
Team Capacity

498 Packages
increased to
1,654 Packages

Enabling the packaging team to do significantly more with the same resources

-92%
App Workloads

607 Days
reduced to
47 Days

Allowing the packaging team to work on complex apps and greater app coverage

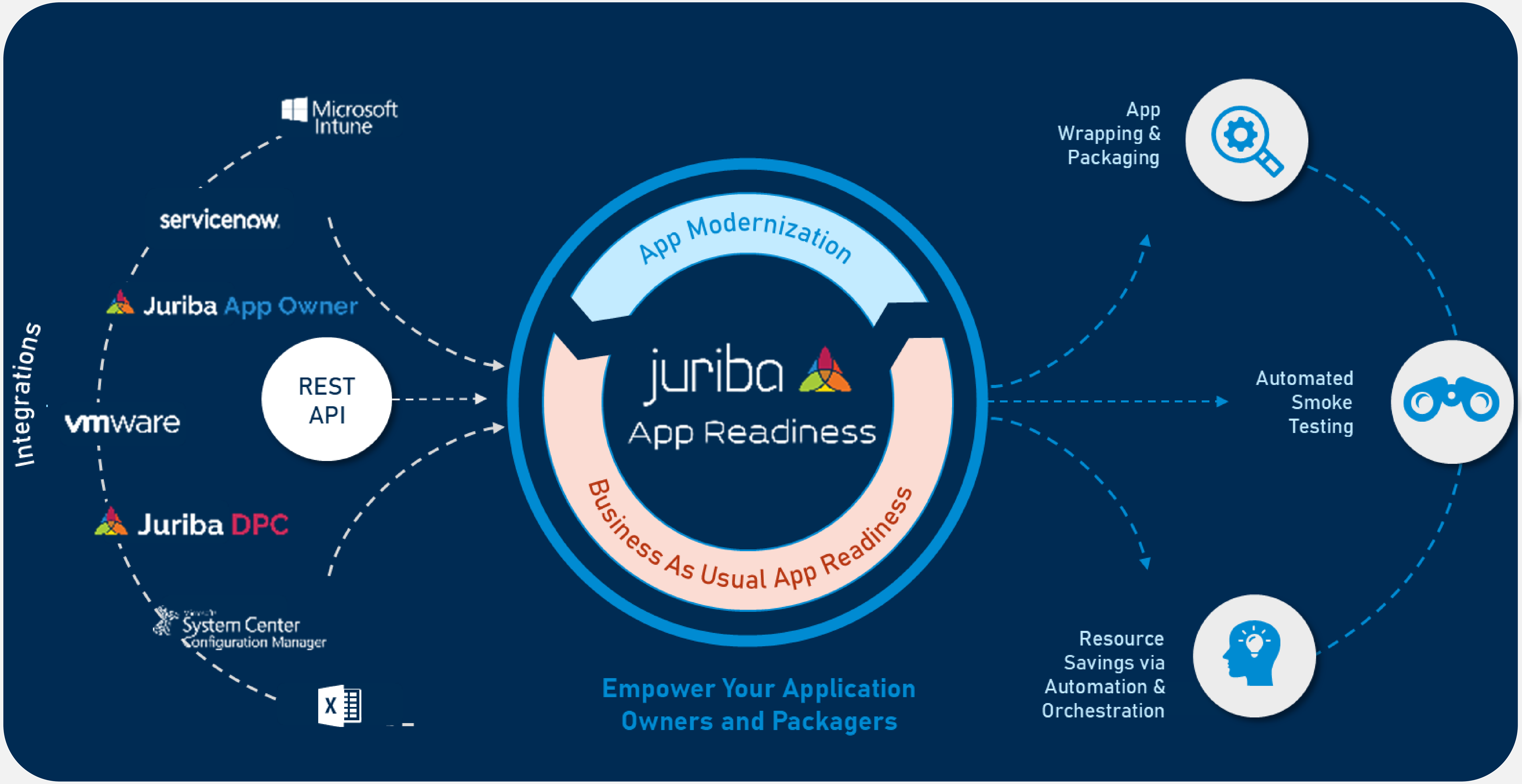
+180%
App Coverage

500 Apps
increased to
898 Apps

Reducing risk by bringing more applications into a managed environment

App Readiness Automates Windows App Management

Below illustrates the App Readiness ecosystem: the platforms it works alongside, and the automation stages it supports, from packaging through validation and publishing.

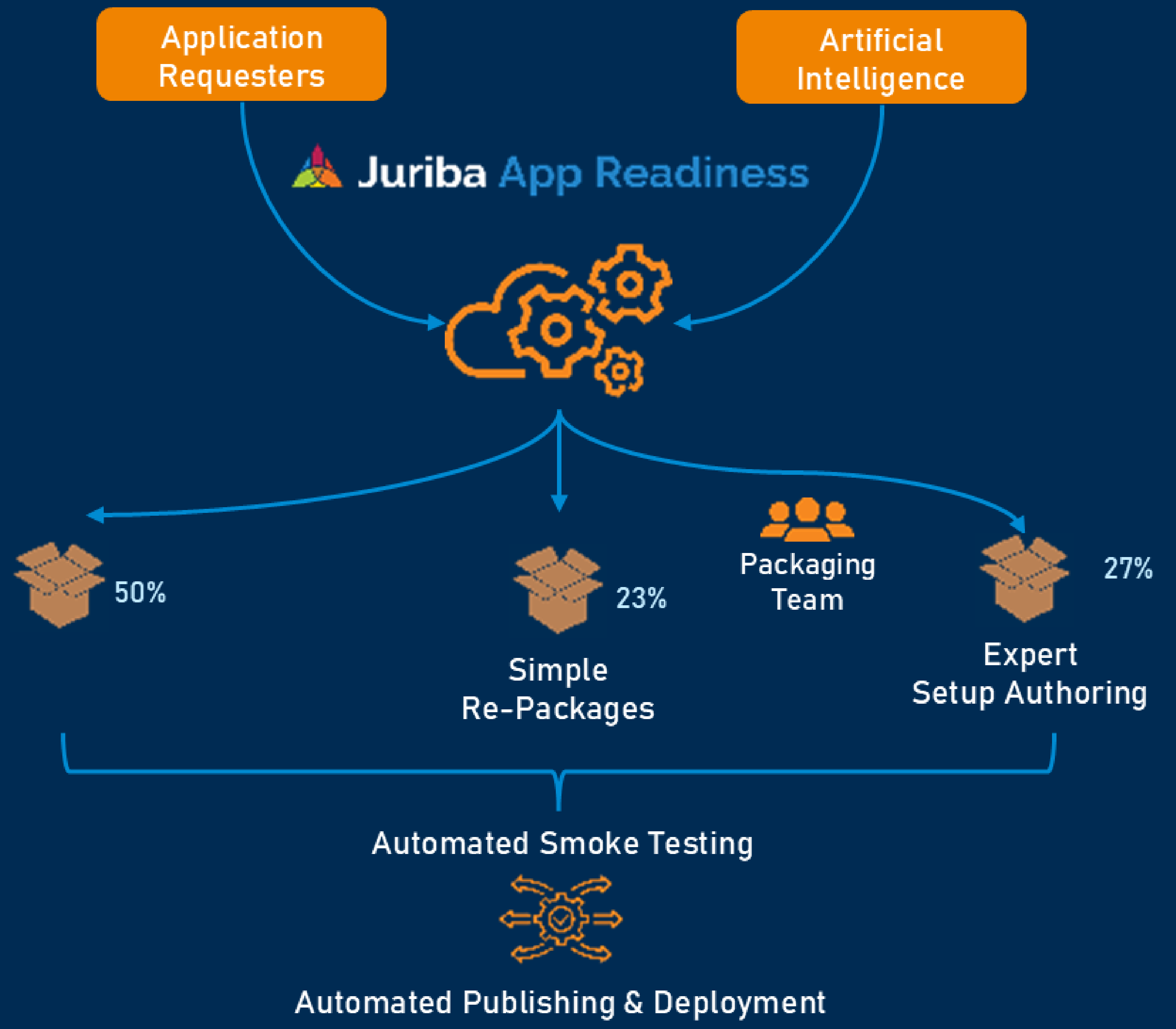


Empower Your Application Owners and Packagers

App Readiness Automates Windows App Management

To drive the following outcomes:

:



How It Works:
Architecture of Readiness Automation

Automation Workflow

Discovery

App Readiness performs analysis and makes recommendations on any application setup (in-house or off-the-shelf).

Packaging

Automate the creation of command line or repackaged installers for deployment with MSI, MSIX, PSADT, and more.

Testing

Automated smoke testing validates the deployment package, confirming successful installation, execution, and removal.

Validation

Workflow automation routes approvals to relevant Application Owners.

Deployment

Integrated publishing to Intune and MECM automates deployment readiness.

Reporting

Central dashboards provide visibility of status, coverage, and risk posture.

Technical Integration

- **Deep Integration** with Intune, MECM, Azure, and more.
- **REST APIs** connect to ServiceNow and many popular ITSM tools.
- **Role-based access** enables controlled collaboration between IT, Application Owners, and Security.
- **AI-assisted command line recognition** speeds unattended repackaging and reduces human error.
- **Event orchestration** automates repackaging and testing based on patch schedules or change events.

This architecture transforms application readiness from a resource-heavy bottleneck to a continuous, governed process

Closing the Managed and Unmanaged Gap

Unmanaged applications represent the "dark matter" of IT, present, active, but invisible.

App Readiness closes this gap by enabling 100% coverage. App Owner provides ownership mapping. Together, they provide you with continuous readiness monitoring. When applications lack an identified owner, IT has clear visibility into unmanaged coverage, enabling targeted review and informed risk management..

This approach turns previously invisible risk into measurable, actionable insight, enabling IT to achieve full coverage without adding headcount or bureaucracy.

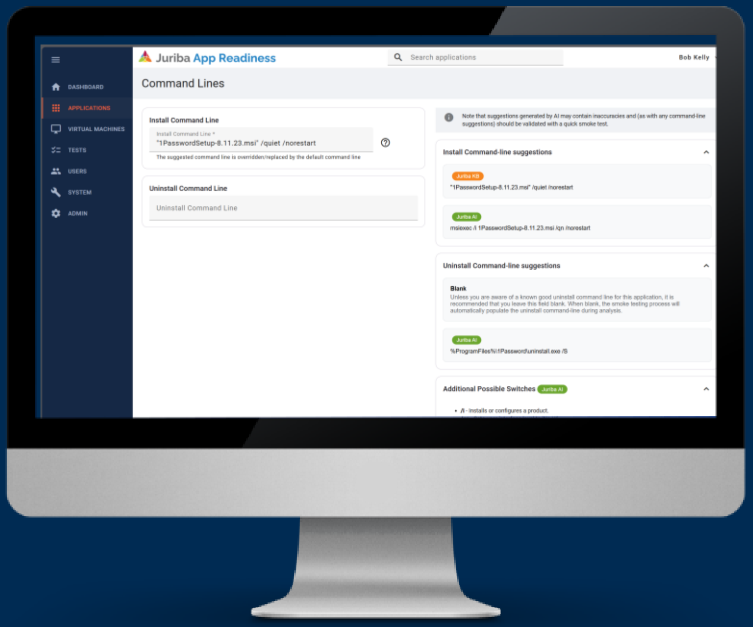
Visibility as the New IT Currency

Visibility has become the ultimate measure of credibility for IT leadership

When every application is tracked, tested, and governed, IT can make decisions based on data, not assumptions. Visibility underpins compliance, resilience, and agility — the cornerstones of enterprise confidence.

Application coverage isn't just an IT metric anymore; it's a leadership measure of control

Automation doesn't just make packaging faster; it makes governance provable.



Command Lines

Install Command Line

Install Command Line *
"1PasswordSetup-8.11.23.msi" /quiet /norestart
The suggested command line is overridden/replaced by the default command line

Uninstall Command Line

Uninstall Command Line

Note that suggestions generated by AI may contain inaccuracies and (as with any command-line suggestions) should be validated with a quick smoke test.

Install Command-line suggestions

```
"1PasswordSetup-8.11.23.msi" /quiet /norestart
msiexec /i 1PasswordSetup-8.11.23.msi /qn /norestart
```

Uninstall Command-line suggestions

Blank
Unless you are aware of a known good uninstall command line for this application, it is recommended that you leave this field blank. When blank, the smoke testing process will automatically populate the uninstall command-line during analysis.

```
%ProgramFiles%\1Password\uninstall.exe /S
```

Additional Possible Switches

- /I - Installs or configures a product.

About Juriba

At Juriba, we help some of the world's largest and most complex organisations orchestrate digital workplace change with confidence.

Our platform combines **Digital Platform Conductor (DPC)** and **Windows Application Management** to provide global, highly regulated enterprises with a single system of record and execution for application readiness, application lifecycle management, device and OS migrations, and continuous change.

Designed for scale, governance, and auditability, Juriba replaces fragmented tools and spreadsheets with automated workflows, real-time insight, and policy-driven control across End User Computing and application management.

Trusted by global enterprises operating across multiple regions, regulatory frameworks, and millions of endpoints, we reduce risk, increase delivery certainty, and enable IT teams to operate with confidence at scale.

Because change is constant and IT is the engine that powers the organisation, it has to be executed correctly, with the end user in mind.

Juriba: Built for IT people, by IT people

Learn More about Application Risk

Application Readiness Risk Qualification Survey

Application Readiness Risk Calculator

Juriba Limited

83 Victoria Street
London, SW1H 0HW
United Kingdom

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

Visit: www.juriba.com