SaaS Security Checklist: Best Practices To Protect Your Company



One of the most powerful and enduring changes digital transformation has brought to the modern business environment is software as a service (SaaS) applications. Serving up software you need to handle your most important business processes without the need for massive investment in localized IT resources or infrastructure, SaaS leverages cloud computing to help you create an integrated and (ideally) secure software environment from diverse sources.

But not all SaaS solutions—or security standards—are created equal, and every SaaS provider you choose should meet rigorous security requirements to help protect sensitive data from data breaches and account takeovers, ensure secure access control, and provide real-time measures that ensure end users have a positive, safe, and productive experience. If you're not sure about your organization's approach to cybersecurity, or simply want a reliable way to ensure it's up to snuff for the applications you rely on, following a SaaS security checklist and implementing some critical best practices for information security will help your team create a secure software environment for your organization.

Why You Need an SaaS Security Checklist

Moving software applications to the cloud with SaaS brings a lot of benefits to your business. Transferring the heavy lifting of data processing to remote servers, eliminating the need for on premise updates and data storage (as well as potentially costly overhead from additional IT staff), and providing role-appropriate, real-time access to stakeholders throughout your organization can save you money and free your staff to focus on more strategically valuable tasks.

Small wonder, then, that SaaS has assumed such a commanding position in the software environments of companies big and small:

- In 2019, Synergy Research found total SaaS revenue topped $100 billion U.S.—with an estimated annual market growth of 30%.
- *Elite Content Marketer* found that same year that the average employee uses at least eight SaaS applications in the course of their workday, and employers spend nearly $2,900 each year in subscription fees per end user.
- A 2019 survey from research firm Gartner found more than a third of organizations had earmarked cloud services as one of their top three investment priorities.

But like many other technologies at the forefront of digital transformation, SaaS applications carry risks as well as rewards. When you're relying on cloud services to store, organize, move, and analyze sensitive data, cloud security is paramount in protecting not just your intellectual property, but your financial assets—and your customers' sensitive information. Without effective information security controls in place on the server side (i.e., from the SaaS provider) and client side (i.e., your internal IT controls and end user experience), you can find yourself exposed to risk of costly cyberattacks that can damage your reputation and bottom line.

Consider this: in 2020, Verizon reported 43% of cyber attacks were directed at web applications from cloud service providers (roughly twice what they were the previous year). 86% were financially motivated, 30% involved internal actors, and a shocking 55% involved organized criminal groups. Perhaps even more concerning, more than one in five attacks involved corporate espionage.

These security issues have truly staggering price tags attached. Cybersecurity Ventures estimates the global cost of cybercrime will hit $6 trillion by 2021. Distributed denial of services (DDoS) attacks, ransomware, brute-force hacking and other malevolent actions by cybercriminals have left corporate giants like Yahoo—who suffered a record-setting hack that exposed more than three billion user accounts and cost the company more than $100 million dollars—reeling. The Equifax breach of 2017 affected more than 145 million customers, and hit the credit reporter with more than $1.25 billion in costs as of 2019, with the potential for even more financial damage from penalties and legal fees.

The risks are clearly substantial. Understanding how SaaS works (as well as the security controls that should be in place on both ends of the process) and then implementing best practices for both data protection and general cybersecurity, goes quite a long way toward minimizing those risks.

> *Mitigating risk exposure comes with just about every part of doing business. SaaS is no different, and having a strategy in place, informed by best practices, will help you establish the security controls and standards you need to ensure both your own team and the vendors you choose are both working to ensure optimal data and network security.*

Identifying Common SaaS-Related CyberSecurity Threats

Companies use SaaS applications in a variety of ways. Gartner found in 2019 that a hefty 36% of companies surveyed used cloud services applications, while 28% used SaaS to outsource critical business processes. And by 2022, the firm estimated, those values would sit at 40% and 30%, respectively.

Regardless of the applications involved, companies face common risks related to using SaaS:

- Incomplete or insufficient internal security controls leading to:
    - Increased vulnerability to Phishing attacks.
    - Lack of training or compliance leading to accidental or intentional exposure of sensitive data, including data theft.
    - Compromised employee accounts and credentials (i.e., “account

hijacking" or account takeovers/ATOs).
        - Lack of single-sign on (also called *federated identity management*), leading to team members having multiple different identities across different SaaS applications (or sometimes modules within the same SaaS application!) and a much higher risk of account hijacking or "ghost" accounts that retain access even when an employee leaves the organization.
        - Increased liability and compliance costs related to failure to provide a secure data environment for users.
        - Lack of access and usage transparency making it difficult to ascertain the organization's needs regarding network security.
- Direct attacks from outside actors.
    - Brute-force hacks.
    - Ransomware
    - Exploits and Zero-Day Malware
    - DDoS attacks

SaaS Security Best Practices

Mitigating risk exposure comes with just about every part of doing business. SaaS is no different, and having a strategy in place, informed by best practices, will help you establish the security controls and standards you need to ensure both your own team and the vendors you choose are both working to ensure optimal data and network security.

1. Develop and Follow a SaaS Security Checklist

As with other business process management tasks, building a formalized strategy for SaaS security begins with needs analysis and clear benchmarks for success. Assess your software environment and identify the security threats and risks you want to mitigate (or ideally, eliminate).

Use this information to build your checklist, prioritize the requirements listed, and ensure you've included not just internal controls, but compliance, performance, and application security standards that should be met by any potential SaaS provider who wants your business.

2. Invest in Security Literacy Education and Cultural Development

A security-minded company whose team members are up to date on the latest threats to data security is a much harder nut to crack for would-be hackers, phishers, and fraudsters.

In addition to ensuring your entire team is fully trained on the functions of your SaaS applications:

- Train your users on role-based access (RBAC) and two-factor authentication (2FA) for all logins, using complex passwords that must adhere to internal controls. This will not only reduce the risk of user accounts being compromised, but allow for user-specific permissions that provide greater security against internal attacks.
- Add additional training to help team members recognize common phishing and hacking techniques, and the best methods for tracking and reporting such attempts.
- Reward proactivity with regard to data security. Choose team members to become “security champions” to help spread awareness and compliance with your security controls.
- Educate your team on the importance of avoiding potentially vulnerable third-party applications (such as password managers)
- Refocus your IT resources to prioritize data security and provide real-time protection in support of whatever software-based protections are baked into the apps you’re using.

  Logging of all application activity should be universal and constant, with the data available in real-time for immediate analysis in the event of suspicious or dangerous network activity.

  Ensure your IT function has plans in place for protecting infrastructure as well, including firewalls, account management based on security levels, and comprehensive backups to protect business continuity and prevent data loss in the event of disaster.

3. Develop and Continuously Update Your Data

Security Policy

Set high standards for password complexity and security. Choose applications that support single sign-on across modules (either proprietary or using tools like Microsoft's Active Directory or Google Accounts). Set firm limits on the use of personal devices for accessing SaaS applications to reduce the risk of unauthorized access. These are just a few of the things you can add to your data security policy to protect data, operations, and company from needless risk.
Formalize your data security policy, make sure both your entire organization and your vendors are familiar with it, and update it as needed to address new threats.

SaaS Security Checklist Essentials

Every company is different, but in working with cloud applications, you can build your own custom checklist based on shared essentials.

For our purposes, let's narrow our focus to the procurement function, which can provide substantial benefits through conversion to an automated solution using cloud computing and provides a powerful opportunity for both modular and comprehensive digital transformation, depending on budget and organizational goals.

A best-in-class eProcurement solution like PLANERGY is built from the ground up to incorporate security as well as convenience. When researching and implementing such an application, your SaaS security checklist might look something like this:

SERVER-SIDE SECURITY PRACTICES

- Application infrastructure is redundant and contains contingencies to protect business continuity and insulate against DDoS attacks, security breaches, or other incidents, without any single point of failure.
- Comprehensive, redundant backups of databases, application code, client files and configurations, etc.
- Recovery plan created with client and tested regularly.
- Internal emergency access for SaaS vendor staff, with protocols to protect against unauthorized access.

- Real-time protection of sensitive data (including account details, email addresses, passwords, etc.) using advanced data masking and database encryption.
- Comprehensive logging of all application and system activity.
- Automatic intrusion detection, antivirus, and support for strong password policies set by the client.
- Continuous patching to ensure users always have the latest, most secure version of the application.
- Protection from SQL injections through hard-coded limitations on direct SQL orders and real-time validation of all SQL commands.
- Client and server-side validations are run in tandem. Also, authentication tokens required to access backend resources are verified on both the client and server.
- Javascript and XML injections are prevented through restrictive field validation.
- All configuration data is encrypted.
- No permissions are stored client-side. Pages containing sensitive information are blocked from being cached.
- All pages are secured with HTTPS.
- Cookies are limited to Secure and HTTPOnly to protect user data and guard against exploits.
- Application is regularly audited and tested (including penetration testing) both in-house and through the use of external testing resources for security risks, compliance with industry, governmental, and client-provided security requirements, third-party vulnerabilities, etc.

CLIENT-SIDE ESSENTIALS

- Client has a public cybersecurity policy in place, including data transparency statement, compliance protocols, and security incident planning.
- Client invests in, and works with providers to protect, a security-minded culture of well-trained and security-literate team members.
- Client has a clear and continuously updated set of expectations for SaaS providers, including compliance certifications such as Security, Trust, and Assurance Registry (STAR), SAS 70/SSAE16-3, PCI DSS, etc.

- Client works closely with SaaS providers to refine security measures, revisit service-level agreements, and update policies as requirements change and new threats emerge.

Choosing a comprehensive, security-focused solution like PLANERGY makes it easy to check all these boxes from the jump.

Leverage Cloud Computing Effectively with Secure SaaS

Whether you're optimizing procurement, managing an online storefront, or managing customer account data, software as a service can help you get it done more quickly and accurately, at a lower price.

And by investing not only in secure SaaS applications, but developing and implementing your own best practices for cybersecurity, you can insulate your business against needless risk, and harness the power of cloud computing to compete and grow in the digital marketplace.

What's your goal today?

1. Use PLANERGY to manage purchasing and accounts payable

We've helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our "Solutions" page to see the areas of your business we can help improve to see if we're a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide “Preparing Your AP Department For The Future”

Download a free copy of our guide to future proofing your accounts payable department. You’ll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts