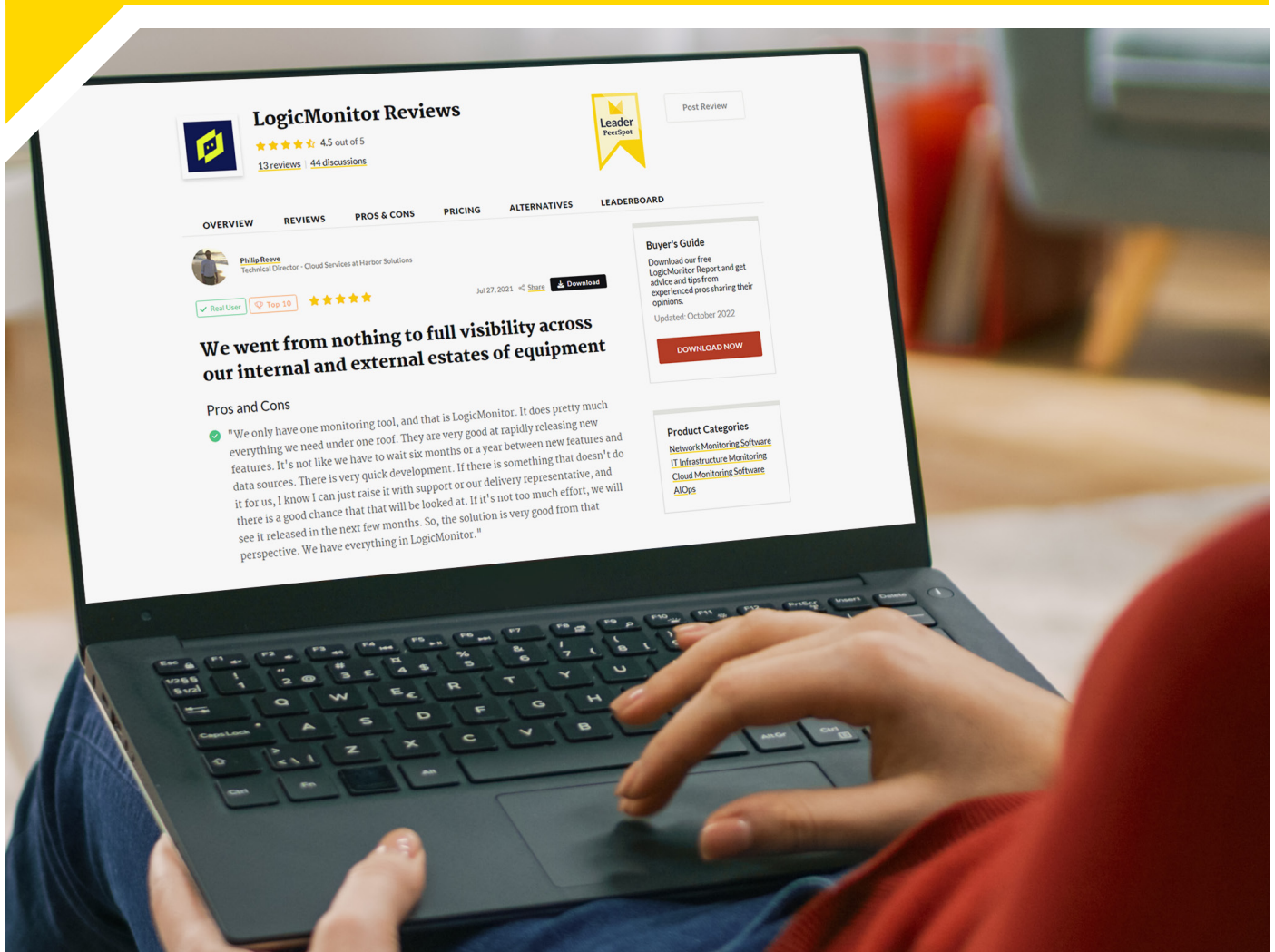


PeerPaper™ Report 2022

Based on Real User Reviews of LogicMonitor

Six Reasons IT Pros are Ditching Legacy Monitoring Tools



Contents

Page 1. **Introduction**

Page 2. **SaaS-based Tools are Essential for IT Infrastructure Monitoring Today**

Page 3. **It's Time to Move Off of Legacy Solutions**

Page 5. **Six Reasons IT Pros Are Ditching Legacy Monitoring Tools**

#1. Tool Sprawl Is Inefficient

#2. Automation Is No Longer A Nice-to-Have

#3. Lack of Visibility into Hybrid and Cloud Environments

#4. Too Much Alert Noise

#5. They Need to Prove ROI

#6. A Need for Future-Proof Tools that Support AI and Machine Learning

Page 15. **Conclusion**

Introduction

IT professionals have their pick of on-premise monitoring tools. However, IT infrastructure is continuously evolving and legacy tools aren't agile enough to keep up with new and complex technology stacks. IT pros are now replacing aging legacy infrastructure monitoring solutions with Software-as-a-Service (SaaS)-based platforms to consolidate toolsets and keep up with the demands of scale.

What are the top reasons IT pros are ditching legacy monitoring tools? According to PeerSpot members, the top reasons they are moving off of legacy monitoring solutions include the growing need for a platform that consolidates toolsets, enables automation, reduces mean-time-to-resolution (MTTR), and opens the door to the use of artificial intelligence (AI) in the monitoring process. Ultimately, these factors drive operational efficiency and enable infrastructure monitoring teams to become less reactive and practice monitoring that is proactive and done in real-time.

SaaS-based Tools are Essential for IT Infrastructure Monitoring Today

PeerSpot members are finding that cloud-based, SaaS tools are essential for IT infrastructure monitoring. As a Senior Director at Optimal+, a software R&D company with over 500 employees, explained, “We switched mainly because we were looking for a SaaS-based solution and a centralized solution.” In their case, because they are managing up to 70 different sites, the overhead of installing a monitoring tool on each server at each site had created a great deal of administrative overhead. SaaS tools are quick to deploy and allow users to monitor all infrastructure no matter the location, whether they are distributed across a variety of locations, on-premise, or in the cloud.

It's Time to Move Off of Legacy Solutions

Moving to a SaaS-based monitoring tool is usually part of a broader effort to modernize IT and support digital transformation across the board. Legacy monitoring tools are often siloed based on the types of infrastructure they monitor. SaaS tools solve this problem with their comprehensive coverage, which allows users to monitor everything they need with one tool instead of many. As a result, they get better visibility across hybrid environments without the configuration overhead of legacy tools . For example, a System Engineer at IFM Efector, a manufacturing company, found his legacy SolarWinds toolset to be “a nightmare.” He explained, “They let you download the product, and then you have to figure out how to set it up and configure everything.” He found LogicMonitor’s deployment process far simpler and more user-friendly.

The enhanced visibility that comes with a comprehensive SaaS platform typically delivers a significant improvement over trying to understand what’s happening in one’s environment with data from multiple tools. “The main reason for migrating to LogicMonitor from Nagios was to eliminate the noise of alerts,” said an IT Operations Manager at a university with over 10,000 employees. He shared, “It may have been because alerts were not properly tuned, but the visibility with Nagios was not complete. It became a bottleneck.”

“...it’s easier to set up, the alert fine tuning is better out-of-the-box, and it has more features and functionality.”

[Read review »](#)

In the same vein, a Technical Architect at Computerworld Group, a tech services company, had previously used three monitoring tools: SolarWinds, PRTG, and SCOM. “Now,” he said, “we only use one monitoring solution. The benefits of LogicMonitor are it’s easier to set up, the alert fine tuning is better out-of-the-box, and it has more features and functionality.”

A desire to reduce cost and complexity drove a Sr. Systems Engineer, Infrastructure at Edgeline, an education company with over 500 employees, to stop using OpenNMS, Cisco Prime, and SolarWinds. He revealed that “the cost and complexity of those solutions is ridiculous. I would never advocate going back to that black hole.” Similarly, the tech company Network Architect related that “monitoring things, especially old legacy things, can be complex.” For the university IT Operations Manager, the issue was the potential for each department to self-manage. He wanted departments to “manage their own dashboards and create their own reports based on their requirements.”

Six Reasons IT Pros Are Ditching Legacy Monitoring Tools

IT pros on PeerSpot offered insights into why they are moving away from legacy monitoring and embracing SaaS solutions. While the motivations vary by organization, monitoring teams are generally adopting SaaS because they want to stop dealing with tool sprawl. They want automation and a reduction in alert “noise.” Proactive monitoring is a broad goal, which SaaS can fulfill far more easily than legacy solutions. The ability to use AI in monitoring, along with visibility into cloud and hybrid cloud environments, is also driving interest in SaaS.

#1. Tool Sprawl Is Inefficient

Consolidating infrastructure monitoring tools is an important reason for moving away from legacy and native monitoring tools. For instance, as the tech company Network Architect explained, “We had a suite of three or four products that we used previously, and we were able to consolidate all of them into LogicMonitor.” These included open-source tools and homegrown utilities. They ran Observium for throughput graphing and Nagios for up/down alerting. Figure 1 captures the complexity and management overhead needed for an unconsolidated monitoring toolset versus one that is consolidated.

“It takes a lot of resources to keep track of so many tools. Consolidation almost always results in savings.”

[Read review »](#)

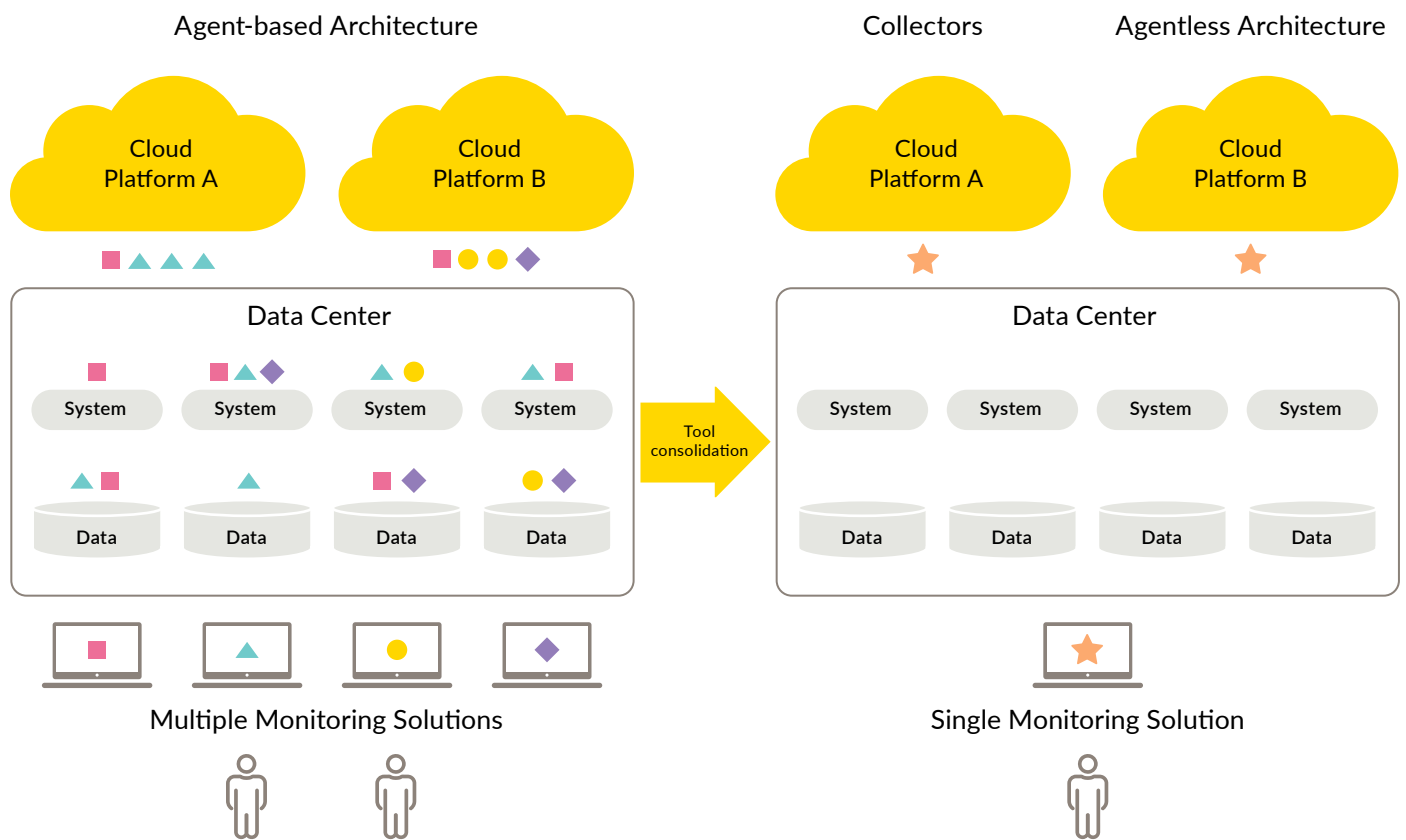


Figure 1 - The effects of tool consolidation, including the requirement for a small monitoring staff and fewer agents to manage

It takes a lot of resources to keep track of so many tools. Consolidation almost always results in savings. In this context, a Senior Systems Integration Engineer at a tech services company with over 500 employees shared, “We consolidated, and switched from the products we were using, due to reduced costs and improved workflow: Not having to watch multiple applications is more efficient.”

“We had a fair number of siloed systems, logs, and other bits and pieces in order to attempt to monitor what we had,” said a Head of IT at a tech services company with more than 50 employees. He added, “Now, we have just LogicMonitor.” Previously, his team had struggled to find the people and time to support Microsoft SCOM, along with bespoke logging mechanisms. The university IT Operations Manager used LogicMonitor to consolidate from four or five third-party tools.

#2. Automation Is No Longer A Nice-to-Have

To go from reactive monitoring to proactive observability, users need a platform that can automate as many monitoring processes as possible. A Network Operations Center (NOC) Manager at a tech services company spoke to this point, saying, “We are able to automate routing of alerts to particular teams and people, reducing the number of tickets we have to check manually.”

The tech services Head of IT offered an example of automation. He said, “If certain alarms are raised, we can create tickets straight into our ITSM platform that will allow us to notify our clients immediately of a failure in some way. We can then run some automatic scripts for known situations to automatically try and repair the fault. Thus, it can all be automated as it’s all a closed loop. Then, we can notify the client that we’ve resolved the issue, all without us touching anything.”

According to the System Engineer at IFM Efector, LogicMonitor’s automated and agentless discovery, deployment and configuration capabilities make automation simple. The tool’s REST API further enhances potential automation. The API is what enabled the tech company Senior Systems Integration Engineer to automate processes like customer onboarding, which saved his group significant time. The tech services NOC Manager took advantage of the tool’s functionality to automate the routing of alerts to particular teams and people. He said, “We don’t want to be a messenger between the monitoring solution and our customers.”

“We are able to automate routing of alerts to particular teams and people, reducing the number of tickets we have to check manually.”

[Read review »](#)

“The tool’s REST API further enhances potential automation.”

[Read review »](#)

#3. Lack of Visibility into Hybrid and Cloud Environments

As IT assets move to the cloud, they require the same intense monitoring as any on-premise asset. Most on-premise or native tools are typically only great at monitoring one type of infrastructure, forcing IT pros to use an additional tool for cloud and virtualization technologies. Thus, the ability to monitor hybrid cloud/on-premise infrastructures within the same pane of glass easily and effectively is a key reason IT pros are dropping legacy monitoring solutions.

The Sr. Systems Engineer at Edgelink provides a good example of how a hybrid monitoring model should work. He said, “We have LogicMonitor Collectors onsite in our data center, but the dashboard and everything else is all the cloud model. We use both AWS and Azure as our cloud providers.” Several users acknowledged the importance of being able to track disconnects between the cloud and on-premises aspects of the system. A Principal IT Consultant at a tech services company with more than 50 employees put it this way: “The solution’s ability to alert whenever we have a disconnection of the collector to the cloud is an advantage.”

“Since deploying LogicMonitor, we have one tool and one location where we can see across all our infrastructure.”

[Read review »](#)

The workloads can get sizable, as the Solutions Engineer at Black Box Network Services revealed. His organization monitors 1,200 devices, though the actual number of items being watched is far higher, once he factors in virtual machines. In addition, he’s keeping an eye on almost 30,000 phones. This level of extensibility across hybrid infrastructure allows IT pros to reduce the number of alerts they are getting from disparate systems. An IT Operations Manager for a university with over 10,000 employees said, “We were especially able to consolidate third-party cloud monitoring for AWS. Within the first two or three months, we were able to bring the false positives down by 50 percent. That’s a big achievement.”

The Senior Director at Optimal+ simply said, “With LogicMonitor we are much more efficient.” For context, his organization has an installed base in over 70 locations worldwide. He said, “We couldn’t see the whole picture across all our infrastructure. Since deploying LogicMonitor, we have one tool and one location where we can see across all our infrastructure. This is a huge improvement for our efficiency.”

“Being able to fine tune alerts allows us to be more efficient and get less false positives...”

[Read review »](#)

#4. Too Much Alert Noise

An excessive volume of alerts, some of which are false positives, creates an overwhelming level of “noise” for monitoring teams. Sometimes presenting as what IT pros call “alert storms,” alert noise is the bane of infrastructure monitoring. They are a drain on personnel time and can quickly cause fatigue for monitoring teams. These noisy alerts keep teams up at night and bury what’s important in a shroud of false alarms. This can cause teams to miss important alerts. For this reason, the ability to reduce false positives and customize alert tuning is a major reason IT teams are getting rid of legacy tools and moving towards a SaaS-based monitoring solution.

A Senior Consultant at Retune AB, a tech services company, spoke on this theme. He found that his previous solutions had been so complicated to set up and lacking in customization that, as he put it, “you end up with so many false positives that it’s pointless having monitoring. We don’t have this issue with LogicMonitor.” The System Engineer at IFM Efactor remarked that his solution “provides extensive out-of-the-box monitoring and gives us the ability to tweak everything to get meaningful alerts, reduce false positives.” This user credited LogicMonitor’s extensibility and threshold customization for the reduction in alert noise. Figure 2 depicts how custom tuning in the monitoring solution can keep alert storms from flooding the monitoring staff.

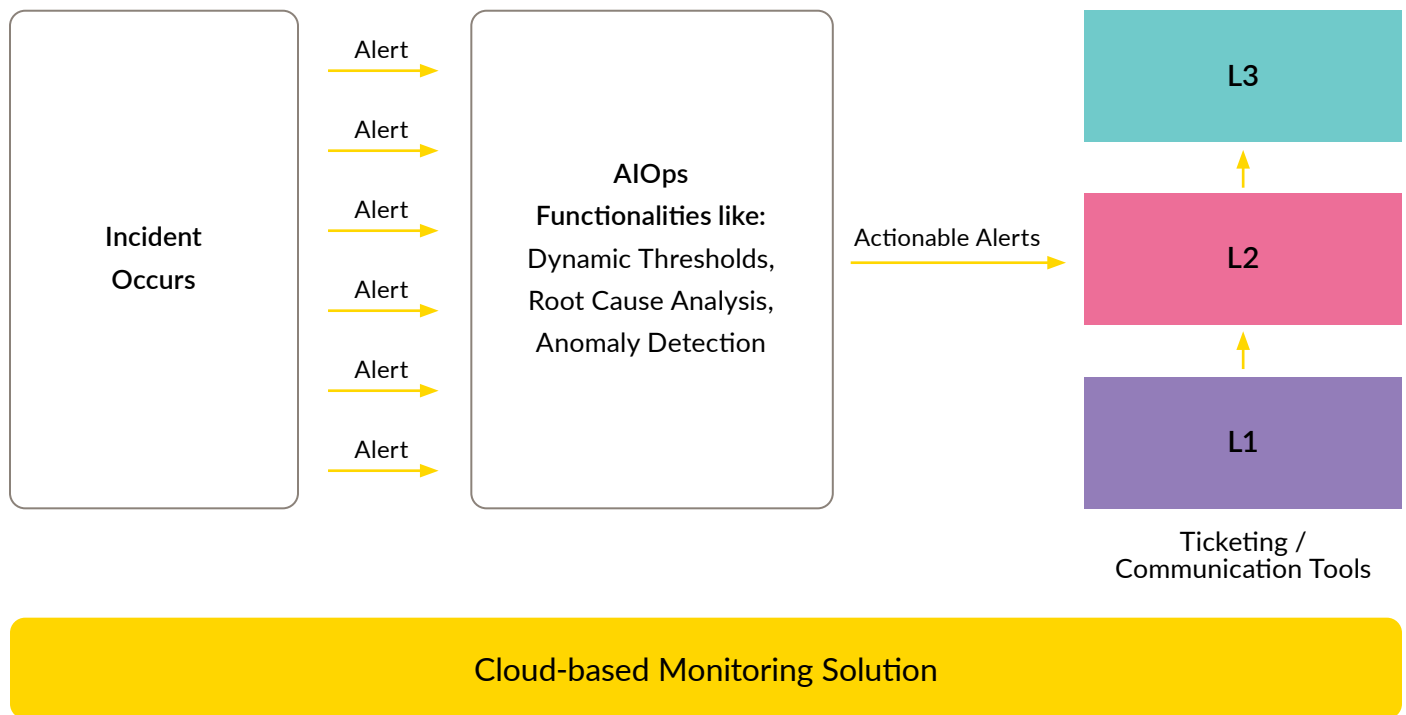


Figure 2 - With custom tuning, a cloud-based monitoring system can shield the staff from excessive alert noise, simultaneously shunting some alerts to automated response processes to further lighten the monitor's load.

The System Engineer at IFM Efactor rated LogicMonitor a 10 out of 10, noting that “the customizability of it, and the ability to tweak everything so you’re getting meaningful alerts and removing false positives, are absolutely incredible.” The results of fewer false positives, according to the Solutions Engineer at Black Box Network Services, include improved reliability, service level agreements (SLAs) and uptime.

“Being able to fine tune alerts allows us to be more efficient and get less false positives,” said the Technical Architect at Computerworld Group. The tech company Senior Systems Integration Engineer similarly found that “the number of false positives has been reduced using LogicMonitor compared to how many we were getting with other monitoring platforms. The ability to fine tune alerting helps achieve that goal.”

Some users are able to quantify their false positive reductions. The university IT Operations Manager cut his by 50 percent. His team believes they can get to 70 percent with further tuning. A Lead Network Engineer / Solutions Specialist at a tech services company has seen a 10 to 15 percent decrease in false positives. Meanwhile, the Solutions Engineer at Black Box Network Services, who experienced a lot of false positives due to the use of VPN tunnels, has realized a striking 70 to 80 percent decrease in false-positive alarms with LogicMonitor.

#5. They Need to Prove ROI

Saving IT pros time is one of the overarching goals of consolidating and automating infrastructure monitoring. Disparate tools, configuration overhead, and ongoing maintenance from legacy tools reduce ROI and put IT teams in the hot seat during budgetary discussions. A demonstrable ability to save people time and money is thus a key reason for leaving legacy tools behind. The tech services Head of IT experienced this with LogicMonitor. He revealed that “it certainly has the value for money given the scale, time saved, and efficiencies that we’ve gained from it. It has been very worthwhile.”

“We have absolutely seen ROI. We sell managed service contracts and the solution is part of that contract.”

[Read review »](#)

“We have absolutely seen ROI,” said the Technical Architect at Computerworld Group. He added, “We sell managed service contracts and the solution is part of that contract. Without it, we would have a tougher time trying to manage calls. We might need to have even more engineers. So, it definitely helps us to save money and provide better service.”

Consolidating monitoring into a SaaS-based platform also means there are no surprises with billing, which can help increase ROI and reduce licensing costs across systems. For managed service providers who resell the platform to their customers, this means immediate ROI. For the Solutions Engineer at Black Box Network Services, this meant reducing license costs. He said, “That’s a huge savings, and it’s great for the customer because it means we can lower our cost and they think we’re losing money, but we’re still getting so much. That was a huge benefit.”

For the tech services NOC Manager, the time-saving advantage came from not having to configure everything manually each time they bring on a new customer. He said, “Instead, we just establish the collector, meaning the monitoring server, within the customer’s networks, and we scan the network and onboard devices with just a couple of clicks. It has probably saved us tens of hundreds of hours per year and per person.”

“AIOps enable us to see patterns in traffic or CPU usage, to know what to expect as normal and understand what is abnormal.”

[Read review »](#)

#6. A Need for Future-Proof Tools that Support AI and Machine Learning

Advances in AI now let the monitoring solution perform some of the more routine tasks that were previously performed by people. This liberates infrastructure monitoring staff from many tedious chores while improving the ability to spot hard-to-see issues before they become big problems. However, siloed, legacy monitoring tools generally lack native support for machine learning and may struggle to run analytics on large data sets. Users want AI and machine learning, so they are moving to new, SaaS-based solutions as a future-proof option.

LogicMonitor calls its AIOps capability LM Intelligence, which empowers IT pros with dynamic thresholds, anomaly detection and root cause analysis. The Senior Director at Optimal+ related that [LM Intelligence](#) was helpful because it tracked the number of files and folders used in extract-transform-load (ETL) procedures. This had previously been a time-consuming matter to track by hand.

Some PeerSpot members utilize LM Intelligence for [root cause analysis](#). This is the use case for the Principal IT Consultant. He explained that technology “definitely helps us to be more proactive in resolving issues and preventing problems because we don’t have to waste time entering, for example, vCenter to look for metrics.” The tech company Network Architect similarly remarked that “AIOps enable us to [see patterns in traffic](#) or CPU usage, to know what to expect as normal and understand what is abnormal.” He also uses dynamic thresholds for [anomaly detection](#).

Conclusion

Monitoring teams are moving away from legacy solutions for a variety of reasons. Operational efficiency and effective, accurate monitoring are their ultimate goals. To get there, they're embracing SaaS-based tools to enable tool consolidation, automation, alert noise reduction, and time savings. Cloud architectures continue to grow more sophisticated, a reality that further motivates IT pros to ditch legacy monitoring tools. The field will never stop evolving, so future-proofing is essential. With the right SaaS monitoring solution in place, it should not be a problem for IT pros to remain efficient in their monitoring efforts, even as the cloud environment changes over time.

About PeerSpot

PeerSpot (formerly PeerSpot), is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

PeerSpot does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, PeerSpot websites, and PeerSpot materials do not reflect the opinions of PeerSpot.

About LogicMonitor

Monitoring unlocks new pathways to growth. At LogicMonitor, we expand what's possible for businesses by advancing the technology behind them. LogicMonitor's SaaS-based monitoring solution allows IT Pros to get visibility for their entire infrastructure within a single pane of glass. With advanced AIOps features built-in, we allow monitoring teams to move from reactive monitoring to proactive observability. Turn on a complete view of your infrastructure within minutes with automated deployment and configuration, turn the dial from optimization to innovation, and turn the corner from sight to vision. Join us in shaping the information revolution.