Overcome the Challenges of Moving Core Banking and Transaction Processing to the Cloud

Avada
Infrared360
provides the security, observability, and management capabilities financial organizations need to mitigate the challenges of Cloud.

…most analyst groups have all published about the importance of maintaining proper observability as you move to modern distributed infrastructures.

Foreword

Banks have been implementing cloud infrastructure for certain low-risk functions since nearly the technology's inception. Many banks, however, have shied away from implementing transaction processing and core banking processes on Cloud. But, in just the past few years, some financial institutions had already begun to migrate more business-critical and transactional processing to the cloud.

Banks and financial organizations have very specific requirements as they move to or expand their cloud infrastructure. Security and compliance risks, technological legacy, transactional latency, misalignment between IT and the business, and a lack of skills are the greatest barriers impeding financial organizations from realizing their cloud goals.

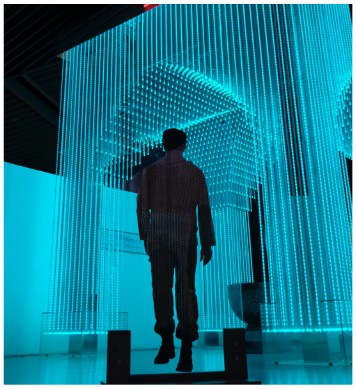
By understanding the proven methods for mitigating these barriers outlined in this document, IT leaders at financial firms can more confidently capitalize on the benefits of cloud as part of their IT infrastructure to meet SLAs and better align with business goals.

Executive Synopsis

The biggest misconception about moving your core banking and transaction processing systems to the cloud is that administration and management now become someone else's problem, someone else's expense. Nothing is administrator-less. While you may see information about your cloud layer or the container layer, no one will be monitoring the messaging and transaction layers within them. Think of it like luggage during air travel. When it gets thrown on the belt, they can see if the luggage itself got damaged, but not if something inside was damaged. Not only is your cloud provider not going to monitor and manage your transactional and message-oriented infrastructure for you, they're not going to notify you of missed transactions, backlogs, or traffic jams – all things that can cost your organization in dollars and time and affect your reputation.

Gartner, Forrester, Bloor, and most analyst groups have all published about the importance of maintaining proper observability as you move to modern distributed infrastructures. It is the one thing that mitigates the largest number of the risks and barriers to cloud for banks and financial organizations. As you move transactional processing and core bank systems into cloud, hybrid infrastructures and emerging architectures (e.g., containers and microservices), an effective monitoring and management solution for your transactional infrastructure can give you the visibility you need into all your systems without sacrificing control just because it's on infrastructure you don't own. You need to know at a glance when everything is running smoothly, but even more so than non-financial organizations, you also need to know exactly where the issue is when something goes wrong - before it's a problem.

The goal is to enable you to manage smarter and more efficiently, so you can devote your resources to core activities that align with core business goals. What follows are seven precepts bank and financial I&O leaders should consider before making the jump to the cloud and a layout of how an effective, cloud-ready solution for monitoring your transactional and sensitive application infrastructure will help you achieve that.



The key to maintaining secure, reliable, transactions and core banking systems over modern distributed infrastructure is the observability of your middleware layer.

You Must Pay Attention to The Old if You Want to Securely Capitalize on the New

When moving sensitive transactional and core financial systems to the cloud, most IT leaders fall victim to the Shiny New Things Syndrome. Cloud providers, Cloud-native applications, multi-cloud, containers, and a plethora of cool things to complete the goal draw your attention. But there's an established, if less glamorous, technology that is key to your success in transitioning these critical applications and transactional systems to the cloud and other modern infrastructures. The integration of these applications and transaction messaging is managed by your middleware layer.

The key to maintaining secure, reliable, transactions and core banking systems over modern distributed infrastructure is the observability of your middleware layer. Do that right, and you mitigate or eliminate all the concerns we've addressed thus far. Unfortunately, many Directors and Executive level IT leaders who don't work with it on a regular basis often overlook or deemphasize this layer of their overall technology landscape in favor of the more "shiny" aspects of it. They often miss the importance of message queues, integration software, message busses, and application servers or even think of them as legacy technology. But it couldn't be more critical to your success here.

1. **Visibility and accessibility to critical resources.** As we mentioned earlier, many people when moving to the cloud are under the misconception that they can set up their transactional infrastructure, like message queues and application servers, on the cloud and forget about it. But it's the opposite. Not only will you not get performance feedback on these middleware systems from your provider – leaving you susceptible to missing valuable transactions – but unless you have an effective, cloud-enabled monitoring and management solution in place, you may not have access to certain transactional endpoints that are locked down by your provider.

...low-latency infrastructure will be important as you make this transition. But, true real-time monitoring and management of the application infrastructure handling those transactions becomes even more critical.

2. **Cloud benefits without compromising security.** The management tool you deploy to monitor and manage this cloud-based message-oriented and application infrastructure can help you mitigate security risks that are inherent to these distributed environments. However, take caution that these management tools have security equal to the transaction and application infrastructure itself, but without adding complexity that can be exploited by nefarious actors. Furthermore, most cloud providers restrict what can be pre-installed in the image upload, so the management solution needs to be free of code and script layers that may get rejected.

3. **Low-latency presents its own issues.** For most organizations fast performance with minimal latency and maximum reliability in their cloud infrastructure is important. For firms that manage fund transfers and other financial processes it is the end-all and be-all of your operations. So, low-latency infrastructure will be important as you make this transition. But, as you move these processes to low-latency cloud infrastructure, true real-time monitoring and management of the transaction-oriented and application infrastructure handling those transactions becomes even more critical. While many solutions claim to be real-time monitors, many actually write to logs and then monitor and alert from the logs. Not only is this not proactive, it's data intensive and costly

4. **Be proactive, not reactive.** Because transactional systems now span many operating systems and many technologies, a new set of management products arose that rely on capturing and analyzing tons of data in either logs or databases. This approach fits into the buzz about 'big data', but these solutions are forensic in nature, boost data and storage costs, and result in added time and labor costs. IT executives should take advantage of the proactive approach to save time, risk, resources, and money (TRRM). The overall cost is less in terms of both initial setup as well as TRRM in the long term. The upfront cost of the 'gadgetry' that enables this is very affordable and scalable as well.

5. **Optimize Existing Skill Sets Without Compromising Security.** As financial orgs. move sensitive data, core banking processes, and transactional processing to hybrid infrastructures and emerging architectures, identifying and resolving incidents can be challenging for your IT and business teams with traditional skill sets. This is especially true if they're working in operational silos. But giving blanket access to the transactional infrastructure so teams can collaboratively identify issues and solutions is a security no-no, especially for sensitive financial transactions. As you move these sensitive transactional systems to a modern distributed infrastructure, it is imperative for your financial organization that your teams can securely collaborate on problem identification and resolution in a manner that prevents unauthorized access to sensitive data, transactions, or even the servers that handle them.

Make sure you're fostering the level of observability that is needed for your transactional environments in the cloud with powerful real-time analytics, full historical data... built-in visualizations... and the ability to port the data to 3rd party analytics tools without the need for scripts and code.

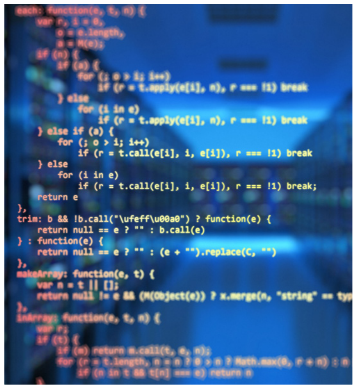
ARE YOU REALLY LISTENING?

There is another very important aspect of a proactive approach that many don't think about but is crucial for financial organizations. As you start to move your more critical transactions into the cloud, you are doing exactly that: moving CRITICAL transactions into the cloud. These are elements of your business that SLAs are built around for a reason. Often organizational reputation, revenues, customer satisfaction, statutory compliance, and even liability are on the line when it comes to the efficacy of these transactions.

Learning about an issue with transaction initiation, transfer, or deliverability needs to happen in real-time. Be careful here, though. When it comes to observability of your messaging infrastructure in modern distributed environments, many solutions proclaim to offer real-time monitoring and alerting, but in reality, they write their data to expensive logs and then trigger alerts based on averages in those logs. That is analogous to a general weather forecast ... where you don't get actual weather changes until after they occur. This can cause delays in finding out about a breakdown in that transaction chain. That delay can cost you money, time, and/or reputation.

6. **Advanced Analytics.** The purpose of the infrastructure layer that handles your transactional messaging is to create an environment so your disparate transaction systems can talk to each other. The native reporting capabilities for elements of this infrastructure, like message queues, have native capabilities to let your team review 30, 60, 100 screens of telemetry into your system. But, reviewing these can be like drinking from a firehose. The data gets dumped into a log where only those who are trained in the specific technology will know what any of it means – and only after parsing reams of data. Make sure you're fostering the level of observability that is needed for your transactional environments in the cloud with powerful real-time analytics, full historical data, and both built-in visualizations of that data as well as the ability to port the data to 3rd party analytics tools without the need for scripts and code.

7. **Do Your Homework.** Recently, the Bank of England released a Financial Stability Report that specifically stated concerns about financial institutions moving to the cloud. They raised concerns that the small number of very large cloud providers who are serving the growing throngs of financial institutions moving sensitive systems to the cloud might one day shift the balance of



power to the providers. Their concern mostly centered around this scenario allowing providers to operate in an opaque and closed fashion and obscure security concerns. It's critical to make sure as you move to the cloud that you have insight into how they manage data security, data governance and business policies, what certifications and regulations are in place, and a laundry list of other precautions - not the least of which is understanding exactly what you'll have access to and visibility of.

Evolving Monitoring Paradigms and Product Requirements

Most technical professionals are aware of the need to monitor their IT services, and almost all organizations have multiple software products and tools in place to do so. But according to Gartner, software platforms have evolved beyond traditional monitoring products and paradigms.

But according to Gartner, software platforms have evolved beyond traditional monitoring products and paradigms.

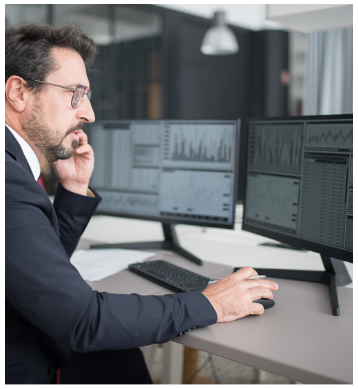
Paradigms

Over the years the typical division of responsibilities has resulted in monitoring often being associated with part of a deployment to a production environment. This led to monitoring being handled as a packaging activity that I&O “plugs-in” when an application is promoted into production. In cases where the failure modes are predictable, this monitoring paradigm can be effective, but only up to a point. This style of monitoring is better at problem identification but is inadequate when it comes to assisting resolution.

DevOps monitoring or synthetic monitoring is a newer paradigm that includes preproduction environments in the monitoring picture. This monitoring methodology is advised for financial institutions moving more and more to the cloud. It isn’t so much about increased observability, but achieving more efficient deployments, fostering continuous deployment, maintaining monitoring continuity, and enabling Dev to become Ops Literate.

Proactive monitoring paradigms vs. forensic or reactive methodologies is an area this document previously touched on. Enabling proactive management is another paradigm where many monitoring applications fall behind in cloud and modern distributed environments. A monitoring and management solution for your middleware in these cloud environments needs to have features and capabilities that foster a proactive monitoring and management paradigm. To achieve that a solution needs to support DevOps, provide real-time monitoring, and enable a collaborative problem-solving approach.

A collaborative approach to problem identification and resolution is not only critical to proactive management as you move to the cloud, but is a key component to improved reliability, faster time to resolution, and better efficiency. Yet,



The move toward agile infrastructure... has challenged the viability of traditional infrastructure monitoring tools and techniques to manage application health and performance.

it's one of the biggest capabilities where monitoring and management solutions fall behind. Most simply can't provide both a collaborative approach that reaches across departmental, location, and role silos while also providing the security needed to keep sensitive data and transactions secure.

Products

The move toward agile infrastructure like hybrid IT, multi-cloud, and containers and modern application architectures, as well as continuous delivery has challenged the viability of traditional infrastructure monitoring tools and techniques to manage application health and performance. As you move your sensitive systems to the cloud you place very different demands on your infrastructure. To ensure a solution can keep up, there are also product-specific considerations you should look at:

Design. A consideration that must be addressed with monitoring modern distributed systems is data location. Whether your architecture is completely unbundled or tied to one or more storage repositories, your ability to analyze, visualize, and/or alert on data uniformly needs to be supported by your monitoring solution. Many tools tout the ability to consume and analyze multiple types of machine data across domains. Most achieve this through costly data log storage in various configurations across the domain and compete on how their configuration fosters consolidation. But, according to analysts like Gartner and others, it is more important to focus on having the right data in the right place at the right time than to prioritize consolidation. They caution that the reduction in complexity should be balanced against potential compromises in capability that can be created by too much reliance on consolidation.

Monitoring and management solution products must be created with an architecture that supports the ability to provide this observability across various types of domains without adding unnecessary costs or reduced capabilities. This is a big part of why Infrared360 was designed to be agentless and scriptless. Deploying it across modern distributed infrastructures is simple and fast and this lack of complexity actually delivers more capability and cost savings, not less. It doesn't matter where your infrastructure endpoints are (on-prem, in cloud, hybrid, multi-cloud, containers, or wherever), the agentless design lets you easily monitor and manage your endpoints.

Hidden Costs. Another key thing to look for in your middleware monitoring product is that they don't force you to incur exorbitant extra, and often hidden, costs associated with moving your transactional and core banking systems to the cloud. One of those costs goes hand in hand with the old forensic paradigm supported by tracing messages. This leads to uncontrolled data storage costs and exponentially increased manpower costs when it comes to resolving incidents. This should be evaluated in the analysis of total cost of ownership along with other cost-inducing aspects like the man-hours spent to deploy agents and scripts or clients and then again, each time you need to update the solution and all those associated elements. Data storage, time to deployment, management of messaging server versions and patches, restriction to OS, and pre-built server images, and others are all areas where you can incur hidden service provider or man-hour costs depending on the product you select.

Security. The most-cited reason for banks and financial institutions to hesitate about moving transactional and core systems to the cloud is security. That's why security has been an overreaching theme in all that this document has discussed. As you modernize with infrastructures like cloud, multi-cloud, and containers, you will keep security in the forefront of your mind and planning. Your monitoring and management product needs to foster your secure approach. Certain modern distributed infrastructures like cloud may introduce inherent risks. Analyst firms like Gartner, Forrester, and others have espoused that proper observability through a modern messaging and application monitoring and management solution can mitigate many of those. But modern architectures mean the solution itself needs to be more secure than ever. It should leverage existing security systems already in place, it should not utilize agents or scripts that introduce new vulnerability points, and it needs to have native security features that manage approved access to your infrastructure.

Further, while your solution needs to foster modern process like DevOps monitoring and collaborative approaches to issue identification and resolution, it needs to do those things in as secure a manner as possible.

Further, while your solution needs to foster modern process like DevOps monitoring and collaborative approaches to issue identification and resolution, it needs to do those things in as secure a manner as possible. Your solution should have the capability to be used across the organization while being secure enough to grant and limit visibility and access to only areas that users, groups, and/or applications should be allowed to access or see. And while that is powerful security, it's not enough. To satisfy many security and compliance SLAs, your solution needs to have full user and change audit trails that you can easily review, package, and send to anyone anywhere that you need to.

Analytics. The term "observability" in the IT Monitoring world describes a holistic and data-centric approach that fosters exploration and enables identification of unknown and unpredicted anomalies. While metrics and analytics are not the entirety of observability for distributed infrastructures, the critical capability is the interaction with data. Modern distributed systems, particularly when the services are created and supported by multiple product teams, make it difficult to understand the details of an application's internal state at any given time, not to mention, whether the application is performing well for everyone.

A wide variety of tools are available to gather the metrics data that is generated by middleware infrastructure and applications. For this metrics collection, these tools often rely on the implementation of agents on a compute node that aggregates metrics data from multiple subsystems and applications and brings it back to a storage platform. Metrics consumption then happens in two ways: visualization (i.e., charts, graphs, and dashboards) and notifications (triggered by thresholds or an anomaly having been detected).

We discussed earlier, in relation to proactive management, how solutions that collect and perform analysis on metrics data this way fall behind the needs of today's modern distributed environments and architectures. In addition to those factors, I&O leaders should assess several additional factors related to a product's analytics capabilities:

- How easy it is to gain access to the needed health and performance data? Are there built in visualizations and analytics tools? Are you easily able to create and edit visualization dashboards?
- Is there integration of visualizations and other data formats like actual queue values in the dashboards?
- Ability to keep a running, visual record available for ongoing analysis and reassurance and to benchmark base line trends
- All this should be native to the solution and not require any additional products, like Grafana.
- But, despite the above bullet, there should be a simple and easy way to integrate with 3rd party tools when needed or desired - without the need for building and maintaining scripts

Additionally, while not part of a visualization, monitoring solutions for modernized middleware environments need to provide easy access log information. Analysis of log and event data augments the collected metrics and should be incorporated into a monitoring strategy to ensure that not just the "What" but the "Why" of an incident can be answered quickly (recall that secure collaborative problem-solving capabilities also hastens discovery and resolution). This is critical for an observability-based monitoring strategy. In modern environments, it is not possible to fully instrument a system using metrics alone. For example, metrics that show latency or delivery issues may point to a time and location. However, it may then be necessary to review an application or system log at an interval slightly before that latency began. There is no silver bullet in complex situations, but there are proactive means to identify and coordinate the pieces needed to expedite MTTR.

How Infrared360® Eases Your Transition of Core Banking and Transaction Processing to the Cloud

Infrared360 is a new paradigm solution, designed to monitor your transactional middleware layer across modern distributed environments before those environments were the de facto go-to architecture. It is a single-interface solution for

Infrared360 is a new paradigm solution, designed to monitor your transactional middleware layer across modern distributed environments before those environments were the de facto go-to architecture.

secure administration, proactive monitoring, synthetic transactions, user auditing, and real-time analytics of your transaction and application middleware. It is designed to give you full observability and secure delegated administration across your disparate and distributed environments. Leading banks and financial organizations worldwide use it for the following attributes:

Secure Observability for your Full Infrastructure Stack

Infrared360's myriad security features such as its 100% agentless design, Trusted Spaces™ and complete user and change audit trails help banking and financial clients mitigate many of the risks of moving transactional and core banking systems to the cloud. And, by fostering end-to-end observability of your full infrastructure stack you're able to better manage and monitor your transactional messaging systems, application servers, Web Services, and even gateway appliances like DataPower and MQ Appliance.

True Real-Time™ Monitoring for Low Latency Cloud Environments

Infrared360 monitors in True Real-Time™ so bank and finance IT professionals can be alerted to and react faster to problems - diagnosing and fixing them before they disturb the user experience or create transaction fidelity issues. Infrared360 does not periodically take snapshots of the performance metrics being tracked and then trigger alerts based off averages of those snapshots, which in-turn degrades the ability to identify when issues first appear. Infrared360 allows you to head off issues and get to the bottom of incidents faster. This proactive management capability has led customers of ours to achieve 99% server up time and see 70% decreases in incident reports.

This proactive management capability has led customers of ours to achieve 99% server up time and see 70% decreases in incident reports.

Trusted Spaces™ for Secure Granular Access and Visibility

Infrared360 lets you have cloud benefits without compromising security. Our unique Trusted Spaces™ feature keeps users seeing and working only in the areas they should and promotes secure collaboration across departments, teams, locations, and partners. This paradigm supports the shift to agile product development and DevOps' shared responsibility, bringing developers into scope of pre-production monitoring – without compromising security of queue managers, application servers and other critical transaction middleware. Plus, when you have true secured delegation capabilities, you are poised for real proactive management of your distributed environment. Check out how Parker Hannifin utilized Trusted Spaces™ to improve efficiencies across disparate business units.

Proactive Management, Reducing the Need for Forensic Reactions

Infrared360 is a new paradigm monitoring and management solution. This is perhaps most evident in the focus on proactive management of your transactional environments. Infrared360's True Real-Time™ monitoring, schedulable synthetic testing capabilities, and Trusted Spaces™ combine to give you proactive capabilities unequalled in other solutions. True Real-Time monitoring instead of scraping logs, the granularity of access security, the ability to string together situational alerts, the array alert triggered reactions (notifications, script calls, etc.), and the ability to securely engage the right personnel to analyze and react in a timely manner, allows you to mitigate incidents in low latency transactional environments. With a proactive approach, you're mitigating the need for all the hidden costs that accompany forensically managing incidents.

Synthetic Transactions for DevOps Monitoring

Failure to include pre-production environments in the monitoring strategy is especially harmful for transactional environments in modern distributed infrastructures. Infrared360 embraced this paradigm and is designed to be used in production and pre-production environments. It employs an easy to use, proactive monitoring approach that lets you emulate transactions from and to anywhere in your environment. Our easy-to-use interface lets you effortlessly create behavioral paths which are monitored in your testing component. No actual traffic is needed, so you're able to schedule and test applications 24×7 or test new architecture elements prior to a live launch.

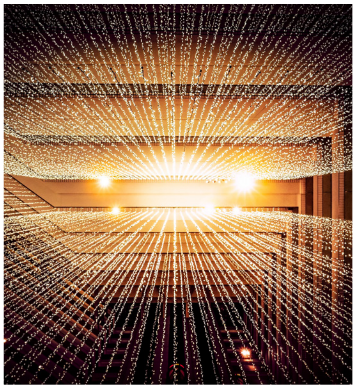
Analytics and 1-Click Reporting for Your Entire Distributed Environment

With Infrared360 you're able achieve the level of observability that is needed for your transactional environments in the cloud with powerful real-time analytics as well as full historic data visualizations. Infrared360's True Real-Time™ monitoring enables unparalleled real time analytics – a key element to proactive management of distributed transactional environments. Analyze data with intuitive drag & drop visualizations. No programming, just insight. You can easily share dashboards, graphs, charts, or reports with anyone to get richer, collaborative insight. Plus, Infrared360's built-in SOA interfaces give you the ability to port any data to 3rd party analytics tools like SNOW or Splunk without the need for scripts and code. All the best practices of data visualization are baked right in.

Scalability without Hidden Costs

One of the most prevalent reasons banking and finance organizations, or any organizations for that matter, move to the cloud is for scalability and elasticity. Infrared360 lets banks and financial organizations achieve that goal with the highest scalability of any monitoring solutions. No user fees, no data storage or access costs, and no clients or scripts to deploy means you can scale to unlimited users with no fees. That means no user fees, no operational and upkeep costs, nothing. And, with Infrared360 you can scale to monitor and manage thousands of endpoints with a single server instance.

With Infrared360 you're able achieve the level of observability that is needed for your transactional environments in the cloud with powerful real-time analytics as well as full historic data visualizations.



Infrared360 is loaded with other features and capabilities that will help you mitigate the challenges of moving transactional and core banking systems to modern infrastructures.

To find out more, CLICK HERE to set up a live demo with the Product Manager.

Dozens More Features and Capabilities

Infrared360 is loaded with other features and capabilities that will help you mitigate the challenges of moving transactional and core banking systems to modern infrastructures. Just a few include:

- Automation and self-healing capabilities
- 3rd-party integration with central management tools and systems like ServiceNow, Netcool, and others
- True Real-Time™ Analytics and Full Historic Data
- Drag and Drop visualizations and one click reporting
- SSL Certificate management and renewal
- Contact us for more product details on these and more

Or CLICK HERE to see a Live Demo of Infrared360 in action.

ABOUT AVADA

Avada Software specializes in Enterprise Middleware solutions. Founded by some pioneers in SOA, MQ and J2EE technology, Avada Flagship product, Infrared360®, is a holistic & innovative private cloud enabled portal providing administration, monitoring, testing, auditing & statistical reporting for Enterprise Middleware including such as IBM MQ®, Apache Kafka®, and TIBCO EMS®, Application Server providers such as IBM, JBoss, & Apache, and SOAP & REST based web services. Infrared360 is a single web application, yet scales to thousands of endpoints without deploying anything (no agents, no scripts) to those endpoints. Using Secure Collaboration™ and delegated administration, the portal uniquely provides different business units or even different application users delegated virtual environments in which to work.

AVADA SOFTWARE

**100 Enterprise Drive. Suite 301
Rockaway, NJ 07866**

**1 (862) 781-6159
info@avadasoftware.com**

**+1 973 6971043
www.avadaSoftware.com**

Images courtesy of Pixabay.com, Unsplash.com. Pexels.com