**What is Software-as-a-Service (SaaS) Security (in Cloud)?**

SaaS securityrefers to the practices and policies implemented by the providers of software-as-a-service (SaaS) to ensure the privacy and security of customer data in cloud-based applications and other information assets. These security policies make SaaS apps safe and trustworthy.

## **What makes SaaS applications risky?**

### **1. Virtualization**

Cloud computing systems run on virtual servers to store and manage multiple accounts and machines, unlike traditional networking systems. In such a case, if even a single server is compromised it could put multiple stakeholders at risk. Though virtualization technology has improved significantly over time, it still poses vulnerabilities that are often easy targets for cybercriminals. When properly configured and implemented with strict security protocols, it can provide significant protection from numerous threats.

### **2. Managing identity**

Many SaaS providers allow for [Single Sign-on (SSO)](https://auth0.com/docs/sso) abilities to greatly ease access to applications. This is most helpful when there are multiple SaaS applications and access is role-based. Some of the providers do have secure data access systems, however, with an increase in the number of applications, it becomes quite complicated and difficult to manage securely.

### **3. Standards for cloud services**

SaaS security can greatly vary based on the provider and the standards maintained by them. Not all SaaS providers conform to globally accepted SaaS security standards. Even those providers which claim to be compliant might not have SaaS-specific certification. Standards such as [ISO 27001](https://www.getastra.com/blog/security-audit/website-security-audit-testing-in-india/#ISO27001) can offer a certain level of confidence; however, if not carefully evaluated they might not have all security avenues covered under the certification.

### **4. Obscurity**

Most of the time customers are not aware of the processes handled by the SaaS service provider. If a SaaS provider tries to be too obscure about the backend details, consider it a red flag. To be completely confident regarding SaaS security the customers must know in detail how everything works.

Most popular SaaS providers are transparent about their backend processes; however, several providers may not disclose details such as their security protocols and multi-tenant infrastructure. In such cases, [Service Level Agreements (SLA)](https://en.wikipedia.org/wiki/Service-level_agreement) are useful since it compels the provider to disclose all responsibilities. After all, customers have a right to know how their data is protected against cyber-attacks and information exposure among other SaaS risks.

### **5. Data location**

SaaS tools might store clients’ data in some other geographical region, but not all providers can promise that due to several factors such as data laws and cost. Sometimes clients would be comfortable with their data being stored within their country. Data location should also be based on factors such as data latency and load balancing.

### **6. Access from anywhere**

SaaS apps can be accessed from anywhere and that is one of the reasons which makes them more appealing. However, this feature has its own set of risks. Incidents such as accessing the application using an infected mobile device or public WiFi without any [VPN](https://www.getastra.com/blog/knowledge-base/why-you-should-invest-in-vpn/) would compromise the server. If the endpoints are not secure it would allow attackers to enter the server.

### **7. Data control**

Since all data will be hosted on the cloud, clients do not have complete control over it. If something goes wrong, clients are at the mercy of the [SaaS provider](https://www.getastra.com/blog/security-audit/saas-security-management/). Once agreeing to a price model, the provider becomes responsible for storing and managing data. In such cases, clients often worry about who has access to it, scenarios of data corruption, and access by third parties and competitors, to name a few. When sensitive data is stored, answers to these queries become

## **Best SaaS Security Practices**

No system is safe and as we saw above, SaaS offerings also have security concerns that need to be resolved. By following the below security practices, you can leverage the powerful features and advantages of SaaS without worrying about security.

### **1. End-to-end data encryption**

This means that all kinds of interaction between server and user happens over SSL connections and are encrypted. However, end-to-end encryption should also exist for data storage. Many providers have the option to encrypt the data by default, while some clients need to explicitly specify this. Clients can also have the option to encrypt specific fields such as financial details by using Multi-domain SSL certificates.

### **2. Vulnerability testing**

You can expect SaaS providers to make high claims regarding SaaS security. But the onus to verify these claims can end up with the clients. If the SaaS provider has tools or checks, they should be reliable and meets all standards. Apart from these, you should also ensure that intensive checks are done on the SaaS systems.

There are multiple ways to assess SaaS security, such as automated tools or manually by security experts. A comprehensive SaaS security check should comprise both automated and manual checks since it would also consider real-world scenarios and the latest threats. A number of quality [SaaS security solutions](https://www.getastra.com/blog/security-audit/saas-security-solutions/) are available to help you with the security testing process.

### **3. Policies for data deletion**

Data deletion policies play an important role in keeping customers’ data safe. SaaS providers should be clear in declaring their data deletion policies to their clients. These policies are mentioned in the service agreement and should include what would happen after the customer’s data retention timeline ends. When applicable, client data should be programmatically deleted from the server and respective logs should be generated.

### **4. Data security at the user level**

Multiple levels of SaaS security can limit the damage from cyber-attacks. At the user level, security protocols such as role-based permissions and access, and enforced distribution of tasks, will protect your system from attacks that leverage internal security gaps.

### **5. Virtual Private Network/Virtual Private Cloud**

VPN and VPC provide a safe environment for clients for their operation and data storage. These are better options and more secure than multi-tenant systems. These also enable users to log in and use SaaS applications from anywhere by securing endpoints and protecting the infrastructure.

### **6. Virtual Machine Management**

Your virtual machine needs to be updated regularly to maintain a secure infrastructure. Keep up with the latest threats and patches on the market and deploy them timely to protect your VM.

### **7. Scalability & Reliability**

SaaS offers great scalability (both vertical as well as horizontal) & reliability features. You have the benefit of adding a new enhanced feature or additional resources as per your wish. Scaling cannot be realized instantly, thus the vendor must put together a plan for horizontal redundancy. A CDN (Content delivery network) adds more robustness to scaling.

### **8. Transport Layer Security and configuration certificates**

SaaS security is greatly enhanced when a provider protects externally transmitted data using Transport Layer Security. Moreover, TLS also improves privacy between communicating applications and users. Make sure that the certificates are appropriately configured and follow security protocols. The same applies to internal data too. Internal data should also be stored in an encrypted format and any intra-application transfer should be protected. Further, [cookie security](https://www.getastra.com/blog/knowledge-base/ways-to-prevent-cookie-stealing/) should be looked into as well.

### **9. User privileges and multi-factor authentication**

Different categories of users should have different levels of privileges. Cybercriminals often misuse privileges to access the core files of an application. Admins should have exclusive access to crucial files and folders. Also, authentication is a major point of entry for attackers. 2 Factor Authentication is the new standard for logging into applications. Make sure the SaaS application adheres to this custom.

### **10. Logs**

Logs help in monitoring SaaS security incidents and help in detecting any cyber attacks. SaaS systems should have automatic logging mechanisms which should be available to clients to assist in audits or regular monitoring.

### **11. Data Loss Prevention**

Data Loss Prevention (DLP) consists of two parts, detection, and action. DLP systems can scan outgoing or transferred data for sensitive information through keyword and phrase searches. Once detected, data transfer is blocked preventing any leakage. For a robust system, the DLP system can send alerts to the administrator who verifies if the detection is correct. There are also SaaS APIs that enforce DLP protocols in your application.

### **12. Deployment security**

Deployment can be either done on public cloud services or a SaaS vendor. In case you decide to self-deploy your SaaS application then you need to test the security thoroughly and adopt enough safeguards to protect your application against cyber attacks.

Most of the big cloud providers take care of all your SaaS security needs, however, when opting for a public cloud vendor, make sure that they follow all globally accepted standards. Asking for a pentest report while making a vendor assessment is fair play on your part.

### **13. Be updated about OWASP security issues**

Open Web Application Security Project® (OWASP)

Whenever testing your SaaS security, always keep an eye out for the top security issues reported by [OWASP](https://owasp.org/www-project-top-ten/). This provides a trusted repository for the latest security issues found and probable fixes. Based on this you can design your tests that can discover security vulnerabilities in your SaaS application. Also, this provides you with enough information to fix these issues and protect against attacks that exploit these.

## **Conclusion**

There are several reasons why a business should adopt SaaS, however, SaaS security concerns can hold them back a lot of times. These concerns arise from the lack of proper understanding of SaaS security protocols and controls. The above points provide a guideline on what to expect from a SaaS provider and [SaaS security assessments](https://www.getastra.com/blog/security-audit/saas-security-assessment).

At Astra Security, we have [SaaS security audits](https://www.getastra.com/blog/security-audit/how-to-conduct-saas-security-audit/) that combine the use of automated and manual testing to find security vulnerabilities. Astra also provides a comprehensive report of all findings and solutions along with step-by-step guidelines for the developers.