SAAS SECURITY FOR BUSINESS 4.0

BIPO | Make Life Easier.

Introduction

Before the pandemic, disruptions in the workplace involved new technologies and their adoption. More than a year into the pandemic, businesses have faced a myriad of challenges – from disrupted labour markets, the increase in remote work, to the adoption of flexible workspaces amidst the need for safe distancing measures.

Industries such as Food & Beverage, Logistics and Tourism have pivoted to technology to solve pain points, and in the process transform their business through the use of digital tools, APPs and a combination of hybrid solutions comprising both online and offline platforms.

A recent survey by McKinsey conducted in April 2021 comprising 29,000 respondents surveyed across 24 countries, showed that the pandemic has driven the rapid adoption of digital channels, and that companies need to gain the trust of such new digital customers by providing excellent experiences.

BIPO | Make Life Easier.

Why Software as a Service (SaaS)

BIPO | Make Life Easier.

SaaS in the #NewNorm

The pandemic has accelerated digital transformation with companies now looking more seriously at adopting Software as a Service (SaaS) technologies.

Gartner estimates that SaaS remains the largest market segment with a growth of US$105 billion in 2020 alone. This is in conjunction with the continued shift from on-premises licence software to subscription-based SaaS modules brought about by the increased need for new software and collaborative tools during the pandemic.

What is SaaS?

- Put simply, SaaS refers to software that is available via a third-party over the internet, as a service.
- SaaS applications are also commonly referred to as web-based software, on-demand software or hosted software.
- Where traditional computer IT systems and software are hosted on-premise, SaaS applications are run on a SaaS provider's servers and can be used for almost all your business systems and processes.
- SaaS, PaaS and IaaS are ways to use cloud for your business.

When to Use SaaS?

Where SaaS was once considered exclusive to Enterprises, the technology has since levelled the playing field with many start-ups, SMEs taking advantage of the technologies, tools and capabilities that SaaS applications offer.

SaaS applications may be the most beneficial option in the following situations:

- Start-ups, SMEs or Enterprises that need to launch a software or application in a relatively short space of time and do not have time for server issues
- Projects that require fast, easy and affordable collaboration
- Applications that require web and mobile access (eg: HRMS platforms that facilitate Manager Self Service and/or Employee Self Service)

Cloud Solutions for Business 4.0

Type	Description	Example
IaaS (Infrastructure as a Service)	Cloud-based services, pay-as-you-go for services such as storage, networking, and visualisation	Amazon Web Service, Alibaba Cloud, Google Cloud Infrastructure, IBM Cloud
PaaS (Platform as a Service)	Hardware and software tools available over the internet	Amazon Elastic Beanstalk, SAP Cloud, Microsoft Azure, Google App Engine
SaaS (Software as a Service)	Software that is available via a third-party over the internet	Google Apps, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot, BIPO HRMS
On-Premises	Software installed in the same building as your business	Such software can be deployed on-premise within the user's data centre for businesses who want more control over their data
Private Cloud	Similar to on-premise installation, such software can be deployed on the user's private cloud, managed by the user	Remote access must be given to the vendor for software installed in this manner

Advantages of SaaS

- Relatively easy to configure and use
- No huge upfront costs
- Cost effective; predictability of costs
- Shortens the implementation time for projects
- Scalability and integration with other systems

- Easily customised, comparatively inexpensive although there are some limitations
- Upgrades are mostly included, not charged separately
- SaaS can be deployed without the involvement of the IT staff
- Automatic data backup
- Enhanced data security, many providers put in place stringent audit control measures
- Flexibility since users can easily access it via the internet
- Removes the need for complex software and hardware management

The Future of Work will see hybrid models of remote work being the new normal, with more businesses adopting SaaS tools to facilitate collaboration, engagement and the scaling up of self-service options for the workforce.

As large amounts of sensitive data can be accessed from any smart device by a mass of users, this poses a risk to privacy and sensitive information, including vulnerability to new malware and phishing attacks. The need for improved security and SaaS security tools that can secure cloud-based programs will play a big role in today's business landscape.

In simple terms, SaaS security are cloud-based security designed to protect the sensitive information that such applications carry due to its widespread use and ease of access.

What are the Potential Risks?

Passwords
Security lapses are one of the most prevalent causes, users recycling passwords or saving them to their systems. Because SaaS programs are hosted on the cloud, this makes them at risk to account takeovers.

Phishing
Businesses of all sizes, including those with robust IT procedures in places are regularly hit by phishing scams, ransom wear and other similar attacks.

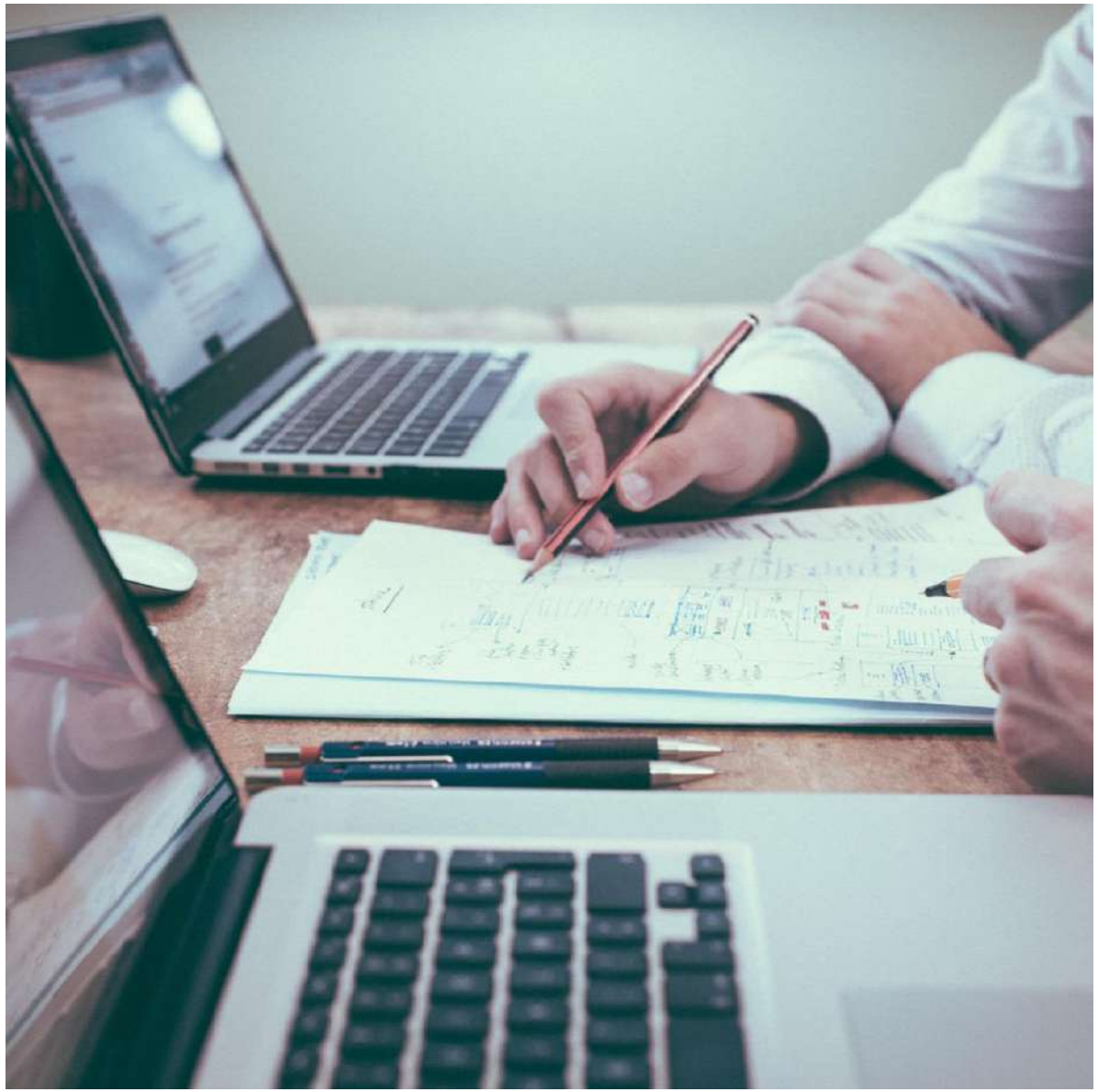
Cyber attacks
These have become increasingly rampant and more savvy in recent years as security systems race to keep up with the changes.

Ways to Mitigate Risks?

Vulnerability Assessment and Pen-Tests
To maintain network and application security, vulnerability assessments and third-party penetration testing must be conducted to identify and address new vulnerabilities. Assessments are done by an independent third-party IT security vendor.

Multi-layered Security
One of the more common methods to mitigate cyberattacks is the use of multi-layered security solutions. These are able to detect and “catch” such hacking and irregularities by using AI that can sense such malicious user activity and block potentially compromising access – at times as advanced as identifying the types of text patterns.

Web Application Protection
Third-application firewall protects websites from web application vulnerabilities. New threats are automatically added into the web firewall database, providing up-to-date protection.

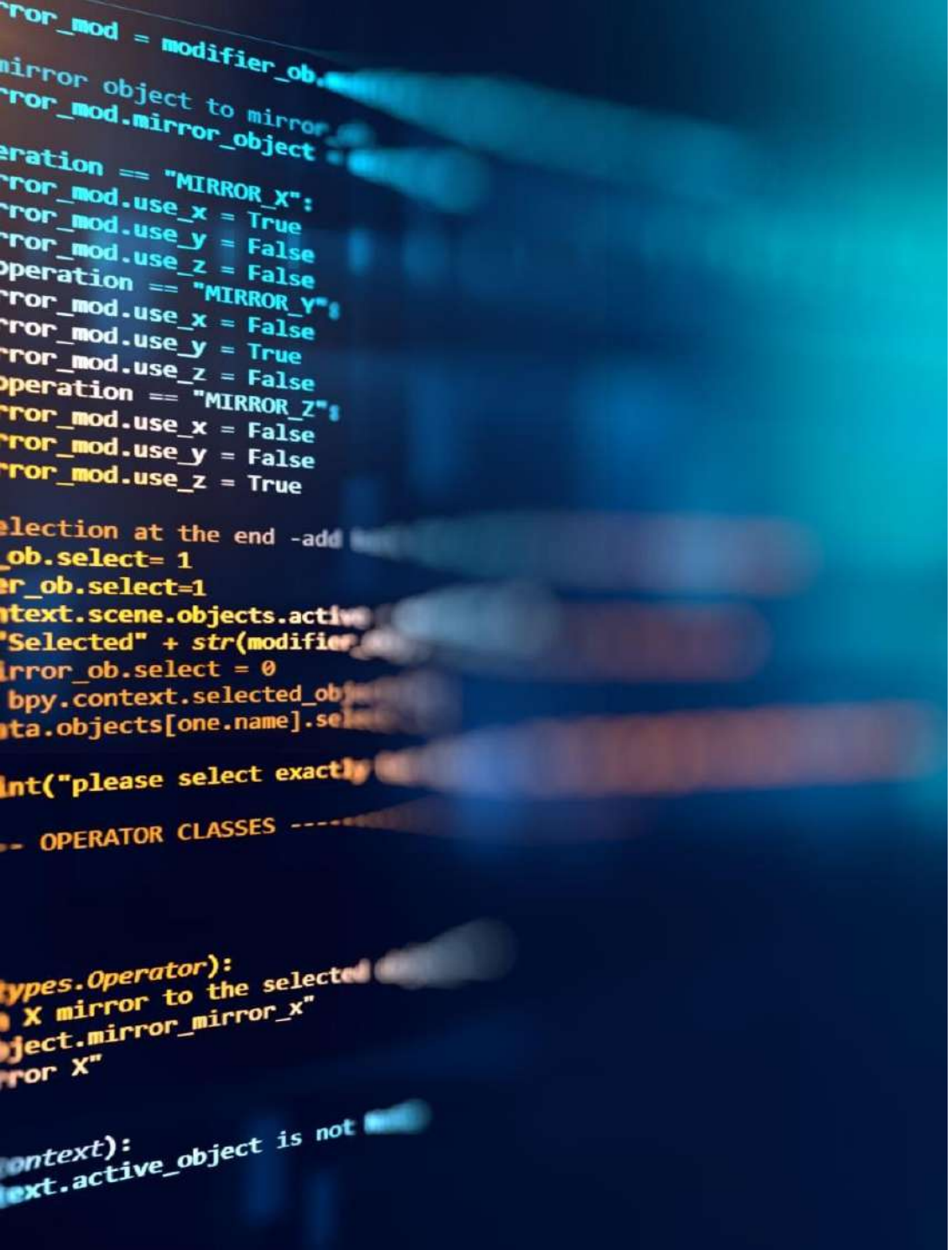


Ways to Mitigate Risks?

Vulnerabilities and Patches
Servers hosting SaaS applications should be patched against new vulnerabilities. Some commonly used examples include Microsoft for Windows Servers and Database Servers.

Public Cloud Infrastructure
Businesses should also consider if their SaaS applications should be hosted on public cloud infrastructures. It is important to choose reliable and reputable third-party vendors such as Amazon Web Services (AWS) and Alibaba Cloud that are well-regarded for their computing, storage and content processing capabilities, and robust practices that safeguard the security of their platforms.

Data that is hosted on such public cloud infrastructures will have their customer data reside in a shared-server model, and each customer database logically segregated from each other for enhanced security.



Ways to Mitigate Risks?

Application Security Control
Ideally, all user activity within the SaaS application should be logged in to the application activity log and data log. The **activity log** captures actions performed within the application while the **data log** captures information before and after changes. All users are IT Administrators who use individual login IDs with their activity logged for auditing and accountability purposes.

Data Security Control
Consider if user access to the SaaS application via the internet is secured by encryption using TLS (Transport Layer Security). This protects traffic from “eavesdropping” and the tampering of messages.

Traffic from the application server to the database should also be secured via encrypted connection for SQL Server instance. In addition, consider too if a secure FTP connection for users to upload data for data import is available, along with the option for data at rest encryption using SQL Server Transparent Data Encryption (TDE) is available.

Ways to Mitigate Risks?

Other considerations include

- Availability on the Web / Web API (Application Programming Interface)
- Audits – frequency, allowing qualified external third-party experts to conduct regular audits
- Back-up & Restore Options
- Server Architecture and High Availability Option Disaster Recovery

10 Best Practices in SaaS Security

1. Create a cloud applications security strategy. Often overlooked, businesses need to put in place a robust strategy for securing SaaS applications, data and access.

   This should also include any revisions in Personal Data Protection that govern the collection, use and disclosure of employee personal data connected with their employment.

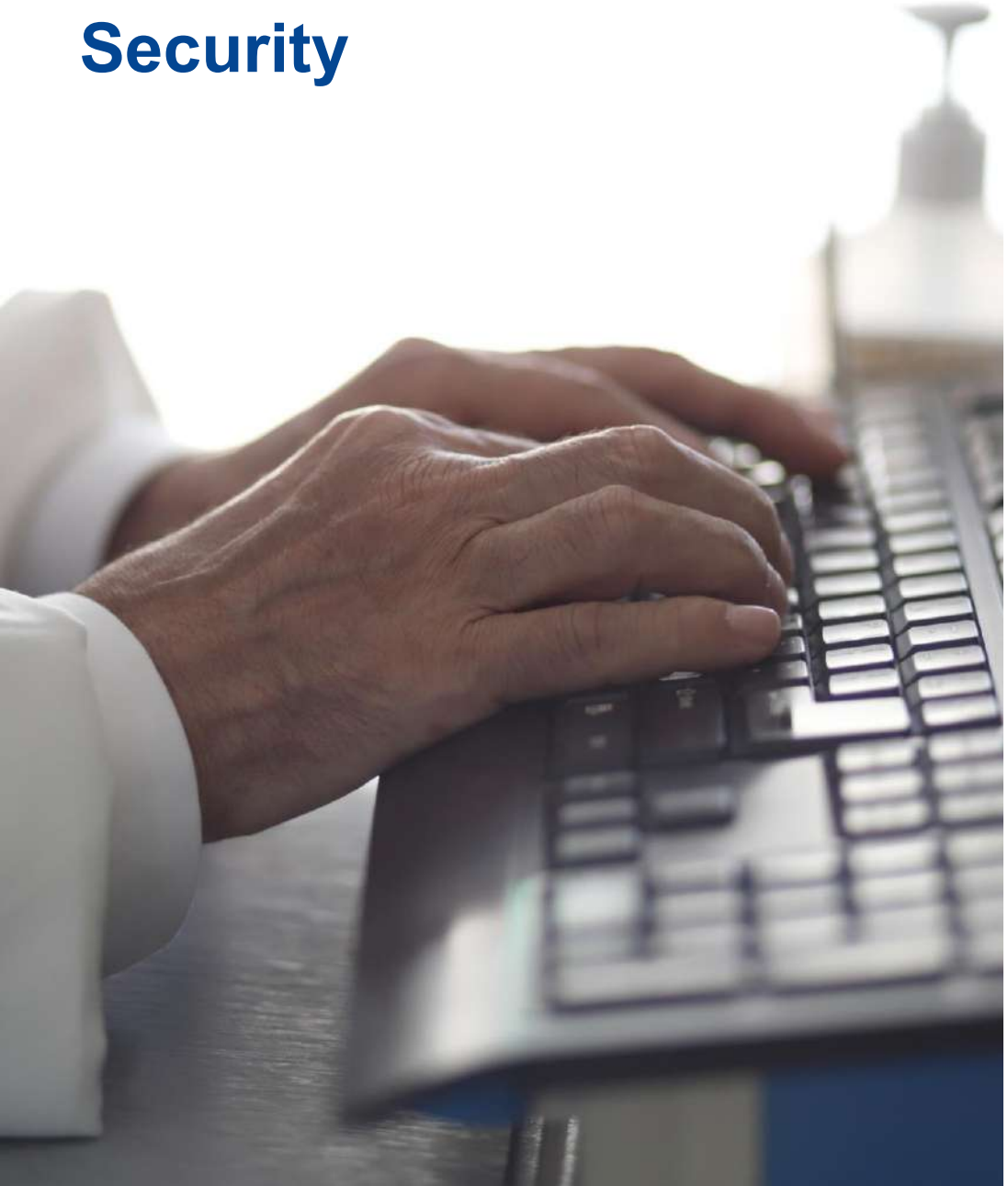
2. SaaS Providers' security certifications policies and compliance. Basic certifications include ISO-27001 Information Security Management, SOC-1/2, etc.

3. Ensure polices are in place for accessing SaaS – these must be created and managed at the organisation level.

4. Enable multi-factor authentication to ensure the safeguard against compromised credentials.

5. Allow privileged access management for administrative users. These should be maintained at the organisational level on a centralised location, ideally with the help of a Privileged Access Management (PAM) tool.

10 Best Practices in SaaS Security



6. Endpoint Security Consideration – access from devices such as smartphones, tablets, desktops, laptops and other mediums must be controlled to prevent misuse of SaaS and data loss prevention (DLP).

7. Ensure secured integration and data import with other applications. As SaaS applications require data import and integration with other systems via API, REST, Files, etc – it is important to ensure that the data from the source and target systems reside in a secure environment so that infected data will not make the SaaS environment vulnerable.

8. Ensure data-encryption for back-up and archival – SaaS databases must be classified and encrypted to the level of the user needs. In addition, data in the lower SaaS environments must be equally secure.

10 Best Practices in SaaS Security

9. Ensure that sensitive databases are protected with periodic back-ups and disk volume snapshots. Back-ups should be store off-site in a highly durable environment (e.g. AWS, Alibaba Cloud OSS storage).

   Back-up files must be encrypted and accessible to users with credentials protection using MFA. Regular restoration testing to ensure back-ups can be successfully restored must be conducted.

10. Continue training and education. SaaS security is critical at all levels within the organisation, to ensure understanding of SaaS usage and security. Prevention through education is often the most effective way to prevent breaches.

Conclusion

BIPO | Make Life Easier.

Conclusion

SaaS security starts with the users of the application. This is equally as important as putting in place robust security solutions to protect your SaaS environment.

When selecting a SaaS application vendor, do ensure they have robust policies in place covering security, cyber threats and disaster recovery efforts. Ensure that the relevant accredited certifications are in place, including regular external audits and penetration testing. It is critical that minimum standards and best practices are in place.

Allowing external experts access to your cloud identity impact should also be considered. Such experts can help to spot misconfigurations and risky privileges, warn about weaknesses of the ecosystem and possible remedies. They may improve the overall security of your ecosystem and help you implement a Segregation of Duties (SoD) and Least-Privilege permissions model in your organization.

Remember, the security of the organisation’s data is everyone’s responsibility.

About BIPO

Established in 2004, and headquartered in Singapore, we are better connected to support your payroll and people solutions needs through a global network of 27+ offices, four R&D centres, and business partners across 100+ countries.

Our enterprise-ready **HR Management System (HRMS)** platform automates HR processes, simplifies workflows, and delivers actionable insights to build the best Employee Experience. Complemented by our **payroll outsourcing solutions** and **global PEO services,** we support businesses to manage today's global workforce.

Contact Us

www.biposervice.com

www.facebook.com/biposvc

linked.in/company/bipo-svc

hello@biposervice.com

BIPO | Make Life Easier.