SAAS SECURITY UNMASKED

Hidden Risks You Might Overlook

Smart SaaS™

Copyright © 2025 by SS Certification Association | All rights reserved.

IN THIS EBOOK

INTRODUCTION

SaaS Security Unmasked 3

PART 1

What is SaaS Security? 4

Three A's of Security 5

Authentication 6

Authorization 8

Accounting 10

PART 2

SaaS Security Risk Factors 12

Shared Responsibility Model of SaaS 13

SaaS Provider Primary Responsibilities 14

Your Primary Responsibilities as a Customer 15

PART 3

6 Signs of Strong SaaS Security 16

Conclusion 17

VISIT US AT

SMARTSAAS.WORKS

Copyright © 2025 by SS Certification Association | All rights reserved.

INTRODUCTION

SAAS SECURITY UNMASKED

Software-as-a-service (SaaS) solutions almost universally make the same promise: “We’ll take care of the technology so you can focus on running your business.”

You don’t have to worry about installation or upgrades, data centers, storage, or hardware. SaaS providers have you covered.

While that may be true for many aspects of software maintenance and costs, it is not necessarily true for SaaS security. SaaS buyers must be savvy about assessing and choosing platforms from a security perspective.

This guide provides insights into security terminology, approaches, and the top issues to consider when evaluating SaaS platforms.

90%

OF COMPANIES HAVE EXPERIENCED ONE OR MORE CYBERSECURITY BREACH.

SOURCE: VERTICE

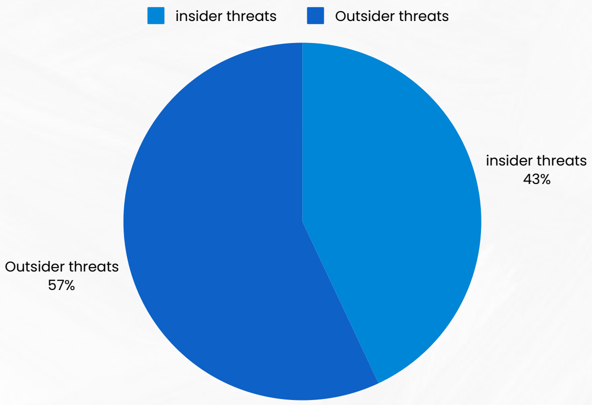
Copyright © 2025 by SS Certification Association | All rights reserved.

PART 1

WHAT IS SAAS SECURITY?

SaaS security encompasses the people, processes, practices. technology, and tools needed to safeguard data stored and accessed via SaaS applications.

Many people equate SaaS security with combatting cyber attacks. And yes, that's a significant component. But keep in mind that security threats can come from internal sources (e.g., employees) and external sources (e.g., hackers or even your SaaS provider's employees). They can be malicious (e.g., intentionally stealing information) or due to human error (e.g., accidentally sharing or deleting important data).



43% OF CYBERSECURITY BREACHES ARE BECAUSE OF INSIDER THREATS, BOTH ACCIDENTAL AND INTENTIONAL.

SOURCE: I.S. PARTNERS

Copyright © 2025 by SS Certification Association | All rights reserved.

THREE A’S OF SECURITY

Any discussion about software security should begin with authentication, authorization, and accounting, also known as the three A’s of security. These concepts represent a security framework for controlling and tracking user access to networks, computers, data, and applications.

In the context of this eBook, we’ll concentrate on how these principles apply to SaaS and why they’re vital to you as a SaaS buyer.

95% **OF CYBERSECURITY ISSUES HAVE SOME HUMAN ELEMENT.**

SOURCE: I.S. PARTNERS

Copyright © 2025 by SS Certification Association | All rights reserved.

AUTHENTICATION

Authentication focuses on verifying users' identity and confirming that they are who they say they are. When a user attempts to access the software, the platform compares the credentials entered with what's stored in the database. If they match, the user is granted entry. If the authentication fails, the user is denied access.

A traditional and common authentication method is to require a username and password to sign in. Other examples include:

- **Social Logins:** Relies on credentials from other well-known platforms, such as Google, Facebook, or LinkedIn, providing seamless sign-on and authentication.
- **Single Sign-On (SSO):** Allows users to access multiple SaaS applications with a single set of credentials, simplifying login and enhancing security.
- **Multi-Factor Authentication (MFA):** Enhances security by requiring multiple forms of verification, such as a password plus a code sent to the user's phone or through a mobile authentication app like Authy or Google Authenticator.
- **Biometrics:** Uses unique biological characteristics like fingerprints or facial recognition for authentication.
- **Magic Links:** Sends a unique link to the user's email to access the application, eliminating the need for passwords.

Copyright © 2025 by SS Certification Association | All rights reserved.

WHY IT'S IMPORTANT?

Authentication is one of your first defenses to keep unauthorized people or processes (e.g., executing an SQL query or API call) from accessing your applications and data. Cybercriminals often use phishing campaigns and other approaches to trick users into revealing their login credentials. Once in, bad actors can wreak havoc on your systems and gain access to sensitive, confidential information.

WHAT TO WATCH FOR?

Look for SaaS providers that arm you with robust authentication functionality, including strong password policies with complex requirements and expiration rules prompting users to change passwords regularly. SSO and MFA are critical for applications that house sensitive data. Many SaaS vendors paywall these security options and only offer them in their higher-priced tiers bundled with other features you might not need. The reality is that once software companies build SSO, there's no additional cost to them to provide you access. Don't get SaaS'd™ by their attempts to gain more wallet share.

31% **OF CLOUD DATA BREACHES IN 2024 WERE DUE TO APPLICATION SECURITY MISCONFIGURATIONS OR HUMAN ERROR.**

SOURCE: I.S. PARTNERS

Copyright © 2025 by SS Certification Association | All rights reserved.

AUTHORIZATION

While authentication and authorization are often used interchangeably, they are distinct functions. Authorization builds on authentication by ensuring that authenticated users (or processes) have been granted permission to perform a specific action or access a particular resource or dataset. In short, authorization dictates what users can see and do within an application.

Authorization control mechanisms include:

- **Role-Based Access Control (RBAC):** You assign different roles to users (e.g., administrator, editor, viewer) and grant permissions based on those roles.
- **Attribute-Based Access Control (ABAC):** You grant access based on various attributes, such as user attributes (e.g., location, department), resource attributes (e.g., data sensitivity, file type), and environmental attributes (e.g., time of day, network location).
- **Fine-grained Access Control:** You implement granular permission levels to provide precise access to parts of the application or data.

61% OF SENSITIVE DATA IS STORED IN THE CLOUD BY ORGANIZATIONS, ON AVERAGE.

SOURCE: SKYHIGH SECURITY

Copyright © 2025 by SS Certification Association | All rights reserved.

WHY IT'S IMPORTANT?

The importance of authorization controls depends on the type of application and the type of data it houses. Regulatory requirements are often a significant factor here. For example, the healthcare industry has strict patient privacy rules—Health Insurance Portability and Accountability Act (HIPAA)—that limit who can access medical records and other patient information. The banking and financial industry is another example. Given the sensitivity of the information (e.g., account numbers, balances) and the propensity for bad actors to go after it, these companies must comply with strict controls over who can see what records, including the need to mask data points on screens.

Beyond security concerns, authorization controls can improve productivity. Limiting employees' access to only the features and data they need to do their jobs removes clutter and makes it easier for them to work efficiently.

WHAT TO WATCH FOR?

Authorization controls are often a differentiator for medium and large enterprises evaluating SaaS solutions. Bigger companies frequently have bigger needs for authorization granularity. But business size doesn't always matter. If you're a healthcare provider, it doesn't matter whether you're a single-doctor practice or a national hospital network; you still need HIPAA-compliant software. Smart SaaS™ providers recognize this and don't nickel and dime you for table-stakes security requirements.

Copyright © 2025 by SS Certification Association | All rights reserved.

ACCOUNTING

Accounting focuses on tracking and logging user activity within a SaaS application.

Common accounting functionality includes:

- **Audit Logs:** They capture and maintain records of user actions, including login attempts, data access, and system modifications.
- **Access Monitoring:** Designed to track and monitor user access patterns to identify unusual or suspicious activity that might indicate unauthorized access or security breaches.
- **Compliance Reporting:** Used to build reports on user activity to meet compliance requirements and demonstrate adherence to security standards.
- **Billing and Usage Tracking:** These features play a key role in understanding usage for billing purposes, as many SaaS models include limits based on the number of users, transaction volumes, API calls, etc.

80% **OF BUSINESSES HAVE EXPERIENCED DATA THEFT.**

SOURCE: SKYHIGH SECURITY

Copyright © 2025 by SS Certification Association | All rights reserved.

WHY IT'S IMPORTANT?

The types of accounting measures you need from a SaaS provider depend on the type of application, the data it houses, and related regulatory requirements. From a security perspective, good accounting security protocols can provide valuable insights into user activity, identify misuse, and uncover other threats.

Additionally, understanding usage by individuals and user groups can help you address resource and capacity issues, allocate costs appropriately across departments, and avoid potential upcharges in SaaS vendor contracts.

WHAT TO WATCH FOR?

If you're in an industry that requires detailed audit logs and audit trails for security investigations and compliance audits, spend time with potential SaaS vendors to understand their ability to track and provide standard reports you'll need if regulators knock on your door. Also, get clarity on how they charge for these features.

This is an area in which software providers have actual additional costs associated with data storage, which they understandably pass on to customers. Capturing and storing detailed logs of user activities can add up quickly. Finally, if a SaaS provider has upcharges based on usage, make sure they give you the tools and alerts you need to manage that process so you're not caught off guard with a budget-busting invoice.

Copyright © 2025 by SS Certification Association | All rights reserved.

PART 2

SAAS SECURITY RISK FACTORS

Different software decisions present different exposure levels—legally, financially, and operationally. As you evaluate SaaS solutions from a security perspective, ask yourself questions like:

- How much damage could occur if you had a data breach with this solution?
- What regulations do I need to keep in mind for this type of software and data (e.g., HIPAA for healthcare data, GDPR for personal data)?
- What are the financial or operational consequences of picking a solution without the appropriate security controls?

Here are key factors to remember when assessing your risks and needs for different security protocols.

Security Risk Factor	Lower Risk	Medium Risk	Higher Risk
Size of Business	Small	Mid-sized	Enterprise
Business Type	Unregulated	Moderately regulated	Highly regulated
Scope of Software	Individual	Inter-department	Enterprise-wide
Software Connectivity	Stand-alone app	Some integrations	Many app connections
Type of Data	Public	Internal	Highly sensitive
Quantity of Data	Minimal	Moderate	High-volume

Copyright © 2025 by SS Certification Association | All rights reserved.

SHARED RESPONSIBILITY MODEL OF SAAS

The shared responsibility model in SaaS security outlines the responsibilities that both a SaaS provider and you, its customer, need to do to ensure security within and around the application's environment. This framework is designed to clarify who is accountable for securing which aspects of the platform and the data housed inside.

Copyright © 2025 by SS Certification Association | All rights reserved.

SAAS PROVIDER PRIMARY RESPONSIBILITIES

- **Infrastructure and Platform Security:** This includes securing the underlying infrastructure (servers, networks, data centers) and the platform itself. The goal is proactively identifying and protecting against vulnerabilities that could impact reliability, data integrity, etc.
- **Security Updates and Patches:** The provider is responsible for regularly updating and patching its network and the platform to address vulnerabilities and maintain a secure environment.
- **Physical Security:** This includes the physical security of data centers and infrastructure and having redundancies and backups in place in case of a breach or failure.
- **Data Center Security:** This includes security measures like firewalls, intrusion detection systems, and other security controls to protect the platform from external threats.
-

Copyright © 2025 by SS Certification Association | All rights reserved.

YOUR PRIMARY RESPONSIBILITIES AS A CUSTOMER

- **Data Encryption:** This can get tricky because data encryption includes "at rest" (data stored on a device or in the cloud) and "in transit" (protecting data as it's transferred between locations). Virtual private networks (VPNs), Transport Layer Security/Secure Sockets Layer (TSL/SSL), and HTTPs can all be used to secure data transmitted between you and your SaaS vendor. Ensuring these protocols, encryption keys, etc., are in place often falls on the customer's shoulders.
- **Security Configuration:** This encompasses implementing security settings within your SaaS environment, such as SSO or MFA, customizing security settings, and implementing data-retention policies.
- **User Access Management:** This includes ensuring only authorized individuals can access data and functionalities, such as managing role-based access controls and adhering to the principle of least privilege.
- **Compliance:** SaaS platforms may offer functionality to aid with meeting legal and regulatory requirements, but you're ultimately responsible for ensuring employees comply with company policies and regulatory standards.
- **Data Backup and Recovery:** All companies need plans and strategies for handling data loss in the event of outages, accidental deletion, corruption, or malicious attacks. Many SaaS providers recommend that customers use third-party backup solutions to ensure complete control and flexibility over their data backups.

Copyright © 2025 by SS Certification Association | All rights reserved.

PART 3

6 SIGNS OF STRONG SAAS SECURITY

SaaS security encompasses a wide range of topics and issues. We've covered many in this guide, and there are many more. As you compare SaaS vendors, here are six signs a SaaS provider takes security seriously.

1. **Table-Stakes Security Functionality:** SaaS vendors that lock SSO and similar features behind a paywall are focused more on wallet share than your security. Seek out providers with essential security functionality built into your plan.
2. **Security Certifications:** Look for proof of compliance with industry standards like SOC 2, ISO 27001, or GDPR, which demonstrate a commitment to best practices.
3. **Regular Security Checks:** Inquire about the frequency and scope of penetration testing, vulnerability scans, and other assessments. Look for a proactive approach designed to protect customers.
4. **Vendor Assessments:** Like you, your SaaS providers rely on third parties for many business needs. Explore what companies they work with for networks, storage, security, and related services. What requirements do they have in place for those vendors?
5. **Security Transparency:** How does the vendor communicate about security incidents and breaches? What are their protocols for fixing these issues and transparently sharing that information?
6. **Robust Internal Controls:** Signing up with a SaaS vendor means you've immediately raised your business's risk profile because some or all of their employees potentially have access to your data. Ask about their access controls, security training, monitoring and other protocols they have in place internally.

Copyright © 2025 by SS Certification Association | All rights reserved.

SAAS SECURITY UNMASKED: CONCLUSION

As you can see, many SaaS security issues overlap in purpose and scope, and it can often be unclear who is responsible for them—you or the software vendor. That's why it's critical to find a SaaS provider that treats you as a partner with a shared interest in addressing your security wants, needs, and priorities.

> ***True SaaS security isn't just about compliance—it's about partnership. Choose a provider that shares your priorities, not just your data.***

If you're ready to take control of your SaaS strategy, explore our expert insights and industry-leading guides. Download our free ebooks—Escape the SaaS Trap™, SaaS Spending 101™, and Don't Get SaaS'd™—to make informed decisions about security, pricing, and vendor relationships. Visit our website to learn more, access exclusive content, and ensure your business stays ahead of the SaaS curve.

Your smarter SaaS strategy starts here.

Join the Conversation

Follow us

Check Out Additional Resources

Copyright © 2025 by SS Certification Association | All rights reserved.