Monitoring Redefined: Digital Experience Insights

Deliver a flawless digital experience with analytics-driven insights.
Table of Contents

Executive Summary 3

Section 1: 4
IT Ops Monitoring Capability Has Reached Critical Mass

Section 2: 6
From Data Chasing to Analytics-Driven: Essential Strategies

Section 3: 13
Extensive Enterprise Value

Section 4: 15
Conclusion
Executive Summary

Challenge
To deliver a flawless customer experience from software, IT operations must ensure that cloud-based systems and microservices stay performant. In these dynamic environments, traditional approaches cannot scale to manage the increased volume, variety and velocity of metrics and logs. By relying on narrow-view data silos and generic analytics tools, businesses risk escalating cost and digital value erosion.

Opportunity
IT operations needs an open, scalable and unified way to collect, search and aggregate millions of metrics and logs across networks, infrastructure and applications. Together with capabilities that incorporate machine learning in context of domain expertise, these solutions will transform monitoring from a reactive, break-fix function into a proactive process that helps future-proof a digital business.

Benefits
Digital Experience Insights, including app-to-infrastructure correlation, helps teams gain complete visibility across modern application environments. By incorporating advanced analytics within modern monitoring solutions and by leveraging an open, extensible platform, teams can:

- Increase software quality without sacrificing speed.
- Troubleshoot and resolve the most complex of problems.
- Predict the operational performance to achieve the best outcomes.
Section 1

IT Ops Monitoring Capability Has Reached Critical Mass

IT operations has always had incredible amounts of data to process, including the instrumentation of servers, end users, applications, logs, metrics, topology maps and configuration management databases (CMDBs). Now, with industry trends such as microservice development, cloud-native applications and the Internet of Things (IoT), the scope of the problem will only increase.

The big data problem: three “v” words

In many ways, IT operations is facing big data challenges that are similar to those confronting the business. Namely, how to gain actionable insights from increased volumes of data, delivered at faster pace, in many different varieties and formats.

Volume. The days of managing monolithic-style applications running on a single platform are coming to an end. Organizations are now committed to delivering their customers a far richer variety of digital services across multiple channels (mobile, web, IoT). This means that applications are more likely to operate from the cloud via a multitude of services that are interacting with virtualized resources, containers and software-defined networks.

While these distributed application architectures are necessary to support digital transformation initiatives, they’re increasingly complex to manage. Many more moving parts means IT operations has more systems to monitor, with each increasing the amount of data that needs to be collected and analyzed.

Velocity. Although IT operations has always collected and processed large amounts of data, the systems and applications being monitored only changed infrequently. Even though information was collected in silos teams had more time to respond when problems occurred. And since these applications generally supported internal business processes or one channel, problems were easier to understand and manageable.

Today’s delivery model is far different. Agile and DevOps practices now enable a continuous flow of customer value. And with businesses competing on the basis of digital dexterity, the speed at which change can be delivered becomes a critical differentiator. Indeed, and as research indicates, high-performing organizations can deliver software 200 times more frequently than their lower-performing peers.1

As businesses rush to develop and deliver modern systems of engagement, IT operations must become adept at diagnosing problems and predicting anomalies before customer experience is impacted. As such, data points and metrics often need to be collected and analyzed in as close to real time as possible.

Variety. Modern application architectures are highly modular and dynamic, making it difficult for IT operations to establish any point from which the end-user experience can be viewed as a whole. Complicating this further is the rich and varied set of monitoring data that now needs to be processed, including millions of time-series data points, together with unstructured logs, events, topological data and qualitative metrics.
Apart from the increased volume, velocity and variety of data, IT operations teams also struggle because of data that they’re not able to collect. In cloud-based development for example, software engineers might be adding new capabilities via cloud services and from systems that IT operations has no visibility into (or control over). This makes it increasingly difficult to establish service level guarantees.

**Keyhole views and small-data tools exacerbate problems**

Even though the scale and complexity of systems has increased exponentially, many organizations haven’t changed their management approach. Applications are generally monitored with multiple, disconnected tools. As systems continue to grow, the tendency has been to acquire discrete monitoring tools for every new technology element introduced. This can include, but is certainly not restricted to: user monitoring, server monitoring, synthetic transactions, event diagnostics and correlation, log reporting, cloud service checking, and network fault and performance monitoring. As a result it’s not uncommon for an IT operations team to be using more than 10 monitoring tools.

The problem for IT operations isn’t the quality of these tools; most do good job at managing specific technology elements. But because these tools are architected to manage technology silos, the data they process is in silos, which limits insight into the customer experience (see figure 1).

Take for example a situation where a team using a network performance tool identifies an alert that results in increased latency for web traffic. With the traditional siloed approach, the network team can identify when an issue such as this will occur, and even where and how the situation eventuates. Teams can even supplement tools with network-flow data to gain more performance visibility to assist with problem root cause analysis.

But even with this visibility, the network team can’t reliably determine which business services will fail to meet expectations in terms of quality and customer experience. This critical insight can only be gained if the network performance information is correlated with other data sources (from other silos) and presented in context to expose higher-value, cross-domain insights.

**Figure 1:**
Stovepipe tools and data silos prevent shared insights.
Section 2

From Data Chasing to Analytics–Driven: Essential Strategies

Breaking down silos requires new approaches into how metrics and logs are collected, aggregated, analyzed and reported. Because this is now beyond the capabilities of IT operations teams and small-data tools, analytics-driven methods should be considered. However, success depends on avoiding past mistakes—that is, discarding generic analytical methods and tools in favor of a holistic approach that combines big data processing, advanced analytics and essential domain expertise. This re-engineering of the monitoring function will be delivered by an architecture that enables analysis of multiple data sources (real-time and historical), provides true application to infrastructure correlation and infuses monitoring solutions with both predictive and prescriptive capabilities.

This analytics-driven approach will elevate monitoring from a reactive, diagnostic fire-fighting function to a cross-domain discipline used to drive improvements across the software delivery continuum. As such, analytics will become a catalyst for increased collaboration, automated feedback and critical to the success of DevOps initiatives.

What follows are the essential elements of a solution that epitomizes an analytics-driven approach.

Gain full data visibility for full insight.

What doesn’t get measured doesn’t get managed, so it’s essential that analytical methods can collect and disseminate all the data that contributes to the customer experience. For specific use cases, some metrics types will be more important than others, while in others, new, derived metrics from combinations will be needed. It’s therefore important that analytics can build models from a systems perspective by gathering data across three key dimensions—applications, infrastructure and networks.

Full insight into a digital experience starts by gathering application-related metrics. This will include key indicators of applications performance, such as latency, traffic, error rates and service saturation. Also important are metrics indicative of usage and live experience, such as mobile app crashes. Supporting the application are the underlying system and network metrics, so for increased model accuracy, associated operational data points, including traffic-flow analysis, cloud instance and container performance, network performance and alarms will also need to be captured.

Logs are also valuable sources of information, but shouldn’t be considered the definitive source of insights. Log analytics solutions can be used to glean hidden patterns from voluminous unstructured data, but are much more powerful when the analysis is surfaced at critical points in time and in the context of work being undertaken by DevOps practitioners (e.g., optimizing performance or troubleshooting problems).

Consider figure 2. Here, CA Spectrum® is being used to monitor faults and alarms across the network. As network element behavior and topologies change, the application can invoke log analytics in context to correlate thousands (or millions) of data elements against known problem points, which can then be traced through data analysis to the root cause.
Leverage an open, extensible analytics platform.

Processing the volume and variety of metrics and logs discussed above requires a scalable, modular, big-data analytics platform. In an IT operations context and as illustrated in Table 1, this platform must support the high-frequency, low-latency, highly diverse processing requirements associated with the most complex, modern monitoring use cases.

Table 1: IT operations monitoring—metric capture and analysis requirements.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>High frequency</td>
<td>How often metrics can be collected.</td>
<td>Some use cases will require metrics to be collected in very short time intervals—seconds vs. minutes (e.g., monitoring dynamic container environments).</td>
</tr>
<tr>
<td>Low latency</td>
<td>The reaction/analysis time once metrics are collected.</td>
<td>Use cases such as optimizing auto scaling cloud deployments will require real-time analysis of performance data.</td>
</tr>
<tr>
<td>High diversity</td>
<td>Processing and analysis across multiple data dimensions.</td>
<td>For increased insight accuracy, data may need to be captured and correlated across multiple dimensions—like CPU utilization -&gt; by container -&gt; by host.</td>
</tr>
</tbody>
</table>
Some operational use cases will need to capture and process millions of events per second, while others will be best served by batch processing. This need for a flexible platform to support multiple use cases and stakeholder teams has guided the development of the analytics architecture supporting CA solutions.

Using open source technologies and built on a microservice architecture, customers can use platform components most appropriate to their needs. This can include:

- **Elasticsearch.** A distributed, multitenant–capable, full–text search engine.

- **Kafka.** A unified, high–throughput, low–latency platform for stream processing/handling real–time IT operations data feeds and metrics.

- **Logstash.** An open source tool used to ingest data from multiple sources.

- **Apache Spark.** Fast, in–memory data processing for the efficient execution of analytical models and machine learning algorithms.

- **Kibana.** Visualization capabilities on top of Elasticsearch. CA solutions provide out–of–the–box reports and Kibana data–studio services for users to create their own custom visualizations and reports.

- **Big data lake.** An immutable store of unprocessed “raw” data, acting as a source for IT operations analytics. This can be unstructured logs, time series, metrics and topological data.

- **Machine learning, statistical models and algorithms.** A collection of analytics services that can be contextually applied based on the deep domain knowledge of CA Agile Operations solutions.

- **Data access APIs.** RESTful APIs to ingest data directly across the technology stack, as well as from CA products, including CA App Experience Analytics, CA API Management and CA Application Performance Management. Customers can also use these APIs to ingest data from other internal sources such as proprietary systems and external sources like Twitter.

This architecture is designed to be modular, with CA solutions leveraging different components to deliver solutions optimized to specific uses cases in terms of scale and performance.

One example is the Browser Agent from CA that monitors web page load performance metrics and critical indicators of customer experience. These metrics must be collected at high frequency and with low latency, so the agent utilizes Kafka for high throughput, together with Logstash as a data–processing pipeline that transforms data into metrics that are consumable by monitoring services.

Another example is CA App Experience Analytics, which has again been architected to leverage many platform components, including analytics services (mobile crash analytics, performance analytics, developer analytics and customizable, role–based analytics).

The result is a solution that uniquely combines the analysis of user behavior together with operational performance. When supported by visualization and data studio services (see figure 3), CA App Experience Analytics reveals a deeper understanding of customers’ overall digital experience as they engage business across web, mobile and wearable apps.²
Exploit advanced analytics with deep domain expertise.

Modern IT operations solutions built on modular, open and extensible platforms will be fueled by proven models and new algorithms that can learn without programming or human intervention. As an enabler of predictive capabilities, these analytics will process large volumes of big data served by the architectures described above.

While machine learning and big data processing may be considered advanced analytics, it doesn’t guarantee success. Crafting an algorithm appropriate for a wide variety of IT operations use cases requires solutions that have undergone extensive development and rigorous validation.

One approach organizations often take is to select generic analytics tools and retrofit them to IT operations use cases. However, this approach can be costly since the organization will need to invest considerable time training staff to train the tools or in worst-case scenarios, hiring data-science specialists and teaming them with domain-level experts.

This combination of data science and domain-level expertise should be applied where it works best: directly from monitoring solutions, in context of the problem at hand and supporting a wide variety of use cases.
This analytics-driven approach has resulted in a rich set of services available across CA solutions that help DevOps practitioners address many different problems, including:

1. **Reduce alerts, detect anomalies and prioritize issues using differential analysis.**

New, distributed systems can generate an exponential increase in alerts. For many teams, this results from the increase in microservice system checks needed to ensure these systems remain performant. Unfortunately, older approaches to baselining built for monolithic environments also contribute to the problem.

Most monitoring systems have teams predict acceptable performance measurements, set those manually and then throw an alert when those thresholds are passed. Even if the predictions are accurate, setting and maintaining so many isn’t sustainable. The main problem with this approach to performance is that it’s a binary, pass/fail test and doesn’t convey any sense of severity. Set them too low and staff can be inundated with alert storms and false positives; too high, and minor but persistent anomalies indicative of serious emerging problems could be missed.

An answer to this problem can be found in the groundbreaking work of 20th-century statistician Walter Shewhart who worked for the Western Electric Company. By calculating the standard deviation of copper line quality, Shewhart showed that simple comparisons against bands of standard deviation could effectively identify points at which the signal is exhibiting uncontrolled variance; something similar to how an earthquake registers on a seismometer. This kind of control charting has come to be referred to as the Western Electric Rules. Informally, these are sometimes called how-wrong-for-how-long algorithms because they can distinguish between small nuisance alerts and anomalous trends worthy of action.

This statistical method is useful in IT operations, and when applied to application performance management (APM) and monitoring microservices, teams can feel confident that the stream of alerts they receive are actionable problems.

CA APM incorporates this approach that employs standard deviations to establish variance intensities, calling it **Differential Analysis**. Unlike traditional baselining that relies on static predictive models, this new technique is purpose-built for the highly dynamic environments typical of microservices.

2. **Continuous improvement with app to infrastructure correlation.**

While reducing noise with predictive methods such as differential analysis can be considered proactive monitoring, correlating events and conditions across a modern technology stack is the ultimate goal. But, and as discussed earlier, data silos limit the value of tools, since the rich information they mine cannot be passed in context to other teams conducting problem triage or optimization activities. This is especially true with regards to network monitoring and analysis, where rich transport, networking and topological data is available, but cannot easily be accessed and analyzed during application performance and business service monitoring.

Digital Experience Insight resolves this by marrying the strengths of behavioral application performance analysis with the granular monitoring across networks and infrastructure. This means that as elements and conditions supporting an application change, solutions can detect these changes, extract only the data that is relevant and correlate it to the application or service being monitored.
Revisiting the web traffic latency problems discussed on page 5, network performance monitoring would still monitor this condition. However, unlike previously where the data cannot easily be viewed by other teams in terms of business impact, digital experience insight services automatically captures and correlates these conditions with CA APM data to expose higher value, cross-domain insights. This is extremely beneficial for both application support and network teams. Network administrators can now see at a glance how network performance is actually contributing to business outcomes (in context of high-value applications), while application support teams can eliminate performance blind spots (network and infrastructure) during problem exercises.

3. Fast, accurate root cause analysis with assisted triage analytics.

Ensuring a flawless user experience is challenging across modern application architectures that comprise multiple services and technologies. When problems occur, engineers must quickly determine why the experience is poor. However, traditional approaches used to triage complex problems become inadequate:

- With distributed applications, teams are often organized by service or function, so it’s rare to find one person who is familiar with the technical workings of an entire business service.
- Finding the single source of truth is difficult because different teams use different diagnostic tools that lack higher-level visibility.
- The distributed nature of teams can make it challenging to set up a war room or conference calls.
- Evidence collection and analysis becomes more difficult because of the amount of data, logs and alarms produced.

To address these issues, CA solutions are engineered to apply analytics in context of their deep domain knowledge. One example is the assisted triage service in CA APM, which uses analytics to build guided workflows that simplify, streamline and speed the problem diagnosis process. Unlike other analytics methods that rely on users knowing what questions to ask the system to arrive at a solution, assisted triage analytics automatically:

- Gathers all relevant information related to the problem or anomaly and presents this via a single, analysis-notebook interface. This includes when the problem first/last appears and the application owner.
- Dynamically surfaces an evidence list of culprits likely to impact performance, including a map view of the offending application components and affected experiences. Time-based comparisons of key performance indicators are also presented.
- Correlates all the application components associated with the degraded experience to quickly and accurately determine the problem root cause.

This approach is extremely valuable because it enables machine learning and analytics to be applied in context of CA APM’s deep understanding of applications. The time-consuming steps normally associated with complex, war-room scenarios are eliminated, and as illustrated in figure 4, teams can use the solution to gain a common and shared understanding of why customer experience is poor and business outcomes are not being achieved. These elements speed problem resolution times and establish the feedback cross-functional teams can use to drive application improvements.
4. Full-stack visibility with In-context log monitoring and analysis.

Modern, distributed applications operating across hybrid-cloud infrastructure can generate an incredible amount of logs. Diverse and often unstructured, this data is often collected and analyzed in piecemeal fashion. Log management tools can find patterns and anomalies within ranges of log types, but struggle when it comes to presenting information in context of troubleshooting and optimization efforts.

To address this issue, CA has developed an approach to log monitoring and analytics that integrates the function within infrastructure management processes and workflows. This ensures that the power of log analysis can be invoked anytime it’s required, with relevant information presented in context of the immediate monitoring task or workflow.

This approach automatically aggregates and normalizes log data from multiple sources, generates actionable dashboards and provides in-context log information against events for proactive issue resolution. These capabilities help IT teams gain more visibility, troubleshoot quickly and confidently and proactively identify opportunities to optimize resources.

Supported by the open and extensible analytics platform described above, CA’s log monitoring and analysis equips teams with new techniques to address complex modern monitoring challenges.

- **Unrestricted data collection** across distributed app and infrastructure environments, including Docker, syslog, Microsoft® Windows® event log, Apache access and error, Tomcat access and Catalina, Microsoft IIS, Oracle Java™ log4j, Oracle, and Microsoft SQL Server®
- **In-context alerting** performs correlation analysis across diverse logs, data sets and CA Unified Infrastructure Management (CA UIM) alarms. Relevant log–event alarms are automatically pushed into a CA UIM log monitoring alarm console to context of infrastructure issues.

- **Ad hoc search** offers easy search of different log types for rapid root cause analysis. Queries can be saved for future use and proactive correlation. Dashboards can be quickly created and customized according to user needs.

- **Automated workflows** seamlessly launches in-context log analysis from alarm consoles to quickly expose patterns, events and anomalies causing issues.

- **Elastic storage** features cloud native, multitenant and scalable architecture to store high volumes of data from multiple sources.

- **Rapid implementation** enables a unified solution combining infrastructure performance and log monitoring for greater ROI. Template-driven configurations allow for fast, consistent deployments across the most complex and diverse network and infrastructure topologies.

---

**Figure 5:**
CA Unified Infrastructure Management log monitoring—quickly uncover operational issues.
Section 3

Digital Experience Insights—Extensive Enterprise Value

In addition to the operational benefits described above, the broader business can realize increased value from adopting analytics-driven monitoring solutions. These should extend to supporting other DevOps stakeholders and seamlessly integrate with other processes to accelerate the delivery of high-quality software.

Cloud auto-scaling

By monitoring real-time application performance indicators and using predictive analytics, teams can optimally and cost-effectively scale cloud services. Predictive insight is critical, since virtual machine instances can take time to activate. The service should also accommodate rapid metric collection and sampling to better predict when scaling is needed, by how much and when resources can be released. While this is valuable from a production perspective, the insights gained about the resource usage implications of application performance can help development identify where code refactoring could lead the more efficient use of cloud resources.

Continuous integration

Analytical insights can be valuable during continuous integration where developers need to check the performance of software components as they are added to the larger code base. By initiating analysis in context of a software-build processes and automating multiple checks, developers can be alerted immediately a performance issue is detected and before it moves to production status where it’s costlier to fix. An example of this functionality is provided by a CA APM–Jenkins integration, which is described in further detail in the white paper, “Shift Left Monitoring Strategies for Agile Operations.”

Release pipeline optimization

In addition to monitoring during build and integration processes, analytics can be integrated within continuous delivery, testing and release processes to identify opportunities to increase software quality. For example, an integration between CA APM and CA BlazeMeter® (a solution to run massive load tests in the cloud) enables CA APM users to incorporate the results of testing as key performance metrics so that service levels requirements are better understood and can be accurately developed before production.

Predictive capacity analysis

One advantage of using a scalable analytics platform is the unconstrained access to large amounts of data needed to accurately predict capacity requirements. By analyzing seasonal demand patterns over longer periods of time and its effect on resource usage and support, teams can use accurate predictive models to: improve planning and optimize resources, quickly detect anomalous patterns, and prevent costly business disruptions.

App design improvements

What constitutes a great user experience is a combination of intuitive app design, error-free code and flawless performance. The most mature analytics solutions provide all these insights so that DevOps teams can work collaboratively to determine if an issue with an app lies in the design, code or infrastructure—before it impacts the customer experience.
CA App Experience Analytics provides these insights, together with the ability to track how customers are using apps. The combination of usage analytics with operational performance benefits teams in many ways.

- **Business analysts.** With analytical insights into usage, user engagement and activity, business can better guide requirements analysis and design decisions.

- **Development.** With code–level visibility into issues, activity logs and real user data, teams can identify which coding practices correlate to the highest levels of customer engagement.

- **IT ops, site reliability engineers.** By segmenting analytics across various dimensions, including network/carrier, geo, OS and device type, performance problems can be quickly prioritized and triaged.

Section 4:

**Conclusion**

IT operations has always had vast amounts of systems data to monitor. Now, trends such as microservices and cloud–native applications have increased the problem dramatically. Traditionally, disparate tools and disconnected silos of operational data were adequate because systems didn’t change regularly. However, with DevOps practices supporting continuous delivery of digital value, old–style approaches to monitoring no longer scale.

To meet this challenge, CA solutions deliver modern, analytics–based monitoring methods that not only help solve problems faster, but also identify opportunities for improvement—as code is designed, tested and released.

Providing this level of insight to ensure a flawless customer experience results from:

- Complete monitoring visibility and the ability to correlate data across applications, infrastructure and networks.

- An open and extensible platform capable of ingesting, normalizing, aggregating and correlating massive and diverse data types—metrics, logs, time series and topology data.

- The application of modern machine learning, analytical techniques and data science in context of the deep monitoring expertise delivered with industry leading solutions.
To learn more about gaining the actionable insights needed to drive better business outcomes from IT operational data visit ca.com/analytics

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.

3 Wikipedia, Western Electric rules.