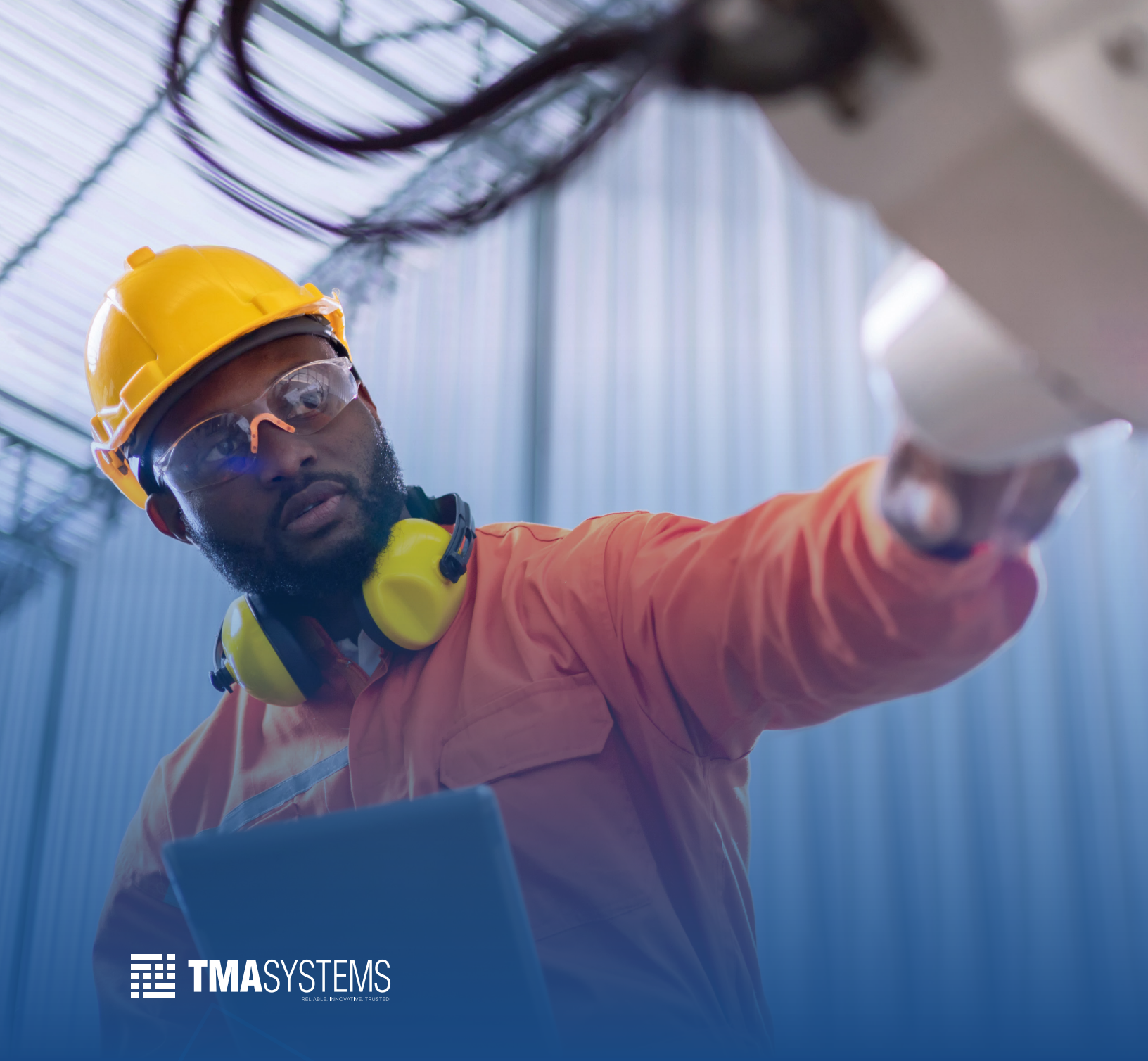


TMASYSTEMS
RELIABLE. INNOVATIVE. TRUSTED.

SaaS and On-Premise Enterprise Asset Management:

Finding the Right Fit for Your Organization

WHITEPAPER 11 - 2024

Selecting and purchasing an Enterprise Asset Management (EAM) software solution is one of the most important investments a facilities operations business leader makes. Not only is the management and operability of interconnected assets at stake, but factors like budgets, resources, and overall business needs must be scrutinized during the due diligence process. And although it might feel like choosing the right vendor for your organization is the end of the decisioning process, it's only the first step to determining which solution will set up your organization for success: Businesses must also evaluate whether a Software-as-a-Service (SaaS) or on-premise model best meets their needs.

Historically, enterprise software served as a process and tech enabler for business units, driving organization and cohesion through a single system. On-premise models were created with these objectives in mind and excelled as monolithic, "single sources of truth" for stakeholders within an organization. But as the technology landscape has grown more robust, companies desire solutions that solve business needs across the entire enterprise; the result is an increased demand for capabilities ecosystems that can seamlessly connect to and interact with other platforms in a company's tech stack. And although on-premise solutions can be configured to accommodate business enablement, APIs and other requirements, the process is often arduous and resource-heavy.

Consequently, users have been quick to adopt SaaS solutions that provide them with enhanced agility and accessibility; the demand for B2B SaaS solutions grew by 179% between 2022 and 2023 alone.[1] What's more, customers are increasingly turning to industry-specific cloud solutions (ICP) to drive business optimization, with 67% of companies citing significant near-term ICP adoption plans.[2] More than 70% of all software used by today's companies are cloud-hosted solutions and 73% of business leaders say that SaaS products enable them to meet all of their business goals.[3]

But amidst the SaaS gold rush, EAM customers have remained loyal to on-premise platforms. According to Gartner, EAM SaaS adoption lags behind other industries and on-premise software is the preferred hosting model by significant margins.[4] Customers cite skepticism that SaaS can deliver comparable security, control and configuration as key reasons for sticking with on-premise; while these are valid concerns, they're not entirely warranted. For some organizations, SaaS is actually the more secure, controlled choice; SaaS vendors make significant investments in security and configuration that often outpaces what a customer can manage with an on-premise solution. In fact, a key benefit of SaaS solutions is its elasticity, enabling customers to quickly, regularly and safely pivot in the face of business, regulatory, and market changes.

Bearing all of this in mind, how do you know whether SaaS or on-premise EAM is right for your business? The answer isn't simple and must be considered on a company-to-company – or industry-to-industry – basis. This paper outlines some of the key differences between and benefits of SaaS and on-premise hosting models to help you evaluate the best fit for your organization.

1 Boston Consulting Group, "Tech Is Cooling Off. B2B SaaS is not," April 19, 2023.

2 Gartner, "2024 Tech Provider Top Trends: Industry Cloud Delivers Growth," December 12, 2023.

3 DevSquad. "103 SaaS Statistics and Trends for 2024."

4 Gartner, "Market Guide for Enterprise Asset Management Software," February 14, 2023

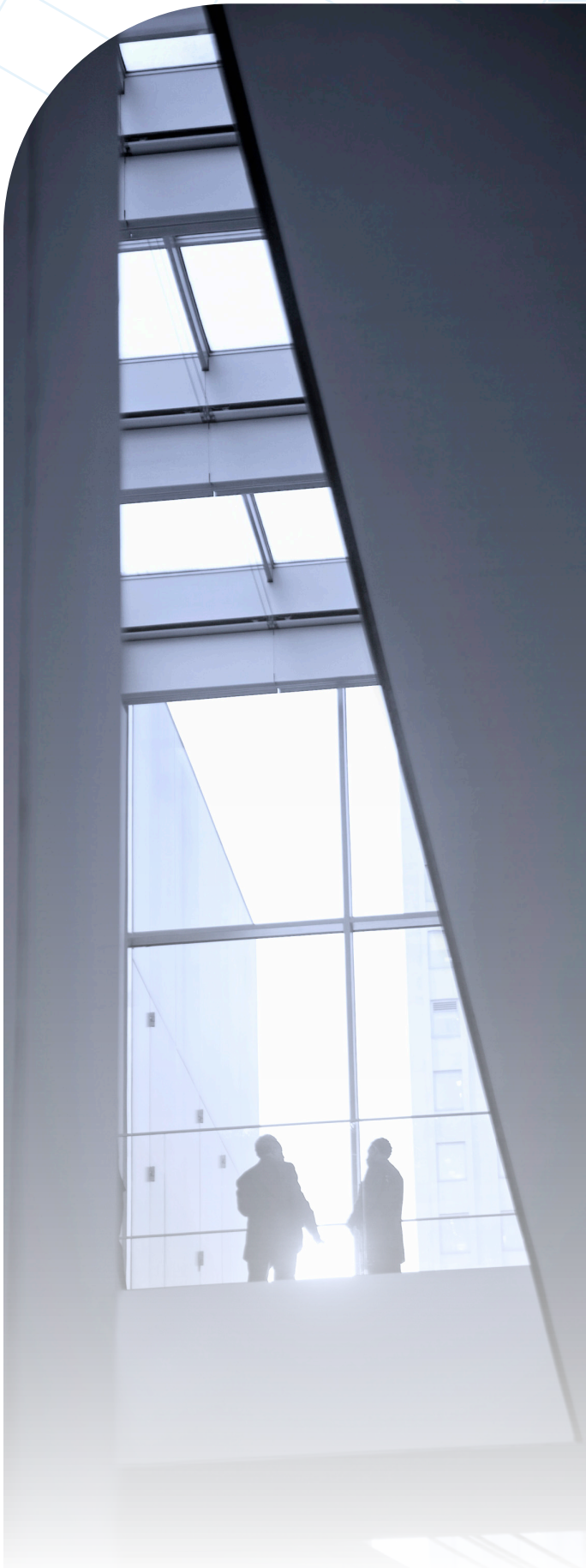
Cost and Management

Digital operations platforms are typically one of the costliest areas of an enterprise and it's critical that buyers understand the differences between SaaS and on-premise expenses before making a hosting decision. Although SaaS is typically viewed as an easier and less risky expense, it's not necessarily a cost-saver in the long-term.[5] A few things to consider when evaluating an EAM software investment include:

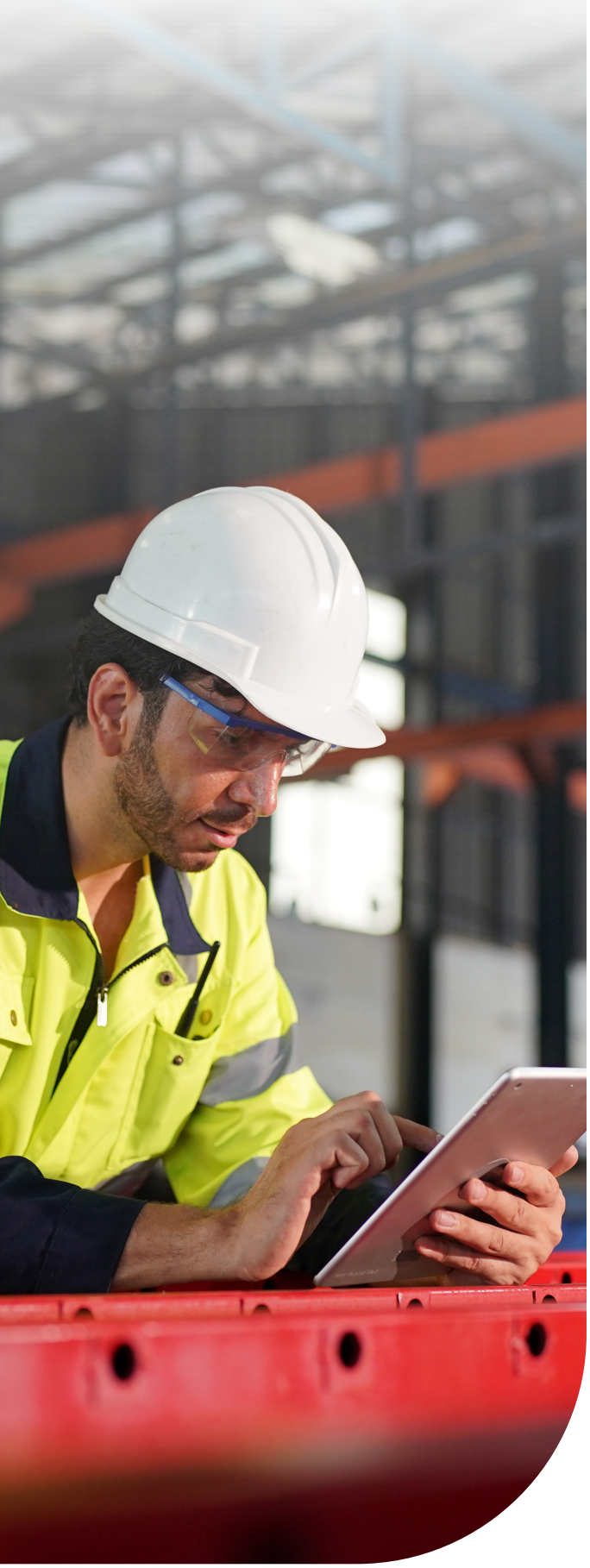
Capital expense (CapEx) v. operating expense (OpEx) categorization

The high up-front costs of on-premise solutions – which include hardware, software, and other equipment – are typically classified as one-time capital expenses that take up significant chunks of a budget. Investing in a capital expense often requires planning – sometimes more than a year in advance – to ensure adequate funds are available. The key benefit of an on-premise capital expense is that a company is more or less "one and done," meaning that once the initial investment is made, the ongoing costs to maintain the solution are typically fairly low.

While a CapEx categorization for EAM software is appealing to many organizations, it's not always possible. Companies in high-growth mode often have several CapEx items flagged and may not have the funds available for an on-premise solution, particularly at the beginning or middle of a fiscal year. In these cases, a SaaS solution – usually classified as OpEx – might make more sense for an organization. In addition to fund allocation, it's often easier to build the business case for an operating expense with lower up-front costs than a large capital expense that requires increased scrutiny and stakeholder review. This alone can accelerate the deployment time for a SaaS-based OpEx solution. However, reducing the up-front investments often means spreading out hosting costs over the long-run – and this doesn't always add up cost savings.



[5] Forrester, "Quantifying the Business Value of SaaS," February 4, 2022.



Deployment and time-to-value

Stakeholders are under more pressure than ever to prove the value of enterprise software investments; one of the first questions we receive from buyers is, "When can my company expect to experience an ROI?" The answer is nuanced and often contingent on if a company makes the capital expenses required by an on-premise deployment versus the simpler start-up costs of a SaaS solution.

When it comes to deployment timelines, there's no contest: Legacy, on-premise solutions usually take 2-3 times longer to deploy than cloud-based platforms.[6] Longer deployments are due to a variety of factors, notably procuring hardware, custom configurations, and testing required before getting up-and-running. Shorter deployment phases naturally enable customers to unlock value – and get to an ROI – faster.

It's also important to remember that the actual deployment is only one piece of time-to-value. A solution is only valuable if it's being used appropriately and a failure to adequately onboard users can create opportunity costs for an organization. In fact, 66% of employees state that digital friction is an impediment to using employer-provided tech solutions.[7] SaaS solutions have an edge over on-premise on this front, as they're usually UI-driven solutions coded specifically to drive seamless user adoption. Regardless of the platform type chosen, adequately training users – whether done internally or with help from third parties – is critical to reducing the time-to-value.

[6] Forrester, "Quantifying the Business Value of SaaS," February 4, 2022.

[7] Gartner, Service Provider Assessment Criteria for Improving SaaS Adoption," October 4, 2023.

Ongoing maintenance and management

For companies deploying an on-premise solution, the real work begins once the solution is up-and-running. In addition to allocating staff and other resources to maintaining the IT infrastructure, users must conduct regular audits to ensure the solution still meets business, security, and compliance requirements; necessary updates and upgrades usually require significant planning, time, and monetary investments. The benefit of this work is – as many on-premise devotees are quick to point out – complete control over how, when, and why changes are made to the solution.

On the contrary, few – if any – internal resources are necessary to support a SaaS solution, as vendors regularly make software updates to accommodate new best practices and enhance security. APIs to popular technology are usually available on-demand and upgrades are automatic. Standard SLAs in SaaS contracts nearly guarantee that vendors address any problems or complications quickly, and without interruption to a customer's business. By handing over the day-to-day management of the deployment, companies can allocate internal resources to higher-value, strategic tasks that have a marked impact on the business, rather than focused on troubleshooting software problems.

Lifetime costs

Ongoing fees to maintain an EAM solution aren't always obvious and customers should crunch the numbers before making a hosting decision. For example, ongoing fees for SaaS platforms – which generally include user licenses, storage and throughput – often seem high on paper, but the ongoing maintenance included in most SaaS contracts can add up to significant lifetime savings. By comparison, on-premise customers must pay extra for ongoing maintenance – and buyers might be surprised to learn that these can often add up 22% or more of total software costs.[8]

Even in cases where SaaS does accrue higher lifetime expenses than an on-premise solution, buyers must balance the benefits of having a simpler, easily maintained platform that costs more over time against the ongoing, constrained ability to configure, customize and update an on-premise investment. In addition to the hard costs of maintaining an on-premise solution, buyers should consider the opportunity costs involved. For example, what is the impact of personnel abandoning critical tasks to focus on solving an emergency issue with your in-house infrastructure? Is your company equipped to handle a major problem or upgrade if it's low on IT staff? Will change management be a struggle when it's time to make a significant update to the platform? The answers to these types of questions – and those asked, in general – are different for each organization, but the point is that it's important to think about costs holistically instead of taking a purely numbers-based approach. The juice isn't always worth the squeeze.

[8] Forrester, "Quantifying the Business Value of SaaS," February 4, 2022.

Breaking Down On-premise and SaaS: **Costs and Management**

PARAMETERS	ON-PREMISE	SaaS/CLOUD
Categorization	On-premise software is typically labeled as a capital expense requiring significant upfront investment.	SaaS is usually categorized as an operating expense, with investment spread across the life of the contract.
Start-up costs	Includes all hardware equipment – like servers, data center space, batteries, back-up systems, etc. – licensing costs, and other implementation/service fees.	Software licenses, consulting services (as/if needed).
Lifetime costs	Cybersecurity infrastructure/ personnel, energy, system maintenance, equipment replacement, consulting (as needed), data center space, software upgrades.	Licensing fees and consulting, as needed.
Time-to-value	Deployment typically takes 2-3x longer than SaaS.	Deployment can be anywhere from mere hours to weeks, but once implementation is complete, users can immediately begin extracting value.
Personnel required	Internal teams are responsible for all system management and monitoring, including cybersecurity; this often requires personnel dedicated to the on-premise solution. External consultants and vendors are often required to ensure end-to-end system management.	All maintenance and ongoing management – including security – is performed by the SaaS vendor. Consulting services might be needed to help with subject matter expertise and configurations as the company scales up.

Security

Advocates of on-premise solutions often point to having complete control over the network security perimeter as a key reason for resisting a shift to SaaS. For some companies – and industries – this factor is enough to dismiss any suggestion of adopting an EAM SaaS solution. But when it comes to security, "control" doesn't always mean "better." In fact, Forrester Research recently stated that "SaaS often outperforms in-house deployment, and SaaS vendors make bigger investments in security and performance than most firms can do on their own." [9]

Ultimately, each organization must evaluate their individual security needs before making a platform decision. Some of the key factors to examine include:

Ongoing security and compliance updates

Many organizations find peace of mind in hosting their EAM solutions within their own walls. Equipment is easily accessible and can be repaired, maintained and managed by designated internal personnel; there's no delay in being apprised of potential security issues. Of course, this assumes that an organization has the appropriate resources for daily monitoring and maintenance of a solution, and can immediately address vulnerabilities.

However, for most businesses, this isn't practical – or even possible. In fact, bad actors often target on-premise solutions knowing that most companies can't provide around-the-clock monitoring for legacy solutions.[10] Only 1 in 3 breaches in 2023 was identified by an enterprise's own security team or tools, indicating that – despite the best of intentions – internal resources are usually inadequate.[11] And once an attacker hacks into a solution, they can access other applications via APIs, permitting entry into a company's entire business ecosystem. This prospect is especially deadly for facilities that include hundreds – or even thousands – of interconnected and IoT devices.

Although cloud-based solutions don't offer organizations the same degree of control over their security, there's freedom in that. Vendors adhere to proactive security approaches, monitoring solutions around-the-clock and conducting patching on-demand. Built to accommodate myriad security and compliance requirements worldwide, they typically follow industry standards and best practices, baking these into the solution infrastructure. Software updates are iterative and as regulations change, updates are quickly made to ensure solutions are up-to-date. The proof is in the pudding: According to IBM's "Cost of a Data Breach" report, data stored in on-premise solutions was compromised at a higher rate in 2023 than data in private clouds.[12]

Keep in mind, EAM SaaS vendors are dedicated to keeping your data secure and within compliance standards – it's a critical part of their business model and a central focus of each provider. Even with the best of intentions, it's unlikely that a customer organization can provide the same level of diligence; unless you're certain your enterprise is the exception, selecting a SaaS solution is usually in the best interest of corporate security.

Is your company equipped to prevent and contain data breaches?

Breaches are identified by internal teams and tools	33%
Days it takes to identify and contain	277
Average cost of a data breach	$4.45M

[9] Forrester, "Quantifying the Business Value of SaaS," February 4, 2022.

[10] CSO. "The Microsoft Server hack: A timeline." May 6, 2021.

[11] IBM. "Cost of a Data Breach report 2023." August 2023.

[12] IBM. "Cost of a Data Breach report 2023." August 2023.

Internal security standards and controls

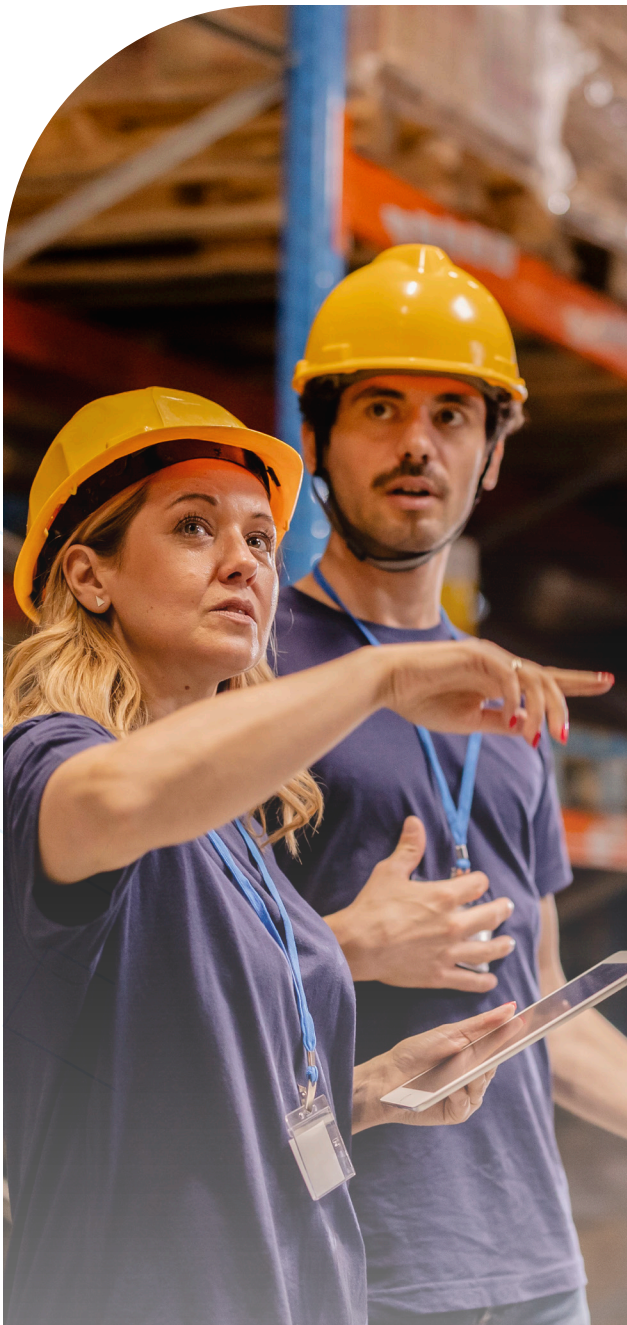
Even the control provided by housing EAM servers under your own roof isn't enough to prevent cyberattacks if there isn't a strong culture of cybersecurity across the entire organization. Most security issues stem from internal behavior, often with employees who make simple mistakes like reusing personal passwords on work equipment. More than half of IT business leaders cite employees as the biggest threat to their security.[13] Verizon validated this assumption in their annual "Data Breach Investigations Report," establishing a 75% year-over-year increase in security incidents caused by internal actors.[14] Interestingly, only 15% of breaches started with a third party – like a SaaS vendor or supplier.

Why does this data matter when evaluating if an on-premise or SaaS solution affords your company with the greatest security benefits? Because it indicates that most organizations – even when they believe they have complete control over their own security infrastructure – aren't as secure as they might think.

In manufacturing, misdelivery by internal actors comprises more than half of all breaches.[15]

For companies adamant that an on-premise solution is the only way to achieve the control they require, it's important to keep in mind that physical control is only a small piece of overall security posture. Unless you are confident that cybersecurity is woven into the fabric of your organization's culture, even designating an entire team to conduct around-the-clock monitoring of an on-premise solution likely won't assure data protection.

Cloud vendors assist organizations with these objectives through best practices and guidelines to improve overall governance. In addition to taking the pressure off an organization to develop protocols themselves, that practice can help identify risks. Granting excessive user privileges is one such area where companies run into problems; Palo Alto Networks found that 95% of users on a cloud platform have access to information and data they don't need. Following guidelines provided by SaaS vendors can help reduce this kind of out-of-control access, thus reducing the potential attack surface for the organization.



[13] Kapersky, "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within."

[14] Verizon. "2024 Data Breach Investigations Report." May 1, 2024.

[15] Verizon. "2024 Data Breach Investigations Report." May 1, 2024.

Breaking Down On-premise and SaaS: **Security**[16]

PARAMETERS	ON-PREMISE	SaaS/CLOUD
Software	On-premise software is run on a company's hardware	Cloud software is stored, run, and managed on the cloud service provider's servers. All of the company's applications are hosted offsite.
Data Rights	Enterprises have complete control over their data and rights, and get extra privacy. In the event of server downtime, the enterprise is responsible for addressing the issue.	A third-party provider regulates data and encryption keys; if there are server downtimes, users may temporarily lose access to it.
Customization	On-premise security solutions can be customized to any degree by enterprises. Users can add or remove security features or components per their business requirements.	Cloud security solutions provide automatic security updates. These features may vary from vendor to vendor and are subject to industry regulations and legal obligations.
Storage Capacity	On-premise security offers limited storage capacities. Enterprises need to invest in additional hardware and storage components to scale up. There may also be migration or upgradation issues.	Cloud security solutions can be easily scaled up or down per business requirements. Data storage is not a problem, and all data centers are monitored by appropriate security measures provided by the vendor in real time, 24/7.
Attack Probability	All hardware and infrastructure components are guarded entirely by internal security personnel. On-premise solutions are easily targeted due to irregular patching/updates and monitoring gaps.	Cloud vendors make significant investments in security that puts them at lower risk of a breach. Patching and monitoring occurs around-the-clock.
Investment and Maintenance	On-premise security solutions require substantial investment, and business owners have colossal startup and operating costs. Maintenance costs may also be high due to infrastructure equipment upkeep and repairs.	Cloud security solutions do not require upfront payments or investments of any sort. Cloud vendors provide a pay-as-you-use model, and businesses pay for how much data storage and other security services they use.

[16] SentinelOne, "Cloud vs On-premise security: 6 Critical Difference." August 25, 2023.

Operational Efficiency

Regardless of the model selected, making an investment in an EAM solution is significant – and not an endeavor any organization wants to undertake every few years. It's critical to choose an EAM platform that can grow with your organization and meet changing needs. In the SaaS versus on-premise discussion, questions about overall efficiency tend to boil down to two key factors: Scalability and upgrades.

Scalability

Both on-premise and cloud-based solutions are scalable – but the ease of achieving this varies. SaaS is deployed with scalability in mind, enabling users to scale up – or down, if necessary – as business strategies and the tech stack changes. This layered approach is ideal for accommodating spikes in traffic and market fluctuations. Capabilities can be quickly and easily added without major up-front investments.

On-premise can also achieve these objectives, but additional planning and investment is needed. System improvements usually require hardware and infrastructure upgrades, especially when "scaling up" to accommodate internal changes or external market forces. Not only does this come at a financial cost, but it takes considerable time to wait for and install new servers.

To truly understand your organization's need for software scalability, it's important to speak with a variety of stakeholders across the business who can help you better understand roadmaps and future plans. Don't assume the status quo or past experiences are indicative of what to expect over the next few years; if there's a product launch or merger that is likely to result in a significant spike in EAM data usage, you need to know about it so you can be prepared.

Support and upgrades

If your enterprise needs assistance with support and making regular upgrades to the solution, it's difficult to argue against SaaS. End-to-end support is intrinsic to the SaaS business model, ensuring that not only do you have access to help when you need it, but that eyes are always on your solution.

This support extends to regular software updates to accommodate everything from innovation to regulatory changes. Changes are incremental, fast, automatic, and frictionless, requiring little-to-no effort from customers. Unlike on-premise solutions that often require costly system downtimes to make updates and changes, SLAs prevent SaaS upgrades from being disruptive to customers. The importance of low system downtime cannot be overemphasized in the EAM space. Taking systems offline to conduct updates to on-premise solutions has significant risks, including production disruption, tangled signals between IoT devices, and reduced predictive maintenance reliability. While it's not impossible to safely make updates to an on-premise solution, it requires intensive advance planning and – often – expense.

It's also important to note that base EAM solutions don't always have the pre-built integrations necessary to manage facilities; APIs are needed to fill in those gaps. Because SaaS platforms "learn" and update based on customer needs, they typically include a full suite of APIs already created at other customers' request; when not available, they're usually easy to request and implement. Similarly, best practices are naturally built into solutions due to the number of organizations using the same platform. In addition to improving operational efficiency, this enables enterprises to gain access to value subject matter expertise without having to swap business cases or experiences with competitors.

Breaking Down On-premise and SaaS: **Operational Efficiency**

PARAMETERS	ON-PREMISE	SaaS/CLOUD
Scalability	Requires time and financial investments to reconfigure and make changes.	Customers can easily scale up or down as business needs/ the tech stack changes.
System upgrades	Often require system downtimes and requires investments in hardware and software infrastructure, and personnel/ consulting resources.	Fast and automatic, with little-to-no effort. SLAs usually guarantee a frictionless process for customers.
APIs	Added at the customer's discretion and expense.	Commonly used solutions are usually available on-demand via pre-built integrations. Can usually be added at a customer's request; time and cost will vary.
Best practices and SME support	Initiated at a customer's request. Usually includes consulting fees. Integrating best practices into the solution framework usually involves reconfiguration of the existing software.	Best practices are integrated directly into the software platform. Customers seeking additional consultation may require professional services beyond the contract scope.
Technical	Onus is usually on the customer to handle technical issues.	End-to-end support is intrinsic to the SaaS business model. SLAs require that technical issues are solved quickly.

Sustainability

Once considered "nice to have," sustainability initiatives are a necessity in today's market. Between increased regulatory scrutiny and stakeholder demands, sustainability is now at the core of many organizations' business operations strategies, with 58% of Fortune 500 companies striving to achieve net-zero goals by 2050 or sooner.[17] And a company's decision whether to select a SaaS or an on-premise EAM solution can have a significant impact on its ability to meet sustainability goals.

Purely based on numbers, cloud solutions are the clear front-runners to meet sustainability objectives. The amount of energy required to run on-premise data centers is significant, with recent research finding that more than half of all data center energy consumption stems from on-premise servers and data storage.[18] Microsoft Azure – the cloud provider that hosts TMA's SaaS solution – estimates that migrating to the cloud can be up to 98% more carbon efficient for an organization[19]; similarly, AWS touts that its infrastructure is up to 4.1 times more energy efficient than on-premise platforms.[20]

Azure by the numbers[21]

98%
more carbon efficient than on-premise platforms

93%
more energy efficient than on-premise

100%
powered by renewable energy by 2025

0 Waste
by 2030

Cloud providers' sustainability initiatives aren't driven purely by idealism and a commitment to the environment – they're hyper-scaling to meet emerging regulatory mandates, like the SEC's upcoming climate disclosure requirements.[22] And – as is the nature of SaaS – when one company benefits from an update, many benefit. By quickly delivering new processes, capabilities and tools that monitor and manage sustainability to customers demanding them, vendors are able to roll out sustainable to solutions to all customers, regardless of individual requirements.

This isn't to say that companies that must adhere to sustainability objectives can't achieve them with on-premise solutions – they just might need to work a little harder to get there. Organizations that pay close attention to the operating condition of solutions and stay on-top of equipment maintenance typically require less time and fewer replacement parts. In addition to reducing e-waste by prolonging the lifetime of hardware, but it can also optimize energy efficiency and, ultimately, result in a higher ROI.

It's also important to keep in mind that EAM software is in a unique position to promote sustainability across the enterprise, as it provides predictive maintenance information for assets across the enterprise. It stands to reason, therefore, that the more up-to-date and functional your EAM platform, the better you can maintain equipment throughout your facility. Not only does this prevent malfunctions and degradation, but it empowers enterprises with the data necessary to optimize energy consumption and reduce waste produced by replacing neglected machinery.

[17] Forbes. "Sustainability And SaaS: 3 Ways To Use Tech To Promote Sustainability." May 23, 2023.

[18] ComputerWeekly. "Hidden energy cost of on-premise data stores." November 23, 2022.

[19] Microsoft. "Sustainability outcomes and benefits for business." June 3, 2024.

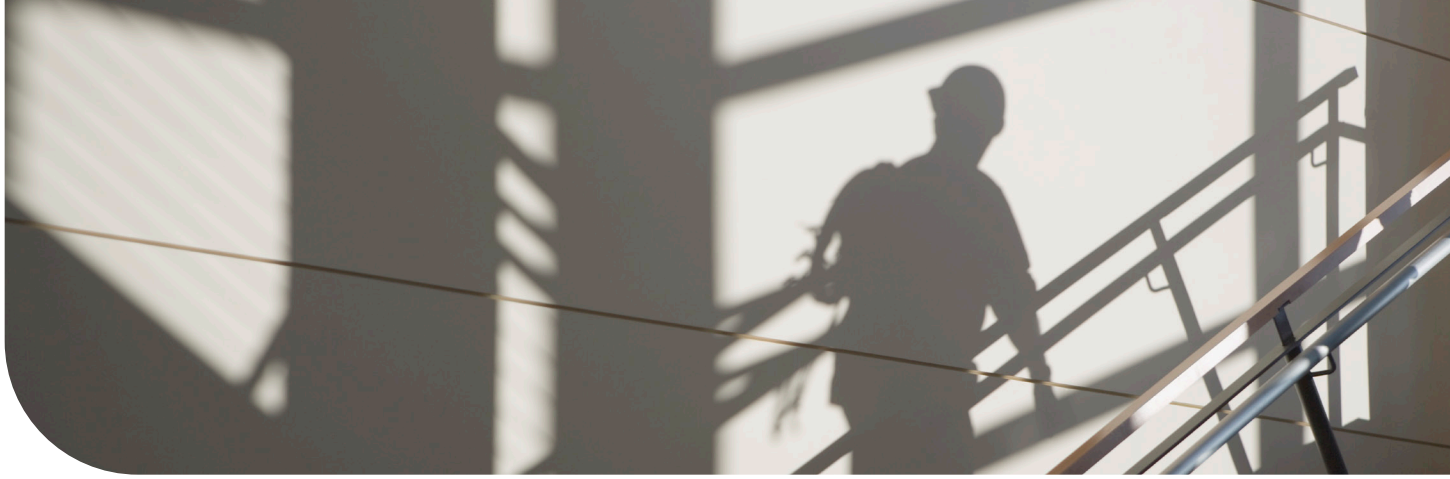
[20] Amazon. "The Cloud." 2024.

[21] Microsoft. "Sustainability outcomes and benefits for business." June 3, 2024.

[22] Forrester. "Predictions 2024: Enterprise Software. October 30, 2023."

Breaking Down On-premise and SaaS: **Sustainability**

PARAMETERS	ON-PREMISE	SaaS/CLOUD
Carbon/energy efficiency	Contingent on a company's individual requirements/ investments in sustainability.	Nearly 100% more carbon and energy efficient than most on-premise solutions.
Regulatory compliance	Varies by company. Depends upon the on-premise customer's preparedness.	Integrated into the technology.
Equipment maintenance and monitoring	Customers must keep software up-to-date to ensure effective monitoring and maintenance of all assets. Failing to do so can result in increased e-waste via equipment replacements instead of appropriate ongoing maintenance.	Automatic. Vendors frequently deliver new processes, capabilities and tools to monitor and manage sustainability.



Conclusion

There are several factors to examine when deciding whether a SaaS or on-premise EAM deployment is right for your organization – and there's often not a clear choice. This paper provides an overview to help steer you in the right direction, but it's important to consult with an SME who can dive deeper into the implications of selecting a solution. Each business case is different and working with a trusted EAM vendor to help align a solution to your enterprise's needs can streamline the selection process.

Reliable. Innovative. Trusted.

Empowering facilities management teams with powerful asset maintenance and management solutions

TMA Systems provides facilities and asset management solutions that can be easily configured to your needs (CMMS, EAM or IWMS). For more than 30 years, TMA has provided reliable, innovative, and trusted software solutions that help facility executives deliver value by reducing downtime, increasing maintenance productivity, improving equipment reliability, and saving money.

WebTMA, our flagship solution, provides all the functionality you need to manage and maintain your capital assets while optimizing maintenance team productivity.

Curious about which CMMS or EAM model best suits your organization's needs? Let us help you find the right fit.

Contact us at
sales@tmasystems.com

TMASYSTEMS
RELIABLE. INNOVATIVE. TRUSTED.