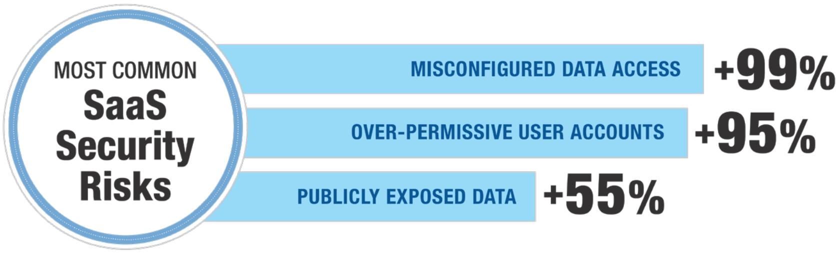
AppOmni
Secure Your SaaS Data

Guide to SaaS Security Posture Management

CONTENTS

SaaS is becoming business-critical in the enterprise—but traditional security measures don't fully protect SaaS applications and the data they contain. And that means businesses may be at greater risk of a breach.



Source: AppOmni Labs

Introduction

SaaS applications such as Microsoft 365, Salesforce, ServiceNow, Workday, and many others support the vital activities of every organization, including sales, communication, source code management, collaboration, and more. Subsequently, these applications—and the data they store, process, and transmit—have become the new systems of record for everything from patient and customer data to employee details. Given the reliance on these applications, the sensitivity of the data, and the need for data integrity, these applications have become part of the critical IT infrastructure stack.

Unfortunately, security teams are typically unprepared to handle this rapid digital transformation.

99 percent of cloud security failures through 2025 will be the customer's fault[2].

And recent studies3 have shown that SaaS applications have become a valuable target for threat actors due to the sensitive nature of the information stored on these systems—and the knowledge that SaaS application security is often less stringent.

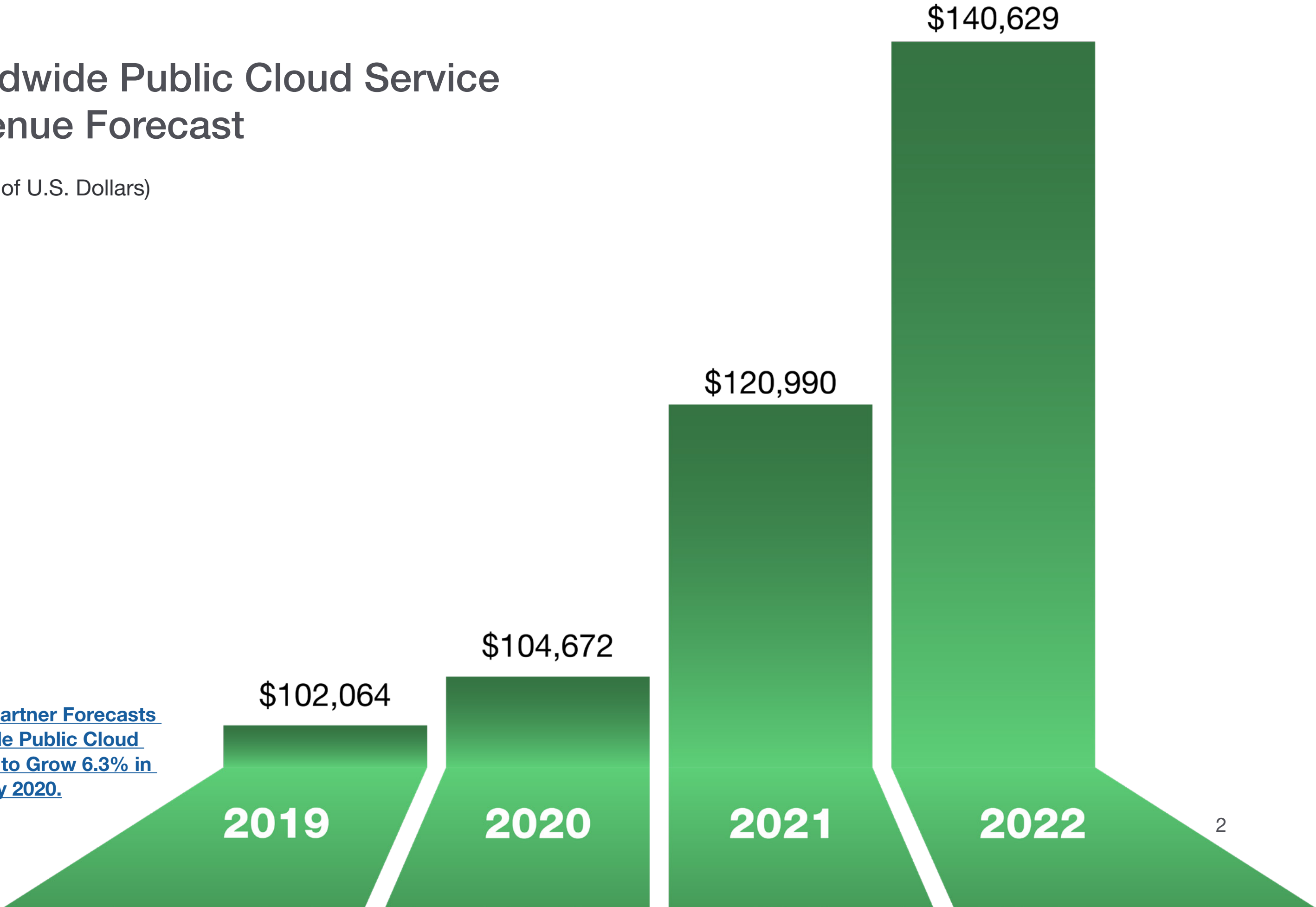
In this guide, we'll examine the unique security challenges associated with SaaS as well as the limitations of both traditional security approaches and native solutions from SaaS providers.

We'll also discuss the need for a new category of products to manage SaaS since it's now part of the critical IT infrastructure: SaaS Security Posture Management (SSPM).

> *"The pandemic validated cloud's value proposition... The ability to use on-demand, scalable cloud models to achieve cost efficiency and business continuity is providing the impetus for organizations to rapidly accelerate their digital business transformation plans. The increased use of public cloud services has reinforced cloud adoption to be the 'new normal,' now more than ever."*
>
> ***- Sid Nag, Research Vice President***
>
> **Gartner®**

Worldwide Public Cloud Service Revenue Forecast

(Millions of U.S. Dollars)



Source: [Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020, July 2020.]

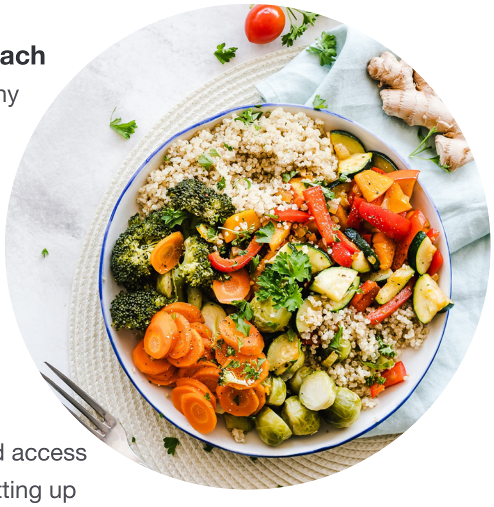
SaaS Security is Critically Important

SaaS Incidents and Business Impact

When it comes to SaaS security, there's no shortage of cautionary tales. According to IBM[4], **the average cost of a data breach is $4.24 million globally**. But that number alone doesn't tell the full story. Productivity losses, potential penalties for non-compliance, reputational damage, recovery and legal costs, and the loss of sales prospects all need to be accounted for when assessing the true impact of a data breach.

Ecommerce Data Breach

Within an international ecommerce company's Salesforce community portal, security configurations had not been properly maintained to prevent external access to internal data. By the time the company discovered the issue, in December 2020, nearly 1.5 million sets of personal and corporate data had been exposed. Upon closer inspection, it became clear that the data had been vulnerable for nearly five years.



Nutrition Company Data Breach

Account owners at a large nutrition company failed to set the proper default access level to "people in your company" for cloud content management provider Box.com. This misconfiguration exposed the data of about 100,000 customers, including names, email addresses, and phone numbers.

Municipal Data Breach

A Salesforce developer misconfigured access to an external-facing portal when setting up the city's 311 database. With no checks and balances to alert team members that sensitive data would be shared, citizens' and employees' SSNs and other PII were exposed.

Analytics Provider Security Breach

When a third-party analytics provider was breached, hackers gained access to some of the company's customer environments, including GitHub and GitLab OAuth tokens.

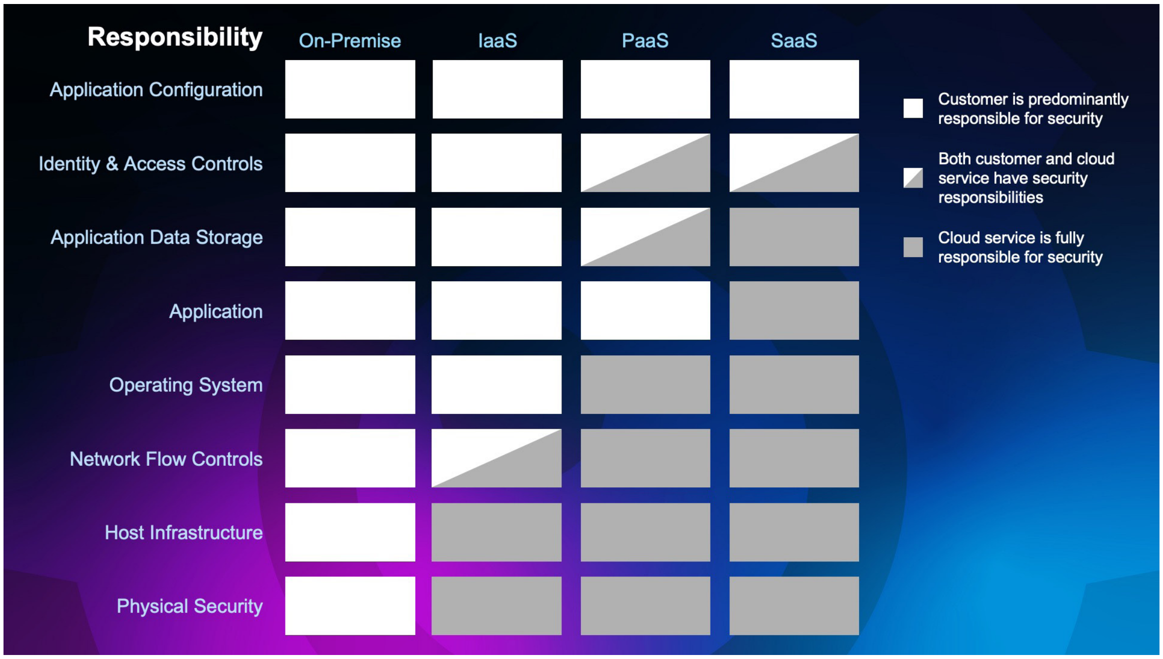
With those and many other examples, it becomes clear that the cost of inaction is far too great for security and IT teams to delay or ignore SaaS security. Critical IT infrastructure and sensitive data must be secured or organizations risk a breach.

Shared Responsibility Model

Government and industry best practices call for a shared responsibility model for cloud security—with cloud providers, product vendors, and customers each assuming responsibility for the security measures that fall under their control. With SaaS, the application provider assumes responsibility for the physical infrastructure, network, OS, and application, while the customer is responsible for data and identity management.

SaaS adoption has grown too quickly for security teams to keep pace with the new risks and vulnerabilities applications bring. Out-of-the-box security settings may not comply with organizational standards and customization makes security more challenging.

According to a report by Oracle and ESG5, 66 percent of all organizations found the shared responsibility model for SaaS confusing. That means organizations are not fully securing the SaaS elements they're responsible for in the shared responsibility model—putting their data at risk.



Responsibility	On-Premise	IaaS	PaaS	SaaS
Application Configuration	□	□	□	□
Identity & Access Controls	□	□	◪	◪
Application Data Storage	□	□	◪	■
Application	□	□	□	■
Operating System	□	□	■	■
Network Flow Controls	□	◪	■	■
Host Infrastructure	□	■	■	■
Physical Security	□	■	■	■

□ Customer is predominantly responsible for security

◪ Both customer and cloud service have security responsibilities

■ Cloud service is fully responsible for security

Shared Responsibility Model

SaaS Security Challenges

With many SaaS applications, "installation" is as simple as entering a credit card number to purchase. Nearly instantaneously, a team, office, or entire business can start using a feature-rich productivity application that hosts sensitive data and is accessible from anywhere, on any device in the world.

The flexibility and customizability of SaaS, coupled with economies of scale, make it a game-changer for productivity. However, those same characteristics make SaaS applications challenging to secure. Gone are the days where a security team could simply rely on a network perimeter to keep sensitive data internal.

Four Challenges in Securing SaaS Platforms

1. Decentralized Platforms and Applications

In the past, organizations stored and managed applications and data on-site, where IT and security had complete visibility and control. Those same departments often selected the applications used by the entire organization and any changes to the status quo required a lengthy governance approval and provisioning process. Now, with the ease of deployment and low upfront cost, SaaS applications are often acquired using local budgets. As a result, these applications fall outside the purview of IT or security, creating a "shadow IT" problem. The Everest Group[6] estimates that shadow IT comprises 50 percent or more of IT spending at large enterprises. Surveys[7] have shown that there can be more than 32 different billing owners for SaaS applications at the average mid-sized company.

The main problem with shadow IT in SaaS is that executives, who are not well-versed in security, are in charge of ensuring that their applications are configured to function effectively and securely.

But that begs the question: "How many non-IT or non-security leaders are equipped to implement appropriate security settings, let alone understand the shared responsibility model?"

The group that could help in securing these applications—the CIO, CISO, or enterprise security team—might not even be aware that these applications are in use. And when they are aware, those teams often don't have the access needed to monitor and manage the applications.

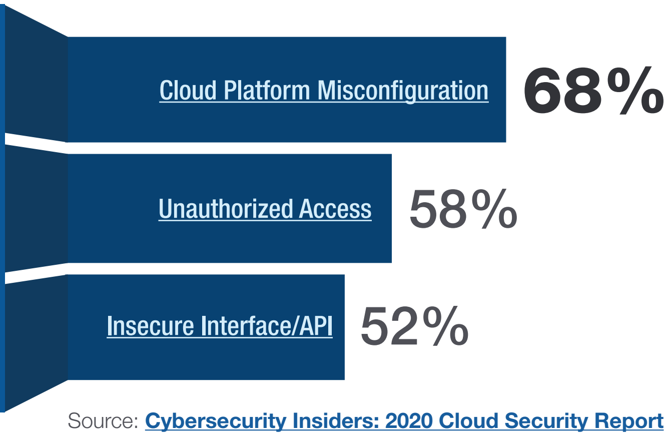
2. Complex and Customized Configurations

The average mid-sized enterprise owns more than 185 SaaS applications8, each with hundreds of unique controls and settings that can be continually adjusted and tweaked to customize functionality. On top of that, each organization—and each group within an organization—has its own needs. Configuring these applications manually can be overwhelming for even the most experienced security teams. The sheer volume of SaaS applications and lack of consistency in settings makes it impossible for security teams to be experts in every application.

Balancing functionality and security is like dancing on a tightrope. Once a SaaS app is customized to deliver the most value for the team using it, default settings don't provide the level of security needed. And that desired custom functionality may conflict with an organization's security and compliance requirements. SaaS applications also interact with other SaaS apps or internal systems. All of this makes it nearly impossible to detect anomalies and investigate weak configurations across applications.

According to the Cybersecurity Insiders' 2020 Cloud Security Report9, organizations ranked misconfiguration of cloud platforms as the biggest security threat facing public clouds. And the lack of a qualified security staff was cited as the biggest hurdle to protecting these environments. That combination can result in breaches that could have been avoided if appropriate security configurations were in place.

When asked about the biggest security threats facing public clouds, organizations ranked **misconfiguration of the cloud platform the highest**. And the **lack of a qualified security staff was cited as the biggest hurdle** to protecting these workloads.



Source: **Cybersecurity Insiders: 2020 Cloud Security Report**

3. Dynamic Environments and User Access

Dynamic business environments mean that anything and everything can change on a daily basis. In today's world of CI/CD (Continuous Integration/Continuous Delivery), SaaS companies push code into production frequently, sometimes changing major functionality and operability—and often affecting security settings. Personnel and their business roles change frequently as well, requiring new privileges for users. Security teams and administrators must have access privileges to make changes as the environment evolves.

The easiest way to ensure that the right teams have the permissions needed to support the environment is to allow broad access privileges. But good security practices call for limiting access privileges to only those who require it, and revoking those privileges when no longer needed. In practice, that's easier said than done. When was the last time a manager remembered to ask the overburdened security team to downgrade user access when a project was done? And how often do people remember there's increased access in place when it's time to provision a new user? Over time, manually managed applications experience configuration drift as the consequences of changed settings compound. And that configuration drift means data can be exposed to internal and external threats.

4. Shadow IT Installation and Management

Third-party integrations into SaaS applications can greatly enhance the functionality and capabilities of the application but also increase the potential of improper exposure.

Many of these third-party solutions can read, write, and delete sensitive data. They can also access user groups, workspaces, or multiple areas in the corporate network, including SaaS applications. Multiple issues can arise with third-party apps, including uncertainty around knowing which apps are approved, what permissions an app has, and who can install an app. It's also often unknown what users are doing with the data accessed by apps, since there's no overarching security monitoring platform.

AppOmni's data shows that on average, there are more than 42 distinct third-party applications connecting into live SaaS environments within an enterprise. More worrisome: About half are connected directly by end-users, not IT or security administrators.

Limitations of Existing Solutions

CASB (Cloud Access Security Brokers)

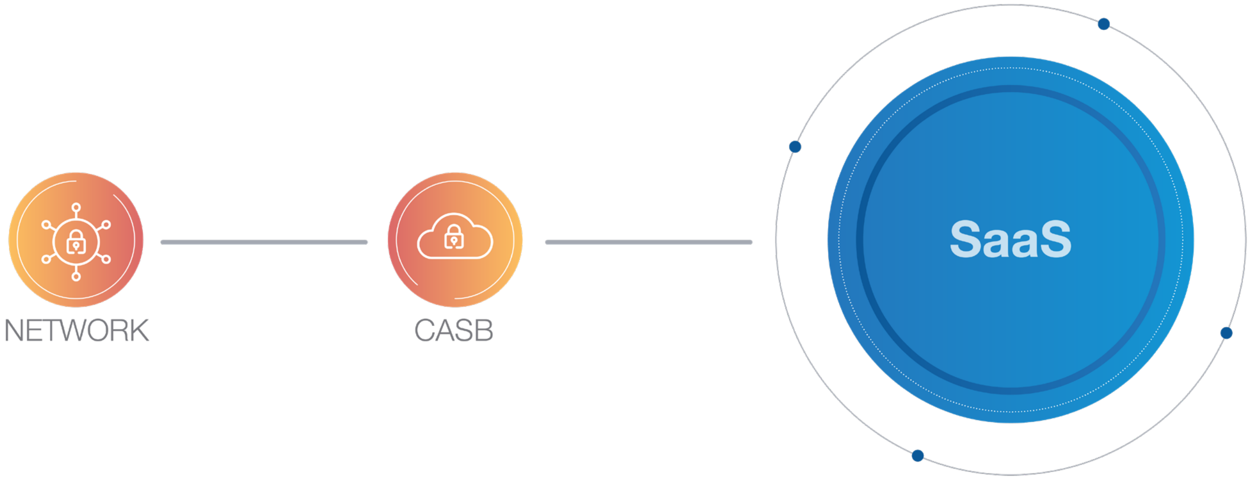
Historically, network security philosophy centered around securing the perimeter and protecting internal resources from external threats. CASBs, one of the most common SaaS security recommendations, were designed to expand that perimeter and broker access to the cloud.

While they can inspect network traffic that flows through the proxy / access gateway, the CASB typically doesn't have visibility into traffic that bypasses the proxy and connects to the SaaS provider directly. SaaS apps have grown into complex platforms with an unlimited number of access points outside the network, beyond the perimeter. Access may be requested by external users, contractors, partners, third-party applications, and IoT devices.

Access may be intentionally granted to users, or granted accidentally through misconfiguration or user error. Either way, CASBs fail to address major blindspots in network security and are yesterday's solution to today's problems.

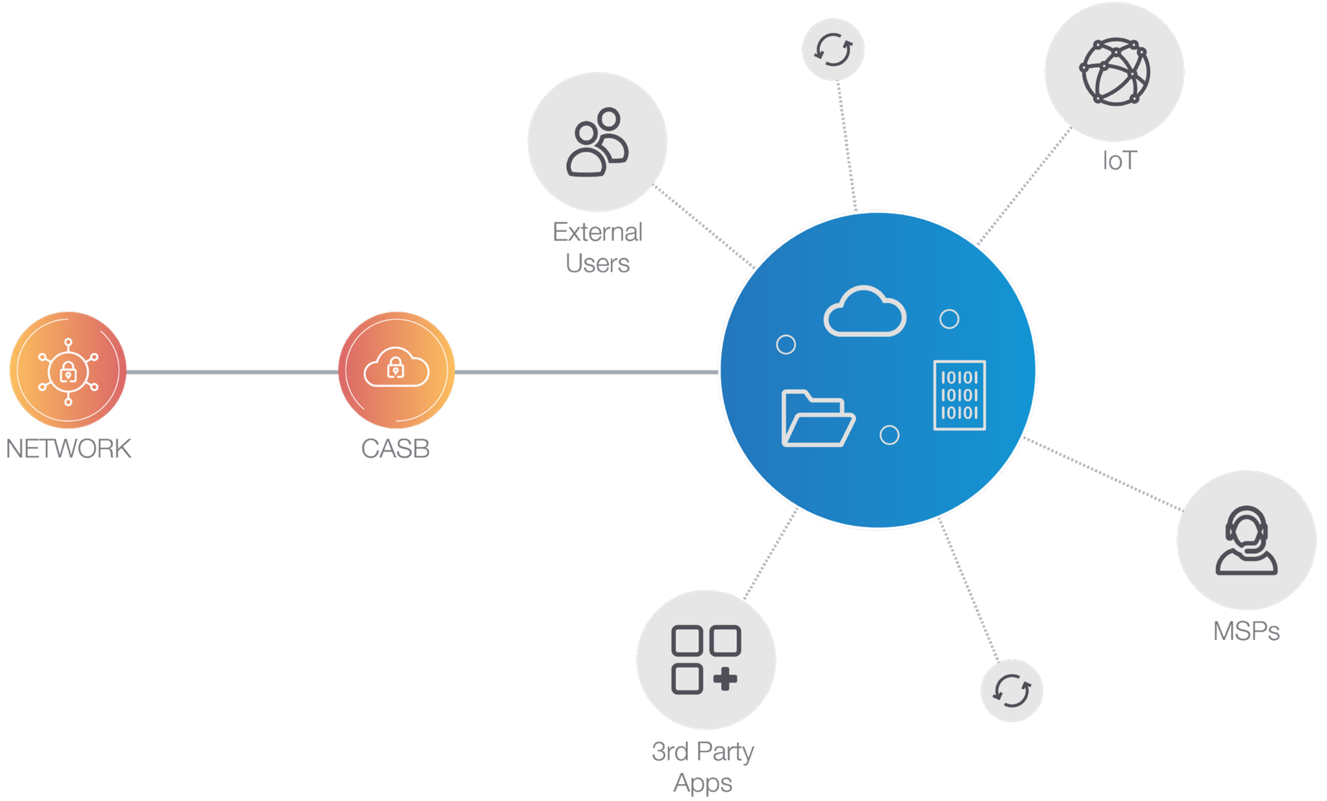
TRADITIONAL SAAS ACCESS

Early on, SaaS applications were relatively simple and accessed primarily through an enterprise network.
CASBs, or Cloud Access Security Brokers, were developed to broker access to the cloud.



CURRENT SAAS ENVIRONMENT ACCESS

Modern SaaS apps have grown into complex platforms that now have an unlimited number of access points. It's no longer just a small percentage of internal employees accessing SaaS - now it's internal employees from across the entire organization (sales, customer service, HR, marketing, etc.), customers, partners, contractors, third-party apps, and IoT devices. These users may or may not be going through the corporate network.



Penetration Tests

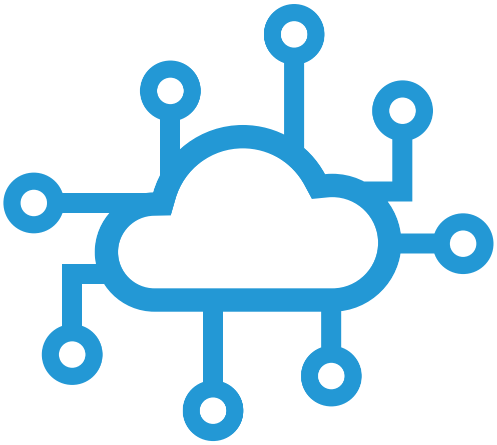
Pentests, or penetration tests, are simulated attacks designed to gauge the security of a system. While they have benefits, there are also several drawbacks. Pentests are typically conducted manually, which means they're expensive, time-consuming, and often inconsistent. And they're usually run by firms that lack expertise specific to SaaS applications. Pentests simply weren't designed to catch every issue that's common in a modern enterprise SaaS environment, including:

1. Installed third-party applications that have not gone through proper vendor approval and/or security review, yet allow access to sensitive data
2. Security-relevant platform misconfigurations, which don't cause classic web application vulnerabilities but expose sensitive data or processes too broadly
3. Over-provisioned users, resulting in excess entitlements to data or business processes
4. Incorrectly configured SaaS-based portals or other public data-sharing vectors that expose internal data to external parties
5. Lack of monitoring or compensating controls for unauthorized actions that privileged users can take due to misconfigurations in SaaS applications

Most notably, pentests only measure the security of a system at a single point in time. Since SaaS systems are constantly changing due to new users, configuration changes, and vendor updates, pentests are often obsolete weeks or even days after completion.

Native Solutions

The largest SaaS providers are aware that their solutions have created huge challenges for security teams to protect data across a distributed ecosystem. In response, some have developed native tooling to help secure their specific application and ease the load on security teams. Unfortunately, each SaaS provider has varying levels of native security functionality and each application has its own interface, terminology, and associated learning curve. Add to that the fact that the average mid-sized enterprise owns more than 185 SaaS applications, and it becomes impossible for security teams to ensure that all enterprise applications are configured correctly. Security teams must also manage and monitor each app on its separate platform to ensure security compliance.



That's a huge burden on an IT or security team that already has a long list of tasks. It's unrealistic to expect that a security team is up-to-date on all security configurations for every application when updates happen regularly and security guides can run into the hundreds of pages. There's also the "not me" challenge, whereby SaaS app security doesn't fall easily under any team's purview so no one is responsible for it. That becomes a huge issue when there's a breach. So what's an organization to do?

Look for The Solution: SaaS Security Posture Management

An effective solution to the challenges of securing SaaS requires a new category of products that builds on the strengths of existing solutions like CASBs and incorporates features of other point solutions, such as compliance and data security software. The solution must keep pace with the speed of change in SaaS environments and satisfy the unique requirements and challenges that come with each stakeholder's responsibilities.

This solution is SaaS Security Posture Management (SSPM), and its key elements and responsibilities for different stakeholders are highlighted below.

Key Elements of SSPM

- SaaS Risk Identification and Management
- SaaS Security Monitoring and Detection
- Software DevSecOps
- Automated Remediation Workflows
- Continuous Compliance

Stakeholders and Responsibilities

Security Teams: Secure and manage data, configurations, user roles, and privileges associated with SaaS applications.

Governance, Risk, & Compliance (GRC): Provide shared processes to help organizations address risks and maintain compliance.

Enterprise IT: Deploy, operate, and maintain SaaS apps in production.

App Admins and Developers: Design, develop, and manage customized SaaS apps.

Executives: Establish SaaS security protocols and prioritize resources to safeguard sensitive information.

SaaS Risk Identification & Management

Security teams need to be able to view and understand the security posture of all SaaS applications in one comprehensive and consolidated view. All third-party applications and OAuth grants should be inventoried. Deviations from best practices in posture policy in any of the applications should be automatically detected—with new, predefined security baselines applied to ensure uniform security posture.

Security teams also need comprehensive visibility into who (employees, contractors, third parties, etc.) has access to what data—within an application or across multiple applications—and why. Policy-based controls are needed to enable security personnel to define authorized access across all managed SaaS applications. If a deviation from predefined data access policies occurs, improper data exposure must be automatically detected and fixed before a possible incident.

Security teams should be able to establish guardrails for data, user, and system configuration policies so application administrators and employees can safely continue operating day-to-day, without compromising the speed and flexibility of SaaS. Continuous monitoring of the SaaS environment should automatically check for deviations outside of those guardrails and notify the appropriate security professionals or provide steps for remediation.

Lastly, when organizations use older versions of applications that may not have all recommended security configurations, security teams should be immediately notified to upgrade. And if an app update modifies any of the existing security features, security teams should be immediately notified of the changes and guided to enhance security. Due to the dynamic nature of SaaS, applications can change very quickly and security needs to remain in lockstep.

SaaS Monitoring & Detection

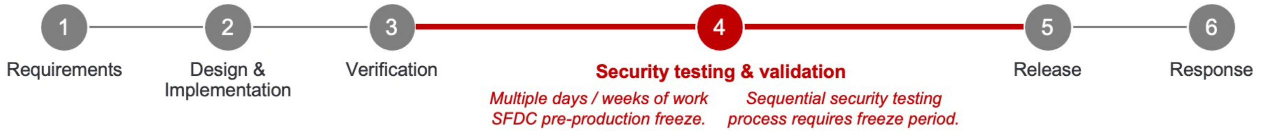
Most security teams are overwhelmed by the challenge of securing a heterogenous SaaS environment that requires real depth of expertise in each application. Because of that, it’s difficult for them to even answer a simple question such as: “Has my SaaS environment been compromised, and if so, how?” SaaS Security Posture Management (SSPM) products should offload this burden from security teams. Any abnormal or inappropriate activity such as suspicious logins, brute force attempts, and data access or deletion should be automatically discovered through built-in detections of SaaS application events.

Essentially, SSPM solutions have to employ a purple team strategy. Not only do SSPM solutions need to be aware of threat actors’ tactics, techniques, and procedures (TTPs) when attacking the vulnerabilities of SaaS applications on the network, the solution must also detect and respond to TTPs through actionable alerts. Detection scenarios and alert summaries should be mapped to MITRE ATT&CK or predefined custom runbooks, allowing security teams to quickly understand the situation and prioritize responses. With SSPM, the intelligence and expertise of the solution cuts through the noise by aligning its findings to recognized security frameworks, and delivering only relevant information to the appropriate security professionals through existing workflows and processes within an organization.

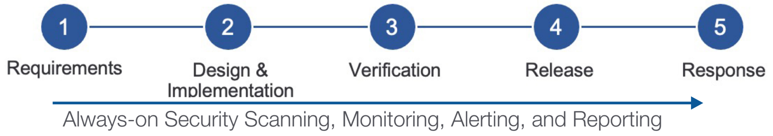
Software DevSecOps

Always-on security enables organizations to create custom policies that automatically scan development environments at each stage of the software development life cycle (SDLC) and identify issues on a continuous basis. Specifically, security and data permission configuration drift should be identified prior to pushing preliminary builds into production. Builds can be automatically sent back into development or straight to production depending on whether or not they passed the automated security checks. By embedding security into the SDLC process, organizations can achieve DevSecOps, increase release velocity, and reduce security risks.

Example 1: Typical SDLC process without security validtion. Monthly releases consist of a sequential SDLC process and defined security test period.


1
Requirements
2
Design & Implementation
3
Verification
4
Security testing & validation
Multiple days / weeks of work SFDC pre-production freeze.
Sequential security testing process requires freeze period.
5
Release
6
Response

Example 2: Always-on security validation throughout the SDLC process will reduce risks and increase release velocity. DevSecOps create custom policies that automatically scan at each stage of the SDLC, and identify security and user-experience issues on a continuous basis.



Automated Remediation Workflow

Workflows

Alerts and events generated from the continuous monitoring of deviations from application-specific settings must be able to launch automated workflows in an organization's existing Security Operations Center (SOC) solutions—such as ticketing systems, SIEM solutions, collaboration tools, and more. Given the tremendous amounts of money, time, and energy invested in SOCs, it's critical that SaaS Security Posture Management solutions plug into existing ecosystems and not ask security teams to use yet another platform.

Automation

Each SaaS application logs activity events in different formats, with differing nomenclature and levels of detail. Moreover, the noise stemming from these logs often leads to alert fatigue. An effective solution automatically aggregates and normalizes all activity events; checks logs against built-in detection scenarios that align with risks inside specific applications; and, if necessary, sends high-fidelity alerts to SOC tooling and teams.

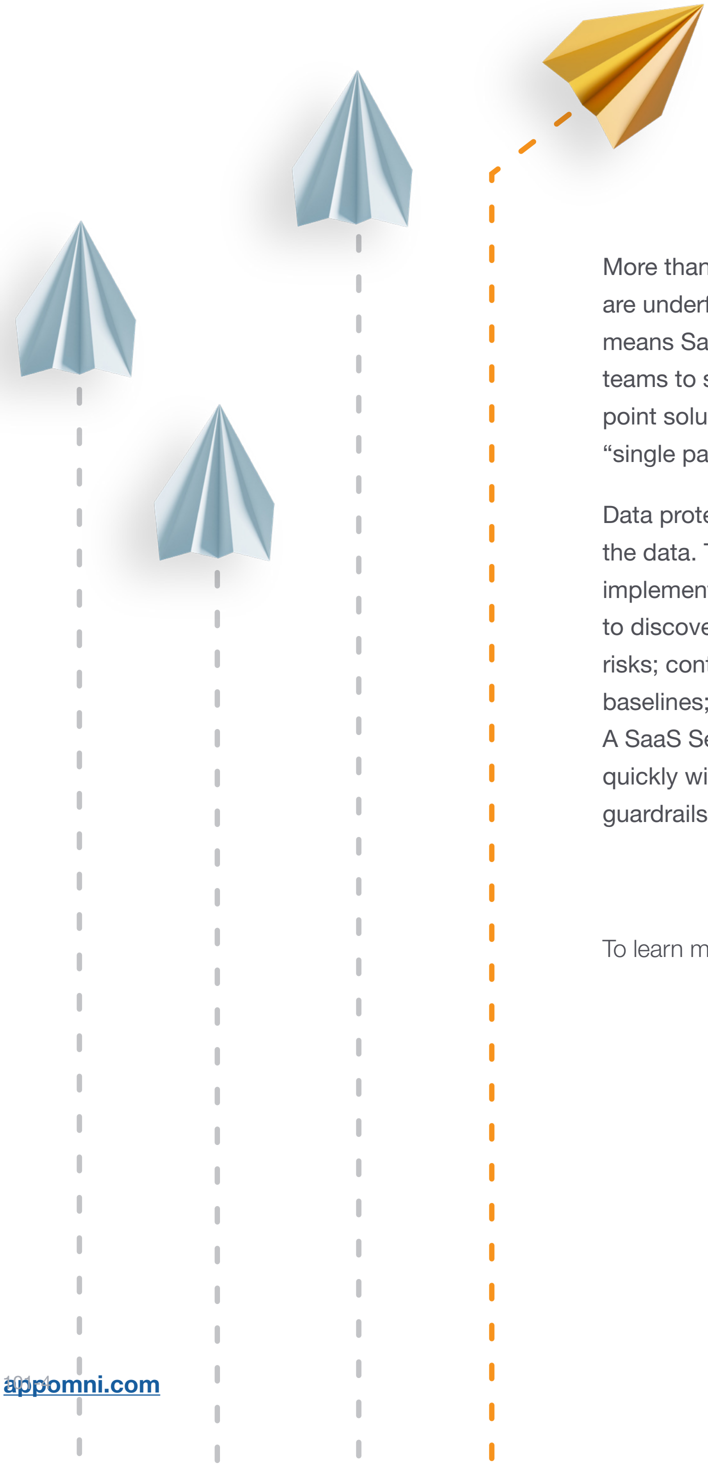
Response

There are dozens of metrics available for security teams to determine success, but mean time to resolution (MTTR) is arguably the most important. While Workflows and Automation are important to drive down MTTR, the last piece of the puzzle is a solution that delivers simple and actionable alerts to the appropriate individuals to make quick, informed decisions. For example, a SaaS Security Posture Management solution should deliver a policy misconfiguration alert to the application administrator and an intrusion detection alert to a security team member. Targeted, easy-to-understand, and informative alerts enable quick resolution and educate stakeholders over time.

Continuous Compliance

Critical compliance needs and security frameworks such as NIST and ISO 27001 should be automatically mapped to security posture controls in SaaS applications. This helps organizations easily enforce continuous compliance. Security configurations and administrative actions should be monitored on an ongoing basis. Misconfiguration or configuration drift should trigger action to remedy the issue across all impacted environments.

Organizations need a current-state view of their SaaS environments at any time. Compliance reports, evaluated against an organization's chosen compliance standards, should also be available at the push of a button to satisfy evidence requirements. This approach is in stark contrast to the manual, interview-based compliance assessments of the past that required exhaustive evidence-gathering exercises.



More than 60 percent10 of organizations believe their cybersecurity budgets are underfunded, while SaaS adoption continues to grow. That divergence means SaaS adoption will likely continue to outpace the ability of security teams to secure their organization's critical data. Traditional solutions and point solutions won't cut it, and security teams don't need yet another "single pane of glass."

Data protection is always the responsibility of the organization that owns the data. The only reasonable way for security teams to bridge the gap is to implement a SaaS Security Posture Management solution with automation to discover security threats; protect SaaS environments from unnecessary risks; continuously monitor applications for drift from established security baselines; and ensure organizations adhere to compliance standards.
A SaaS Security Posture Management solution lets organizations move quickly with confidence, so the business can grow while relying on security guardrails to protect sensitive, business-critical data.

To learn more, email us at **info@appomni.com** or visit **appomni.com**.

Resources

1. https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021
2. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/
3. https://securityboulevard.com/2019/11/phishing-increasingly-targets-saas-webmail/
4. https://www.ibm.com/security/data-breach
5. https://www.oracle.com/a/ocom/docs/cloud/oracle-ctr-2020-shared-responsibility.pdf
6. https://www.everestgrp.com/2017-04-eliminate-enterprise-shadow-sherpas-blue-shirts-39459.html/
7. https://martechtoday.com/new-blissfully-report-most-companies-have-orphaned-saas-apps-in-their-stacks-231064
8. https://chiefmartec.com/2020/04/saas-adoption-trends-start-2020/
9. https://www.cheshireandmerseysidepartnership.co.uk/wp-content/uploads/2020/12/Cybersecurity-Insiders-Cloud-Security-Report-2020.pdf
10. https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2019/isacas-state-of-cybersecurity-2019-survey-retaining-qualified-cybersecurity-professionals