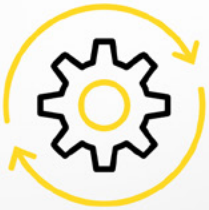
CLEARDATA

Making the Right Choice

DIY SaaS Versus Managed Services for Your Healthcare Cloud



In today's healthcare landscape, the adoption of cloud technology has become essential for organizations to streamline operations and improve patient care. However, with the increasing volume of sensitive data and the ever-present threat of cyberattacks, healthcare leaders must prioritize cloud security.

How do you know if you're ready for a DIY approach with a software-as-a-service (SaaS), or if combining it with managed services is the right choice for your organization? Let's explore the factors to consider when making this crucial decision.

SaaS/DIY Versus Managed Services

So, what's the difference between choosing a SaaS or DIY option versus using a vendor's managed services together with your chosen software? There are a few key pros and cons of each route.

A SaaS/DIY solution provides software functionality delivered over the cloud that gives an organization more hands-on control over its operations with little to no delay in time to implementation. Typically, you can begin to use the software immediately without waiting weeks or months to deploy it. Cloud-based SaaS services can also scale relatively easily as a business grows and as needs change.

With a standalone, cloud-based SaaS, organizations avoid the cost of installing software on legacy systems. A DIY SaaS can offer a more simple and cost-effective pricing model than most managed services options. It's ideal for teams that already have a strong in-house bench of IT and cloud cybersecurity and related healthcare expertise who can manage both the day-to-day and longer-term needs of their security and compliance in the public cloud, including discovery, automation, enforcement, and remediation. A SaaS also provides wider availability and accessibility to its users – all they need is Internet access.

Managed services offer a more comprehensive approach to IT management of your cloud environment. As opposed to a DIY SaaS, organizations using managed services have more control over implementation, ongoing support, and assistance addressing unique security challenges. Going the managed services route provides a holistic solution that encompasses software management, hardware support, and IT strategy transformation.

Managed services extend beyond traditional software management to include hardware support. By outsourcing tasks like maintaining security on IT networks, healthcare organizations can benefit from expert recommendations to upgrade and improve their hardware infrastructure. For example, managed security services may recommend replacing ailing servers with cloud-based services, ensuring optimal performance and scalability.

One of the key advantages of managed services is the ability to identify opportunities for integration and process improvement. For instance, by linking cloud-delivered plugins for a healthcare organization's website, managed services enable immediate communication between sales representatives and customers through a website chat app, improving customer engagement and satisfaction.

First, Understand Your Needs

Before deciding between a standalone software or managed services , it's important to assess your organization's specific needs and objectives as well as your current cloud maturity.

Consider the following factors:

1. Budget Limitations

Evaluate your budget and determine if investing in a dedicated in-house team or outsourcing your managed services aligns with your budgetary constraints. Be sure to look closely at the shorter-term versus longer-term cost implications and what budget limits you have to heed for both software and full-time staff headcount. If budget poses an issue, your organization may be well-suited for a DIY SaaS solution – if you have the right team in place to manage it.

2. Resources and Expertise

Now that you have thought about budget, it's time to assess your existing staff's expertise and capabilities. Do you have the necessary resources to implement and manage a CSPM solution effectively? Be sure to look at both healthcare-specific knowledge as well as cloud security and compliance skillsets. And, does your current team have the bandwidth to manage your cloud infrastructure deployment and day-to-day needs, including 24/7 monitoring and remediation? If not, managed services can provide the expertise and availability that you need.

3. Cloud Maturity

Are you already a cloud-enabled organization? What servers, applications, and cloud services are you currently using? Or are you currently using on-prem services and resources and ready to move to the cloud? Your current cloud maturity will play a major role in which path to take. If you're well established in the cloud already, DIY may be the right choice. If you're in the early stages of your cloud journey, an expert team can provide immense value.

4. Scalability

Consider your organization's growth trajectory. Will your cloud infrastructure expand in the future? Managed services can offer scalability and adaptability to meet your evolving needs. That said, a DIY solution may be a smarter path for smaller, leaner startup companies that are now moving to the cloud who are looking to accelerate their speed to market – then, you can always explore adding on managed services down the line as your business grows and scales.

5. Compliance Requirements

Healthcare organizations face stringent regulatory requirements. While a SaaS solution will work to help ensure continuous compliance using automation and remediation, in-depth healthcare knowledge from a team of humans can provide much-needed insight. A managed compliance service will aid in the creation and maintenance of a consistent compliant cloud environment. Compliance engineers help navigate audits gathering requested evidence for managed assets, and they also assist in the proactive design of new resources with the necessary compliance lens. They will apply a criticality score to the findings and work closely with you to assess and understand risk, to resolve or assist with remediation, and to talk through any questions or issues.

In short: Determine if your team currently has the in-house expertise to navigate these complexities or if partnering with a managed service is what you need to ensure compliance.

6. Risk Tolerance

Evaluate your organization's risk tolerance level. Are you comfortable managing potential security risks independently, or would you prefer the added assurance of expert guidance from managed services? A managed security service acts as an extension of your security team. This means that team members deploy, maintain, tune, monitor, and react to threats detected. With a DIY solution, security is automated, remediated, and enforced, and this may be more than enough protection and confidence for you depending on your particular team and organization.

Questions to Ask

To make an informed decision, ask yourself and any potential cloud partner these questions:

1. How much day-to-day control do I need?

Will a standalone software solution provide the necessary customization and flexibility?

2. How long will it take?

How quickly can I implement and integrate a CSPM solution? Will my team be able to handle the implementation process efficiently?

3. How much support do I need?

Can my team handle the day-to-day management and maintenance of the CSPM solution, or do I need the expertise and support of managed services?

4. Does this DIY solution meet my needs?

How does it address my organization's unique security challenges? Is it healthcare specific or for multiple industries? Can it adapt to our specific compliance and security requirements?

5. What are the risks and benefits?

What should we consider as concerns versus value-adds for each approach? How can a cloud partner mitigate the risks and maximize the benefits?

Securing your healthcare cloud environment is paramount to protect sensitive patient data and ensure regulatory compliance. ClearDATA's CyberHealth™ platform offers a comprehensive CSPM solution tailored to the unique needs of healthcare organizations – now available as a DIY software or together with our managed services, depending on your needs.

Whether you choose the standalone software or opt for managed services, ClearDATA empowers you to make an informed decision based on your budget, resources, and specific requirements. By partnering with ClearDATA, you can confidently safeguard your cloud infrastructure and focus on quality of patient care and improved health outcomes, growing your business, and innovating in the cloud.

Still have questions? Our team will help you understand the possibilities and guide you on the best path to take and factors you might not have considered to help you make the right choice.

Speak with our healthcare cloud experts to see for yourself why ClearDATA's CyberHealth™ platform is the proven CSPM solution purpose-built for healthcare organizations like yours.

CLEARDATA™

ClearDATA.com (833) 99-CLEAR

Leverage our proven healthcare-specific cloud security posture management software and services and the strength of our expert teams to improve healthcare, protect patient privacy and data, and innovate in the cloud.

Schedule a Consultation