# Security as a Service: Why Does it Make More Sense?

# SaaS vs. On-Premise: How to Choose the Right Solution for Your Organization

SaaS (Security as a Service) has been building its case for rapid user acceptance and training for years.

WhiteSource was developed as a SaaS product. Although we offer on premise and hosted (private cloud) solutions, over 85% of our customers prefer using our SaaS service.

While many organizations, of all sizes and verticals, continue to purchase SaaS solutions for their software, others are still reluctant to do so – for a variety of reasons: some are concerned about loss of control, some are concerned with data privacy and security issues and feel keeping solutions on-premise is the safer solution.

We put together a list of the main areas where some organizations remain uncertain regarding the move to SaaS services, and created this guide to help you evaluate the best solution for your organization during the due diligence process.

# 7 Reasons Why SaaS Makes More Sense When It Comes to Open Source Management Platforms

## 1. Fast Deployment

The deployment method is one of the main differences between SaaS and on-premise solutions. The time to a working solution is much shorter with SaaS, as opposed to the deployment process for an on-premise solution which requires that your internal IT team install and configure the necessary software and hardware for the new infrastructure and environment. Since this deployment project is most often one of many of the IT team's tasks and ongoing projects, this can take several months.

Deploying the WhiteSource SaaS application can take as little as half an hour: since the software is already installed and configured, it can be accessed immediately - and the application is ready for use: you can begin to integrate the WhiteSource plugins with your CI servers, build tools or repositories in minutes, without impacting on the build runtime.

This eliminates the time spent provisioning an environment, as well as any issues that might arise in a traditional deployment process.

## 2. New Product Features and Updates

With an on-premise solution, updates and added features can be expensive projects: budgets need to be updated, software and hardware might need to be purchased, and the IT team needs to allocate time for provisioning, installing and updating. Sometimes it even means downtime for other teams and departments in your organization.

Our SaaS upgrades require practically no involvement from our customers, or their IT staff. Updates are performed automatically, around the clock as necessary, no downtime is required and many new features are added for free, with their release.

One example is the WhiteSource selection tool – an easily installable browser plug-in that allows developers to check an open source library: quality, security, policies- via their browser, even before they download. As part of our SaaS offering, the tool was made available to all WhiteSource customers at no additional cost as soon as it was released, and is continually updated in real time with new information from WhiteSource's database and the customer's open source inventory to ensure a clear and current view of a component's vulnerabilities and its compatibility with organizational policies.

## 3. Continuous Vulnerability Addition

Once a new vulnerability is discovered in an open source component, we immediately add it to our database – which contains over 3M open source components & 70M source files, over 230k vulnerabilities sourced from the NVD, security advisories and issues trackers. The database is updated continuously and all SaaS customers that are using a newly added vulnerable library or component are alerted.

As soon as a new fix for an open source vulnerability is published, it is added to our database, and we notify our customers so that they can remediate it in the relevant libraries.

For on-premise and hosted (private cloud) customers the updates are scheduled.

## 4. Round the Clock Support

On premise solutions require ongoing system maintenance tasks. When Issues like buggy firmware and failing hard drives arise, organizations needs to free up the resources to patch, fix or replace them right on time, whether the fixes were scheduled or not.

With a SaaS solution, support is easy: system maintenance tasks like rolling out OS patches are performed automatically. Under our SaaS model, we take on the responsibility for maintaining the software and upgrading it, ensuring that it is reliable, meeting agreed-upon service level agreements (SLAs), and keeping the application and its data secure. We monitor the system around the clock, and notify our customers directly, in real time when necessary.

With our SaaS solution, our reports are continuously updated and if issues arise they are immediately addressed and remediated by our support team. Customer requests and queries are addressed immediately by our dedicated support engineers and resolved swiftly.

## 5. Lower TCO (Total Cost of Ownership)

The total cost of ownership (TCO) of an on-premise investment includes: hardware, network, backup and development systems. This also includes the cost of human capital, like project management, database, server, firewall, security, backup and help desk resource. This doesn't include the overtime pay required for round the clock maintenance and emergency fixes.

On-premise solutions usually also require higher fees due to the need for expert consulting throughout the project lifecycle: planning, installation, deployment, training and upgrades.

The WhiteSource SaaS pricing plan allows you to spread out your costs over time with one of our subscription plans and minimize your entry cost, as well as save on the ongoing cost of IT, software and hardware maintenance and resources. In addition, our cloud based solution doesn't require additional and costly consulting for the project.

## 6. Scalability

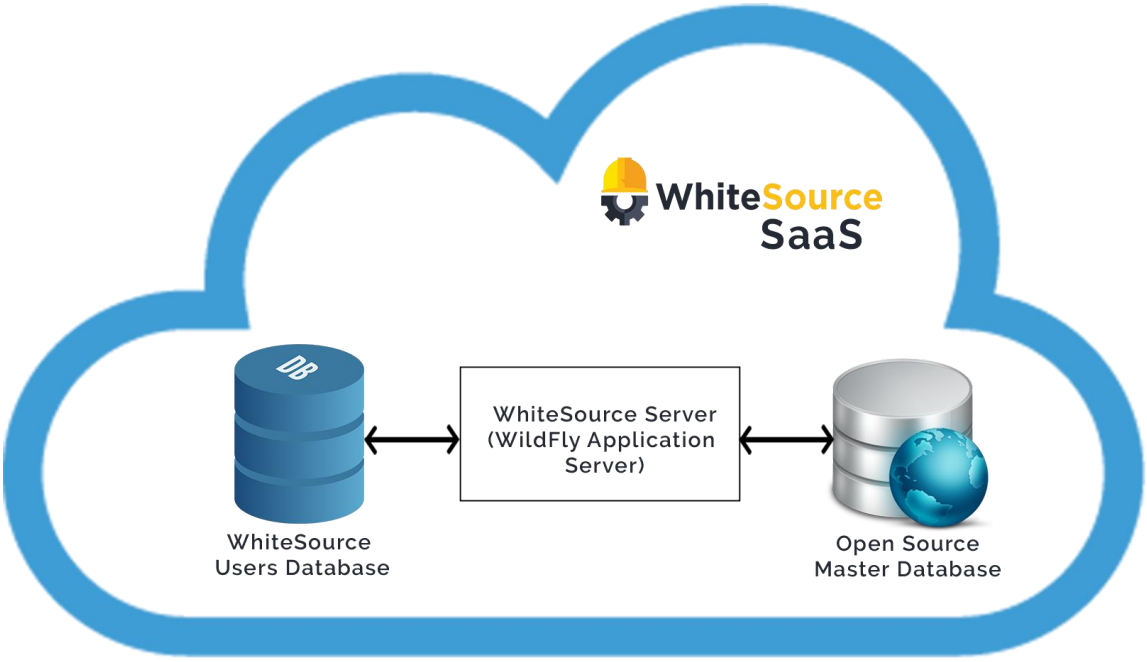
Whether your organization is growing rapidly or you're expanding your business to new territories, when running your operations on-premise, scaling requires major adjustments to bandwidth and database storage capacities, and involves purchase and deployment of servers: a project that will cost more valuable time and money. SaaS allows you to scale rapidly, we balance load between virtual servers, or add more servers and capacity.

Another consideration is your network load: if your organization has occasional peaks in activity, you can scale up when necessary, and then scale back down as the work load lightens, without a need for long term planning and investment in all the extra infrastructure and effort.

# 7. Security

Privacy and security concerns are often the main barriers to SaaS adoption, but shouldn't be considered an issue when it comes to WhiteSource. Your code remains secure, as well as your organization's and your customers' privacy.

Your WhiteSource plugin does not scan or access your code, it identifies your open source components and only sends a signature to WhiteSource, using transport layer Security (TLS) encryption, also known as HTTPS, for all transmitted data.
Your proprietary code is never sent to the WhiteSource cloud. Since we only calculate the checksum of libraries and then cross reference it with our database, there's no trace of proprietary code and the checksum of the open source libraries cannot be accessed or even reverse engineered. In addition, we only send the checksum of newly added components - not all components, and the product and projects that may be related to the components are unidentifiable. This means the data is not at risk in any way.




*Your components' digital signatures are sent to the cloud-based WhiteSource server and are then cross-referenced against our database.*

In addition, our cloud services are up to the highest security and privacy standards:
WhiteSource is hosted at Amazon Web Services (AWS) and is ISO 27001 certified. The data and PID (personal identifiers - email, organization ID and position) are stored on AWS.
Access to data requires VPN and designated private keys, and access to AWS requires two-factor authentication (2FA).
All business data, sensitive data and PID is hosted on AWS EC2 machines, and their access control is done using AWS Security Groups, one for each server type (app server, DB machine, build server, source control, test environments, etc.):
Each security group whitelists a specific, minimal port list allowing communication (inbound and outbound) only for components of that server type's purpose. In addition, each security group requires a different private key, and their access and management of all machines requires a VPN connection with a private key file and 2FA (2-Factor Authentication).
Access is granted to specific people and to specific server types based on functional needs of their role (on a need-to-access basis), and on a least-privilege principle.

# Conclusion

While open source offers great advantages and answers many organizational needs, companies must manage these components continuously to ensure that security and compliance are always up to standard. WhiteSource offers an automated and agile open source management solution to this growing need.
The ease of a quick and hassle-free deployment process and the low cost of ongoing maintenance, support and product updates that our SaaS solution offers, while providing the highest measures of protection for security and privacy, should make choosing our SaaS solution an easy one.