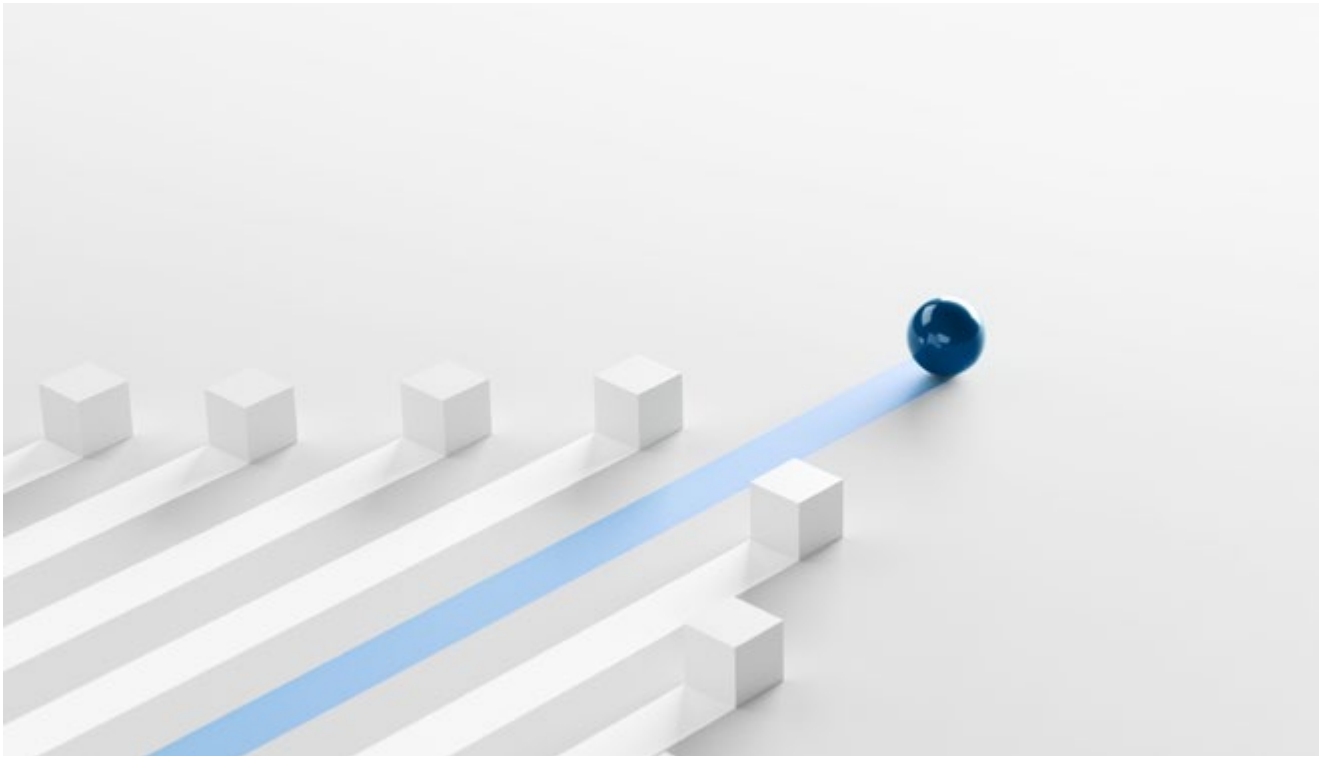
Whitepaper

True SaaS or a cloudy promise?

A guide to navigating SaaS and achieving imaging excellence



This whitepaper explores the transformative role of Software as a Service (SaaS) in medical imaging. It delves into the evolution, benefits, and challenges of SaaS. It highlights the unique advantages of True SaaS over other cloud models, emphasizing its potential to improve healthcare efficiency, strengthen cybersecurity, and ensure regulatory compliance.

The rise of SaaS in medical imaging

SaaS adoption in medical imaging is gaining momentum, aligning perfectly with the evolving demands of the healthcare industry. It offers a timely answer to many critical challenges, including enhancing cybersecurity, relieving IT resource constraints, and providing cost-effective data storage solutions. Beyond strengthening security and lightening the load for in-house IT teams, SaaS improves data accessibility and presents opportunities for cost savings1. Its agility, a hallmark of cloud computing and SaaS, shines through in quick software updates, the ease of scaling computing resources, and its ability to integrate seamlessly with advanced technologies like generative AI2.

However, this transition also comes with its challenges. Besides addressing regional data center shortages and navigating complex data protection laws2, there is also the task of understanding varied market offerings. Vendors use terms like “SaaS,” “fully managed,” and “cloud-native” differently, making it challenging to identify the true value and potential of these solutions.

Healthcare organizations can align their expectations with reality by carefully evaluating each vendor’s offerings and noting key differences. This informed approach enables them to confidently upgrade their medical imaging technology. It also allows them to enhance patient care with solutions that are advanced, accessible, and secure.

SECTRA

Knowledge and passion

A refresher on cloud deployment models

The cloud computing landscape is rich with options, each designed to suit different organizational needs, strategies, and resources. Let's start with an overview of the common models:

- **SaaS:** True SaaS solutions are hosted entirely in the cloud and managed by the service provider. This includes regular system upgrades, security patches, and compliance checks, all bundled into a single contract with contractual Service Level Agreements (SLAs). The beauty of this model lies in its ability to substantially reduce the IT workload, as responsibility seamlessly shifts to the vendor, offering a streamlined, hands-off experience.

- **Hybrid cloud:** Hybrid models combine on-premises infrastructure with cloud components, offering a balanced option. They retain critical servers and short-term data storage on-site while using the cloud for long-term storage needs. This approach is favored by those looking for a gradual transition to full cloud adoption.

- **BYO (Bring Your Own) cloud:** Tailored for organizations seeking control and the ability to use existing cloud resources, BYO cloud allows for full customization and management of IT and cloud infrastructure. This autonomy, however, entails comprehensive responsibilities for maintenance, upgrades, and security, often requiring a robust internal IT department.

Beyond the surface: not all SaaS is what it seems

While the deployment models described above provide a clear framework, selecting True SaaS can be slightly more intricate. Not all offerings labeled as SaaS genuinely align with the model. Hybrid models, which include on-premises components, are easily identified as not True SaaS due to significant differences. The real challenge lies in recognizing pseudo-SaaS—cloud offerings marketed as SaaS but concealing their true nature.

True SaaS: Fully managed

One vendor: A single vendor manages the entire service, from software to cloud infrastructure.

One contract: A comprehensive contract covers software, infrastructure, and associated services with very strict SLAs since only one vendor is managing the entire service.

One bill: Customers receive a consolidated bill for the complete service.

One point of accountability: A clear and singular point of accountability ensures software functionality, performance, capacity management, and security, among other things.

Unified experience: Customers enjoy a smooth and unified experience with a single vendor for everything, including inquiries, support, and issue resolution.

Pseudo-SaaS: Not quite fully managed

Two vendors: Involves interacting with separate entities—the software vendor and the cloud provider.

Two contracts: Separate agreements, each with distinct terms, conditions, and SLAs.

Multiple bills: Distinct billing from each vendor introduces financial complexity.

Distributed accountability: Responsibility is divided between the software vendor and cloud provider, often blurring lines, creating confusion, and leading to finger-pointing and blame games.

Fragmented experience: Results in varied points of contact and responsibilities, leading to coordination challenges and a complex customer experience.

True SaaS: defined by cloud-native principles

SaaS grounded in cloud-native principles, stands out for its effectiveness, scalability, and security.

- **Immutable infrastructure:** A key component of True SaaS, immutable infrastructure involves deploying new, pre-configured environments for updates. This minimizes disruptions and enhances security, as users consistently access the most current software versions. In contrast, traditional SaaS might use mutable infrastructure, where existing environments are modified, leading to potential inconsistencies and security vulnerabilities.

- **Cloud elasticity:** Elasticity in cloud environments allows True SaaS systems to efficiently handle varying user loads by scaling resources to match demand. This ensures optimal resource use and stable performance, providing an uninterrupted service experience. Traditional models might rely on static or manual scaling, resulting in underused resources during low demand or performance issues during surges.

- **Multi-tenancy:** True SaaS employs multi-tenancy, sharing infrastructure among multiple customers while ensuring data privacy and security. This contrasts with traditional SaaS, which may use single-tenancy, allocating separate software instances for each customer. Single-tenancy is less resource-efficient, leading to higher operational costs.

Each of these principles—immutable infrastructure, cloud elasticity, and multi-tenancy—contributes to the superiority of True SaaS over traditional models. By adhering to these cloud-native principles, True SaaS offers a more secure, scalable, and cost-effective solution.

The role of governance

Understanding the distinctions between True SaaS and pseudo-SaaS highlights the value of True SaaS. However, a seamless True SaaS experience relies on SaaS governance, which covers contractual obligations, security, and performance. Here's a summary of what the vendor manages and why it matters:

User Access Management. Ensuring secure and authorized access to applications.

Policy Enforcement. Upholding data handling policies compliant with standards like HIPAA.

Regulatory Compliance. Keeping software in line with healthcare regulations such as the HITECH Act.

Data Governance. Managing data quality, security, and privacy in accordance with GDPR.

Audit and Reporting. Providing tools for system usage monitoring and compliance reporting.

Risk Management. Proactively addressing risks, including cybersecurity threats and operational challenges.

Change Management. Efficiently managing updates and changes to minimize service disruptions.

Incident Management. Quickly resolving incidents like security breaches or system downtime.

Resource Optimization / Capacity Management. Managing resource allocation and utilization within the SaaS environment.

Service Excellence Ensuring the platform consistently meets service-level goals like uptime and responsiveness.

Vendor Management. Overseeing third-party services and integrations for seamless operations.

In True SaaS, the vendor takes responsibility for the entire infrastructure and security, enabling customers to focus on their specific data and application needs. A clear understanding of roles and responsibilities, usually defined in SLAs, is crucial for a secure and compliant experience in this model3.

A cyber nightmare in healthcare

Healthcare CIOs face a critical challenge: the escalating threat of cyberattacks. Some even consider these attacks more daunting than the COVID-19 pandemic4. In 2023, the healthcare sector endured a staggering 475 cyberattacks, impacting over 106 million individuals—equivalent to nearly one in three Americans4. The worst-case scenario? A healthcare facility hit by a cyberattack, potentially forcing the relocation of critical patients, including those battling life-threatening conditions like cancer4.

Adding to the complexity, healthcare organizations face a shortage of IT experts, with many struggling to recruit and retain

skilled staff5. A 2023 KLAS Research report highlighted these struggles, particularly when it comes to proactively managing third-party products and services6. This double burden presents a stark reality for healthcare organizations, making it increasingly challenging to balance the demands of IT management and cybersecurity.

Elevating security with True SaaS

- **Cybersecurity expertise:** True SaaS leverages the combined in-house cybersecurity expertise of both the software vendor and the cloud provider. With dedicated security teams, extensive investments in cybersecurity, and adherence to industry standards, True SaaS provides comprehensive protection that would be challenging for many healthcare organizations to replicate.

- **Centralized security management:** In True SaaS, security management is centralized, ensuring consistent security policies, monitoring, and updates. This centralized approach minimizes the risk of misconfigurations and vulnerabilities.

- **Automatic updates and patch management:** True SaaS providers handle automatic updates and patch management, ensuring that the software and infrastructure are always up-to-date with the latest security fixes. This reduces the risk of exploitation of known vulnerabilities.

- **Multi-layered security:** True SaaS solutions implement multi-layered security measures, including firewalls, intrusion detection systems, and encryption at rest and in transit. This layered approach adds multiple barriers for potential attackers.

- **Compliance and certifications:** Many True SaaS solutions adhere to industry-specific compliance standards (e.g., HIPAA, GDPR) and hold certifications (e.g., ISO 27001, CSA STAR) to demonstrate their commitment to security and privacy.

- **Distributed Denial of Service (DDoS) protection:** SaaS providers often have DDoS protection mechanisms in place to mitigate and absorb large-scale attacks that could disrupt services.

Conclusion

In conclusion, **the adoption of True SaaS in medical imaging is a strategic decision that merges advanced technology with streamlined management.** By choosing a single vendor for all imaging needs, organizations not only reduce their IT workload but also ensure continuous access to the latest software advancements. This model **simplifies management and maintenance,** traditionally shouldered by IT teams, and goes a step further by optimizing performance and ensuring high system efficiency. True SaaS offers a comprehensive solution, centralizing responsibility and bolstering security for the entire service.

Going forward, it is essential to recognize that True SaaS is more than just a simplification of IT tasks; it is a comprehensive, future-focused solution that meets the evolving demands of medical imaging. Explore the unique advantages of True SaaS with Sectra One Cloud, where simplicity, innovation, and security unite, shaping the future of medical imaging technology.

This is a marketing material and may be changed at any time without prior notice. Sectra will not be held liable for any errors or misconceptions herein.
DOC-EKAN-C9RHLC-1.0 © 2024 Sectra Medical AB

SECTRA
Knowledge and passion