FROM BLIND SPOTS TO RESILIENCE: INTELLIGENT OBSERVABILITY FOR MODERN FINANCIAL SERVICES

By: Jeff Collins

Key Takeaways

- Blind spots in financial IT have already triggered breaches, outages, fines, and lasting damage to trust [1,2,3,4,5,6]
- Failures spread because systems are tied together in ways that aren't visible, such as a payment switch linked to trading, a SaaS tool tied into compliance, or a cloud service supporting multiple workflows.
- As financial institutions move toward AI-first and cloud-native operations,[7] traditional tools like CMDBs and legacy SIEMs struggle to keep pace.
- Regulators now require continuous inventories and proof of resilience.[8,9,10]
- Real-time payments plus shared third-party providers magnify systemic risk. [11][12][13].

The State of Financial Infrastructure: Fast, Digital, and Fragile

Finance has never moved faster, and it has never been more brittle. Transactions clear in seconds, but one connection can be the fault line that brings down critical services.
The CrowdStrike outage in July 2024 proved it. One flawed update rippled through banks and payments worldwide, crashing 8.5 million Windows devices, disrupting services from New York to London, and costing the Fortune 500 about $5.4 billion, with the banking sector eating roughly $1.15 billion. [2][3] What should have been recoverable became systemic because hidden dependencies were not mapped in real time.

THE DANGER OF HIDDEN DEPENDENCIES

Hidden dependencies are the behind-the-scenes links between systems, services, or providers that your teams cannot see. If those links are not mapped as the environment changes, a small fault can cascade outward and turn a local issue into a sector-wide shock.

This is bigger than security tooling. Instant payments are surging, which shrinks the recovery window. [14] Put that next to what we just lived through, and the picture is clear. Faster settlement leaves less room to recover, and one fault can ripple outward with systemic consequences. [11][12][13][2][3]

Real-time payments. Last year saw 266 billion instant payments, tracking to roughly 575 billion by 2028. [14] Once an instant payment is sent, it is gone. There is no human in the loop to catch a bad transaction. [12]

AI at scale. Most banks now have at least one generative-AI use case in production. [15] To make that work, teams are wiring AI-first data pipelines: ingestion and cleansing, embeddings or feature stores, vector databases, RAG retrieval, continuous model and data monitoring. Traditional inventory and monitoring tools struggle to track these fast-moving, third-party-heavy dependencies. [16]

Regulators and industry surveys warn that without better cybersecurity and observability, these stacks can expand blind spots instead of closing them. [17][18]

Fragmented systems and third-party links. The industry's dependence on external providers — cloud, data, analytics — accelerates delivery but raises operational and concentration risk. [19] In hybrid and multi-cloud, failures do not stay put, they spill across providers and get harder to trace to root cause. IIF–McKinsey calls out the same thing: cloud-native adoption introduces new operational risks that require stronger cybersecurity and observability. [7]

Regulators are not hedging. They are aligning, and they are putting dates on it.

- **NYDFS**: maintain a complete asset inventory by November 2025. [8]
- **PCI DSS 4.0**: universal MFA and script monitoring by March 2025. [20]
- **DORA (EU)**: credible third-party exit strategies by January 2025. [9]
- **UK FCA/PRA:** prove operational-resilience impact tolerances by March 2025. [10]

The message is simple. Blind spots are not inefficiencies you can explain away. [8][9][10] They are risks to financial stability.

The Three Blind Spots Putting Financial Firms at Risk

Most firms still have the same three blind spots. On paper they look like simple operational problems, but in practice they can turn into full-blown crises.

Blind Spot 1: You don't know what you have.

Many organizations don't have a clean, up-to-date inventory of their IT assets. Old systems stay powered on with nobody looking after them. Test apps get left open on the internet after projects end. Business units spin up SaaS tools without telling central IT. It doesn't take much, a scheduling app or an analytics plugin, and suddenly you've got assets nobody is tracking.

That's when they become entry points for attackers, for auditors, or for outages. A forgotten server, an exposed test API, or an unmanaged SaaS connection can all be the hole in the fence.

Look at Equifax in 2017. Attackers didn't need fancy malware. They used a known flaw in Apache Struts on a server Equifax had basically forgotten about. That one unpatched box opened the door to data on 147 million people. The financial hit was $575 million in settlements.[1] The reputational damage was even worse. Resignations followed, congressional hearings dragged on, and the company faced years of trust rebuilding.

The real issue wasn't the software bug. It was that Equifax couldn't see everything it owned. Nobody took responsibility for that server. Scanning tools missed it. And a single untracked asset turned into one of the most damaging breaches in financial history.

Blind Spot 2: You don't know what matters

Even when firms manage to keep an inventory, they still miss the bigger question: which failures

actually matter. The blast radius is what counts. That's the ripple effect of a failure: how many customers, transactions, or obligations are hit when one system goes down. Without that context, every alert looks the same.

The 2018 **TSB migration outage** is a good example. A flawed core banking migration left millions of customers locked out for weeks. Regulators later found TSB didn't have end-to-end mapping of its dependencies, so they couldn't triage effectively.[4] The disruption dragged on for months, drew heavy press and political fire, and left scars that went way beyond the cost of remediation.

The **SWIFT hacks** between 2016 and 2018 show the same weakness from another angle. Attackers compromised local bank systems to send fraudulent SWIFT messages, stealing tens of millions at a time. In Bangladesh, a compromised access point resulted in $81 million in fraudulent transfers.[5] The issue wasn't SWIFT itself. It was that individual banks couldn't see how their local systems, credentials, and gateways were tied together. What initially appeared to be a local breach ultimately created international financial exposure.

That's why so many security and ops teams fall into alarm fatigue. They're chasing every red light, but they don't know which ones are meaningless and which ones can cascade into a full-blown outage that takes core systems offline. And without that context, executives can't prioritize or explain their choices to regulators.

Blind Spot 3: You don't know how to fix it without breaking something else

Here's the third blind spot. Even when teams see the problem, they can't fix it with confidence. Financial systems are too interconnected. A patch that closes one hole can open another, just because the underlying relationships aren't visible.

Take the **Visa Europe outage** in 2018. One piece of hardware failed in a single data center, but the effects spread into transaction failures across Europe. What should have been a local glitch turned into a continent-wide disruption because the network's interdependencies weren't visible.[6] The result: millions of frustrated customers and regulators openly questioning Visa's resilience planning.

Executives know this pattern. A planned change that unexpectedly takes down a core system. A patch that fixes one problem but breaks something else. Without clear dependency mapping, even basic maintenance starts to feel like a gamble.

Why these blind spots persist

So why do these blind spots keep showing up? It is not because people do not care. For decades, firms have leaned on tools that keep lists: spreadsheets, asset registers, and CMDBs. Those tell you what exists, not how it is wired together or what breaks when one piece fails.

Resilience today means moving from static lists to living maps. You need to see ownership, data flows, runtime dependencies, and third-party links as they change. That lets teams answer the only questions that matter in a crisis: if this server or API fails, which customer journeys stop, which payment flows miss the cut-off, and which obligations slip. That is the difference between a nuisance incident and a systemic outage.

What Needs to Change

All three blind spots point to the same root problem. Financial institutions do not fail because they lack data. They fail because they lack context. A spreadsheet can list systems and a monitoring tool can raise alerts. If you cannot see how things connect, you cannot tell which failures matter or act with confidence when something breaks.

Closing that gap means rethinking resilience:

From static inventories to dynamic discovery.
Quarterly scans and manual CMDB updates cannot keep up with daily changes in cloud workloads, SaaS adoption, and third-party links. Firms need asset maps that update continuously so forgotten or unmanaged systems do not become entry points.

From alert volume to impact-based prioritization.
Ops teams don't need more dashboards. They need to know which failures put payment flows, trading platforms, or compliance obligations at real risk. That requires mapping dependencies and calculating the blast radius in real-time.

From reactive fixes to confident action.
Patches and configuration changes are unavoidable. What matters is knowing downstream impact before deployment. Digital twins and predictive modeling let teams test changes safely and cut self-inflicted outages, like a patch that fixes one system but accidentally brings down a customer portal. [21] This is not about making operations a little smoother. It is about making sure the next small issue does not become the next crisis. Regulators in New York, London, and Brussels now classify blind spots as risks to financial stability, and one outage or breach can undo years of trust. [8][9][10]

What we're really doing is giving financial institutions the ability to see problems before they cascade. A small issue shouldn't derail transactions or shake customer confidence. If you can see the connections, you can contain the failure.

How WanAware Helps

Financial institutions face fast-changing infrastructure, hidden dependencies, and strict regulatory pressure. WanAware tackles these challenges by replacing static lists and siloed tools with living maps of assets and their relationships.

Discover and understand your infrastructure (AIM)

WanAware's **Asset Inventory Management (AIM)** continuously discovers assets across data centers, cloud, SaaS, and third-party connections, without relying on quarterly scans or manual CMDB updates. It captures ownership, location, and status in real time, so forgotten servers, exposed test APIs, or shadow SaaS don't slip past controls.

Outcome: A single source of truth that eliminates untracked assets, strengthens compliance readiness, and reduces entry points for attackers or auditors.

Quantify impact and prioritize what matters (Knowledge Discovery Engine)

The **Knowledge Discovery Engine (KDE)** builds a live dependency map across payments, trading platforms, customer apps, and vendor services. It calculates the **blast radius** of failures in real time, showing how many customers, transactions, or obligations are affected.

Outcome: Teams can separate minor issues from massive risks, respond faster, and defend risk-based decisions with regulators.

Resolve with confidence (Digital Twin)

WanAware creates a **digital twin** of your environment, so patches, configuration changes, or vendor updates can be tested before they're deployed. Teams can see downstream effects in advance and confirm that critical flows stay intact.

Outcome: Fewer self-inflicted outages, faster recovery, and auditable proof of control.

Enable automated remediation (Remediation Module)

With dependencies mapped and risks modeled, WanAware can automate repeat fixes, such as rebooting a failing device, reconfiguring a misaligned setting, or dispatching a crew when the same sensor goes offline. Guardrails are placed to ensure automation only acts where it's safe, and automatically escalates anything outside those limits to human oversight.

Outcome: Faster recovery, less strain on staff, and more predictable operations.

What we're really doing is giving financial institutions the ability to see problems before they cascade. A small issue shouldn't derail transactions or shake customer confidence. If you can see the connections, you can contain the failure.

Conclusion: From Blind Spots to Resilience

Financial institutions can't stop every failure. But they can stop small problems from turning into systemic shocks. That requires moving beyond static asset lists and siloed monitoring tools to continuous discovery, dependency mapping, and context-aware action.

Regulators are already making this shift mandatory. NYDFS, PCI DSS 4.0, DORA, and the UK's operational resilience rules all expect firms to prove not only that assets are tracked, but that risks are prioritized and dependencies are understood.[8,20,9,10]

The firms that will stay resilient are the ones that can see changes as they happen, understand the impact, and act with confidence. The choice is clear: close the blind spots now or let them trigger the next crisis.

Next Steps

- Download the *Financial Services Blind Spot Checklist* — Quickly identify the same gaps that have led to industry-wide breaches, outages, and fines. Use the checklist to find hidden assets, untracked connections, and overlooked third-party dependencies before they become the next crisis.

Uncover Risks in Your Environment

- Start your *30-day trial of AIM* — In minutes, uncover assets you didn't know you had, before they show up in an audit or as an attack path. Build a live, accurate inventory that keeps pace with your environment and exposes blind spots you can fix right away.

See Your Live Asset Inventory Today

References:

1- U.S. House Committee on Oversight and Government Reform. (2018). The Equifax Data Breach: Majority Staff Report.

2- Parametrix via Reuters. (2024). CrowdStrike Outage Estimated Impact.

3- Investopedia. (2024). CrowdStrike Global IT Outage Explained.

4- Financial Conduct Authority (FCA). (2019). TSB Migration Report.

5- SWIFT. (2016). Customer Security Programme.

6- Visa & UK Payments Systems Regulator. (2018). Visa Europe Outage Review.

7- McKinsey & Company & Institute of International Finance. (2024). The cyber clock is ticking: Derisking emerging technologies in financial services.

8- NYDFS. (2023). Cybersecurity Regulation Amendments (23 NYCRR 500).

9- European Commission. (2022). Digital Operational Resilience Act (DORA).

10- FCA/PRA. (2021). Operational Resilience Framework (PS21/3).

11- U.S. Treasury Department. (2025). Financial Services Sector Risk Management Plan.

12- Federal Reserve Bank of Atlanta. (2023). Key Risk Considerations for Implementing Instant or Real-Time Payments.

13- KPMG International. (2024). Managing Critical Third Parties.

14- ACI Worldwide. (2024). Prime Time for Real-Time Payments.

15- IBM Institute for Business Value, 2024 Global Outlook for Banking & Financial Markets.

16- McKinsey, "Capturing the full value of generative AI in banking" (data/architecture to scale GenAI); Google Cloud, "What is RAG?"; AWS, "What is RAG?"

17- U.S. Treasury, Artificial Intelligence in Financial Services (notes model-inventory expansion and third-party risks; cites IIF–EY 2023)

18- FSOC, 2024 Annual Report (AI adoption may amplify system/model/data risks)

19- Financial Stability Board. (2024). Final Report on Enhancing Third-party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities.

20- PCI Security Standards Council. (2022). PCI DSS v4.0.

21- University of Maryland, Baltimore County. (2023). Change Management using Generative Modeling on Digital Twins.

www.wanaware.com