UNLOCKING THE GATE TO SAAS SECURITY

While there are many issues to consider when it comes to adopting software as a service (SaaS), the decision-making process passes through two primary decision points or *gates*. The first relates to financial preferences: CapEx or OpEx. CapEx means going with on-premises apps and their associated capital expenditures. OpEx means going with SaaS apps and their pay-as-you-go cost model.

The second gate is all about security. As organizations consider their evolution to an Autonomous Digital Enterprise, the future state of business, Adaptive Cybersecurity is a required tenet, and cloud can be an enabling technology, given its flexibility. To proceed through this gate, you need to thoroughly vet the SaaS provider to ensure that your business data receives the appropriate level of security for your organization. The compelling advantages of SaaS are enticing more and more organizations to overcome their concerns about cloud and approach this second gate.

Quite frankly, the security people in your organization hold the keys to the second gate. In many cases, they have the ability to delay or even stop a SaaS project in its tracks because of security concerns.

In this blog, I focus on that second gate and what it takes to unlock it.

THE SAAS SECURITY GATE HAS TWO CHECKPOINTS

To unlock and safely pass through the second gate, you need to clear two checkpoints: security control and data sovereignty.

Security Control

Security control requires adjusting to a new reality. With SaaS, you give up your control of security and place it in the hands of the SaaS vendor. The vendor is now in charge of security policy. The situation is analogous to *renting* a house versus *owning* it. When you own a house, you set the house rules. When you rent a house, the landlord sets them. The landlord may, for example, restrict the number of people who can occupy the house.

At this point, it's important to clear up a common misunderstanding. Some people mistakenly believe that by signing a SaaS provider contract, the customer organization is agreeing to comply with the same security policies that govern the vendor organization. However, the vendor's policies apply only to the vendor organization and not to the customer organization. For example, just because the vendor complies with the Payment Card Industry Data Security Standard (PCI DSS) doesn't mean the customer has to comply with it.

Data Sovereignty

With respect to data sovereignty, you need full knowledge as to where your data will be hosted, where it will be processed, and who will be accessing it. That sounds simple enough. However, it's extremely complicated because a SaaS vendor's data centers and personnel are typically scattered across various locations around the world. In this complex landscape, you need to make sure that:

- The data will be housed only within the areas allowed by your internal policies, industry standards, or government regulations.
- The data will be processed only within the areas allowed by your internal policies, industry standards, or government regulations.
- The data will be accessed only by the people who are authorized by your organization.

CLEARING THE CHECKPOINTS

Major security breaches are highly visible and they often have severe consequences. As a result, senior leaders typically give security people strong veto power over SaaS solutions. If you've made the OpEx decision to go to SaaS and you want to pass through the security gate with minimal friction, involve the security team right from the beginning. Doing so avoids costly surprises that can delay or even halt your SaaS adoption efforts.

Let's return for a moment to the own-versus-rent analogy. Before you sign a rental agreement, it's wise to scrutinize the terms to fully understand the landlord's rules. Likewise, before you sign up for a SaaS subscription, you need to examine the vendor contract and security policies so you know what level of protection you can expect. Your security people can serve as a valuable resource in this effort. They know precisely what to look for and can help you ask the right questions to ensure that your data or services won't be compromised.

The first thing to do is to ask the vendor for a list of the security standards with which the vendor complies. The standards worldwide are many, varied, and are based on geography and industry sector. The more prevalent ones are below:

- ISO 27001 (International Organization for Standardization) is a worldwide certification standard for information and cyber security.

- HIPAA (Health Insurance Portability and Accountability Act) is a U.S. law requiring the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.
- National Institute of Standards and Technology (NIST) is a cybersecurity policy framework of computer security guidance information.
- PCI DSS (Payment Card Industry Data Security Standard) is the information security standard for organizations that handle branded credit cards from the major card platforms.
- FedRAMP (Federal Risk and Management Program) is a cyber security risk management program for the purchase and use of cloud products and services by U.S. federal agencies. Government agencies may work only with cloud service providers that have gained FedRAMP approval.

You need to be sure that the vendor complies with all the security standards relevant to your situation and that the vendor's security policies meet your requirements. For example, you may require that all data be processed within a certain area or region, or that data be encrypted to a specific standard.

After reviewing the vendor contract, security standards compliance, and security policies, you will probably have questions. In this case, the security team can help you put together a questionnaire for the vendor. Many security teams have a questionnaire tailored to their organization's particular requirements. If not, a multitude of questionnaires and customizable questionnaire templates are available online.

PROCEEDING TO THE BENEFITS

Once you have cleared the checkpoints and passed through the security gate, you're ready to move ahead with your SaaS implementation. Soon you'll be enjoying the significant advantages of SaaS, which include seamless scalability and greater agility in meeting rapidly changing market requirements. Most important, you can proceed with confidence knowing that your data is secure.

If you need assistance with your transition to SaaS, please fill out our form and a BMC Customer Success expert will reach out to get started.