Why SaaS businesses need to rethink their penetration testing approach

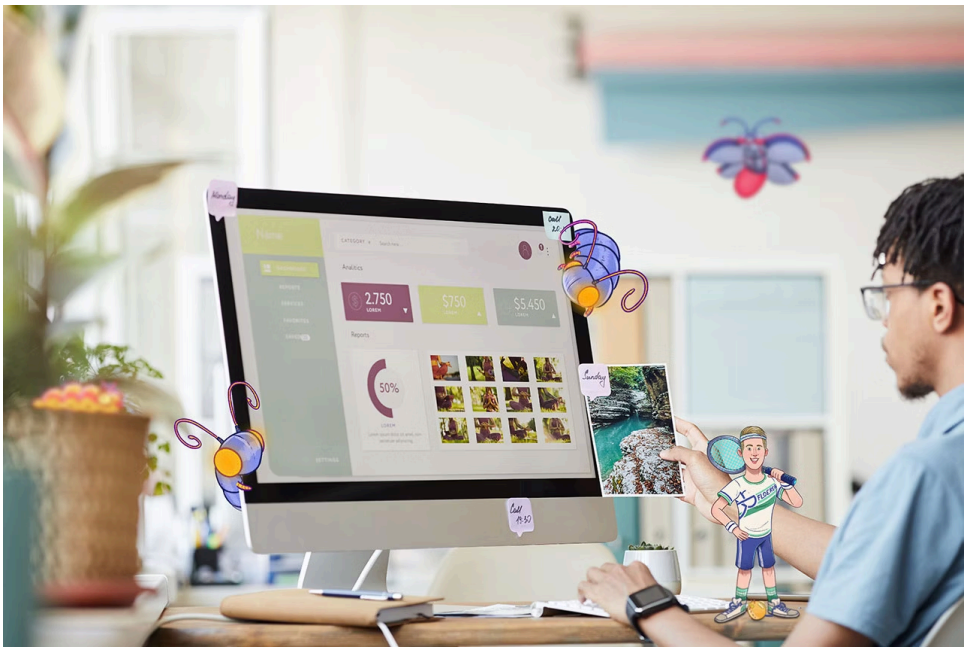
BY ANNA HAMMOND · MARCH 18, 2024 · LAST UPDATED ON MARCH 6, 2025

Every year, companies increasingly rely on software-as-a-service platforms (SaaS) to handle a variety of tasks, such as website analysis, accounting, payroll, and email automation. Reliance on SaaS is unavoidable. But it introduces risks and security issues, making security testing even more business critical.

In this blog post, we'll explore why security testing for SaaS businesses must evolve to keep pace with the changing threat landscape. We'll also highlight how organizations can adopt a proactive and informed approach to security testing. By taking these steps, SaaS businesses can stay ahead of cybercriminals and strengthen their defenses against potential breaches.

SaaS and the expanding attack surface

By 2022, the average company was using 130 SaaS platforms, a significant increase from just 8 in 2015, according to Statista. However, the real number is probably much higher. Venturebeat's article highlights that it's hard to know the exact number of SaaS platforms used in a company. Often, IT leaders don't have complete visibility of all the SaaS platforms their employees use.



Undeniably, the SaaS model has revolutionized the way businesses operate, offering increased flexibility, scalability, and cost-effectiveness. However, this convenience comes with an inherent risk: an expanded attack surface. SaaS businesses, by their very nature, store and process sensitive data in the cloud, making them particularly vulnerable to cyber threats.

Unlike traditional on-premise software, SaaS applications are hosted by a third-party provider, exposing them to the vast expanse of the internet. This means that any vulnerability in the provider's infrastructure or application can serve as an entry point for attackers. Moreover, SaaS providers often have complex and interconnected systems, making it challenging to identify and mitigate vulnerabilities.

Another challenge is that customers are often responsible for securing their own data within the SaaS environment. However, many lack the necessary expertise or resources to implement robust security measures, leaving critical data vulnerable. This shared-responsibility model can lead to security gaps that attackers are eager to exploit.

To compound the risk, the growing popularity of SaaS has made it an increasingly attractive target for cybercriminals. Attackers are continuously developing sophisticated techniques to exploit vulnerabilities in SaaS applications, from phishing attacks to malware injections.

Taking this all into consideration, SaaS providers have a duty to customers to ensure their products are as secure as possible. However, given this evolving threat landscape, traditional penetration testing methods are no longer enough to safeguard SaaS businesses.

The importance of continuous security testing for SaaS providers

With the relentless innovation of cyberattack techniques, hackers are constantly refining their strategies to exploit vulnerabilities in SaaS applications. Continuous security testing makes sure that organizations remain proactive in identifying and mitigating new vulnerabilities before they can be leveraged for malicious purposes.

Moreover, ongoing security testing provides a comprehensive assessment of an application's security posture. Knowing an organization's security maturity empowers them to make informed decisions regarding their cybersecurity investments and strategies. For example, by gaining a holistic view of their security vulnerabilities, organizations can prioritize their resources effectively, focusing on the most critical areas of risk. This proactive approach optimizes security spending, maximizes protection, and helps organizations comply with industry regulations and standards.

Continuous security testing for SaaS businesses also helps foster a culture of security awareness within an organization. By regularly involving development and security teams in the testing process, businesses instill a mindset of constant improvement and vigilance. This collaborative approach encourages ongoing learning, knowledge sharing, and the adoption of best practices, ultimately enhancing the overall security posture of the organization.

Combining traditional pentesting with modern techniques

A common tactic for modernizing security testing methods for SaaS businesses is to use traditional penetration testing and bug bounty programs in tandem.

A bug bounty program follows a persistent security evaluation approach. Ethical hackers strive to uncover unexplored methods to breach a company's cyber defense systems. Companies only compensate ethical hackers with a bounty for identifying legitimate security flaws, also known as bugs. However, the

opportunity to earn a bounty is a key driver for many ethical hackers today. By leveraging a variety of skill sets, bug bounty programs allow businesses to expand their coverage through a unified network.

Ethical hacker motivations for hacking [Source: The Ethical Hacker Insights Report 2021]

Both bug bounty programs and pentests have the same goal of discovering vulnerabilities that malicious hackers could manipulate. However, they have distinct differences. For example, pentests are conducted at a single point in time, while bug bounty programs are ongoing. Additionally, although a pentest may provide a certificate of security, it cannot guarantee that the system will remain secure after future updates. This is where bug bounty programs excel as a post-pentest measure.

Another approach to leveling up security testing to match the sophisticated threat landscape is Hybrid Pentesting. This method combines the benefits of traditional penetration testing with the flexibility and incentivization aspects of bug bounty programs. Importantly, organizations can test their SaaS applications more frequently and comprehensively, without the need for dedicated hardware or software.

SaaS providers must level up security testing to match today's threat landscape

It's time that penetration testing for SaaS businesses modernized to meet new demands. Continuous testing helps organizations stay ahead of evolving threats, and through this approach, SaaS organizations can find security issues as quickly as possible to promptly address them.

To learn more about bug bounty programs and pentesting for SaaS providers, get in touch