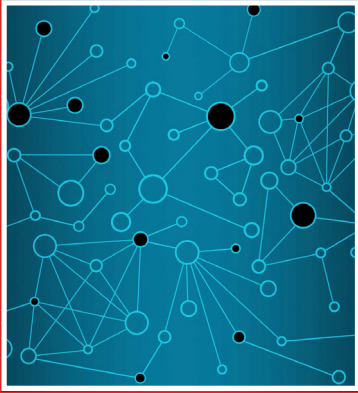# Five Challenges & Solutions When Modernizing Your Middleware Infrastructure

Avada Software's Middleware monitoring and administration solution, **Infrared360** gives you the observability you need across modern infrastructures.

According to Gartner and others, many of the tools available for middleware monitoring don't fully support modern applications or the modern architectures they run on.

Modern architectures like cloud platforms and containers, as well as modern processes like DevOps, have led to an enormous increase in workloads across distributed enterprises. This challenges SRE and I&O professionals as they attempt to manage and maintain aggressive service-level objectives. These modern architectures and processes have added to the complexity of managing distributed systems and have highlighted gaps in available monitoring processes and products.

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 leading analyst firms like Gartner and others, many of the tools available for monitoring your distributed network, including enterprise messaging and application transactional environments, don't fully support modern applications or the modern architectures they run on like hybrid IT, multi-cloud, containers, etc. These distributed systems are used more and more today yet they place drastically different demands on your infrastructure and monitoring capabilities than the classic monolithic architectures.

Analysts often discuss the basic areas where these monitoring and management solutions fall short in terms of two distinct aspects: Process and Product.

Processes

Over the years the typical division of responsibilities saw monitoring being associated with Development teams only as part of a deployment to a production environment. This led to monitoring being "plugged-in" by I&O as an application is moved into production. This may have sufficed in cases where the failure modes are predictable, but only up to a point. This process of monitoring is better at problem identification but is inadequate when it comes to assisting resolution. This has an impact on several modern processes:

DevOps monitoring or synthetic monitoring is a newer paradigm that includes preproduction environments in the monitoring picture. This methodology 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. Monitoring and management solutions need to be able to foster a DevOps monitoring approach. Some tools offer synthetic transactions and claim to be DevOps monitoring friendly, but to really support a full production/pre-production monitoring process or paradigm, your solutions need to grant or limit access to individual objects based on user roles and permissions. This way Dev can only see or access what Dev is supposed to see and access. Most tools don't provide this. For a deeper dive, check out how Parker Hannifin capitalized on this modern paradigm.

For a middleware monitoring solution to provide value to IT and therefore to the business, it must foster this proactive approach and identify problems before users are affected and business processes are disrupted.

Proactive management is another modern process or paradigm where standard monitoring solutions get left behind. There have been many papers and research results on the enormous costs and efficiency drains that come from forensic management for IT infrastructure (including enterprise messaging and middleware).

For a middleware monitoring solution to provide value to IT and therefore to the business, it needs to foster this proactive paradigm and identify problems before users are affected and business processes are disrupted. But, without the ability to securely collaborate on problem identification, there is no closed-loop capability to manage identified problems, mitigate impact, and prevent re-occurrence. This cycle for continuous improvement is key to proactive management. A monitoring and management solution's ability to permit a secure collaborative approach to problem identification is therefore the key to improved productivity and reducing the cost of ITIL problem management.

In addition to a collaborative capability, there is another proactive management staple that should be considered. For most organizations minimal latency and maximum reliability in their messaging and transaction infrastructure is critically important. But as you transition to modern, low-latency distributed infrastructures, this can become even more important. As a result, true real-time monitoring and management of your messaging and application infrastructure becomes even more critical to a proactive management approach. While many monitoring solutions claim to be real-time monitors, many actually write to logs and then monitor and alert based on averages from those logs. In addition to being a data intensive and costly monitoring paradigm, this adds latency to your monitoring process and delays delivery of alerts and notifications that you rely on to maintain service levels and an effective proactive process.

A monitoring and management solution for your distributed enterprise needs to have features that support these processes - like secure collaboration capabilities, powerful but easy-to-build alert and notification rules, and true real-time monitoring and alerts that mitigate latency issues. These capabilities foster a proactive monitoring and management process and avoid the need for forensic or reactive incident resolution whenever possible. Check out our recent case study to learn how a variety of organizations cut costs and improved efficiencies with a monitoring tool that fostered their proactive management approach.

Product

As you modernize, you place very different demands on your middleware infrastructure and on your monitoring and management solution. To ensure a solution is able to keep up, there are also product-specific considerations you should look at:

Monitoring and management 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.

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 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.

Security. 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 Garner, 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 approach 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
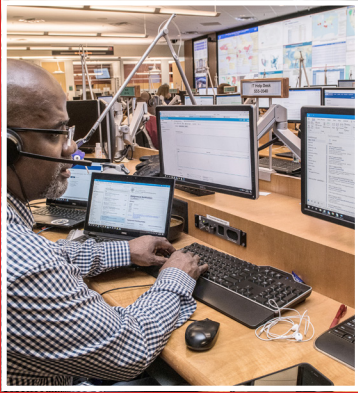
Tools that collect data into logs and then trigger alerts based on averages in those logs are not enabling proactive management.

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).
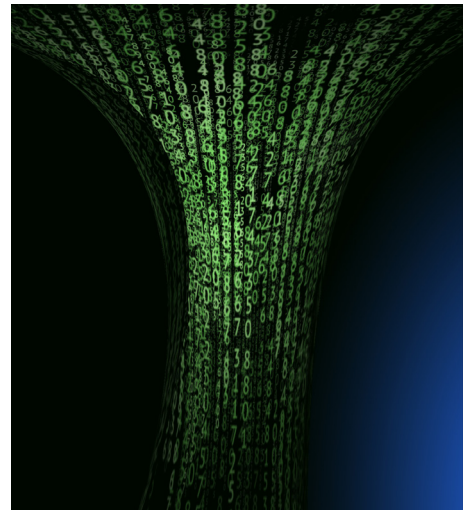
We discussed earlier, in relation to proactive management, how solutions that collect and perform analysis on metrics data this way fall behind the needs of today's modern distributed environments and architectures. In addition to those factors, I&O leaders should assess several additional factors related 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
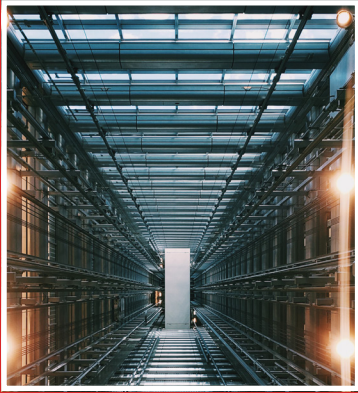
In short, to keep up with advances in infrastructure, middleware monitoring and management products need to support modern processes and have these capabilities that support modernization.

- All this all 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.

In short, to keep up with advances in infrastructure, monitoring and management products need to help you meet security and compliance scrutiny and not introduce new vulnerability loopholes. They have to support the granular observability needed for modern infrastructures. They must support processes like the shift to agile product development and DevOps shared responsibility, bringing developers into scope. And, products must have monitoring and analytics capabilities required to support business performance and availability objectives.

Deploying a Middleware Management Solution on Modern Middleware Infrastructure

You've decided to modernize your middleware infrastructure because you want to reduce your total cost of ownership, improve availability, increase deployment capabilities, or capitalize on a myriad of other potential benefits.

Avada Software created Infrared360 to be platform agnostic. It is designed to work with modern middleware environments, on-prem, coud, containers, anywhere.

Avada Software created Infrared360 in 2006 to be platform agnostic, cloud/on-premise/hybrid agnostic, private versus public cloud agnostic. Subsequently, it's even designed to easily run in containers. The emerging importance of the cloud meant we would be browser-based with no client on the desktop, with an eye toward not only how people were working more than a decade ago, but also with an eye on how people would be working today and into tomorrow.

Designed for Modern Architectures
Infrared360 is browser-based and cloud-native. It's agentless and scriptless design was created to support the ability to provide observability across various types of domains without adding unnecessary costs or reduced capabilities. The agentless design allows you to easily implement Infrared360 in any modern in infrastructure, cloud, hybrid, containers, etc. Plus, there is no client to install nor any changes/modifications/configurations required to your middleware or managed endpoints. No clients, no agents, no scripts, & built-in metric visualizations means our customers can deploy and get value from Infrared360 in hours, not weeks or months. Infrared360 leverages the security framework already in use, so there are no concerns about adding layers of code that may leave systems vulnerable or be restricted by your cloud provider. All you need is the IP address of the touchpoint you want to manage and (leveraging your own security measures) you're in. Deploying Infrared360 requires only a simple file or container deployment on a central server.

Enables Proactive Management
Infrared360 is a new paradigm monitoring and management solution. This is perhaps most evident in the focus on proactive management of your middleware 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, service calls, etc.), and the ability to securely engage the right personnel to analyze and react in a timely manner, allows you to identify and mitigate incidents before they negatively impact your SLAs or the business. Plus, with a proactive approach enabled, 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.

True Real-Time™ Monitoring for modern and/or Low Latency Environments
Infrared360 monitors in True Real-Time™ so I&O 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 rely on periodical snapshots of 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's True Real-Time™ monitoring allows you to head off issues and get to the bottom of incidents faster. This pro-active 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 enables 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 middleware. Plus, when you have true secured delegation capabilities, you are poised for real proactive management of your distributed environment. Beyond user credential security, our Trusted Spaces™ feature lets you delegate administration. For example, let's say that after a merger *Acquiring Co.* isn't quite ready to hand the reins of control over to *Purchased Co.* In that case Infrared360 can be set up to allow *Admin-Purchased* to only control groups, roles, alerts, or charts in the Purchased Co. middleware environment. There are many other potential scenarios. Connect with one of our experts to learn how Trusted Spaces™ lets you grant or limit granular access all the way down to individual objects.

Analytics and 1-Click Reporting for Your Entire Distributed Environment

With Infrared360 you're able to 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 environments. Analyze data with intuitive drag & drop visualizations. No programming, just insight. When it comes to reporting, you can easily share dashboards, graphs, charts, or reports in a variety of formats with anyone to get richer, collaborative insight. All the best practices of data visualization are baked right in.

If needed, Infrared360's built-in SOA interfaces give you the ability to port metrics or alert instances to 3rd party analytics tools like SNOW or Splunk or even external graphing tools like Grafana, without the need for scripts and code.

Plus, our Trusted Spaces™ feature lets you securely collaborate with easy-to-access object logs to review and identify the "Why," when needed.

Less is more, but less is really hard. The reality for those who manage middleware is that they have access to too much information. "I have five windows open at one time," is a frequent complaint. "Which one should I be looking at?"

Infrared360 provides reporting capability into middleware by distilling the information most critical to you into easily digestible, drag and drop portlets from which you can build dashboards, alerts, reports, and test cases.

Portlets are windows of information that contain graphs, data grids, diagrams, or other screens that provide whatever information an end user requires to grasp the state of the health of the middleware landscape.

The portlets are drag-and-drop configurable and combinable to create a dashboard or series of dashboards in any view that is appropriate for a user or group of users. And, our Trusted Space™ feature means they're customizable for each user's view, so only the right people are seeing the right information.

ADDITIONAL AVADA ADVANTAGE:

SECURITY WITHOUT COMPLEXITY

While AVADA doesn't pursue a specific vertical, it is no coincidence that fifty percent of our clients come from the financial sectors. When transaction efficacy means money is on the line, you have to be risk averse, and a cloud-ready middleware management tool solves that.

As AVADA realized early on, adding a layer of additional security is inefficient and risky. Our model has always been "don't build what's already built." In the case of security, the user credentials security model for Infrared360 is fool-proof in that it simply piggybacks on the existing LDAP and SSO credentials without an additional layer.

Beyond user credential security, and our Trusted Spaces feature explained earlier, Infrared360 provides complete user and change audit trails so you'll never have to fret about compliance and security audits again.

Alert to Resolution All In One

The dashboard is only one part of the advantage of a middleware management tool. Another big advantage is an alert system, one that advises you of issues regardless of whether the source is on-prem, in the cloud, or both. While

To keep up with advances in infrastructure, your middleware monitoring and management solution needs to help you work smarter, not harder - regardless of whether your systems are on-prem, on the cloud, or in containers.

you could monitor middleware with a live person, what you really want to do is manage it smarter. Infrared360 comes with a robust alert notification feature, based on True Real-Time Monitoring™, so there is no additional layer of latency and you know when a system is functioning within your service level parameters, when it is at risk, and when (and more specifically, where) there is an exception.

Getting an alert of a business process exception or when a business process is at risk is all well and good, but only if you can do something about it. Root-cause analysis should not be a fix-it later process, such as having an administrator pore over logs (which could be gigs of data) to seek out an error on the server.

In Infrared360, your notification can include a link to the page where, based on the business rules you establish, you can view and make the necessary corrections—if you have permissions per your role. Your team can drill down and access the specific area where the exception is occurring, regardless of where it is, cloud or on-prem. If the issue is in an app or with an app process, Infrared360 can drop you into the pertinent environment to address it.

ADDITIONAL AVADA ADVANTAGE

AUTOMATION

We designed Infrared360 with automation (set it and forget it) and the future of cloud in mind. Our mantra quickly became "work smarter, not harder." In fact, Infrared360 was named An Essential Automation Tool for The Enterprise by Datamation.

- Infrared360 can automate onboarding. It will read customer repositories like LDAP and create a user or list of users.

- Infrared360 facilitates automated, rule-based analysis of problem conditions.

- Infrared360 facilitates automated corrective actions to problem conditions.

This functionality is particularly critical when you move to a hosted cloud environment because your apps and processes could be on servers outside your direct control. What cannot be sacrificed by that loss of control is visibility and access into your systems. Infrared360, which from the beginning was built on a foundational group/role model, gives you that.

## Modern Infrastructure Needs Modern Monitoring

To keep up with advances in infrastructure, your middleware monitoring and management solution needs to help you work smarter, not harder - regardless of whether your systems are on-prem, on the cloud, or in containers. A good middleware management solution should work the same in any environment.

The very best not only provide telemetry into the health of your system, they foster modern processes and paradigms that are inherent with modernized infrastructures. They must help you meet security and compliance SLAs and not introduce new vulnerability loopholes. Supporting the granular observability

AVADA SOFTWARE

100 Enterprise Drive

Suite 301

Rockaway, NJ 07866

1 (862) 781-6159

info@avadasoftware.com

+1 973 6971043

www.avadaSoftware.com

Click here to schedule a no-obligation live demo of Infrared360,

Or

Still have questions? For more information, call 1 (862) 206-9322

needed for modern infrastructures, modern solutions must foster processes like agile product development and DevOps monitoring. And, solutions must have monitoring and analytics capabilities required to support business performance and availability objectives.

As you prepare to modernize your enterprise messaging and middleware infrastructure, take some additional time to understand the potential risks of proceeding without a modern middleware management system and the benefits of having one. One of our experts can provide free evaluation and advice. Contact one of our experts at 1 (862) 206-9322 or CLICK HERE to schedule a no-obligation live demo of Infrared360 so you can see first-hand how the secure, self-service interface of Infrared360 saves you time, headaches, and resources. We'll even tailor the preview to reflect your own environment.
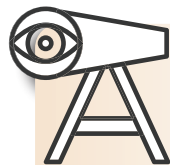
THE AVADA ADVANTAGE

AVOID '20/20 HINDSIGHT'

Don't wait to implement Infrared360 until after you've updated your middleware environment. Modernizing can require a steep learning curve. Many organizations find the complexity of managing their updated middleware environment requires far more internal resources than originally projected. By incorporating Infrared360 before you begin your migration, you'll be able to eliminate complexity and cut the time for deployment.

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.