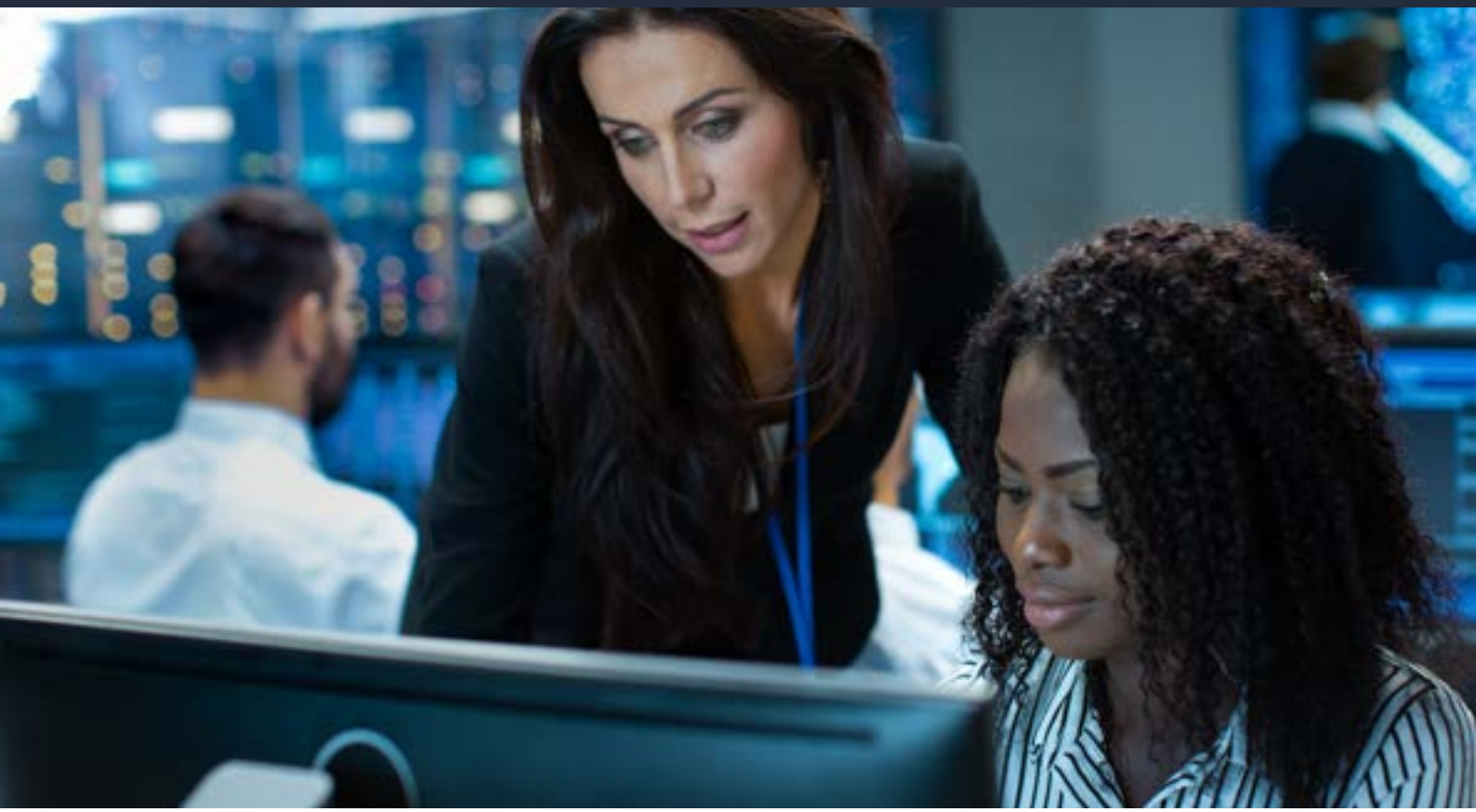
Security Guide

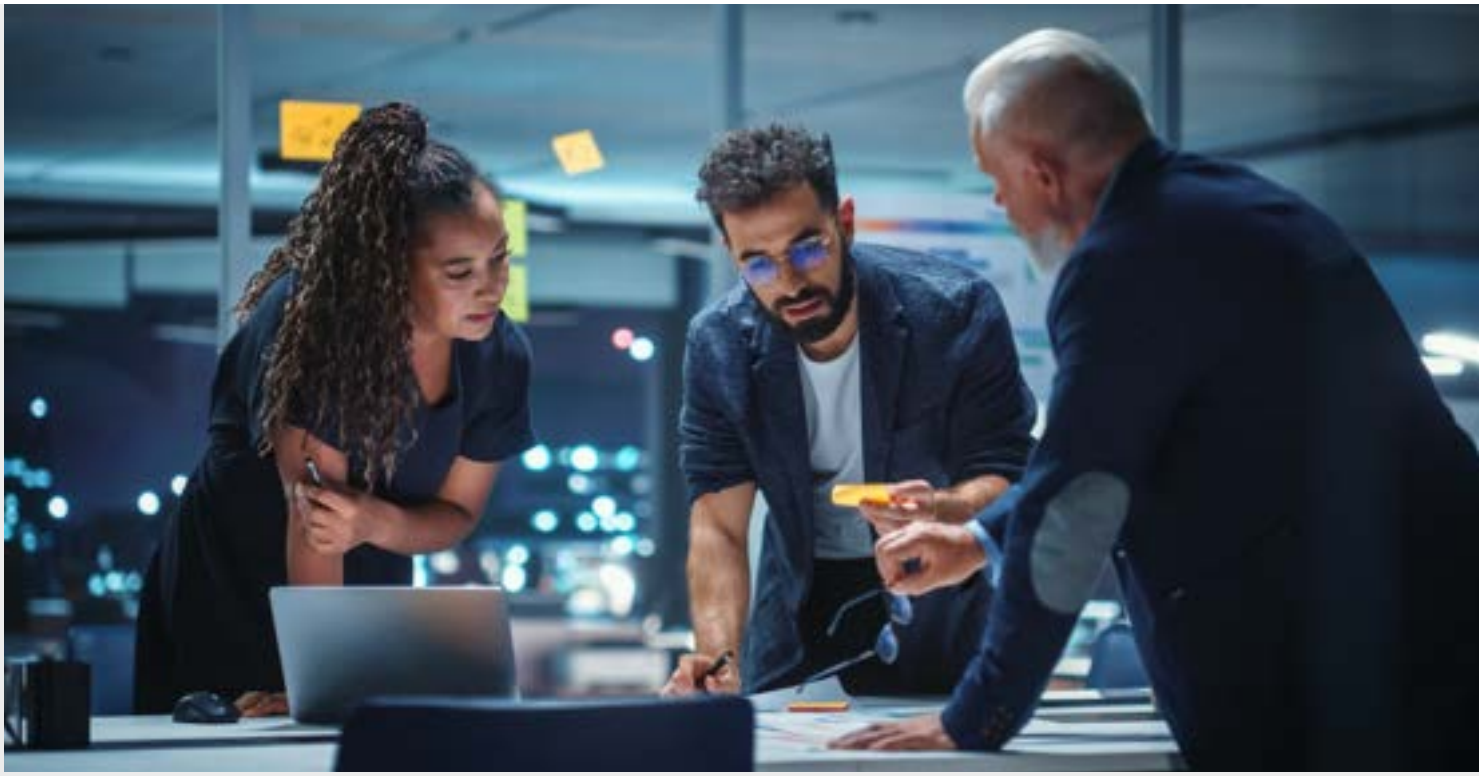
panintelligence
always thinking.



Security considerations when embedding third party applications into your SaaS environment.

With scarce development resources, more and more SaaS vendors are turning to third party vendors to provide the ancillary app such as payment gateways, subscription management, onboarding, and analytics & business intelligence. However, when it comes to embedding these applications, security becomes paramount.

For more on the reasons why SaaS vendors choose to embed third party applications check out our other guides "**Say good bye to your backlog**" and "**The Buyers Guide to Embedded Analytics**".



SaaS vendors place a strong emphasis on security, as they understand the importance of safeguarding their customers' data. A security breach can result in devastating consequences, including compromised data, loss of customer trust, financial loss, and reputational damage. To avoid these outcomes, SaaS vendors adopt a rigorous security approach to detect and mitigate potential threats to their systems and protect their customers' data.

When considering embedding a third-party application, SaaS vendors need to carefully evaluate the security measures in place to ensure that their customers' data remains secure.

SaaS vendors are looking to applications that can provide their customers with the assurance that their data is safe and always protected. This approach can help to maintain customer trust, confidence, and protect against the risks and consequences of security breaches.

This guide highlights key security areas SaaS vendors should consider when look at third party applications to embed.

The Three A's – Authentication, Authorization and APIs

This section covers the "Three A's" of Authorisation, Authentication and API. These three essential elements are crucial for achieving complete security integration with your SaaS application.

Authentication

Authentication is a critical process for SaaS vendors, as it involves verifying the identity of their users to ensure that they are authorized to access their systems or services. When embedding third-party apps, SaaS teams should prioritize solutions that integrate seamlessly into their existing authentication framework. As a result, third-party apps must provide multiple authentication models to meet the security standards of SaaS vendors and ensure a secure and smooth user experience.

When embedding third party applications always look for vendors who integrate with authentication models that align with your framework.

Authorisation

After authenticating your users, the next step is to control access to the features and data within your system. This is important when looking to embed third party applications as you will need them to adhere to the authorisation access model that you have deployed.

To achieve this, SaaS providers establish granular authorization policies that define the resources and data that users can access based on their role, group, or individual permissions. With a well-defined authorization model, you ensure that users only have access to the resources that they need to perform their tasks, minimizing the risk of unauthorized access or data breaches.

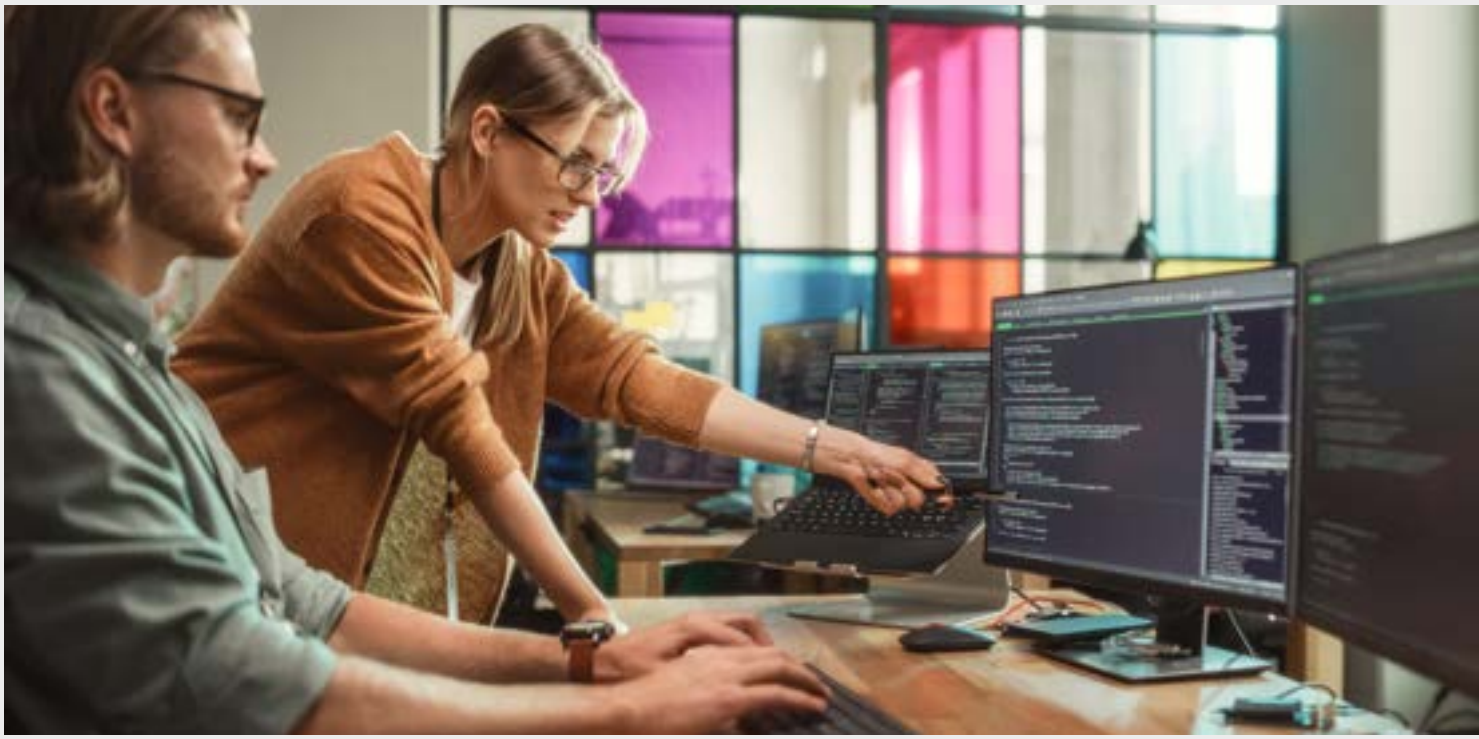
It is important when looking to embed third party applications as you will need them to adhere to the authorisation access model that you have deployed.

API

APIs offer a standardized approach for software applications to communicate with one another, providing a reliable and consistent method for data exchange. APIs allow third-party applications to be seamlessly integrated into other software applications, enabling data and functionality to be shared effortlessly between applications.

Accessing an API also provides developers with full control over their security needs, allowing them to implement custom security measures that align with their software application's specific requirements. This level of control is critical for ensuring that data is exchanged securely and confidentially between applications, especially for SaaS vendors who prioritize data protection and security.

When evaluating a vendor's security capabilities, it's essential to check whether they support an API. By supporting an API, a vendor demonstrates their commitment to security and their willingness to provide an easy and secure way to integrate their software application with other third-party applications. This level of integration can enhance the functionality of a SaaS vendor's application, improving the overall user experience while maintaining high levels of data protection and security.



Don’t move your data

In the current era of increasing high-profile data breaches, it is important for SaaS vendors to prioritize the security and sovereignty of their customers’ data.

This concern is heightened when embedding applications as certain vendors in this space require SaaS vendors’ data to be moved into their environments for processing. The transfer of data to external vendor environments raises significant concerns about data security and sovereignty. It is imperative that data quality and sovereignty are given utmost importance during the vendor selection process

When considering a potential vendor for your SaaS needs, it is essential to ask how they access and handle your data. In particular, it is important to understand whether they may need to move your data to another location, as this can have serious implications for the security and control of your data.

If a vendor does need to move your data, it is important to take this as a warning sign and carefully evaluate the reasons for doing so. While there may be legitimate reasons for moving data, such as for backup or disaster recovery purposes, it is generally more secure for your data to remain within your own domain and under your control.

About pi – secure embedded analytics and business intelligence built for SaaS

Panintelligence's "pi" platform was originally developed for the highly regulated and data-sensitive financial services industry, where security is of paramount importance.

This environment demands a rigorous approach to data protection, and the pi platform was purpose-built to meet these exacting security standards. With a range of advanced security features and capabilities, the platform provides a robust, secure, and reliable solution for organizations looking to safeguard their sensitive data.

Today, the pi platform is the leader in secure, embedded data analytics & business intelligence for SaaS vendors worldwide.

pi embeds seamlessly into your SaaS app to give you self-service dashboards, interactive reports, and predictive analytics. It easily embeds into your existing data stack, can be white-labelled using your own branding, is low code for you and no code for your customers, can manage multi-tenant environments with different visualisations without ever moving data from source.

pi also gives your customers the ability to set permission based restrictions, so app users only see the data that they need to, when they need it - delivering information through a business intelligence platform into the heart of your users' workflows.

Discover more about Secure Embedded Analytics

Book a discovery call with one of the team