EBOOK

THE *INFRASTRUCTURE* AI AGENTS NEED TO OPERATE IN INSURANCE

Growing AI capabilities without compromising security, speed, or control

In times of uncertainty, insurance becomes deeply personal. Behind every policy is a family, a business, or a community relying on clarity, speed, and sound judgment when it matters most.

Today, that responsibility is intersecting with a powerful wave of generative AI that is changing how insurers operate. Traditional AI has long supported actuarial modeling and risk analytics. Generative AI expands those capabilities by interpreting unstructured data and enabling more personalized, context-aware customer engagement. Agentic AI goes further still, automating complex workflows across underwriting, claims, distribution, and service. Together, these technologies have the potential to fundamentally transform the insurance value chain.

Scaling AI in insurance is not simply a technology challenge. It's an operational one. While adoption is growing, enterprise-wide integration remains rare. According to McKinsey & Company, most insurers have implemented AI somewhere — but only a small percentage have scaled it across domains in ways that deliver measurable business impact.[1]

Unlocking AI's full potential requires more than isolated pilots or point solutions. It demands domain-level modernization that reshapes underwriting, claims, and distribution operations around modern data foundations, standardized development environments, and secure, reproducible delivery practices.

Early results speak volumes: Domain-based AI implementations have driven double-digit improvements in sales conversion and premium growth, reduced onboarding costs by 20–40%, and improved claims accuracy.[2] The opportunity of AI for insurers is real — the question is whether existing technology foundations are built to support it.

How modern software delivery practices are changing outcomes

Against this backdrop, Docker partnered with theCUBE Research to quantify how modern software delivery practices are changing outcomes across large enterprises. The independent study surveyed 393 IT and application development leaders to measure the impact of Docker's standardized development environments, secure software supply chain controls, and DevOps enablement on AI delivery, security posture, productivity, modernization, and ROI.[2]

This industry guide applies those findings through an insurance lens. It focuses on how industry leaders are utilizing Docker to achieve AI success at scale, driving security, productivity, modernization, and ROI.

Continue reading to explore how insurance companies can build secure, AI-ready software delivery foundations with Docker. You'll learn how these foundations can help reduce friction for development teams, strengthen governance and security controls, accelerate modernization, and drive business outcomes that leaders can stand behind.

"Docker gave us more than containers. It gave us control. Now, every developer has a consistent, secure environment, and we ship confidently every day."

Dheeraj Arani, Head of DevOps, InCred Financial Services

Why the current models can't keep up

AI holds immense promise for insurers.
But scaling it across the enterprise remains the exception, not the norm.

Security risks, rising infrastructure costs, supplier lock-in concerns, talent shortages, governance gaps, and deeply embedded legacy systems frequently slow progress.[4] Although the insurance industry leads in AI adoption, roughly two-thirds of insurers remain in piloting stages. Only a small minority — approximately 7% — have moved beyond proof of concept and into production throughout the organization.[3]

The greatest constraint isn't funding — it's foundational. Weak data and AI foundations, fragmented technology stacks, and poor alignment between business and technology teams stall enterprise adoption.[4] Legacy technology compounds the challenge, with policy administration, underwriting, and claims systems frequently operating across siloed platforms with inconsistent tooling, environments, and workflows. Scaling AI in insurance, therefore, requires more than adding new tools. It demands domain-level rewiring: modernized data foundations; standardized development environments; secure, reusable AI components; and consistent controls that operate reliably across development, testing, and production.

At the same time, development teams are no longer just building applications. They are architecting intelligent, autonomous systems that must be secure, compliant, reproducible, and instantly scalable. Fragmented environments and inconsistent supply chain controls introduce risk precisely where insurers can least afford it: inside underwriting decisions, claims automation, fraud detection, and customer-facing AI services.

And as AI adoption intensifies, insurers must deal with privacy, bias, traceability, security, compliance, employee adoption, and regulatory ambiguity, with many executives rating these challenges as "highly challenging."[5]

Here's the good news for insurers: Organizations that standardize development environments, embed security earlier in the lifecycle, and tightly align development with CI/CD and delivery practices are materially better positioned to scale AI safely and efficiently.[2]

Docker sits at the center of that shift, providing a standardized, secure development foundation that insurers rely on to accelerate AI-enabled software delivery while reducing operational and regulatory risk.

More than a container tool, Docker provides a purpose-built container platform designed to drive developer productivity, secure the software supply chain, and scale cloud-native and AI-driven applications.

"(Docker is) not just a tool — it's a symbol of the shift toward modern, developer-friendly practices…(it) has improved engineer satisfaction, supports onboarding, and enables the kind of innovation that helps us retain top talent in a competitive market."

Sarah Andres, Former Principal Architect, Availity

What the data reveals: key findings from theCUBE Research

Independent findings from theCUBE Research show that organizations adopting Docker as a standardized software delivery foundation achieve materially better outcomes across AI delivery, security posture, productivity, modernization, and ROI. Docker delivers this through:

- **Standardized development environments**
- **Secure, trusted content**
- **Reliable access controls**
- **AI-accelerated development**
- **Continuous supply chain insights**

The following insights highlight the outcomes that matter most in today's regulated, high-risk environments.

AI acceleration and reliability

For insurance organizations, speed and reliability are business imperatives. Today's digital and AI systems underpin core functions across underwriting, claims processing, fraud detection, pricing, distribution, and policy servicing. These systems influence risk selection, loss outcomes, customer experience, and regulatory compliance. As they grow more complex — and more central to decision-making — delivering them quickly, securely, and with full auditability becomes a competitive and fiduciary necessity.

Yet many insurers struggle to scale these AI initiatives because development environments vary across teams, regions, and lifecycle stages. That inconsistency introduces configuration drift, testing gaps, and deployment failures — risks that can directly affect underwriting accuracy, claims automation reliability, and regulatory auditability.

Research from theCUBE shows that Docker addresses this barrier by standardizing the developer inner loop with reproducible, production-aligned environments. AI agents don't just need models; they need infrastructure. To operate reliably in production, agents must spin up environments, call tools, and run code in ways that are sandboxed, governed, and secure by default. Docker provides exactly that: the execution layer that makes agentic workflows secure, governed, and production-ready in regulated environments. As a result, organizations reduce setup friction, strengthen validation rigor, and significantly lower failure rates as AI systems move into production.

% of surveyed orgs	Outcome
41%	51–75% faster AI setup time
44%	26–50% fewer project failures or delays
53%	Significantly improved AI testing and validation

These results are driven by Docker's integrated AI development capabilities, which standardize how models and agent systems are built, tested, governed, and deployed across the enterprise:

- Docker Model Runner enables secure, GPU-accelerated model execution with full control over data privacy, so AI models can be validated in isolated environments before they ever touch production data.
- The MCP Catalog and Toolkit provide centralized authentication and governed access across containerized AI services, giving insurance teams consistent control over which tools agents can access in compliance-sensitive environments.
- Docker Agent removes the complexity of building and deploying AI agents. Teams define models, tools, and behaviors in simple YAML, then package and share agents through an OCI registry to run consistently across every environment. This means less custom code, faster iteration, and agents that behave predictably in production.

What the data reveals: key findings from theCUBE Research

Security, compliance, and vulnerability reduction

As AI adoption increases, so do regulatory expectations around privacy, bias, traceability, and supply chain security. Docker strengthens these challenging elements by embedding protection earlier in the software lifecycle, helping to reduce vulnerabilities before applications reach production:

% of surveyed orgs	Outcome
43%	26–50% vulnerability reduction
17%	50%+ vulnerability reduction
53%	Significant improvement in security posture
81%	Achievement of compliance goals

Reducing vulnerabilities at the source improves audit readiness and aligns with regulatory expectations for software supply chain and third-party risk management. Docker delivers this through multiple layers of protection:

- Docker Hardened Images provide minimal, signed, and continuously verified base images built to meet enterprise security and compliance standards, reducing CVE exposure before it reaches production.
- Docker Scout delivers continuous vulnerability analysis and policy evaluation across containerized services, giving security and compliance teams ongoing visibility into risk across the development lifecycle.
- Hardened Docker Desktop enforces policies and isolates environments directly on developer workstations, reducing endpoint risk in compliance-sensitive environments.
- Docker MCP Toolkit centralized authentication restricts credential exposure, preventing unauthorized tool access across agent development workflows.

What the data reveals: key findings from theCUBE Research

Developer productivity and DevOps maturity

Modern insurance technology teams must bridge legacy systems with cloud-native architectures while maintaining strict compliance controls. Docker improves developer productivity by standardizing environments and aligning inner-loop development with CI/CD workflows.

Docker improves developer productivity across key workflows:

- Accelerates development workflows with fast, consistent environments that reduce setup times and friction, so your teams spend less time configuring and more time building.
- Reduces rework and release failures by standardizing workflows from development to production, eliminating the configuration drift that creates risk in complex, regulated systems.
- Streamlines onboarding and collaboration across engineering teams, using shared container standards and reusable dev environments, helping you scale development capacity without sacrificing consistency or control.

% of surveyed orgs	Outcome
73%	Significant workflow efficiency gains
64%	Productivity improvements of 26–50%
39%	Completion of a full DevOps transformation
65%	Significant improvement in development and CI/CD alignment
68%	Improved cross-team collaboration

More consistent workflows reduce rework, errors, and release fragility while preserving governance. The result is faster iteration, fewer environmental issues, smoother collaboration, and a significant boost in developer productivity and organizational DevOps capabilities — all of which make Docker a foundational accelerator for modern software delivery.

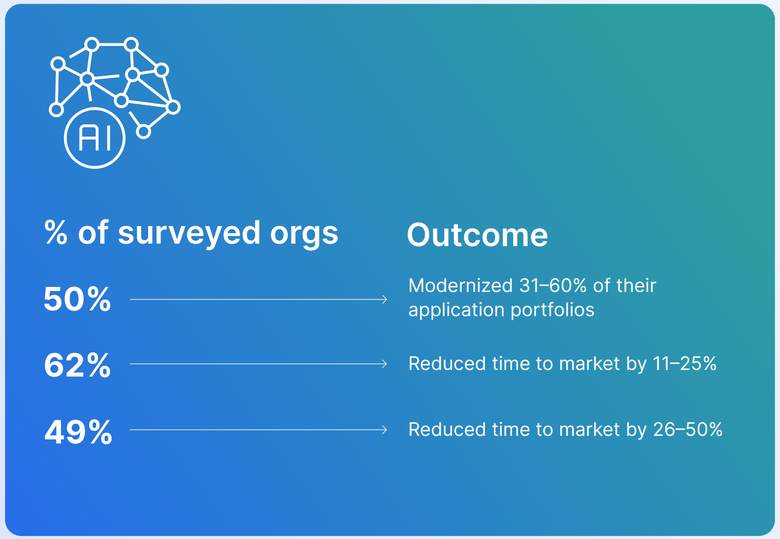
What the data reveals: key findings from theCUBE Research

Application modernization and time to market

Modernization is a top priority in insurance, but few organizations can afford to rip and replace critical systems. Docker enables incremental modernization by bridging legacy platforms and modern cloud-native architectures, allowing teams to deliver new capabilities without destabilizing existing systems.

Docker supports modernization and faster time to market across the application lifecycle:

- Containerizes legacy applications without replatforming, allowing insurance technology teams to modernize policy administration, claims, and underwriting systems without disrupting core operations.
- Introduces new features and services faster, using consistent packaging and deployment workflows and reducing delivery friction in environments where release reliability is nonnegotiable.
- Supports hybrid environments and gradual migration, enabling teams to bridge legacy infrastructure with cloud-native architectures at a pace that manages operational and regulatory risk.
- Scales cloud-native and AI-driven applications while preserving controls, helping you modernize securely within existing compliance frameworks.



theCUBE Research shows the impact of these modernization strategies:

theCUBE Research findings show that Docker enables incremental modernization and materially accelerates delivery timelines. These outcomes allow insurers to modernize underwriting, claims, and distribution systems without destabilizing core platforms.

What the data reveals: key findings from theCUBE Research

Business value and ROI

The research makes clear that these gains translate into measurable financial outcomes. Respondents consistently reported meaningful cost savings and strong ROI.

Docker's business value extends beyond development efficiency. By reducing vulnerabilities before production, accelerating modernization timelines, and enabling teams to deliver AI capabilities faster, Docker delivers measurable financial impact that CFOs and CISOs can quantify:

% of surveyed orgs	Outcome
43%	Saved $50,001–$250,000 annually
22%	Saved $250,000–$1 million annually
6%	Saved more than $1 million annually
41%	Achieved 101–200% ROI
22%	Achieved 201–500% ROI
6%	Achieved an ROI above 500%

Docker delivers substantial financial impact by reducing operational costs, accelerating modernization, and increasing development efficiency. Organizations consistently report meaningful annual savings and high ROI — often far exceeding initial investment — confirming Docker's abilityto translate technical acceleration into bottom-line business value.

"We've achieved over $1 million in annual savings (with Docker). The productivity gains and reduced infrastructure overhead alone justify the investment."

Ian Brown, Engineering Manager, JVM Ecosystem, Netflix

Next steps for foundational AI-ready software delivery

Insurance organizations are at a crossroads. Across underwriting, claims, distribution, and service, AI is moving from experimentation to operational necessity. At the same time, regulatory complexity, customer expectations, and competitive pressures continue to intensify. The question is no longer whether to adopt AI but whether existing technology foundations can support it at scale.

The research points to a clear conclusion: Insurers that establish a standardized, secure foundation for software delivery are better equipped to scale AI, reduce operational and regulatory risk, modernize legacy systems, and deliver measurable business value.

For insurers, progress does not require abandoning core platforms or taking on unnecessary risk. It means strengthening the foundation that underpins how applications and AI systems are built, secured, and deployed.

Docker's practical blueprint helps insurers achieve AI success at scale through five essential steps:

1

Establish consistent development environments across teams to reduce variability, improve collaboration, and standardize how underwriting, claims, and policy applications are built and tested.

2

Implement centralized controls for identity, policy, and access to enforce organization-wide security and compliance standards across development and production.

3

Integrate container-based delivery into existing infrastructure to enable incremental modernization without disrupting core policy administration or claims systems.

4

Operationalize AI development workflows by providing secure, governed access to third-party services and ensuring development environments are aligned across domains.

5

Align software delivery with enterprise CI/CD practices to reduce time to market, increase release reliability, and support continuous improvement at scale.

This path enables insurers to support AI initiatives that are secure, reproducible, compliant, and scalable. Insurance organizations that build on Docker aren't just solving today's delivery challenges; they're laying the groundwork for the next generation of autonomous, AI-driven operations.

To explore the full findings behind this guide, read the complete theCUBE Research x Docker report.

To see how Docker can help your organization build secure, AI-ready software delivery at enterprise scale, connect with the Docker team.

1. Milinkovich, N., et al., "The Future of AI in the Insurance Industry," July 2025.
2. "Docker's Impact on Agentic AI, Software Supply Chain Security, Developer Productivity, ROI," theCUBE Research, October 2025.
3. Khoury, J., et al., "Insurance Leads in AI Adoption. Now It's Time to Scale.," Boston Consulting Group (BCG), September 2025.
4. Suhrada, S, et al., "Are Insurers Truly Ready to Scale Gen AI?," Deloitte Center for Financial Services, April 2025.
5. "The Impact of Artificial Intelligence on the Insurance Industry," KPMG, 2024.

docker