EBOOK

A NEW REALITY FOR FINANCIAL SOFTWARE DELIVERY

Fresh insights from theCUBE Research analysis of IT and AppDev leaders

Financial services organizations are facing a convergence of pressures reshaping how software is built, secured, and delivered. Digital-first customer expectations continue to rise, necessitating faster releases and always-on availability. At the same time, security threats are becoming more sophisticated and persistent, while regulatory scrutiny intensifies around software supply chains, third-party risk, and operational resilience. For banks, payment providers, and capital markets firms, software delivery has become a critical control point for maintaining speed, security, and trust.[1,2]

AI is accelerating this transformation. As financial institutions begin deploying AI in production systems — for everything from fraud detection and transaction monitoring to credit decisioning and customer engagement — the reliability and governance of the underlying delivery process matter more than ever.

These systems directly influence financial outcomes and regulatory exposure. In response, technology leaders are under pressure to modernize development practices without increasing operational or compliance risk.[3]

Financial institutions can't meet today's digital, security, and AI demands with fragmented tools and inconsistent environments. Modern software delivery requires a unified foundation that standardizes how applications are built and run, embeds security earlier in the lifecycle, and enables teams to move faster without sacrificing control. This foundation is essential not only for scaling reliably but also for strengthening security posture, modernizing legacy systems, and delivering business value across the enterprise. Docker solves this by providing a standardized, secure, and developer-friendly container platform that accelerates software delivery across any environment.

Continue reading to explore how financial services organizations 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.

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.[4]

This industry guide applies those findings through a financial services lens. It focuses on how financial institutions are utilizing Docker to address regulatory requirements, legacy environments, and the rising pressure to accelerate the safe delivery of digital and AI capabilities.

The challenges for financial services leaders as digital, security, and AI pressures converge

For banks and financial institutions, digital and AI initiatives often begin as isolated pilots. As a result, development environments may differ from team to team. In many cases, security and compliance controls are unevenly applied. Moving from experimentation to production becomes slow, fragile, and risky. Time to value stretches out, failures increase, and confidence erodes.

This challenge reflects the broader strain across financial software delivery in the AI era.

Legacy core systems are being combined with cloud-native architectures, requiring development teams to operate across hybrid environments. The resulting tool sprawl slows the inner development loop. It also leaves security teams to govern increasingly complex software supply chains with controls that were never designed for modern delivery models.

Expectations on technology leaders have reached a tipping point. Now, more than ever, boards and executive teams want clear answers to practical questions:

- How quickly can we deliver new capabilities without increasing risk?
- How do we strengthen security earlier in the lifecycle?
- How do we modernize incrementally without disrupting core systems?
- How do we prove that these investments deliver measurable business value?

Yet most financial institutions remain constrained by fragmented environments and inconsistent controls, making it difficult to answer these questions with confidence.

itaú

“Docker has proven to be an effective solution for achieving the level of security and virtualization that meets our institution’s requirements.”

Lucas Polaquini, Staff Software Engineer, Itaú Unibanco

Why the current models can't keep up

For many financial services organizations, the gap between what the business demands and what delivery models can support is widening. Secure AI adoption, cloud-native development, and modernization efforts are moving faster than the engineering foundations beneath them.

While financial services use cases continue to expand, the underlying environments remain fragmented. AI- and agent-based development, in particular, is straining existing practices. Dev teams rely on inconsistent configurations, tooling, and data access patterns across business units and infrastructure. Setup is slow. Testing is non-standardized. Moving models from development into production introduces delays and risk at precisely the point where reliability matters most.

This fragmentation creates practical consequences. Projects stall while environments are rebuilt. Failures surface late in the lifecycle. Confidence drops as teams struggle to reproduce results across development, testing, and production. What begins as an innovation initiative often turns into a coordination problem.

Security and compliance pressures intensify these challenges. Existing governance models are strained as financial institutions adopt cloud-native architectures and begin deploying AI. Vulnerabilities in the software supply chain are increasing faster than organizations can manage with traditional tools. Many software businesses lack structured, AI-specific risk assessments and controls, particularly for generative AI systems introduced into existing delivery pipelines.

Regulators and central banks increasingly emphasize model risk, third-party dependency, and systemic exposure, placing greater scrutiny on how AI systems are built, tested, and governed.[5]

Developer productivity is also constrained. Tool sprawl, legacy processes, and misalignment between development workflows and Continuous Integration/Continuous Delivery (CI/CD) pipelines slow delivery. Engineers spend significant time resolving environment-wide issues rather than improving applications. Releases become fragile and cycle times lengthen even as expectations for speed increase.

Modernization efforts face similar friction. Financial institutions rarely have the option of wholesale replacement of core systems. Modern architectures must coexist with legacy platforms during long transition periods. Without consistent packaging, predictable environments, and reliable deployment paths, modernization becomes risky, costly, and slow.

The common thread across all these issues is structural. Current delivery models were not designed for AI-first workloads, hybrid environments, or the level of regulatory and security scrutiny banks and financial services providers now face.

"Although FinServ firms are bullish on GenAI, there is a critical gap in GenAI-specific privacy and risk assessments, with many firms not yet doing structured risk reviews."

State of Generative AI in Financial Services, Forrester Research, 2024

Here's the good news: Financial institutions that address these problems at the foundation level see materially better outcomes. Standardized development environments, secure software supply chain controls, and alignment between development and delivery are becoming go-to optimizations for scaling digital and AI innovations, modernizing safely, and driving value.

Docker helps financial institutions deliver software faster, more securely, and with greater consistency — across every environment. By standardizing how teams build, test, and deploy applications, and embedding security earlier in the lifecycle, Docker reduces risk and accelerates the move from experimentation to production. These capabilities form the foundation modern financial services need to scale AI initiatives, modernize safely, and meet growing regulatory expectations.

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 financial institutions, speed and reliability are business imperatives. Today's digital and AI systems underpin critical services, including fraud detection, transaction monitoring, credit decisioning, Anti-Money Laundering (AML) workflows, customer interactions, and more. As these systems grow more complex, delivering them quickly and securely has become a critical advantage.

theCUBE Research explicitly identifies environment inconsistency and setup friction as major barriers to AI execution. Standardized, reproducible environments reduce setup time, eliminate environment drift, and ensure teams can ship AI workloads to production with greater speed and confidence.

The research shows that Docker reduces one of the primary barriers to AI execution: inconsistent development environments. By providing standardized, reproducible environments, Docker customers significantly reduce setup time, improve testing rigor, and prevent failures as AI projects move into production.

41% of organizations using Docker reduced AI setup time by 51%–75%

44% prevented 26%–50% of AI project failures or delays

53% 53% reported significant improvement in AI testing and validation

These outcomes are made possible with Docker's AI capabilities:

- Run and test models locally with Docker Model Runner, enabling isolated, consistent environments that reduce setup time, cut cloud costs, and accelerate iteration for AI development workflows.
- Access trusted AI services through the MCP Catalog and Toolkit, allowing teams connect to hundreds of containerized MCP servers with one-click authentication while eliminating manual setup and configuration across clients.
- Define and govern agent systems using cagent, versioning complete agent stacks in YAML to ensure reproducibility, auditability, and policy enforcement from development through production.

What the data reveals: key findings from theCUBE Research

Security, compliance, and vulnerability reduction

Security and compliance are board-level concerns in the financial services industry. Organizations can't efficiently accelerate AI or modern application delivery without strengthening the software supply chain, reducing risk at the source, and ensuring consistent compliance. According to Forrester Research, "striking the right balance between innovation and regulation will be crucial to ensuring that digital and AI initiatives remain a force for positive transformation rather than disruption."[5]

Docker strengthens security by embedding protection earlier in the software lifecycle, helping to reduce vulnerabilities before applications reach production:

26%–50% reduction in vulnerabilities (43%)

More than 50% reduction in vulnerabilities (17%)

Significant improvement in security posture (53%)

Extremely effective or very effective security compliance outcomes (112% combined)

Reducing vulnerabilities at the source improves audit readiness and aligns with regulatory expectations for software supply chain and third-party risk management.

Docker provides trusted, minimal, and continuously verified images that reduce vulnerabilities early in the lifecycle and deliver a secure-by-default foundation. The result is quicker deployment of fraud models, risk analytics, and real-time decisioning without increasing operational risk.

Organizations using Docker report substantial declines in security vulnerabilities, major improvements in security posture, and far more consistent compliance outcomes.

Docker strengthens the security posture of financial services organizations through multiple layers:

- Reduces common vulnerabilities and exposures (CVE) with Docker Hardened Images, which are minimal, signed, and continuously verified base images built to meet enterprise security and compliance standards.
- Protects developer workstations with Hardened Docker Desktop, enforcing policies, isolating environments, and reducing endpoint risk in compliance-sensitive environments.
- Governs access to AI tools with Docker MCP Toolkit, centralizing authentication, restricting credential exposure, and preventing unauthorized tool use across agent development.
- Enforces consistent security policies across the SDLC, ensuring centralized auditable controls from local development to production deployment.

Developer productivity and DevOps maturity

Developer productivity directly impacts business continuity, operational resilience, and delivery speed, especially in financial services, where engineering time is expensive and environments are complex. theCUBE Research shows that improving development workflows reduces operational risk, strengthens collaboration, and increases release reliability.

Docker improves developer productivity across key workflows:

- Accelerates local development workflows, enabling fast, consistent inner-loop environments that reduce setup time and friction across teams.
- Reduces rework and releases failures by standardizing dev-to-prod workflows, eliminating configuration drift, and supporting CI/CD alignment.
- Streamlines onboarding and collaboration across engineering teams, using shared container standards and reusable dev environments.

These outcomes are reflected in key findings from theCUBE Research:

73% reported significant workflow efficiency gains.

64% achieved productivity improvements of 26%–50%.

39% completed a full DevOps transformation.

65% reported significant improvement in development and CI/CD alignment.

68% improved cross-team collaboration.

More consistent workflows reduce rework and 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.

A new scenario for AI delivery:

Advancing from a series of isolated AI pilots to a repeatable, production-ready solution

Common scenario

A large financial services institution set out to expand its use of AI across fraud detection, transaction monitoring, and credit decisioning. Initial pilots showed promise, but progress slowed as projects moved toward production.

Typical obstacles

Dev teams used different environments and infrastructures. Setup times varied by team. Testing results were not easily repeatable. Security was reviewed late in the process, triggering rework and delays. As AI workloads increased, leaders grew concerned about safety, scalability, and reliability.

Docker solution

By standardizing development environments and embedding security controls earlier, the organization reduced setup time, improved reliability, and strengthened visibility into risks and dependencies. AI projects moved from pilot to production faster, with fewer failures and greater audit confidence.

Application modernization and time to market

Modernization is a top priority in financial services, 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 modern development practices without disrupting core systems
- Introduces new features and services faster, using consistent packaging and deployment workflows that reduce delivery friction
- Supports hybrid environments and gradual migration, enabling teams to bridge legacy infrastructure with cloud-native architectures
- Reduces time to market while preserving control, helping financial services organizations to modernize securely within existing compliance frameworks

theCUBE Research shows the impact of these modernization strategies:

50% modernized 31%–60% of their application portfolios.

62% reduced time to market by 11%–25%.

49% reduced time to market by 26%–50%.

Faster delivery enables financial services organizations to introduce new digital- and AI-driven capabilities without disrupting core systems, improving competitiveness while preserving stability. theCUBE Research findings show that Docker enables incremental modernization and materially accelerates delivery timelines.

"Beyond the technology, Docker and Itaú collaborate to accelerate adoption and embed containerization best practices across the organization."

Pedro Ignacio, Sr. Platform Engineer, Itaú Unibanco

Business value and ROI

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

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:

- **43%** save $50,001–$250,000 annually.
- **22%** save $250,000–$1 million annually.
- **6%** save 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 ability to translate technical acceleration into bottom-line business value.

"The turnaround time from commit to deployment is just three minutes on average across our 50+ backend applications. It's a hard metric we track, and one we were able to achieve after adopting Docker."

Dheeraj Arani, Head of DevOps, InCred

Next steps for foundational AI-ready software delivery

Financial institutions are entering a new phase of software delivery. AI and real-time digital services are becoming core operational capabilities. At the same time, regulatory scrutiny, security threats, and legacy complexity continue to intensify.

The research findings point to a clear conclusion. Organizations that adopt Docker as a foundational software delivery platform scale AI more reliably, reduce vulnerabilities, modernize faster, and deliver measurable business value.

For financial services executives, the path forward does not require abandoning existing systems or taking on unnecessary risk. It demands strengthening the foundation underpinning modern software delivery. As theCUBE Research confirms, financial services organizations seeking to accelerate AI initiatives, standardize development workflows, and reduce the operational burden of compliance and security would benefit from adopting the Docker approach.

Docker's practical blueprint for financial services software includes these five steps:

1

Establish consistent development environments across teams to reduce variability, improve handoffs, and standardize how applications are built and tested.

2

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

3

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

4

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

5

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

This proven path enables banks and other financial institutions to move confidently from experimentation to execution, supporting AI initiatives that are reliable, auditable, and scalable. Docker customers drive rapid software innovation without compromising trust.

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

To learn how organizations are applying these principles in practice, engage with Docker to see how secure, AI-ready software delivery can be built at enterprise scale.

1. "Data evolution in banking: 2024 Banking & Capital Markets Survey," Deloitte, 2024
2. Mehta, B., et al., "AI in Financial Services Survey Shows Productivity Gains Across the Board," 2024
3. "Docker's Impact on Agentic AI, Software Supply Chain Security, Developer Productivity, ROI," theCUBE Research, October 2025
4. "Smarter, Secure Software Delivery in the AI Era with Docker," the CUBE Research, October 2025
5. "The State Of GenAI in Financial Services, 2024," Forrester, June 2024
6. "The State Of GenAI in Financial Services, 2024," Forrester, June 2024

docker