

| EBOOK

The Path to Zero Disruption in Financial Services

From Connected Visibility to
**Preventive, Controlled
Autonomous IT**

riverbed®



Table of Contents

- 3** Visibility is the Foundation. Prevention is the Next Step
- 5** Why Preventive Resilience Matters
- 6** When Friction Matters as Much as Failure
- 7** Protect the Complete Financial Services Journey
- 9** Turn Connected Visibility into Early Warning
- 10** Reduce Noise and Accelerate Action
- 11** Progress Toward Controlled Autonomous IT
- 13** Govern the New AI Workforce
- 14** Five Practical First Moves
- 15** From Visibility to Measurable Value
- 17** Identify Your First Move Toward Zero Disruption



Visibility is the Foundation. Prevention is the Next Step

In financial services, disruption is felt in moments that matter: a customer waiting for a payment confirmation, an advisor trying to prepare for a client conversation, a claims handler standing with a customer in the field, or a frontline employee hoping the next screen loads before the interaction stalls.

Many institutions have made significant progress in gaining insight across increasingly complex digital environments. But as digital adoption, operational risk, customer expectations, and AI-enabled operations accelerate, knowing what happened is no longer enough.

By connecting customer, employee, and operational experience data, IT teams can identify problems more quickly, determine where issues begin, and understand which users, services, and business processes may be affected.

But visibility alone does not prevent disruption.

A payment may still take longer than expected. A claims application may still become unresponsive. An advisor may still wait for critical client information. A contact center agent may still apologize to a customer while systems lag in the background.

The issue may now be easier to diagnose. But the customer has already waited, the employee has already lost time, the service team has already reacted, and confidence in the digital journey has already been tested.

The next step is to turn connected visibility into preventive action.

It means spotting early warning signs, understanding where they could create business impact, and taking controlled action before disruption reaches the high-value services people depend on.

This is the path to Zero Disruption.

Zero Disruption is the controlled progression from reactive operations to earlier detection, preventive action, and governed remediation, not an overnight leap to unrestricted automation.

As you read, consider where visibility is strongest today, where disruption still reaches users, where AI could assist safely, and which first move would create the greatest impact with the least operational risk.

From Zero Blind Spots to Zero Disruption

Zero Blind Spots provides a connected understanding of the complete digital experience.

Zero Disruption uses that understanding to recognize risk earlier, prioritize according to likely impact, and stop more issues from reaching customers and employees.

**Visibility shows what is happening.
Prevention changes what happens next.**



SEE

Complete
experience



UNDERSTAND

Cause and impact



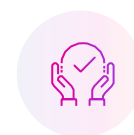
RECOGNIZE

Emerging risk



ACT

Controlled
response



PREVENT

Disruption



Why Preventive Resilience Matters

Fast Response Still Means Disruption Happened

Traditional IT operations follow a familiar sequence.

An issue occurs. Someone notices. A ticket is raised. Teams investigate. The issue is escalated. Service is eventually restored. Better tools and processes can make this sequence faster. But the operating model remains reactive.

Disruption still happens first. For banks, insurers, payments providers, and wealth firms, that gap matters.

Digital banking services, payment platforms, claims systems, advisor applications, branch operations, contact centers, and employee workflows are now fundamental to how the business operates. For ITOps, digital experience, workplace, and resilience leaders, technology performance is no longer a back-office concern. It is directly connected to customer service, employee productivity, operational risk, and brand trust. At the same time, the environment supporting those journeys has become more complex.

Core and legacy systems coexist with cloud infrastructure and SaaS platforms. Employees connect from branches, contact centers, remote locations, and mobile devices. Customer journeys depend on applications, networks, and services that may cross organizational and third-party boundaries.

The result is a harder operating challenge: more dependencies, more data, more teams, and less tolerance for delay.

Always On Does Not Always Mean Under Control

A service can remain available while the experience deteriorates.

A transaction can complete while taking longer than expected.

An application can remain online while thousands of employees lose time waiting for it to respond.

A workflow can function while creating repeated frustration for customers or frontline teams.

Preventive resilience changes the objective.

- Establish normal performance
- Recognize meaningful changes
- Understand which journeys may be affected
- Identify the likely cause
- Apply an appropriate response
- Prevent similar disruption from recurring

The goal is no longer simply to recover quickly. It is to prevent more disruption from happening in the first place.

The best operational outcome is often the one customers and employees never have to notice.

When Friction Matters as Much as Failure

Disruption Often Starts Small

The most visible technology problems are not always the most damaging.

A major outage creates an immediate response. Teams convene. Escalation paths are clear. Restoring service becomes the priority.

Everyday disruption is different.

It appears as a slight delay, an intermittent access problem, or an inconsistent workflow. No individual event may be severe enough to trigger a major incident. Yet the effect accumulates across customers, employees, locations, and transactions.

Consider a Contact Center Interaction

A customer calls with a question about an account or payment. They are not thinking about infrastructure, application dependencies, or backend response times. They simply need the service to work.

The agent opens the customer record. The application is available, but the record takes five seconds to load instead of one or two. The pause is short, but the experience changes.

Nothing has failed. No critical alert is triggered. Yet the agent is left waiting, the customer hears the silence, and the interaction starts to feel slower than it should.

Across one conversation, the difference may appear minor.

Across thousands of agents and customer interactions, it becomes an operational problem.

Call handling time increases. Customers wait. Employees lose productivity. Queues grow. Over time, the organization absorbs the cost of a service that remains technically available but is no longer delivering the experience people expect.

The Experience is the Service

Infrastructure availability remains important. But it does not tell the complete story.

- A customer completed a payment without delay
- An advisor accessed information when it was needed
- A claims handler completed a workflow efficiently
- A branch employee served a customer without interruption
- A contact center agent experienced consistent application performance

The real question is not only whether a component is working. It is whether the complete journey is working as intended.

A transaction does not need to fail to damage the experience.

Protect the Complete Financial Services Journey

Financial services technology teams share many operating pressures, but the moments that matter differ across banking, payments, insurance, and wealth management. A Zero Disruption strategy should begin with the journeys where even small delays can affect confidence, productivity, operations, risk, or business performance.

Banking

Modernize Without Losing Operational Control

Banks are balancing core modernization, cloud adoption, SaaS applications, regulatory obligations, and rising expectations for digital services. Customer and employee journeys may cross modern and legacy environments, making it difficult for ITOps, service management, and digital experience teams to understand how a change in one part of the technology estate affects the complete banking experience.

Protect: Digital banking, customer access, core applications, branch operations, and contact center services.

Objective: Modernize critical banking services without losing visibility, resilience, or control.

Payments

Prevent Friction Before It Becomes Failure

A payment journey is more than a final success or failure status. Performance can be affected at multiple points, from the customer interaction and application logic to the network path and supporting infrastructure.

Protect: Transaction initiation, authentication, processing, application performance, and customer confirmation.

Objective: Protect the complete payment journey, not only the final transaction status.

Example: If authentication latency begins to rise during peak mobile banking activity, teams can connect user experience, application, network, and infrastructure signals to understand whether the issue is isolated, spreading, or likely to affect transaction completion.

One prevention-first model.

Different critical financial services journeys.

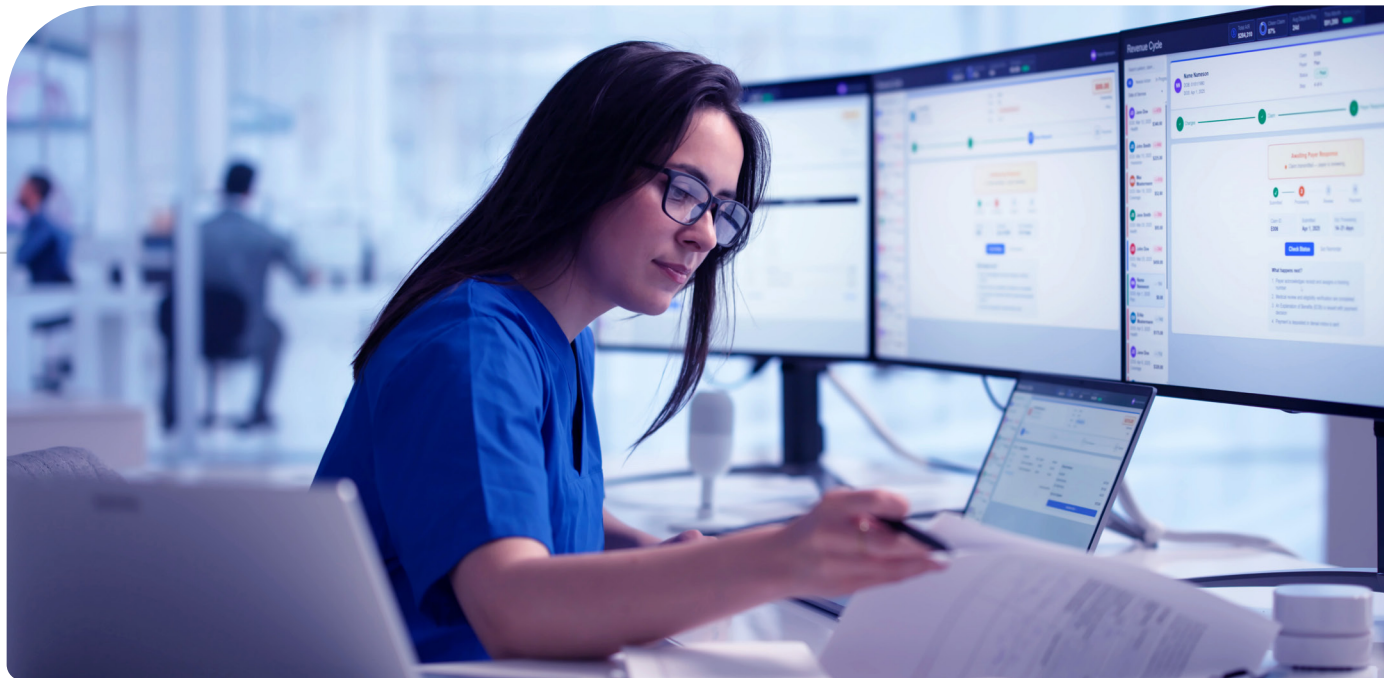
Insurance and Wealth Management

Keep Critical Customer and Advisor Workflows Moving

Insurance organizations increasingly rely on digital claims interactions and mobile-enabled workflows used by frontline claims teams in the field. Wealth management teams depend on responsive applications, reliable connectivity, and timely access to client information across distributed locations. In both environments, inconsistent visibility into frontline devices can make it harder to detect friction before it affects claims handling, advisor productivity, or customer service. Connected context helps teams determine whether an issue originates in the application, device, network, or another service.

Protect: Digital claims, frontline worker devices, mobile claims workflows, client records, advisor applications, document submission, customer communication, and distributed work.

Objective: Protect claims, advisor, and frontline workflows by improving visibility into frontline devices, detecting experience issues earlier, and enabling shared context and controlled action.



Turn Connected Visibility into Early Warning

Most financial services technology teams are not short of monitoring data. The challenge is turning signals from different tools and teams into a shared understanding of what people are experiencing, what is causing the issue, and which response will make the greatest difference.

A network tool may identify a change in traffic. An application tool may report increased response time. An endpoint tool may show higher resource use. A service management platform may contain several related tickets. Each signal is useful. Viewed separately, however, each provides only one interpretation of the issue. Zero Disruption requires shared context.

See. Understand. Recognize.

See the Complete Experience

Capture direct, full-fidelity telemetry across users, endpoints, applications, and networks. Maintain visibility across cloud, SaaS, zero-trust, and off-network environments. Include real-user experience, not only infrastructure status.

Understand Cause and Impact

Correlate signals across domains. Identify what changed and establish the most likely source of the issue. Connect technical conditions with the affected employee, customer, workflow, or service.

Recognize Emerging Disruption

Establish what normal performance looks like. Identify meaningful deviations from that baseline. Assess whether an emerging condition could affect more users, transactions, or locations. Prioritize according to likely experience and business impact.

Experience Becomes Evidence

A user report can tell IT that something went wrong. Experience evidence can show what happened, when it happened, what the user experienced, and which conditions contributed to the issue. That context helps teams select a more effective response and reduce the likelihood of the same disruption recurring.

Riverbed Aternity Replay combines session replay with full-fidelity telemetry to show what users experienced and provide troubleshooting context. That evidence helps teams move beyond guesswork, repeated user reproduction, and isolated alerts, giving them greater confidence to understand what happened, improve the response, and reduce the likelihood of similar disruption recurring.

In financial services, the confidence to automate cannot exceed the confidence in the data, context, and controls behind the decision.



SIGNALS

Reveal experience



EXPERIENCE

Becomes evidence



EVIDENCE

Provides context



CONTEXT

Enables action



ACTION

Prevents disruption

Reduce Noise and Accelerate Action

When operational context is fragmented, issues are routed between teams.

The network team checks connectivity. The application team checks response times. The service desk asks the user to reproduce the problem. Infrastructure and workplace teams investigate separate parts of the same experience.

Each team may be working correctly, but no team has the complete picture.

This creates escalation, duplication, and delay.

Shared context changes the process. When teams can see the experience and understand the application, device, network, identity, and service conditions around it, they work from the same evidence. That helps them move faster from triage to the right response, with fewer handoffs and less duplicated effort.

Move from Investigation to Prevention

Process

- Detect issues before they generate widespread disruption
- Correlate telemetry, dependencies, and context to understand scope
- Prioritize according to actual user and business impact
- Determine the likely cause and recommended response
- Confirm remediation fixed the issue
- Capture outcomes to improve future response

Outcomes

- Ensure resources are focused on the issues that matter most
- Reduce manual investigation
- Reduce escalations and handoffs
- Accelerate resolution
- Lower service desk volume and minimize future disruptions

Financial Services Results

Arab National Bank enhanced network monitoring, improved visibility, and seamless troubleshooting during a major core banking system migration with Riverbed.

Faisal Islamic Bank improved end-to-end visibility across applications, network, and infrastructure, resolved application issues 67% faster through streamlined troubleshooting, and improved root-cause identification with Riverbed.

Progress Toward Controlled Autonomous IT

Autonomous IT does not need to begin with complete automation. For regulated environments, the practical route is a measured progression: start with recommendations, move to approved actions for repeatable issues, and expand automation only when the data, policy, and outcomes can be trusted.



Reactive Operations

Most IT teams still operate in a reactive model today. Issues are typically investigated after customers or employees are affected. Teams rely on alerts, tickets, monitoring tools, and user reports to understand what happened, and success is measured by how quickly service can be restored.



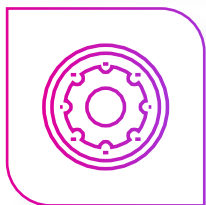
Assisted Operations

AI helps correlate evidence, identify likely causes, and recommend next steps. For example, it might group related branch connectivity tickets, highlight a common network path, and suggest the right diagnostic workflow. Human teams retain decision-making and execution responsibility.



AI-Enabled Operations

AI analyzes conditions, recommends actions, and prepares remediation workflows for defined, repeatable issues. For example, it may recommend restarting a known problematic service, clearing a device cache, or adjusting a configuration after evidence confirms the pattern. A human reviews and approves the response before execution.



Controlled Autonomous Operations

AI automatically evaluates conditions and executes approved responses within defined policies and guardrails. Examples might include applying a pre-approved fix for a recurring endpoint issue, routing traffic around a degraded path, or triggering a rollback when performance thresholds are breached. Actions and outcomes remain visible, governed, and auditable.

Automate at Your Pace

Not every journey, condition, or response should move toward automation at the same speed. Institutions should expand automation based on confidence, governance, and risk.

Consider:

- Criticality of the journey
- Confidence in the available data
- Predictability of the condition
- Reversibility of the action
- Security and compliance requirements
- Potential effect of an incorrect response
- Operational risk tolerance

A repeatable device or application issue may be suitable for early automation. A change affecting a critical payment platform may require additional evidence, approval, and human oversight. Both can be part of a Zero Disruption operating model. The difference lies in how the response is governed, measured, and expanded.

What Enables Controlled Autonomy?

Controlled autonomy depends on more than automation alone. Teams need full-fidelity visibility, context-aware intelligence, and governance to understand what is happening, decide what action is appropriate, and apply that action with confidence. This is where AI observability becomes the foundation for trusted Autonomous IT.



Complete visibility:

Direct, full-fidelity data across devices, applications, and networks.



Context-aware intelligence:

Correlation that determines cause, context, and likely impact.



Trusted, governed AI:

Actions applied with precision, defined controls, and visibility into outcomes.

Autonomy should increase with confidence, not run ahead of it.

Govern the New AI Workforce

Generative AI changed how employees create and access information. Agentic AI goes further. AI agents can perform tasks and remediate known issues within enterprise environments. For regulated institutions, this creates significant opportunity. Agents can help IT teams investigate issues, prioritize impact, execute known responses, and prevent recurring disruption with greater consistency and speed. But the ability to remediate introduces new responsibilities. Organizations must understand what their AI agents are doing, which resources they can access, how outcomes are measured, and where human approval remains necessary.

AI Assurance for Financial Services

Agents and Models

Know which agents and models are active, who is using them, and for which tasks.

Actions

Define what an agent can recommend or execute and where approval is required.

Cost and Value

Monitor resource use and determine whether it is appropriate for the task and resulting value.

Access

Understand which systems, applications, and data each agent can access.

Performance

Measure whether recommendations and actions produce reliable operational outcomes.

Risk and Oversight

Confirm that agents operate within policy and that actions can be reviewed, stopped, reversed, or escalated.

Trust Requires Evidence

Governance cannot depend on the assumption that an agent is operating correctly. It requires evidence. Financial institutions need to see the data informing a decision, the context behind a recommendation, the action taken, and the resulting outcome.

Controlled autonomy requires visibility before action, guardrails during action, and outcome validation after action.

Five Practical First Moves

The path to preventive operations does not need to begin with a large-scale transformation. The most effective starting point is a contained, high-value journey where disruption is frequent enough to measure, important enough to improve, and safe enough to use as a model for wider progress.

1 Choose One Critical Journey

Select a payment workflow, digital banking service, claims process, advisor application, contact center interaction, or critical employee service. Define where the journey begins and ends, who depends on it, and what successful performance looks like.

3 Establish Normal Performance

Use direct experience and operational data to define normal behavior. Identify where small changes could create significant impact when repeated at scale.

5 Define the Control Model

Decide which actions remain human-led, where AI can recommend a response, which responses can be automated with approval, and where policy-bound autonomy is appropriate.

2 Map the Complete Experience

Identify the applications, devices, networks, services, and dependencies involved. Include the customer or employee experience, not only the status of the supporting technology.

4 Target Recurring Disruption

Look for frequent, understood conditions supported by reliable evidence and suitable for a consistent response. Begin with AI-assisted decisions or lower-risk approved actions.



SELECT
A journey



CONNECT
The evidence



BASELINE
Normal



RESPOND
With control



EXPAND
With confidence

From Visibility to Measurable Value

Measure Fewer Disruptions, Not Only Fewer Tickets

Ticket reduction and resolution speed remain valuable operational measures. But neither provides a complete measure of Zero Disruption.

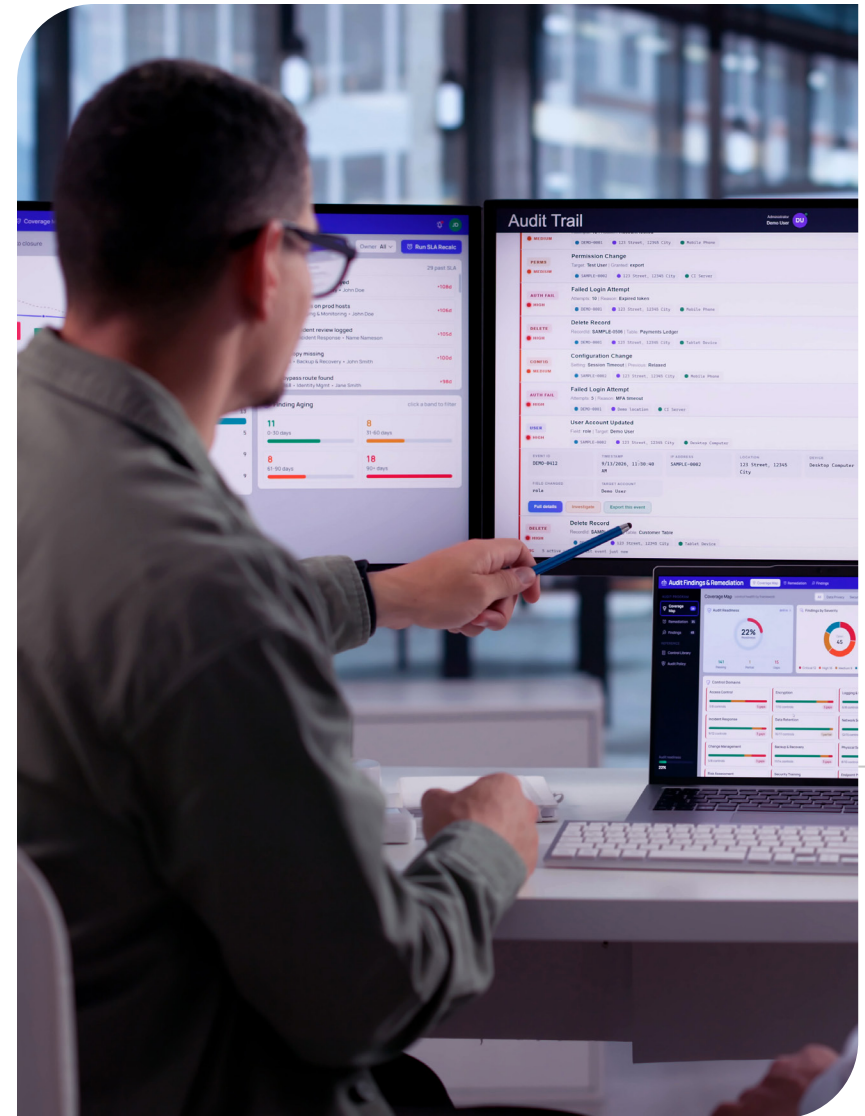
A decline in ticket volume could mean that fewer issues occurred. It could also mean users stopped reporting them or more troubleshooting effort was shifted to employees.

The real measure is whether disruption was reduced.

A Broader Measure of Progress

- Identify issues before user impact
- Prevent recurring disruption
- Reduce avoidable support and escalation demand
- Improve the speed and accuracy of diagnosis
- Apply appropriate automated responses successfully
- Protect important customer and employee journeys
- Expand automation within defined policies

These examples show how improved visibility and faster diagnosis can support measurable operational outcomes across financial services environments. They also illustrate why progress toward Zero Disruption should be assessed through journey performance, avoided disruption, and the effectiveness of controlled remediation, not ticket volume alone.



Evidence from Financial Services



ARAB NATIONAL BANK

Core banking migration

Enhanced network monitoring, improved visibility, and seamless troubleshooting during a major core banking system migration.



FAISAL ISLAMIC BANK

Faster application resolution

Resolved application issues 67% faster through streamlined troubleshooting and improved end-to-end visibility.



HALKBANK

Digital banking resilience

Safeguarded access to banking services, increased network availability despite 1.5x more traffic, and monitored 40+ critical applications.

The Path Forward

Financial services organizations already understand the importance of visibility. The next stage is to turn visibility into preventive action.

That means protecting the complete journey rather than monitoring individual systems in isolation. It means using real experience as evidence, connecting that evidence with full-fidelity operational data, and understanding both cause and likely impact.

It means applying the appropriate response, whether human-led, AI-assisted, or automated, within clearly defined guardrails. And it means expanding autonomy at the pace that confidence, evidence, and operational control allow.

Zero Disruption is not automation for its own sake. It is the ability to recognize emerging issues, understand what matters, and stop more disruption from reaching the customers, employees, and business-critical services that depend on technology working as it should.

Protect the journey. Prevent disruption. Keep financial services moving.

Identify Your First Move Toward Zero Disruption

Pinpoint where disruption is most likely to affect your critical customer and employee journeys and explore how AI-powered observability, full-fidelity experience data, and trusted automation can help you move from reactive response to preventive action.

Talk to an Expert About Your Zero Disruption Priorities

Connect with a Riverbed expert to identify your most critical journeys, assess current visibility gaps, and define practical first moves toward preventive, controlled, and AI-ready IT operations. Where useful, a tailored demo can show how the approach applies in your environment.

Leave with a clearer view of where disruption is most likely to appear, which journeys to prioritize first, and how Riverbed can help build a more resilient path forward.

TALK TO A ZERO DISRUPTION EXPERT

About Riverbed

Riverbed, the leader in AI observability, helps organizations optimize their users' experiences by leveraging AI automation for the prevention, identification, and resolution of IT issues. With over 20 years of experience in data collection and AI and machine learning, Riverbed's open and AI-powered observability platform and solutions optimize digital experiences and greatly improve IT efficiency. Riverbed also offers industry-leading Acceleration solutions that provide fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of market-leading customers globally – including 95% of the FORTUNE 100 – we are empowering next-generation digital experiences. Learn more at riverbed.com.

© 2026 Riverbed Technology LLC. All rights reserved. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein may not be used without the prior written consent of Riverbed or their respective owners. CS-1567_FSI-Ebook_100726