catchpoint

WHITEPAPER

Beyond APM: Building Digital Resilience in Financial Services

Executive summary

The financial services industry is undergoing rapid digital transformation. Traditional on-premises self-contained systems have given way to cloud-based, distributed architectures built on APIs, SaaS platforms, and interconnected ecosystems. This shift has unlocked new agility and innovation—but it's also introduced complexity, fragile dependency chains, external risks, and visibility gaps that traditional monitoring tools were never designed to handle.

Application Performance Monitoring (APM) remains essential for observing custom applications. But on its own, APM is no longer sufficient to ensure the resilience of complex distributed systems, third-party APIs, cloud services, and internet pathways that now define how services are delivered and experienced.

Across banking, insurance, and wealth management, the top reason customers give for switching providers is a desire for a better digital experience—with **51%** of banking customers citing it as their primary reason.

This report explores how leading financial institutions are expanding their monitoring strategies with Internet Performance Monitoring (IPM)—a complementary, outside-in approach that provides real-time insight into what users, systems, and regulators truly care about: experience, reachability, reliability, and performance.

By combining IPM with traditional APM, IT leaders can close critical visibility gaps, anticipate outages before they escalate, and ensure their digital services consistently meet rising customer and regulatory expectations. In today's high-stakes digital environment, this dual approach isn't just smart—it's strategic.

The evolution of technologies that support financial institutions

To understand the current state of banking technology, it is essential to first explore how infrastructures have fundamentally transformed over the past two decades. This section explores how banks have moved from centralized, monolithic systems to flexible, distributed architectures powered by cloud computing, APIs, and advanced digital services—setting the stage for both new opportunities and fresh challenges.

Over the past 15 years, financial institutions have shifted much of their infrastructure to the cloud, adopted more FinTech solutions, and integrated with other cloud-based systems—creating complex, interdependent environments spanning multiple locations. This cloud migration provides greater flexibility, scalability, and cost-efficiency, but it also introduces new complexities and dependencies that must be carefully managed.

Cloud services enable firms to leverage advanced technologies (artificial intelligence, machine learning, big data analytics, etc.) to enhance operations and customer experiences. However, these services also create additional layers of complexity and potential points of failure that traditional monitoring approaches struggle to observe. The distributed nature of cloud services—often spanning multiple providers and regions—further complicates the monitoring landscape and requires a more sophisticated approach to ensure digital resilience.

The four pillars of digital resilience

To ensure continuous service delivery and optimal user experience, financial institutions must monitor more than just uptime. True digital resilience hinges on four critical dimensions:

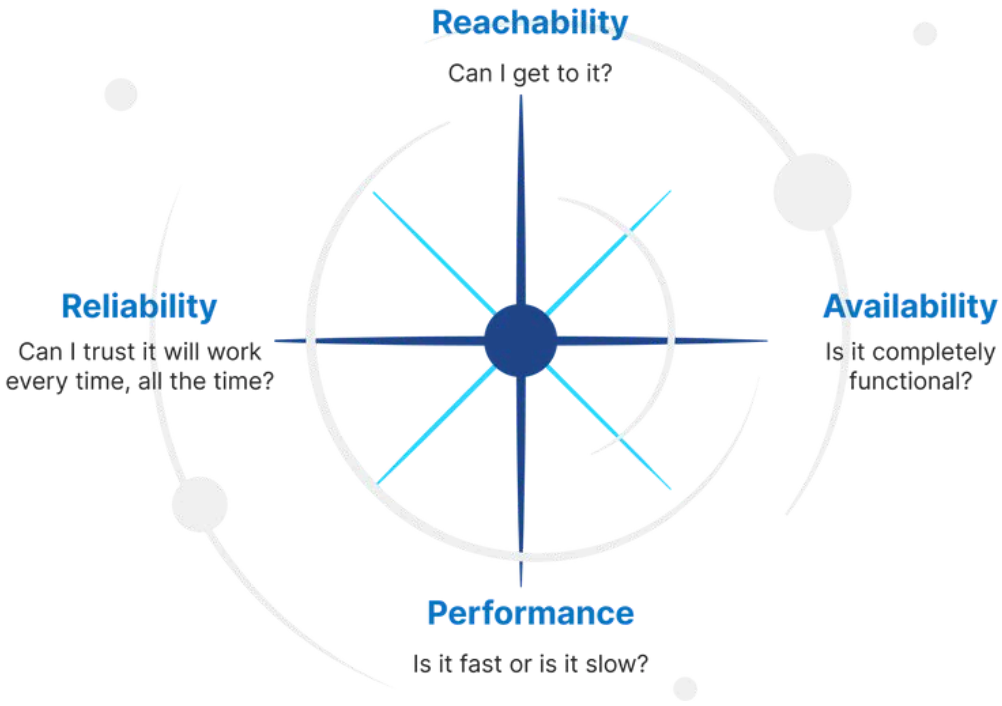

Figure 1: The four pillars of digital resilience

This resilience formula provides a practical framework for evaluating the health of digital services from the perspective of the users consuming an application, not the infrastructure or the systems themselves.

- **Reachability** is important because distributed users—whether they are tellers in a branch, traders in an office, or users on a PC or mobile device—must be able to reach the system, wherever they are. Local ISPs, routing, and other factors may impact reachability.
- **Availability** requires proactive testing of functional capabilities, even when no users are accessing the system, to ensure all tasks important for users can be completed.
- **Performance** is now more important than ever, as users are impatient, and a slow system is often more frustrating than a system that is down. As the saying goes, "Slow is the new down."
- **Reliability** is especially important when today's complex systems are constantly changing with updates, config changes, systems scaling, migrations, enhancements and other factors.

Ensuring digital user experience, or Internet Resilience, requires more than focusing on system health or application code efficiency. The opportunity is to understand these four factors of resilience from the user perspective.

From monolithic to distributed systems

Banking infrastructure has undergone a dramatic transformation over the past two decades, evolving from centralized, somewhat monolithic systems to complex, distributed architectures that span multiple environments, clouds, and services, and integrate with legacy components. Traditionally, banks operated within self-contained environments where applications ran on centralized mainframes and critical functions were housed within a single, controlled infrastructure.

These legacy systems, while stable, often created significant barriers to innovation, requiring lengthy development cycles and limiting banks' ability to respond quickly to market demands. The inflexibility of these monolithic architectures became increasingly problematic as customer expectations shifted toward digital-first experiences, forcing banks to reimagine their technological foundations.

This evolution has not been merely incremental but represents a fundamental restructuring of how banking systems operate and deliver services.

Today's banking landscape is characterized by highly distributed components that operate across on-premises data centers, private clouds, public clouds, and edge locations.

> ***82%** of large banks plan to move more than half of their mainframe workloads to the cloud, with nearly a quarter aiming to migrate over 75% of workloads within five years.*

This shift has been driven by the need for greater agility, scalability, and the ability to deliver innovative digital experiences to increasingly demanding customers. Banking systems have become remarkably complex, with significant reliance on Software-as-a-Service (SaaS) applications and partner APIs for various critical functions, including loan origination, transfers, trading, core banking, mobile applications, security, and fraud prevention.

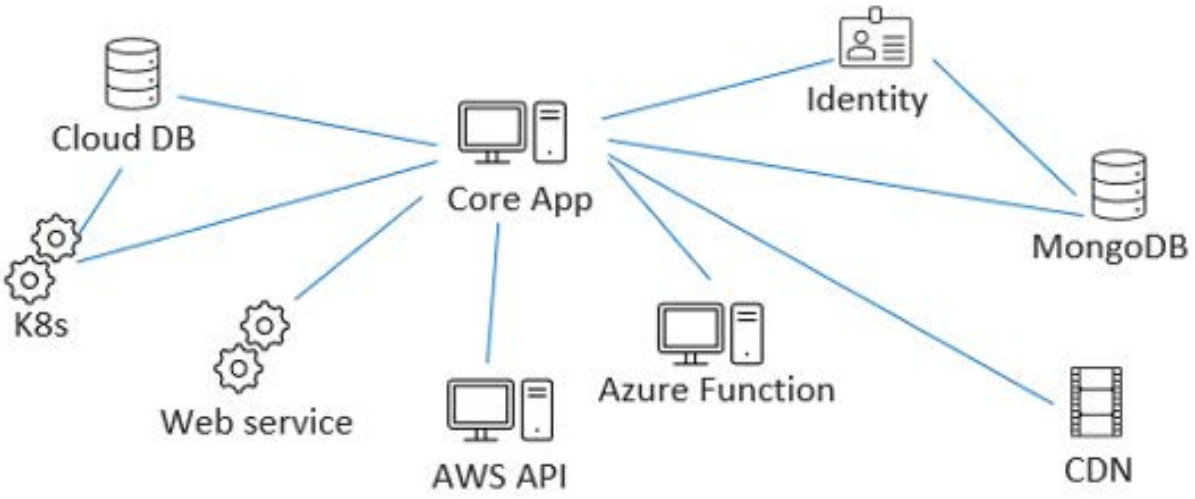

Figure 2: Distributed banking systems

The transition to distributed systems has enabled banks to break down silos, implement more agile development practices, and deliver new features and services at a pace that would have been impossible under the previous model. **However, this evolution has also introduced new challenges** in terms of monitoring, managing, and ensuring the resilience of these complex environments.

According to a McKinsey & Company report, banks worldwide invest millions in maintaining core banking systems that must reliably handle vast transaction volumes while interfacing with numerous systems. These legacy platforms, although historically dependable, are now under pressure. With the rise of digital banking, cloud adoption, and APIs, McKinsey notes that "banks have seen a significant shift in the way banking products and partnerships are constructed."

The API-driven banking ecosystem

The adoption of APIs and cloud services represents a pivotal aspect of the financial services infrastructure evolution. APIs have emerged as the essential connective tissue of modern banking, enabling different systems, applications, and services to communicate and share data seamlessly. They allow banks to integrate with external providers, leverage third-party services, and create a more interconnected ecosystem that extends far beyond the boundaries of the institution's own infrastructure.

API Adoption by the Numbers

- 90% of financial institutions use APIs
- 85% have adopted open banking APIs
- 2B+ daily API calls in 2023
- 69% manage over 100 APIs
- APIs drive 40% of revenue growth in leading banks

This API-centric approach has revolutionized everything from payment processing to account opening, enabling banks to compose sophisticated customer journeys from a combination of internal and external services. However, it also introduces new layers of complexity. Each customer interaction may depend on dozens of interconnected services—many outside the bank's direct control—creating operational blind spots and new challenges for monitoring and resilience.

> *Banks must now proactively monitor not just their own infrastructure, but also the performance and availability of the many external APIs and services on which they depend.*

The critical challenge: managing complexity to deliver exceptional digital experiences

The culmination of these changes is that banking systems have become complex, distributed, cloud-centric, service-oriented, and dependent on dozens or hundreds of external connections that must all function properly for the bank to operate effectively.

This complexity is further intensified by the increasing reliance on mobile banking, mobile payments, and third-party payment applications (such as Stripe, Zelle, and Venmo) that must deliver reliable and fast experiences to meet growing customer expectations.

The stakes could not be higher: 51% of banking customers switch providers due to poor digital experiences, and 83% would consider switching after just one negative interaction.

> *The market demands exceptional digital experiences, and banks must ensure their complex architectures can consistently deliver these experiences across all channels and touchpoints.*

However, traditional monitoring approaches, which were designed for simpler, more centralized architectures, often struggle to provide complete visibility into these complex, distributed environments. This complexity presents significant challenges for IT operations teams responsible for ensuring the reliability, performance, and security of banking systems. As banking infrastructure continues to evolve and become more complex, so too must the approaches to monitoring and ensuring digital resilience.

Why this matters

- **Customer churn is costly:** Acquiring a new banking customer costs 5-30x more than retaining an existing one.
- **Regulatory pressure is mounting:** Regulations like DORA require banks to demonstrate operational resilience across all digital services, including third-party dependencies.

Barriers to Internet resilience: Inside today's banking infrastructure

Modern banking's rapid digital transformation has brought tremendous benefits—but it also introduces new challenges. This section explores the most pressing obstacles banks face as they integrate new technologies, connect with external providers, and manage increasingly complex systems.

As a direct result of this API-driven evolution, banks now face the challenge of managing a vast and fragile web of external dependencies. Each customer transaction might traverse dozens of third-party APIs, payment processors, SaaS platforms, and even AI-powered services like ChatGPT or CoPilot. Every external integration is a potential point of failure—one that is often outside the bank's direct control but still impacts the customer experience.

This interconnectedness means that a disruption in a single provider can cascade across multiple banking services, amplifying risk. For example, a latency spike in a partner API can delay loan approvals or payment processing, while an outage in a cloud provider can take down critical customer-facing applications. Traditional monitoring tools, designed for simpler environments, often detect only the symptoms—not the root cause—of these failures, leading to longer outages and higher operational costs.

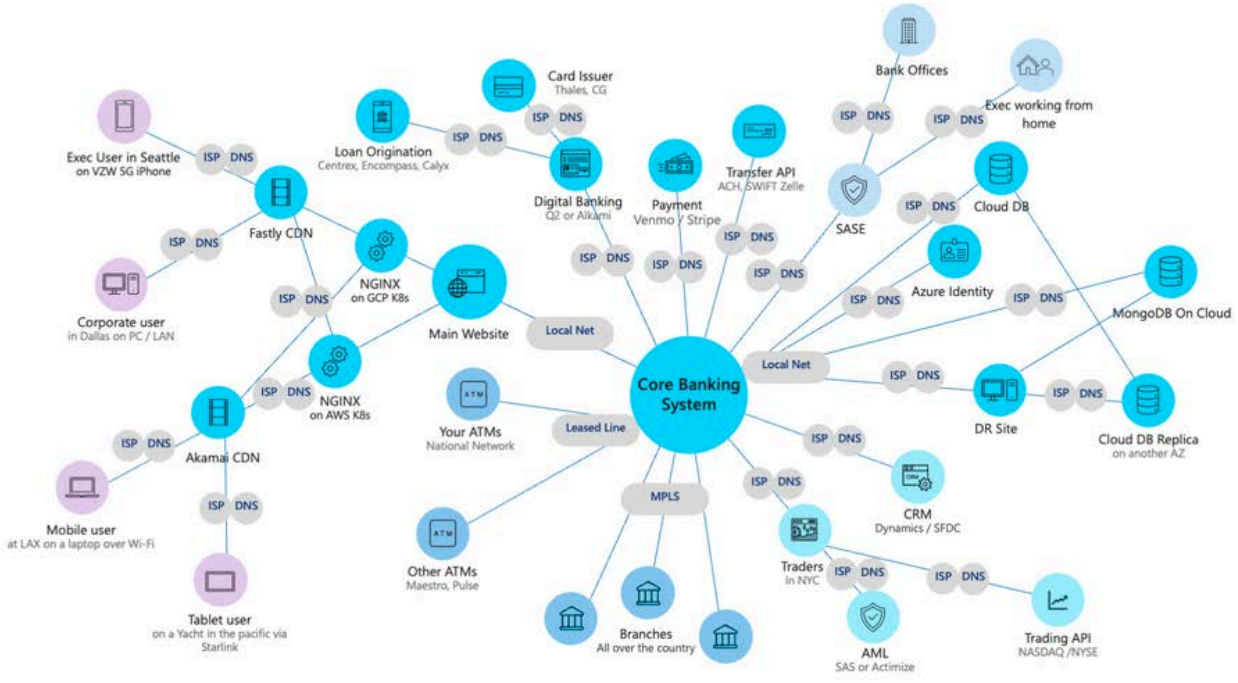

Figure 4: The vast web of APIs, cloud services, and third-party connections transactions rely on

Without comprehensive visibility into the entire service delivery chain, banks may find themselves dependent on external providers for problem detection and resolution, putting them in a reactive rather than proactive posture.

This dependency can lead to increased mean time to resolution (MTTR), extended service disruptions, and ultimately, a diminished customer experience that may drive customers to seek banking services elsewhere.

The complexity of these dependency chains also creates challenges for change management and risk assessment. When making changes to banking systems or introducing new features, banks must consider:

- The impact on all connected services and third-party dependencies.
- The risk of introducing new issues or missing critical integration points due to incomplete visibility.

Without a clear understanding of these relationships:

- Change failure rates increase.
- Release cycles become longer and more cautious.
- Opportunities for innovation and service improvement are often missed

As banking systems continue to become more interconnected and dependent on external services, managing and monitoring these complex dependency chains will be increasingly crucial for maintaining service reliability and customer satisfaction.

The Limitations of Traditional APM Tools

As banking systems have grown more distributed and reliant on external services, traditional Application Performance Monitoring (APM) tools are being pushed beyond their limits. Here's where APM excels, where it falls short, and why banks need new approaches to achieve true digital resilience in today's complex environments.

While APM remains a foundational component of IT operations, it was designed for an era of centralized infrastructure and internal control. These tools continue to deliver value when it comes to monitoring internal performance metrics, application health, and system diagnostics. However, in modern banking environments—where services rely on third-party APIs, cloud platforms, and internet-based delivery mechanisms—APM alone can no longer provide the full picture.

This imbalance creates critical visibility gaps that leave banks vulnerable to service degradation, customer complaints, and compliance risks.

This interconnectedness means that a disruption in a single provider can cascade across multiple banking services, amplifying risk. For example, a latency spike in a partner API can delay loan approvals or payment processing, while an outage in a cloud provider can take down critical customer-facing applications. Traditional monitoring tools, designed for simpler environments, often detect only the symptoms—not the root cause—of these failures, leading to longer outages and higher operational costs.

What APM does well	What APM misses
Monitors internal systems such as servers, applications, and infrastructure	Lacks visibility into external dependencies like third-party APIs, payment processors, and SaaS platforms
Tracks application performance metrics(response time, throughput, error rates)	Can't diagnose issues outside the application layer or beyond organizational boundaries
Provides infrastructure utilization metrics (CPU, memory, I/O, network)	Doesn't monitor Internet routing, DNS, BGP, CDN, or last-mile connectivity
Supports transaction tracing within multi-tier applications	Relies on cloud-based test nodes that don't reflect real-world user conditions
Offers log analysis to detect errors and anomalies	Blind to end-user experience from branch offices, remote employees, or customers on mobile and edge networks
Some synthetic testing capabilities for pre-deployment QA	Provides a false sense of security if cloud metrics appear healthy while users still experience problems
Works well in centralized or on-premises environments	Not built for distributed, cloud-native, and internet-reliant architectures

Table 1: The limitations of APM

The experience gap

Despite their value in tracking internal systems, traditional APM tools fall short in one critical area: monitoring the **actual digital experience of real users.** These tools typically gather data from a limited number of cloud-based locations, which are often far removed from the environments where customers, employees, partners, or integrated systems actually access services.

This creates a fundamental disconnect:

- **Users aren't in the cloud.** Customers, employees, and partners access services from branches, homes, offices, or mobile networks—not from data centers.
- **Real-world network conditions vary.** Unlike the high-speed, low-latency connections of cloud environments, end-user connectivity is often unpredictable and inconsistent.
- **Cloud-based monitoring can be misleading.** APM tools may show perfect performance metrics while users encounter delays, errors, or outages.
- **Experience blind spots become business risks.** Undetected performance issues can erode trust, drive up support costs, and lead to churn or regulatory scrutiny.

As banks continue to serve increasingly diverse and distributed user bases, bridging this gap in visibility is no longer optional—it's essential for maintaining service quality and customer trust.

This broader approach enables IT and ops teams to see what's happening across the entire delivery chain—not just where their code lives, but where real users experience it.

The cost of poor digital experience monitoring

Poor digital experience monitoring creates blind spots that affect customer satisfaction, retention, revenue, and operational efficiency. And with customer expectations higher than ever, even minor digital failures can translate into major business consequences.

Banks that fail to deliver seamless digital experiences risk losing customers to more agile, tech-savvy competitors. Research shows that digital experience is now a primary driver of customer satisfaction and loyalty. When digital services are slow, unreliable, or difficult to use, customers are quick to look elsewhere. The relationship between digital experience and customer retention highlights the business impact of effective monitoring and the potential costs of missing issues until it's too late.

Customer expectations continue to rise: today's users want mobile and web applications to respond in 2–3 seconds and payments to process instantly. Banks that can't meet these standards risk frustrating their customers and damaging their reputation. Outages and slowdowns not only inconvenience users but can also have a direct impact on people's lives and financial wellbeing.

How outages and poor CX drive customers away

- Banks are losing one in five **(20%)** of their customers due to poor customer experience, with slow digital transformation directly resulting in missed opportunities to win new customers.
- **17%** of UK banking customers were affected by IT failures in the past year, with an average disruption time of six hours
- **Over a third (34%)** of Brits are worried about the potential of IT failures at their banks, and 25% now keep cash on hand as a precaution against outage
- **32%** of all customers would stop doing business with a brand they loved after one bad experience. In Latin America, 49% say they'd walk away from a brand after one bad experience.

Alison Barker
Director of Specialist Supervision at the UK's Financial Conduct Authority

"Outages are not just an inconvenience; they can have a real impact on people's lives."

Jim Marous
Co-Publisher of The Financial Brand

"In the financial sector, trust is everything. Any disruption can erode that trust and lead to customers taking their business elsewhere."

Beyond customer impact

Poor digital experience monitoring also leads to higher operational costs. Without comprehensive visibility, banks often resort to “war room” tactics—pulling together large teams to troubleshoot problems reactively. This approach is time-consuming, resource-intensive, and expensive compared to proactive monitoring that identifies and resolves issues before they affect customers.

As banking becomes increasingly digital-first, the operational and business costs of poor digital experience monitoring will only continue to grow, making comprehensive monitoring not just a technical necessity but a business imperative for forward-thinking financial institutions.

How Internet Performance Monitoring empowers digital resilience

As banking becomes increasingly digital and distributed, traditional monitoring tools fall short of providing the visibility needed to ensure seamless, resilient service. This section explores how Internet Performance Monitoring (IPM) addresses these blind spots—empowering banks to proactively manage digital experiences, reduce risk, and maintain a competitive edge.

What is Internet Performance Monitoring?

Internet Performance Monitoring (IPM) represents a specialized monitoring discipline focused on measuring the performance, reliability, and overall quality of internet connections, as well as the performance of web applications and services delivered over the internet.

According to Gartner, IPM typically includes monitoring the speed, reliability, and overall quality of internet connections, as well as the performance of web applications and services offered over the Internet.

Unlike traditional APM tools that primarily monitor internal infrastructure and applications, IPM is focused on the Internet Stack, the collection of technologies, protocols, and systems that make today's digital systems possible, while providing an outside-in perspective that offers real-time insights into the actual experience delivered to users.

What's included in the Internet Stack?

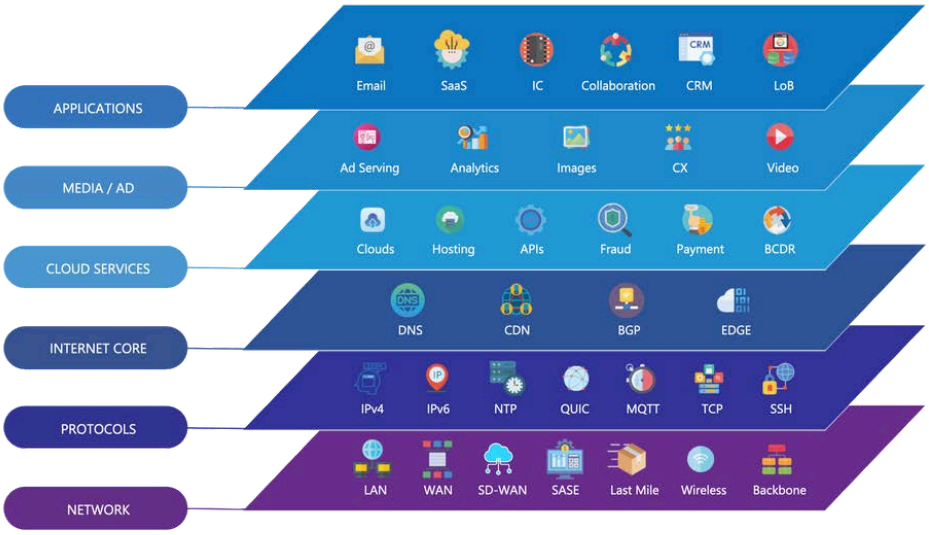

Figure 5: The Internet Stack

Key features of IPM

- **Monitors from the user's point of view:** Captures real-world experience by testing from diverse geographic locations and network environments, not just cloud data centers.
- **Covers the full Internet Stack:** Includes internal networks (LANs, SD-WAN, VPNs), external APIs, cloud services, third-party vendors, and the public internet.
- **Proactive, high-frequency testing:** Identifies issues before they impact customers, with test intervals ranging from minutes to sub-seconds for critical applications.
- **Comprehensive visibility:** Tracks backbone, routing, third-party services, origin servers, firewalls, and more—anything that could impact user experience.
- **Supports regulatory and business requirements:** Provides the documentation and insights needed for compliance with frameworks like DORA and for demonstrating operational resilience.

IPM represents a necessary evolution in monitoring approaches, addressing the blind spots that have emerged as banking infrastructure has become more distributed, cloud-centric, and dependent on internet connectivity. Gartner research has recognized the importance of this discipline, with Catchpoint noted as "the highest rated vendor overall for internet performance monitoring," reflecting the growing recognition of IPM as a critical component of comprehensive monitoring strategies.

As banks continue to expand their digital offerings and serve increasingly diverse and geographically distributed customer bases, the insights provided by IPM become increasingly valuable for maintaining service quality and competitive advantage.

Use cases for IPM

IPM delivers value across the entire banking ecosystem—from employee productivity to customer experience, third-party integration, and regulatory compliance.

Here is a summary of the most impactful use cases for IPM in banking, highlighting the specific business challenges, the unique value it provides, and the tangible benefits for financial institutions.

Use Case	IPM's Strategic Role
Ensuring Workforce Productivity	By measuring performance from the same environments employees operate in—home offices, branches, corporate locations—IPM provides real-time visibility into user-facing issues.
Delivering Superior Customer Experience	IPM monitors customer journeys from the networks and regions your customers use—surfacing local issues, CDN inconsistencies, or third-party failures before they impact satisfaction scores or trigger churn.
Ensuring Resilience and Performance of Tier-1 Applications	By providing end-to-end visibility across both internal and external dependencies, IPM helps banks trace performance degradation to its source—whether that's a payment gateway timeout or a BGP routing issue.
Optimizing Edge, CDN, and Cloud Deployments	With observability agents across thousands of global vantage points, IPM enables banks to compare CDN and cloud provider performance by geography, helping them optimize routing, validate SLAs, and isolate underperforming zones before users are affected.
Monitoring API Performance and Reliability	IPM continuously tests APIs from outside the bank's infrastructure, simulating actual user or partner conditions. This ensures issues—especially with partner APIs—are surfaced early, even when the internal system appears healthy.
Ensuring Network Reachability	By leveraging advanced tools like ECN traceroute and global agent-based testing, IPM provides actionable insight into where and why reachability is compromised—across branches, ATMs, partner environments, or mobile apps.
Web Performance for Revenue and SEO	By testing real browser interactions across actual devices and geographies, IPM surfaces issues like slow TTFB, third-party content delays, or mobile performance drops that wouldn't show up in internal QA tests.

Table 2: The most impactful use cases for IPM in banking

These use cases demonstrate that Internet Performance Monitoring is not just a technical upgrade—it's a strategic necessity for banks seeking to deliver reliable digital experiences, minimize risk, and maintain a competitive edge in an increasingly complex environment.

Key Benefits of Internet Performance Monitoring for Banks

Having explored the most impactful use cases for IPM, we now turn to the core benefits banks can expect—benefits that extend from IT operations to customer satisfaction, regulatory compliance, and the bottom line.

Here is a summary of the most impactful use cases for IPM in banking, highlighting the specific business challenges, the unique value it provides, and the tangible benefits for financial institutions.

Shifting from reactive to proactive monitoring

A major advantage of IPM is its ability to transform monitoring from a reactive, firefighting exercise into a proactive, preventative discipline. Traditional approaches often rely on customer complaints or support tickets to signal problems, meaning issues are only addressed after they have already impacted users and business outcomes. This reactive model leads to extended resolution times, unnecessary strain on IT resources, and reputational damage as banks scramble to identify and fix issues after the fact.

With IPM, banks gain the ability to detect emerging issues at their earliest stages—often before customers or employees are even aware of them. By continuously monitoring the digital experience from the outside in, operations teams can spot warning signs, investigate root causes, and resolve problems before they escalate. This proactive stance not only reduces the duration and reach of incidents but also allows for more efficient resource allocation and minimizes the business impact of disruptions.

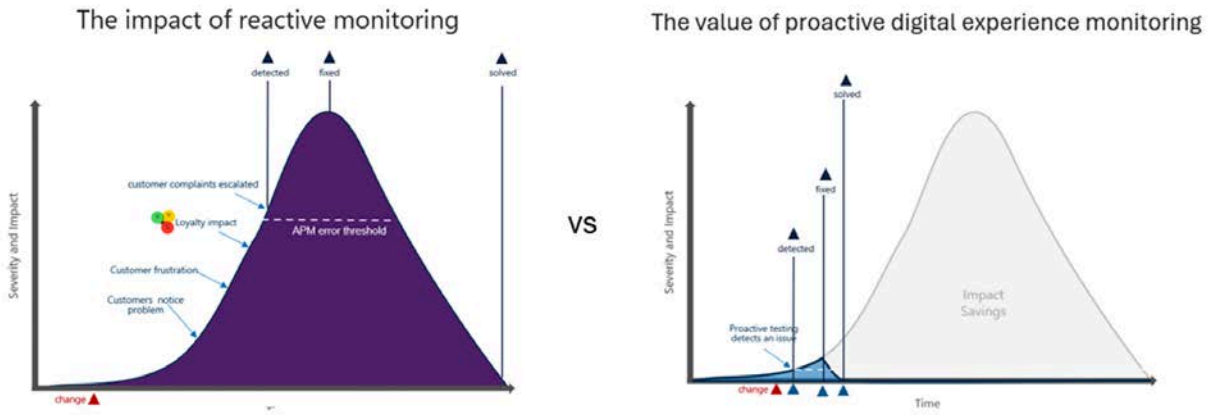

Figure 6: Reactive vs. proactive monitoring

The difference between reactive and proactive digital experience monitoring is illustrated in Figure 6. As shown, reactive monitoring typically detects issues only after customers are impacted, leading to escalated complaints and loyalty loss. In contrast, proactive monitoring enables early detection and resolution, dramatically reducing both the severity and the overall business impact of incidents.

The power of AI-driven proactive monitoring

Modern IPM solutions further enhance proactive monitoring with AI and machine learning. These systems analyze vast amounts of performance data to identify trends, predict potential issues, and alert operations teams before disruptions occur. For example, AI might detect that an authentication service is showing increasing response times during peak periods, signaling a capacity issue that could be resolved before it impacts users. By leveraging proactive monitoring, banks can address root causes early, maintain high service quality, and reduce the operational burden of incident management.

Measuring Experience Level Objectives (XLOs)

Traditional monitoring often focuses on technical Service Level Agreements (SLAs) that do not always reflect the actual user experience. Metrics like server CPU utilization or network latency, while important, may not correlate with how customers or employees perceive digital banking services. IPM enables banks to shift focus to Experience Level Objectives (XLOs)—metrics that directly measure the quality of digital experience from the user's perspective.

XLOs bridge the gap between IT and business, aligning performance monitoring with outcomes that matter most: how quickly a trader can complete a transaction, how long a teller waits for a process to finish, or how fast a customer's mobile app responds. These experience-level metrics are directly tied to customer satisfaction, employee productivity, and business success. For example, a bank may set an XLO that the login page must load in under three seconds, or that a payment transfer via API must complete in less than 500 milliseconds and be available 99.99% of the time.

This focus ensures that monitoring efforts are aligned with business goals and customer expectations, providing a shared language for IT and business leaders to drive performance improvements and competitive advantage.

Cost Savings and Regulatory Compliance

Implementing IPM delivers significant cost savings by reducing the frequency and impact of service disruptions. Proactive detection and resolution of issues mean fewer large-scale incidents, less time spent in "war room" troubleshooting, and lower support costs as fewer customers experience problems. This operational efficiency translates directly into financial savings and improved profitability.

The business case is further strengthened by the impact on customer retention. Since acquiring new customers is far more expensive than retaining existing ones, delivering a consistently high-quality digital experience produces a substantial return on investment.

IPM also helps banks meet the monitoring and resilience expectations set by regulatory frameworks such as DORA and the UK's Operational Resilience Regulation, as discussed earlier in this report. By providing comprehensive, real-time visibility across all digital services—including third-party dependencies—IPM enables banks to identify vulnerabilities, address them proactively, and demonstrate compliance to regulators, reducing the risk of fines, legal costs, and reputational damage.

According to GigaOm, IT decision-makers must choose between bearing the full weight of these outages, or investing in an Internet Performance Monitoring solution to navigate them intelligently.

Building a comprehensive monitoring strategy

As digital banking ecosystems grow more complex, a siloed approach to monitoring is no longer sufficient. Here, we outline how integrating APM and IPM creates a truly comprehensive strategy—giving banks full visibility from internal systems to real-world user experience, and enabling faster, more effective incident response.

Integrating APM and IPM

Mix-and-match monitoring tools create fragmented visibility, complexity, and higher costs. Consolidating APM and IPM into a unified observability platform delivers improved visibility, faster incident response, simplified management, and reduced operational costs.

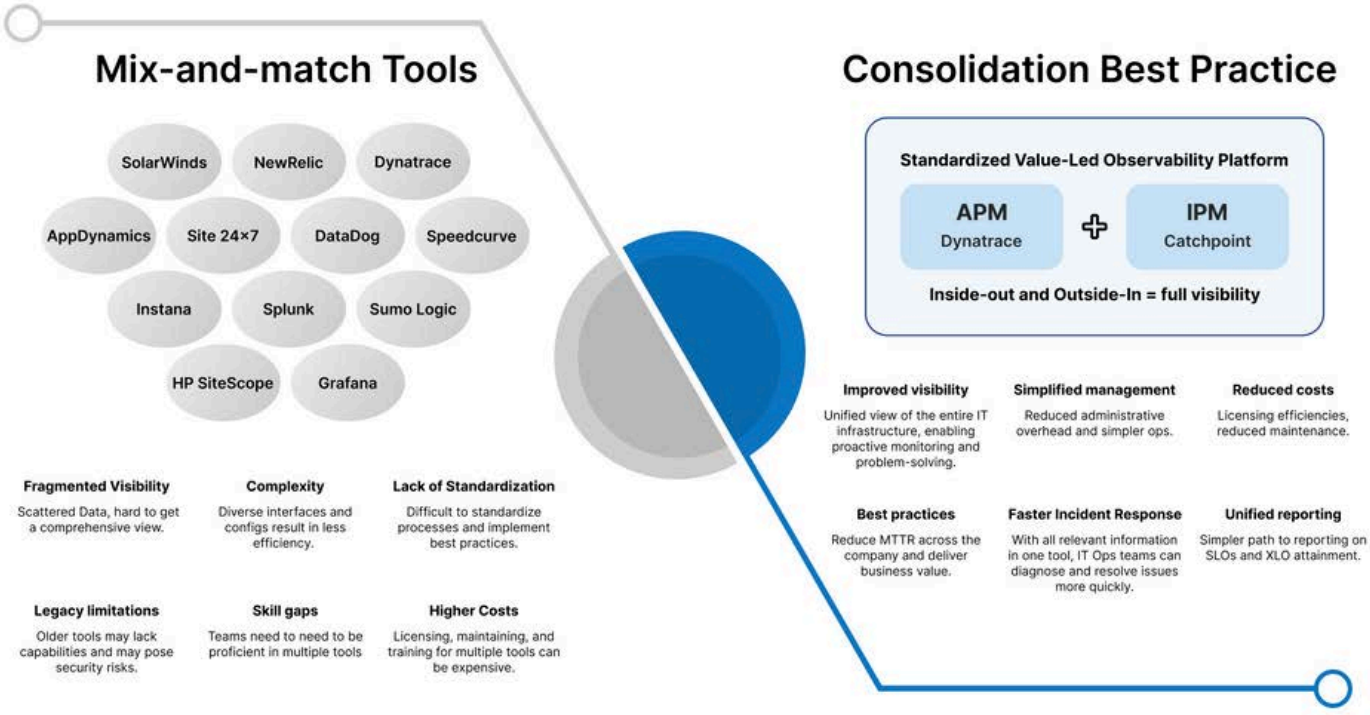

Figure 7: Fragmented vs consolidated observability approach

APM and IPM are complementary, not competing, approaches. When combined, they provide both deep internal diagnostics and an outside-in view of user experience—ensuring banks can identify and resolve issues wherever they occur.

Table 3 illustrates how APM and IPM complement each other, and why integrating both is essential for achieving complete visibility and control over digital banking operations.

Capability/ Focus	Application Performance Monitoring (APM)	Internet Performance Monitoring (IPM)	Combined Value
Perspective	Inside-out: monitors internal systems, code, and infrastructure	Outside-in: monitors from the end-user's perspective across the entire digital delivery chain	360-degree visibility, from backend systems to real-world user experience
Primary Coverage	Application code, servers, databases, internal networks	Internet routing, DNS, APIs, SaaS, cloud, ISP, CDN, last-mile connectivity	Identifies issues anywhere in the service chain, internal or external
Strengths	Deep diagnostics, transaction tracing, resource utilization, code-level bottlenecks	Detects external outages, network slowdowns, regional issues, third-party/vendor problems	Faster root-cause analysis and incident resolution
Limitations	Limited or no visibility into external dependencies or user environments	Does not provide code-level or infrastructure metrics	Eliminates blind spots by correlating internal and external performance data
Key Use Cases	Optimizing application performance, troubleshooting backend issues, SLA management	Ensuring digital experience for customers/employees, proactive outage detection, vendor accountability	Ensures both system health and optimal user experience across all channels
Best Practice	Monitor and optimize what you own	Monitor what you depend on but don't control	Integrate both for a unified, actionable view of digital operations

Table 3: How APM and IPM complement each other

Conclusion: Digital resilience starts with visibility

As financial services accelerate toward digital-first delivery, the challenge is no longer just uptime—it's experience, resilience, and trust. Legacy monitoring tools, built for static infrastructure, can't keep pace with the dynamic, distributed, and internet-dependent ecosystems that define modern banking.

This paper has shown how Internet Performance Monitoring addresses the critical blind spots left by traditional Application Performance Monitoring (APM). While APM provides deep insight into internal systems and code-level performance, only IPM can reveal how services perform for real users, across real networks, in real time.

Together, these capabilities form the foundation of a comprehensive monitoring strategy—one that aligns technical performance with business outcomes, accelerates incident response, strengthens regulatory readiness, and protects both customer experience and operational continuity.

Banks that integrate APM and IPM don't just detect problems faster—they become proactive, predictive, and experience-led.

As regulators demand greater operational resilience, and as customers demand seamless, instant experiences across every touchpoint, the message is clear: visibility isn't a technical upgrade—it's a strategic necessity.

Additional Resources

- See how leading banks use IPM to protect customer experience: Financial Services | Internet Performance Monitoring
- Discover strategies to optimize your observability investment: A 7-Step Approach to Optimize Observability IT Expenditure
- Visualize your digital dependencies in real time: Internet Stack Map
- Learn how to eliminate firefighting and "war rooms" with proactive monitoring: No More War Rooms

About Catchpoint

Trusted by the world's leading brands who understand in the digital age performance is paramount, Catchpoint is dedicated to monitoring what matters from where it matters to catch issues across the Internet Stack before they impact business.

The Catchpoint Platform offers a comprehensive suite of Internet Performance Monitoring capabilities, including Internet Synthetics, RUM, BGP, Tracing, performance optimization, and advanced analytics, all supported by high-fidelity data and flexible visualizations. Leveraging thousands of global vantage points inside the critical systems that make the Internet work, Catchpoint provides unparalleled visibility into what affects customer experiences, workforce efficiency, network performance, websites, applications, and APIs.

Today's digital world requires resilience and exceptional performance, which is why *The Internet Relies on Catchpoint*.

Learn more at: www.catchpoint.com

Follow us on LinkedIn