The Ultimate Ops Checklist for APM
The Ultimate Ops Checklist for APM

Uptime and end-user experience are two of the most important aspects of a business application. One of the primary objectives of IT ops teams is improving the observability of their application ecosystem. After all, a performance bottleneck or service outage of a few minutes can mean significant revenue and productivity loss.

For example, a single hour of downtime on Prime Day was reported to cost Amazon $72 million or more. Of course, large enterprises aren’t the only ones with much to lose. According to a 2020 report, the majority of small-to-medium businesses indicated an hour of downtime costs at least $10,000. As a result, the popularity of Application Performance Monitoring (APM) solutions built to provide granular insights into application health have surged in popularity in recent years with the APM market growing to an estimated $5.7 billion in 2020.

Today, there’s no shortage of tools offering some sort of APM functionality, but they’re not all created equal. What works for a DevOps team dealing strictly with distributed cloud-based apps may not be the right solution for a traditional data center. Similarly, the requirements of a startup will be significantly different compared with those of a large enterprise.

This means finding the right APM to meet your needs will take some research and require you to ask the right questions.

In this checklist, we’ll cover 25 points to consider when evaluating which APM is right for you. We’ll cover everything from end-user benefits to configuration and deployment. For each item, we’ll summarize why the item is included, and then include a Key Question to Ask – a shortcut for the item to be sure you’re considering it in your APM decision. While we won’t cover the items in detail, this list should bring everything you need to make an informed decision.

Whether you’re a DevOps engineer, a developer, or an IT leader working for a startup or a Fortune 500 company, by the end of this list, you should have the information you need to confidently make your APM decision.
1. End-user benefits

First and foremost, APM is about optimizing end-user experience. This basic concept should influence specific technical and business decisions you make. While it may seem counterintuitive as a place to start for a “back-end” tool, taking your end-user benefits as your starting point helps to contextualize your APM strategy.

Of course, the details are what matter here. Simply focusing on the metrics related to availability and performance misses the point. While metrics are useful, user journeys are what matters. For example, ping and HTTP request/response times provide some insight into application performance, but they don’t necessarily represent end-user experience. The application may be working fine for a user in London while it slows to a crawl for a user in Los Angeles.

Further, knowing the app response times are “slow” isn’t enough to deliver end-user benefits. You’ll need more granular information to quickly address the problem and improve user experience, and your APM should enable you to drill down and do that.

Simply put, your APM selection process should begin with end-user benefits and requirements in mind. This means quantifying:

• The application infrastructure impacting user journeys
• Where your users are located geographically
• How your users interface with your apps
• Acceptable and ideal levels of performance
• Existing pain points and targets for improvement

With this information, you can contextualize which features of an APM matter most for your team.

KEY QUESTION TO ASK:
What specific end-user benefits should your APM solution enable?

2. Build versus buy

Next, one of your key decisions (as it is for nearly any IT solution) is “Build versus Buy.” Should you build your own custom solution optimized for your use case or should you go with a pre-built APM solution from a third-party vendor? There’s never a one-size-fits-all answer, and your unique situation (budgets, staff skills, project history, support personnel, resources, and so on) will guide your decision.

KEY QUESTION TO ASK:
Do the business benefits of building outweigh the complexity and cost of buying a purpose-built solution?
Almost every modern business has workloads in the cloud and the APM solution you choose—whether you build or buy—needs to support your critical cloud apps. For many businesses, this means you’ll need a multi-cloud APM solution to monitor across cloud service providers like AWS, GCP, Azure, Digital Ocean, Heroku, and Linode.

This is criteria where the details matter. Most solutions will have some level of support for a wide variety of cloud platforms. However, there’s a big difference between deriving up/down status using ping or simple HTTP requests and capturing in-depth performance metrics.

**KEY QUESTION TO ASK:**
Does the APM solution support your (multi)cloud infrastructure?
4. Backend monitoring

The performance of web servers, databases, and responsiveness of third-party dependencies can impact the performance of your application. Granular visibility into resource utilization and performance of your technology stacks is a must—both for proactive maintenance (such as knowing when it’s time to scale up a server) and incident response (such as addressing brownouts and blackouts).

When considering back-end monitoring options, it’s important to find a balance between collecting data at regular intervals (such as polling an API endpoint or SNMP data) and event-driven notifications (such as syslog messages, SNMP TRAPs, and so on). The former can help identify trends, build time-series data for reports, and identify when devices go offline. The latter can quickly alert you when specific application events occur.

**KEY QUESTION TO ASK:**
Does the APM solution provide the back-end monitoring granularity you need?
5. Frontend monitoring

At its core, APM is about end-user experience. While CPU, memory, disk I/O, and other back-end metrics are good indicators there's a problem, they don't directly represent what the end user of a web application experiences.

Frontend monitoring addresses this by focusing directly on application frontends. This category includes features like real user monitoring (RUM) and synthetic monitoring and focuses on metrics like JavaScript errors, server responses, and page load times.

For public-facing apps—particularly those needing to support geographically distributed users and various devices (such as mobile and desktop)—frontend monitoring can be one of the most important aspects of APM.

**KEY QUESTION TO ASK:**
Does the APM solution provide the level of frontend monitoring you need?

6. IoT and device-level monitoring

Generally, the conversation around APM is focused on apps running on top of cloud infrastructure or on-prem servers. However, edge computing and IoT are changing this dynamic. Today, a mission-critical application can run on anything from a smart sensor in an industrial setting to an embedded system at a remote edge location. Full end-to-end APM needs to account for all of these deployment models.

**KEY QUESTIONS TO ASK:**
What devices are running mission-critical applications in your environment?
Can your APM solution monitor them effectively?
7. CapEx and OpEx

Ultimately, your investment in an APM solution is a business decision. As such, you must consider the capital and operational expenses associated with your choice. At one end of the spectrum, building an on-premises solution from the ground up has high upfront capital costs but little or no recurring subscription or licensing costs. However, you’ll still need to maintain the software and hardware to support a custom APM, so you still account for OpEx.

At the other extreme, cloud-based subscription APM tools are almost purely OpEx. Between those two extremes, licensing a third-party solution and running it on your own servers eliminates the need to write and maintain your own software, but still leaves you shouldering the infrastructure maintenance.

When comparing the cost of different APM solutions, there are several “gotchas” you shouldn’t be overlooked. These include licensing, maintenance, hardware costs, and the often-overlooked topic of complexity. It’s relatively easy to estimate the costs of the first three, but complexity often bites ops teams in the long run. If a solution is complex to maintain or operate, not only does that mean more maintenance costs, it also means a higher probability of misconfigurations, undetected issues, and/or alert fatigue limiting the usefulness of APM.

**KEY QUESTION TO ASK:**
What mix of capex, opex, and complexity is right for your business?

8. Scalability

Generally, the conversation around APM is focused on apps running on top of cloud infrastructure or on-prem servers. However, edge computing and IoT are changing this dynamic. Today, a mission-critical application can run on anything from a smart sensor in an industrial setting to an embedded system at a remote edge location. Full end-to-end APM needs to account for all of these deployment models.

**KEY QUESTIONS TO ASK:**
What devices are running mission-critical applications in your environment?
Can your APM solution monitor them effectively?
9. Analytics

Every APM can give you data. However, not every APM can give you relevant, actionable, and timely information. The difference between the two boils down to the ability to process raw data using intelligent analytics. Often, the reports generated from an APM will be the main driver of business, infrastructure, and product decisions, so the importance of quality information can’t be overstated. Ensure the APM you choose offers the right mix of standard reports, customization, and intelligence to enable you to make informed decisions in production.

**KEY QUESTION TO ASK:**
What information (not just raw data) do you need from your APM?

10. Observability

Generally, the conversation around APM is focused on apps running on top of cloud infrastructure or on-prem servers. However, edge computing and IoT are changing this dynamic. Today, a mission-critical application can run on anything from a smart sensor in an industrial setting to an embedded system at a remote edge location. Full end-to-end APM needs to account for all of these deployment models.

**KEY QUESTIONS TO ASK:**
What devices are running mission-critical applications in your environment?
Can your APM solution monitor them effectively?

11. Security

When evaluating the security of an APM platform, it’s important to consider the security of data in transit and data at rest. Additionally, support for secure authentication methods, multi-factor multi-factor authentication (MFA), single sign-on (SSO), and/or integration with your existing authentication, authorization, and accounting (AAA) servers are important criteria to consider.

The other side of the APM security coin is how it enables your ability to detect and respond to threats. By improving your application ecosystem’s observability and enabling granular visibility into application performance, a properly configured APM can help you identify threats faster.

**KEY QUESTION TO ASK:**
How secure is the APM implementation and how can it enable your existing SecOps efforts?
12. Compliance

In many industries, compliance to standards like Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley Act of 2002 (SOX), and Payment Card Industry Data Security Standard (PCI DSS). In some cases, this means you’ll need an APM solution designed to meet a specific set of standards for encryption, security, and/or data retention. In others, this means you’ll need to have a compliant level of monitoring and alerting for relevant applications.

**KEY QUESTION TO ASK:**
Does the APM solution meet compliance requirements for data retention, security, and encryption?

13. MTTR

Simply put—downtime brings productivity to a halt, hurts your brand image, and costs money. So, the faster you can address it, the better. As a result, mean time to resolution (MTTR) is one of the most important ops metrics available. When a mission-critical application goes down, the ability to get it back online quickly is vital and identifying issues before they result in an outage is even better.

An APM should provide you with enough tools not only to rapidly detect and alert you to outages but also the tools to proactively address performance issues before they become full-blown outages.

14. Root cause analysis

A direct corollary to MTTR is the speed at which an ops team can identify the root cause of an issue. A simple ping can tell you a latency issue exists, but how much digging do you have to do to learn if the root cause is a memory leak, database I/O, CPU utilization, or a network problem?

A quality APM should provide you with enough visibility on both application performance and dependencies, so you can quickly and reliably narrow down the root cause of problems when it counts.

**KEY QUESTION TO ASK:**
Does the APM provide enough granularity to quickly and precisely identify the root cause of common performance bottlenecks?
15. Intelligent alerting

Just about everything in IT sends alerts. Printers, applications, servers, network gear, UPSes, and smart cameras are some of the devices that can flood your inbox with unnecessary information. This is why alert fatigue is a real thing. It’s also why you should take a close look at how an APM solution handles alerts.

What you’ll want to alert against will vary depending on your requirements, so make sure the APM you choose offers enough customization—both in thresholds and business logic—to meet your needs.

**KEY QUESTION TO ASK:**
Can the APM alert against conditions you care about without sending a flood of messages you don’t need?

16. Integrations

When evaluating how different APMs integrate into your existing environment, it’s important to consider integrations for:

- Your existing application infrastructure. Apps and development pipelines today reside both on-prem and in the cloud and range from legacy monolith servers to distributed microservice architectures. With quality premade integrations for the components of your app stacks, you can save time and improve the overall observability of your application ecosystem.

- Your existing tools. The typical IT team has various discrete tools for ticketing, monitoring, and collaboration to go along with the infrastructure in their application ecosystems. The easier your APM can integrate with those tools, the more streamlined your IT ops team becomes.

**KEY QUESTION TO ASK:**
Does the APM solution offer integrations for my existing—and planned—tools and infrastructure?
17. Granularity and quality of MELT data

The type of data any IT monitoring system can provide can be grouped into four categories: metrics, events, logs, and traces. Together, these data categories are referred to as MELT. Let’s take a closer look at each one:

- **Metrics** – Metrics are a set of measurements and other data points captured using a polling mechanism. Metrics generally include or are stored with a timestamp and aggregated to enable reporting, measuring system health, creating performance baselines, and identifying trends. When considering an APM, keep in mind what metrics matter to you (such as CPU utilization, disk space, and so on), how you’ll use the data, and your organization’s storage and retention requirements.

- **Events** – While metrics are a snapshot of data points over time, an event is a discrete condition or action that can occur at any time. For example, the percentage of server CPU utilization on July 4, 2022 at 10:07 a.m. is a metric, while server CPU utilization exceeding a predefined threshold is an event. Identifying high-priority events is a critical component of an alerting strategy. Additionally, events can serve as valuable data for AIOps tools to analyze and provide actionable insights.

- **Logs** – Logs (for example syslog messages) are generally more granular and contextualized than events. For example, when an engineer debugs a single server CPU utilization event, they may parse through dozens or hundreds of individual logs. Log data also sometimes lacks structure, which can make extracting relevant information from a sea of data difficult. Your APM should be able to ingest and present your logs in a way that makes them easy to extract actionable information from.

- **Traces** – Trace propagation data is vital for teams responsible for troubleshooting distributed applications. For applications and the APMs monitoring them today, the important takeaway is understanding what trace data you have available to work with, and how your APM can process and present it.
KEY QUESTION TO ASK:
What’s the granularity and quality of the MELT data the APM can capture and present?

18. Business continuity and disaster recovery

Business continuity and disaster recovery (BCDR) planning is a fundamental part of IT operations. While an APM won’t be the tool to perform and restore your backups, it can still be an important part of your overall BCDR strategy.

For example, an APM can provide proactive monitoring of your backups and the tools used to manage them. The more tightly integrated your BCDR and monitoring tools are, the less complexity—and probability of error—you’ll have as you implement your business continuity plans.

KEY QUESTION TO ASK:
How well does the APM fit into my BCDR strategy?

19. Initial configuration and deployment

As a general rule, you shouldn’t have to be an expert to deploy and perform the initial configuration of an APM. Unfortunately, many APM solutions have steep learning curves that can complicate deployments and leave ops teams either wasting time getting up to speed or worse, settling for a configuration that limits their visibility and troubleshooting capabilities when it matters. While there will always be a complexity versus functionality tradeoff to some extent, ops teams should prefer tools designed to allow them to get the functionality they need without wasting too much time and effort better spent on core business functions.

Demos and trials enabling you to use the software in a real-world environment can go a long way in revealing the complexity associated with the deployment of a particular APM.

Pro-tip
SolarWinds AppOptics™ distributed transaction tracing enables ops to tie together the complete path of a trace to quickly identify bottlenecks and end-user impact.
KEY QUESTION TO ASK:
How much time and effort are required to provision the APM on day 1?

20. Maintenance and management

Any tool you deploy, including APM solutions, inherently become one more item to maintain on an ongoing basis. Like with initial configuration and deployment, you should account for the time and effort it will take to maintain your APM. At one end of the spectrum, on-premises APM solutions you build will require managing and patching server hardware, powering and cooling the hardware, and maintaining the APM codebase.

Cloud deployment models, particularly SaaS APM solutions have an advantage here because they eliminate the need for server maintenance and patching completely.

KEY QUESTION TO ASK:
How much time and effort are required for ongoing maintenance of the APM?

21. Deployment model

As we alluded to in the maintenance and management section, where your APM is deployed will have a significant impact on your monitoring strategy, pricing, scalability, and complexity versus control tradeoffs. Regardless of whether you build or buy, you can deploy on-prem using physical servers or in the cloud using an IaaS platform. Further, there are SaaS-based APM solutions designed to abstract away the complexities of management and maintenance.

There’s no one-size-fits-all answer, however, in many cases, the cost and complexity reduction plus the flexibility of SaaS make it a good fit for teams looking to gain APM functionality without taking on the burden of additional infrastructure to maintain.

KEY QUESTION TO ASK:
Which deployment model offers the optimal set of tradeoffs for your organization?

22. SEO

If your applications are public-facing web servers wanting to rank in organic search results, you should care about page speed. As Google has made clear for years, page load time has a direct impact on search engine optimization (SEO). Why does this matter for APM? Because your APM can help you track app performance in real time and quickly drill down to identify bottlenecks and areas for improvement.

Pro-tip

Go beyond simply measuring page speed and leverage end-user monitoring to gain deeper insights into user experience. Tools like SolarWinds Pingdom® which support real user monitoring (RUM) and synthetic monitoring can enable real-time end-user monitoring.
23. Stages of the development cycle

APM and DevOps go hand in hand. This means APM tools are vital for how teams improve the observability of their development pipelines. Therefore, when you’re choosing an APM, it’s important to consider how it will integrate into your development pipeline. The earlier in the pipeline you can integrate APM metrics, the better.

Why? Because visibility improves code quality and the sooner you can gain insights into how your latest code performs, the faster you can optimize. The ability to drill down and check metrics like CPU utilization, write IOPS, and allocated memory early in the development cycle (such as part of automated post-build tests or within a QA or staging environment) means higher quality code in production.

**KEY QUESTION TO ASK:**
How well can the APM integrate with your current DevOps toolchain?

24. Support for containers and container orchestration tools

Container runtimes like Docker and container orchestration tools like Kubernetes (K8s) are the building blocks of distributed microservices architectures. If you’re using platforms like Docker or K8s, you need an APM to work with them seamlessly and provide granular real-time metrics on performance.

**KEY QUESTION TO ASK:**
Can the APM provide insights into the health of your containers, clusters, and pods?

25. API

Application Programming Interfaces (APIs) make any platform highly extensible and easy to integrate with a wide variety of systems. The quality and availability of APIs among different APM solutions vary widely, so take the extra step and review API docs and feature sets in your review process.

**KEY QUESTION TO ASK:**
Can you capture data from and control your APM programmatically with a standard API?

---

**Did you know?**
The SolarWinds Snap Agent is based on Intel’s Snap Telemetry Framework. Snap is an open framework designed to streamline the publishing of system data via a single API.
RIGHT-SIZING YOUR APM SOLUTION WITH SOLARWINDS
APM INTEGRATED EXPERIENCE

So, there you have it—25 key items to consider when choosing your APM solution.

While it’s true there’s no one-size-fits-all APM solution, SolarWinds APM Integrated Experience was designed to cover nearly any solution by enabling ops teams to pick and choose the features and functionality they need from an APM. SolarWinds APM Integrated Experience is a cloud-based solution designed to enable you to choose the APM components you need, without adding the cost or complexity of features you don’t. For example, with APM you can:

• Enable end-user monitoring with Pingdom RUM and Synthetic Monitoring tiers
• Leverage scalable full-stack log monitoring, management, and analytics with SolarWinds Loggly®
• Perform real-time infrastructure and application monitoring for on-prem and cloud servers, virtual machines, cloud services, and containers with AppOptics Infrastructure
• Use distributed tracing and live code profiling to enable rapid troubleshooting and debugging with AppOptics Full-Stack APM

With this information, you can contextualize which features of an APM matter most for your team.

KEY QUESTION TO ASK:
What specific end-user benefits should your APM solution enable?

Additionally, with AppOptics infrastructure at its core, SolarWinds APM Integrated Experience is simple to provision and deploy with over 150-plus plug-ins and integrations and standard metrics and prepopulated dashboards to help you hit the ground running.

To try SolarWinds APM Integrated Experience for yourself, [sign up for a free trial today](#)!
ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of simple, powerful, and secure IT management software. Our solutions give organizations worldwide—regardless of type, size, or complexity—the power to accelerate business transformation in today’s hybrid IT environments. We continuously engage with technology professionals—IT service and operations professionals, DevOps and SecOps professionals, and Database Administrators (DBAs) – to understand the challenges they face in maintaining high-performing and highly available IT infrastructures, applications, and environments. The insights we gain from them, in places like our THWACK community, allow us to address customers’ needs now, and in the future. Our focus on the user and commitment to excellence in end-to-end hybrid IT management has established SolarWinds as a worldwide leader in solutions for observability, IT service management, application performance, and database management. Learn more today at www.solarwinds.com.