WHITEPAPER

SaaS vs. On-Premise Monitoring

9 Reasons SaaS Makes More Sense

You know that cloud-based services provide advantages, including low upfront costs, fast deployment, and simplified administration. We know that the SaaS to on-premise comparison differs for every technology. Sometimes a SaaS approach has special benefits that are not initially apparent. Take a look at why network and server monitoring is particularly suited to a cloud-based model and how a SaaS monitoring solution can offer higher reliability, better support, and lower costs.

Reason 1: Removes the Single Point of Failure

On-premise monitoring products share a single-point-of-failure with the systems they monitor. If there is a power outage, broken network link, or infrastructure problem affecting the part of the data center housing the monitoring server, monitoring abandons you at the very time you need it. Your monitoring tool needs to help you assess the situation and restore operations. On-premise monitoring leaves your IT staff blind precisely when visibility is most needed.

With a SaaS solution, monitoring runs from geographically distributed data centers in the cloud.

WHITEPAPER

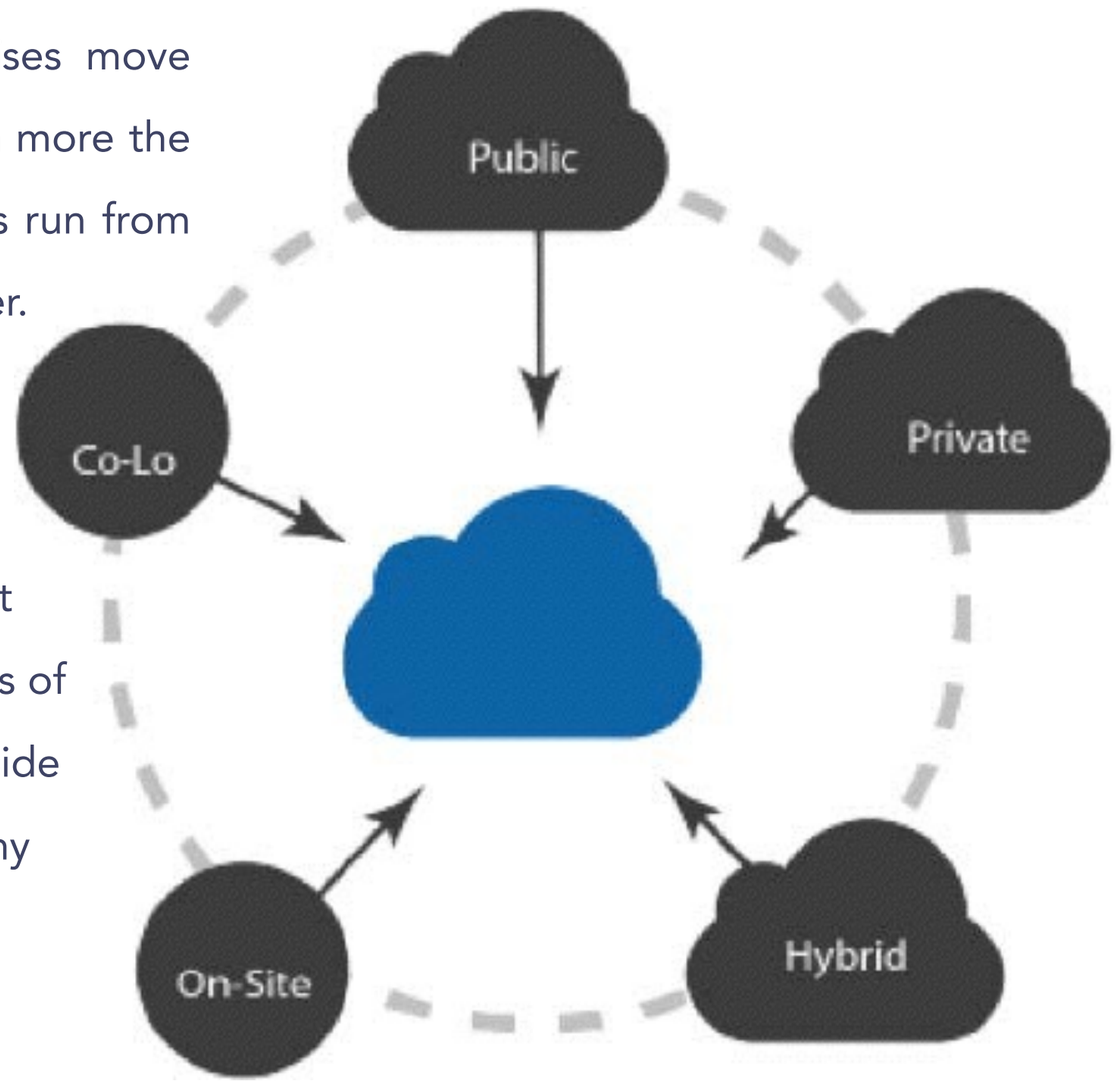
SaaS vs. On-Premise Monitoring: 9 Reasons SaaS Makes More Sense

Your SaaS monitoring solution detects a local outage and alert you, preventing critical issues from going unnoticed for extended periods.

External, geographically diverse monitoring helps you recover from major disasters as well as localized problems.

Reason 2: Easier Monitoring of Hybrid Environments

While the migration to the cloud has arrived, few enterprises move everything into the cloud overnight. Moving gradually is much more the norm, resulting in hybrid environments in which some services run from the cloud and some continue running from a private data center.



Configuring premise-based solutions to monitor applications and infrastructure in multiple locations often requires significant spend on location-specific hardware, as well as the complexities of configuring VPN links and modifying firewall rules to allow outside locations to talk to the main monitoring servers behind company firewalls.

SaaS monitoring solutions allow for seamless, unified monitoring of the entire IT ecosystem, regardless of location or type: physical, virtual, or cloud-based. LogicMonitor provides a lightweight data collector for each location at no cost, and data flows through outgoing-only SSL connections to the monitoring data centers. No VPN links or special modifications to firewall rules are required.

WHITEPAPER

SaaS vs. On-Premise Monitoring: 9 Reasons SaaS Makes More Sense

Reason 3: Fast Deployment

Before an on-premise monitoring product provides value, you need to:

- Purchase servers and install them at each location
- Install and test the monitoring software
- Configure monitoring for every device and application to be monitored
- Set alert thresholds for every monitored service
- Create graphs to help monitor key data and trends

With the size and complexity of today's IT environments, these activities can take weeks or even months.

In contrast, a SaaS solution like LogicMonitor can be live and providing value in less than an hour.

Reason 4: More Efficient Effective Support

The complexity of IT environments continues to grow and the monitoring demands grow in lock step. Often this growth outstrips the in-house monitoring expertise required to effectively analyze all the applications and underlying infrastructure. Excellent vendor support is indispensable, especially when problems occur under unusual conditions.

With on-premise products, the monitoring vendor has no direct visibility into your monitoring environment. You need to open a ticket and try to explain what you see. The vendor support staff evaluates this information second-hand and attempts to work through you to troubleshoot and resolve the problem. Information round trips and miscommunication waste time and delay problem resolution. In addition, support contracts often cost thousands of dollars annually and often allow for limited incidents.

WHITEPAPER

SaaS vs. On-Premise Monitoring: 9 Reasons SaaS Makes More Sense

With a SaaS monitoring solution, you get more than a piece of software. They're buying a service that includes continuous support and training at no additional cost.

Provided permission is granted, the vendor's support staff has instantaneous access to customers' monitoring data, allowing them to aid in the troubleshooting of complex problems. The customer essentially gets a team of outsourced IT professionals to consult at no additional cost.

Reason 5: Lower Capital Expense and TCO

SaaS adoption continues to accelerate. IDC estimates sales of SaaS and cloud-based applications growth at 24% annually, reaching $67.3 billion by 2016. A recent Gartner survey highlighted factors driving this rapid growth, including lower total cost of ownership (TCO), fast deployment, lower capital expenses, and shortages of skilled IT staff to implement on-premises solutions.

Source: Gartner (October 2012)

WHITEPAPER

SaaS vs. On-Premise Monitoring: 9 Reasons SaaS Makes More Sense

Lower capital expense and TCO apply to IT infrastructure monitoring. Monitoring is a mission critical function and on-premise monitoring tools require a hefty server. You can easily see a capital expenditure (CapEx) of $3,000 - $5,000 in each major location, with a hardware replacement or upgrade every three years.

SaaS solutions require no capital expense for hardware or software. The monitoring solution provider bears the cost of the monitoring infrastructure.

When evaluating monitoring tools, do not overlook the cost of labor. Setting up and maintaining a premise-based monitoring infrastructure, keeping monitoring configurations up to date for all applications, and the underlying infrastructure components such as routers, switches, firewalls, web servers, application servers, database servers, email servers, hypervisors, and storage arrays easily consumes one or more fulltime engineers.

SaaS-based monitoring leaves monitoring server and infrastructure administration to the provider. LogicMonitor employs an entire team of operations experts to maintain their monitoring infrastructure — a major expense the customer avoids.

Reason 6: No Vendor Lock-In

On-premise monitoring products generate large capital expense spend for hardware. The initial and ongoing time investment to configure the software and keep it configured for many devices and applications adds to the stickiness of the solution. These sunk costs create switching costs that can prevent you from moving to alternatives, even if you know the alternatives are better.

Risks are much lower with SaaS solutions. No CapEx, fast deployment, automated configuration, and month-to-month agreements mean you regain the freedom to make the best decision at all times.

WHITEPAPER

SaaS vs. On-Premise Monitoring: 9 Reasons SaaS Makes More Sense

LogicMonitor goes one step further and automates the discovery and inclusion of new devices added to your technology stack and network fabric, limiting ongoing expenses for configuration and updates.

Reason 7: Higher Reliability

On-premise monitoring products expose you to outages through the advent of many events: hardware failures, power outages, software bugs, human error, and natural disasters. Any outage or suspected issue requires your staff to troubleshoot and restore the monitoring system back to functioning status.

A well-designed SaaS solution provides high levels of redundancy, with backup and replication across geographically distributed data centers, enabling rapid recovery from major interruptions. Your SaaS vendor must maintain expert staff with 24x7 coverage of their and your infrastructure to ensure maximum uptime.

Reason 8: Scalability and Predictable Budgeting

With on-premise monitoring products, when the number of devices and amount of monitored activity grows, you need to upgrade, add, and logically link new servers. Your on-premise databases grow in kind. Costs escalate in direct proportion to time spent and downtime incurred during expansion. Because upgrade costs are also lumpy, occurring when they occur and at market cost, they can place unexpected strain on your budget.

SaaS solutions scale on demand, without the CapEx costs of additional monitoring hardware. Monthly subscription costs are tied to the number of devices being monitored, so they grow smoothly, predictably, and proportionately to the value you receive.

WHITEPAPER

SaaS vs. On-Premise Monitoring: 9 Reasons SaaS Makes More Sense

Reason 9: Elevated Security

Conventional wisdom points to premise-based monitoring solutions as more secure than SaaS. When we explore security from the following perspectives, application level security and physical security level, this wisdom proves false.

If you are a small company with premise-based applications, concerns around application-level security tend to be low. The company is small, and everyone is trusted to some degree. Locating the application behind a firewall, cutting it off from outside access, provides fairly good security. Small companies rarely have physically secure premise-based servers. Servers run in a small server room (or closet), without the benefit of alarms, 24-hour guards, or any of the other features of a SaaS datacenter.

If you can physically access a server, you can access the data on the server.

As your company grows, you will solve issues with physical security. Now your application security comes under scrutiny, security-sensitive applications must be restricted to a subset of employees. Most often, developers write premise-based applications, especially open-source solutions and internally developed solutions, without any thought to access control. Administrators log in directly to the server, often as root. As your company continues to grow, sections of your premise-based applications will need to be accessed by remote offices, telecommuters, contractors, and other agents outside the firewall, posing yet another hurdle. Granting that access securely is not trivial.

You can configure reverse proxy firewalls or SSL VPNs to provide some sort of remote access, but now the simple choice of premise-based software for security reasons is getting more and more complicated, labor intensive, and expensive.

WHITEPAPER

SaaS vs. On-Premise Monitoring: 9 Reasons SaaS Makes More Sense

With a SaaS monitoring solution such as LogicMonitor, all data collection happens from a lightweight collector residing behind your firewall. The collector makes outgoing connections only over SSL and accepts no connections from the network. Monitoring servers reside in locked cabinets inside SSAE 16 SOC1 Type 2 data centers, manned 24x7x365, with ingress and egress secured with electronic keycards and biometric hand scans, high resolution motion-sensitive video surveillance, fully redundant power and HVAC, VESDA fire-threat detection and suppression. Strong internal application controls protect data even from root users.

Simply put, you will have less security issues and incur less cost overall with a SaaS-based solution.