The Fundamentals of **API Monitoring**

ca technologies | Runscope

The Fundamentals of **API Monitoring**

Software quality toolsets have evolved significantly over the past decade. Whereas uptime monitoring and debugging tools were once the primary resources available to engineers seeking to deliver a smooth user experience, today's IT professionals have a host of sophisticated DevOps-friendly solutions at their disposal.

Automated testing platforms make it easy to test applications quickly within continuous delivery pipelines.

Application performance management (APM) tools enable engineers to pinpoint certain types of performance problems. Infrastructure monitoring suites help to prevent downtime and guarantee application availability.

Error trackers help developers and admins trace application problems back to their source. Modern DevOps teams commonly leverage these tools to facilitate a faster, more efficient and more comprehensive approach to software quality management than was possible a generation ago.

API Monitoring: The Missing Piece in Software Quality Toolsets

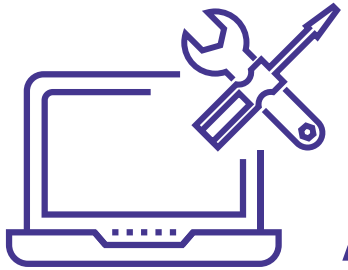
Yet these tools are not sufficient on their own to maximize application quality. There is another type of software quality tool that many DevOps teams still overlook when they build a quality assurance strategy: API monitoring.

By identifying and helping to address performance and availability issues that impact APIs, API monitoring software enables visibility into parts of the application that other software quality tools (such as APM suites and infrastructure monitoring software) cannot track.

For this reason, API monitoring is critical for avoiding software performance problems that can degrade the user experience and drive customers away.

API monitoring is especially crucial today, as organizations move toward cloud-based, microservices-oriented software environments. APIs are the glue that holds disparate cloud services and microservices together. API performance problems will quickly cause these software environments to fail.

This white paper explains what API monitoring means, why it's so important for assuring software quality and a positive user experience, and how businesses in three specific industries—retail, finance and telecommunications—can leverage API monitoring to give their applications a quality boost that other types of software quality tools simply cannot deliver.



"API monitoring software enables visibility into parts of the application that other software quality tools (such as APM suites and infrastructure monitoring software) cannot track."

What Is API Monitoring?

To explain what API monitoring means, let's begin with an overview of APIs and their role in modern application deployment.

Simply put, an API is a communication pathway that allows different parts of an application—or multiple distinct applications—to communicate with one another. APIs are used to send and request data, allow services to identify one another, and enable interactions with third-party applications.

APIs are essential in a world where applications are typically deployed in the cloud and communicate via the network. In addition, as more and more applications are refactored or rewritten to run as a set of distinct microservices, APIs play a crucial role in allowing microservices to discover and communicate with one another.

API monitoring refers to the processes that enable software engineers to track the status of APIs, understand the traffic that traverses them and diagnose and solve performance and availability issues within APIs.

Unlike other types of monitoring and software quality tools, which use metrics like service response time and application availability to identify performance issues, API monitoring works directly at the level of APIs themselves.

This is what makes API monitoring so powerful: It identifies performance and availability problems that would not be visible using other sorts of tools, allowing engineers to pinpoint exactly which type of API-related issue is degrading application performance. Monitoring APIs themselves is crucial because, as noted below, there are multiple types of problems—such as uptime issues, performance challenges and data validation errors—that might impact API performance, and tracing the precise nature of an API issue is possible only when engineers have direct visibility into APIs.

Effective API monitoring tools support internal APIs developed by in-house DevOps teams as well as external APIs provided by third-party organizations. Both types of API monitoring are essential for achieving comprehensive visibility into APIs and the applications they support.

API monitoring tools should also deliver continuous monitoring in order to be most effective. Continuous monitoring means constantly checking the availability and performance of APIs. It delivers significantly better results than periodic checks or retrospective analyses, which are not sufficient for identifying and correcting API performance problems in real time.

"This is what makes API monitoring so powerful: *It identifies performance and availability problems that would not be visible using other sorts of tools, allowing engineers to pinpoint exactly which type of API–related issue is degrading application performance."*

The Three Pillars of API Monitoring

To perform API monitoring effectively, organizations require tools and processes that enable visibility into the three distinct factors that shape API performance (and, by extension, overall application performance): uptime monitoring, performance measurement and data validation.

Uptime monitoring

As the term implies, uptime monitoring refers to verifying that an API is available to the applications and services that need to access it.

Often, when an API fails, the problem will become obvious quickly enough. In this sense, uptime monitoring may seem so basic that it doesn't require dedicated tools.

But API uptime monitoring is more complex than it might seem. Some API failures go unnoticed because they involve APIs that are not critical or that support features that are not used often. These API availability failures can still pose a serious problem. For example, consider the damage if a failure occurs in an API that supports a data backup application that runs once per week. The failure might go unnoticed for some time because the application does not run frequently. And because of the failure, critical data will not be backed up, creating a potentially serious problem.

API availability monitoring is also important because organizations must be able to identify API downtime quickly, before it impacts end users.

They also need to be able to get to the root of an API uptime problem fast by determining which API within an application has failed and what caused it to fail. This type of information is not evident by simply knowing that an API has failed.

Performance measurement

Maintaining API uptime does not necessarily guarantee application quality. APIs might remain available but deliver inadequate performance due to issues such as network traffic congestion or slow service discovery. Poorly performing APIs can also create a domino effect that causes other APIs to experience problems, and can eventually make APIs stop responding altogether.

API performance measurement allows DevOps teams to establish baselines for healthy API performance and identify issues that might cause poor response times, slow connectivity and other performance problems.

An important nuance for API performance measurement is that API performance can vary based on factors such as the geographic distance between an endpoint and the data center. APIs that perform adequately in some regions may underperform in others due to connectivity issues. This is why testing API performance from multiple locations is important for maximizing performance visibility.

Data validation

A successful API response is much more than a 200 status code. Validating the data that an API returns involves looking at its status code, headers and bodies. Every API is unique in the way that it is built and in the way that the validation of it must be handled.

To send and receive data effectively, APIs must be able to request and deliver data in the format that the sender and the recipient both expect. It's important that an API not only returns the expected values in a JSON or XML format, but also that the structure of the objects is also consistent. A simple change to a property from a string to an array can have catastrophic effects in certain applications.

It's also important to consider the values in an API response. For example, an e-commerce application that has a complex workflow of API calls for a customer who is purchasing an item would want to make sure that at the end of a successful purchase, the customer shopping cart has exactly zero items in it.

Inconsistencies in data content or structure can lead to failed interactions, undercutting the value of APIs. The risk of data validation issues is especially great when API versions change, which can create incompatibilities with other APIs.

"It's also important to consider the values in an API response. For example, an e-commerce application that has a complex workflow of API calls for a customer who is purchasing an item would want to make sure that at the end of a successful purchase, the customer shopping cart has exactly zero items in it."

API Monitoring Use Cases

To illustrate the significance of API monitoring in real-world settings, consider the value that API monitoring tools can deliver within three specific verticals: retail, finance and telecommunications.

Retail

Modern retailers rely heavily on internal as well as customer-facing applications. Internally, retailers use apps to help employees manage everything from scheduling to product inventory. Externally, retailers use apps to maintain an online presence—a crucial feature in today's market.

Given the heated competition of the retail industry, as well as the very tight operating margins that retailers must manage in order to turn a profit, maximizing the quality and efficiency of both internal and external applications is crucial.

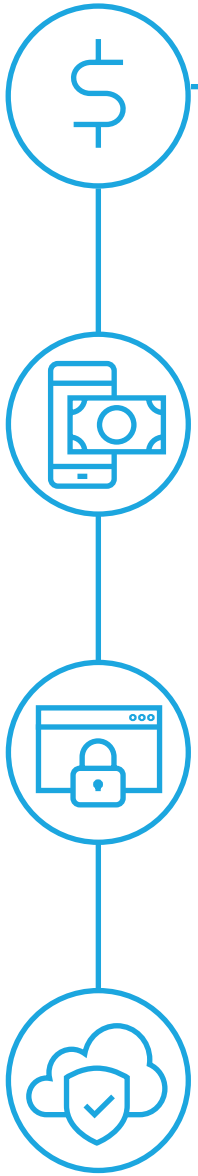
Software quality problems leave retailers at risk of losing customers as well as creating operating inefficiencies that can undermine the strength of their business.

Consider, for example, the business a retailer could lose if an API goes down or performs poorly during a peak sales period, such as Black Friday or Cyber Monday. Preventing such problems requires not just testing APIs under normal operating conditions but also performing ongoing, real-time API monitoring. The extra demand created during times of peak activity might cause API problems that are not evident during normal operations.

Even during normal operating periods, slight delays in retail software performance can undercut the bottom line. For every additional one-second delay that occurs during page load time—a problem that could be caused by slow API response—7 percent fewer sales conversions will occur.1

Retailers rely on APIs not just for powering customer-facing software but also for mission-critical applications they use internally. For example, a retail app that helps a company monitor its inventory might rely on an API to connect automated sensors that track product locations to the application. Sensors can even help retailers monitor in-store customer behavior in real time, with APIs serving the data to applications that display and interpret it.

For these use cases and more, API monitoring is essential within the retail industry in order to guarantee application quality, efficiency and reliability. In this very tight vertical, API management is one factor that can make or break a business.



Finance

The finance industry is tremendously competitive. Although customer loyalty to financial institutions was once strong, times have changed, and today's consumers are increasingly likely to switch banks and other finance service providers when they have an unsatisfactory experience.[2]

Software performance problems play a key role in pushing consumers away from financial services providers. As one study of mobile banking app reviews concluded,

"Customers care about saving time, and if the mobile banking app prevents that with confusing or frustrating functionality, then customers will abandon it for another bank."[3]

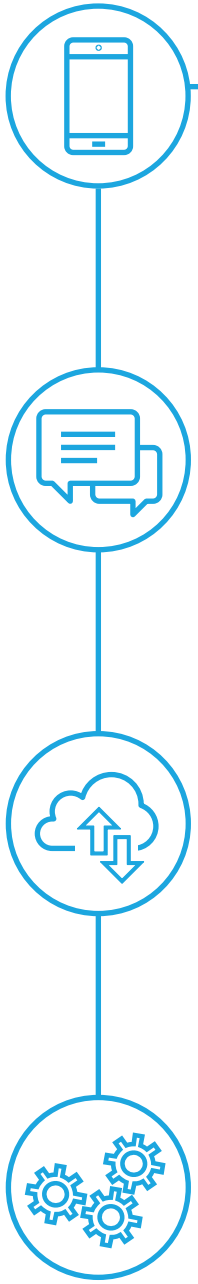
Concerns about security issues within finance apps also frequently play a role in driving consumers elsewhere. And although not all software performance problems are indicative of security vulnerabilities, performance issues of any kind may undercut users' faith in the ability of an app to keep money and private data safe.

For all of these reasons, guaranteeing an exemplary customer experience is vital for businesses seeking to stay ahead of competitors in the finance industry.

While quality assurance tools like APM suites and infrastructure monitoring software can prevent some of the problems that could lead to a poor user experience, they can't address API-related issues.

Only API monitoring tools can identify uptime, performance and data validation problems that prevent application services from interacting properly.

API monitoring is particularly important for financial services companies due to the highly integrated nature of software within the industry. Today, it's common for financial services companies to partner in building customer-facing applications. For example, a retail bank might work with an investment firm to create an application with which users can track personal bank accounts and investment accounts from the same interface. This type of functionality will likely depend on APIs that can aggregate data from multiple sources in order to deliver a streamlined user interface. If an API performance problem arises, the application will fail, leaving consumers unhappy with both companies.



Telecommunications

The telecommunications industry is in the midst of a radical transformation. Telcos are replacing legacy technology with software-defined infrastructure that virtualizes functionality traditionally delivered by analog hardware.

By decoupling storage and networking from underlying hardware, software-defined infrastructure provides telcos with a number of benefits, such as greater scalability and cost efficiency.

However, software-defined infrastructure also creates new management challenges. Chief among them is the

difficulty of monitoring the APIs that meld complex software-defined infrastructures together.

When telcos virtualize their entire infrastructure, API availability or performance issues can pose a serious threat to their ability to maintain services.

For example, consider the role of software-defined infrastructure in enabling a telco to provide data bursts to smartphone users when they open a data-intensive application. In this scenario, data bursting allows telcos to maintain application performance and a positive user experience without the requirement of maintaining a high-bandwidth network connection for all users at all times.

However, data bursting will fail if the APIs that support it become unavailable or underperform.

A software-defined switch that depends on APIs to detect a customer in need of a data burst may not work if the API does not respond quickly enough. Similarly, problems with an API that enables a telco's software-defined network to gauge the amount of bandwidth required in order to deliver a data burst could prevent the network from accurately calculating how much bandwidth to provide, leading either to wasted resources (in the event that the network supplies more bandwidth than necessary) or customer experience issues (in the event that not enough bandwidth is made available).

Beyond the move to software-defined infrastructure, telcos have also long leveraged APIs for integrating their services with customers and partners. For example, a video streaming company might partner with a telco to help deliver its content to customers, with APIs enabling the interaction between the company's software and the telco's infrastructure. The importance of maintaining excellent API performance for third-party integrations adds another imperative to API management for telcos.

So does the global communications infrastructure that telcos have to maintain. As noted above, API performance can vary between geographic regions. Because telcos tend to operate across broad geographic areas,

monitoring API performance across global networks is especially important in the telecommunications industry.

A telco cannot ensure adequate service for all of its customers if it does not monitor API performance in all the regions where customers exist.

Conclusion

APIs play an increasingly crucial role in connecting the complex web of microservices and cloud resources that power modern applications. API monitoring tools are the only way to gain visibility into API availability and performance, diagnose the source of problems and resolve them before they lead to serious application quality issues.

Many organizations have not typically included API monitoring solutions within their software quality toolsets. However, the importance of APIs to modern software means that API monitoring has become a must-have for maintaining application quality, alongside other quality management tools, like APM suites and automated testing platforms.

As one of the first providers of a dedicated API monitoring solution, Runscope by CA Technologies delivers the focused, comprehensive suite of API monitoring that DevOps teams need to improve software quality and provide for a positive user experience across a range of industries.

Try Runscope API Monitoring free for 14 days.

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.

1 Eric Kazda, "Infographic: How Page Load Time Can Help or Hurt Conversion Rates, March 25, 2017
2 FICO, "FICO Survey: Millennials 2 to 3 Times More Likely to Switch Banks," August 11, 2016
3 Christine Reyes, "What We Learned From 100 Mobile Banking App Reviews," March 10, 2016

200-356225_0518

ca technologies | Runscope