Definitive Guide™

to

SaaS Security

Navigating SaaS Security Strategies
for Safeguarding Your Assets

Crystal Bedell

FOREWORD BY:
Brian Soby

Compliments of:

AppOmni

About AppOmni

AppOmni is a leader in SaaS Security and enables customers to achieve secure productivity with their SaaS applications. With AppOmni, security teams and SaaS application owners can quickly secure their mission-critical and sensitive data from attackers and insider threats. The AppOmni Platform continuously scans SaaS APIs, configurations, and ingested audit logs to deliver complete data access visibility, secure identities and SaaS-to-SaaS connections, detect threats, prioritize insights, and simplify compliance reporting. AppOmni provides unmatched depth and scalability across a diverse range of SaaS environments and serves 25% of the Fortune 100 and global enterprises across industries. Learn more at www.appomni.com.

Definitive Guide™

to

SaaS Security

Navigating SaaS Security Strategies
for Safeguarding Your Assets

Crystal Bedell

Foreword by Brian Soby
CTO and Co-Founder, AppOmni

CYBEREDGE PRESS℠

Definitive Guide™ to SaaS Security

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyberedgegroup.com

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyberedgegroup.com.

ISBN: 978-1-948939-41-6 (Paperback)
ISBN: 978-1-948939-42-3 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Colleen R. Abel
AppOmni Contributors: Chad Knipschild, Chandra Sekar, and Brian Soby

Table of Contents

Foreword v

Introduction vii

Chapters at a Glance vii

Helpful Icons viii

Chapter 1: Taking the World by Storm 1

Sizing Up the Cloud 1

Infrastructure-as-a-service 1

Platform-as-a-service 2

Software-as-a-service 2

The View from the Ground 3

SaaS, by the numbers 3

But wait... there's more 4

Chapter 2: Setting the Record Straight 5

An Expanding Attack Surface 6

Attack incidence is growing 6

Any data can be SaaS data 7

A False Sense of Security 9

Limited visibility skews perceptions 9

No one is taking responsibility 10

Current tools provide security 'to' SaaS – not 'of' SaaS 11

Chapter 3: Exposing SaaS Security Risks and Threats 13

SaaS Risks 13

Misconfigurations 13

Permission drift and excessive access 14

Limited insights into SaaS 16

SaaS Security Threats 16

Access 18

Persistence 18

Defense evasion 18

Lateral movement 19

Privilege escalation 19

Data exfiltration 19

Chapter 4: Understanding SaaS Security Challenges 21

Lack of Scalability 21

Decentralized Application Ownership 23

Lack of Visibility and Access 24

Chapter 5: Reducing the SaaS Attack Surface 27

Enabling Risk-based SaaS Security 27

Posture and configuration management 28

Identity and access controls 29

Threat and anomaly detection 31

Security of connected apps 31

Key Features of a SaaS Security Solution 33

Chapter 6: Implementing a SaaS Security Program 35

Gather Your Resources 35

People 35

Process 36

Technology 36

Implement Your Program 37

Phase 1: Initialization 38

Phase 2: Adoption 38

Phase 3: Formalization 39

Moving Forward 39

Foreword

The rise of the software-as-a-service (SaaS) operating model in modern enterprises marks a pivotal shift in how business is conducted. The reality, however, is that the extent of customer-side responsibilities for securing this new operating model is not adequately understood.

The insights from the *Definitive Guide to SaaS Security* illuminate both the challenges of and the solution for securing business-critical SaaS ecosystems. This guide emphasizes the criticality of a risk-based approach for safeguarding these digital assets in the cloud.

Security and risk leaders understand the monumental role SaaS plays in the enterprise. It's not merely about adopting technology. It's also about embracing an ecosystem that fuels agility, innovation, and growth. In fact, in many ways, the SaaS ecosystem can be seen as an organization-specific enterprise operating system.

Concerningly, the risks to sensitive data and workflows now residing in everyday SaaS applications are not well understood. Adding to the challenge is the rapid proliferation of these applications, which amplifies the attack surface risk. The growing importance of SaaS and the need to secure it represent a call to action that we cannot afford to ignore.

Customer-side SaaS security vulnerabilities, often arising from identity and permission misconfigurations, underscore the necessity for a strategic overhaul in our approach. SaaS security cannot be effectively tackled manually, app by app. The advent of SaaS security posture management (SSPM) platforms offers a beacon of hope by providing the visibility, continuous monitoring, and control essential to mitigate SaaS security risks efficiently and at scale.

However, SaaS security isn't just about deploying security tools. It's also about a fundamental shift in security thinking, recognizing the collective responsibility and need for collaboration by application owners and security teams.

As cybersecurity leaders, we must acknowledge this shared responsibility model in cloud security. Likewise, within each organization, protection of SaaS assets is not solely the domain of security teams, but rather a collective endeavor. This effort includes implementing comprehensive cloud security measures, such as adopting SSPM solutions and building a robust SaaS security program underpinned by education, awareness, and cross-functional collaboration.

A secure, SaaS-first digital future is within reach. This guide to SaaS security provides actionable insights and best practices to help security and risk leaders navigate the complexities of the SaaS landscape.

Adopting a risk-based approach to SaaS security can not only safeguard the enterprise but also ensure our competitive advantage in the SaaS-first age. Going forward, security of SaaS ecosystems cannot be just an afterthought, but instead must serve as a cornerstone of digital transformation strategies.

Brian Soby
CTO and Co-Founder
AppOmni

Introduction

SaaS is taking off. SaaS applications are being adopted by nearly every function in the enterprise, from finance to IT, security, marketing, sales, and human resources. Even organizations in highly regulated industries use SaaS applications to deliver mission-critical functionality. SaaS has become, in essence, the new operating system for business.

Unfortunately, many companies are unaware of the risks associated with SaaS applications. The impression that their SaaS applications are secure is simply not true, as evidenced by the growing number of SaaS breaches.

As cybersecurity leaders, we often focus our attention on IaaS security risks. However, the rapid growth of SaaS has created a large, unprotected cloud attack surface that provides ample opportunity for attackers.

It's time to take a risk-based approach to securing cloud environments, which necessitates prioritizing SaaS security. This guide will show CISOs, CIOs, security architects, and GRC professionals how to do it.

Chapters at a Glance

Chapter 1, "Taking the World by Storm," discusses cloud adoption trends and the rapid growth of SaaS.

Chapter 2, "Setting the Record Straight," reviews the misconception many organizations have about the security of their SaaS applications and data.

Chapter 3, "Exposing SaaS Security Risks and Threats," examines common security issues that put sensitive SaaS data at risk.

Chapter 4, "Understanding SaaS Security Challenges," describes the hurdles teams encounter when defending and protecting SaaS applications.

Chapter 5, "Reducing the SaaS Attack Surface," explores how to address SaaS security within a cloud security strategy.

Chapter 6, "Implementing a SaaS Security Program," outlines the components of a SaaS security program and how to put them in place.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the web.

Chapter 1

Taking the World by Storm

In this chapter

- Explore the global cloud computing market
- Learn how SaaS adoption compares to IaaS and PaaS
- Understand SaaS's sprawling nature

Cloud computing has revolutionized the way organizations handle their data and applications. Once considered a convenient way for teams to spin up IT resources on demand, the cloud has become a requirement for operating in today's highly competitive business environment. But, despite the push to go cloud-first, organizations often have an inaccurate picture of the scale and scope of their cloud environment—particularly software-as-a-service (SaaS). It's time to put that picture into perspective.

Sizing Up the Cloud

As a term, cloud is somewhat nebulous. Cloud refers to IT services delivered on demand and managed by a third party—the cloud service provider (CSP). But that definition covers a variety of service offerings that are generally broken up into three categories.

Infrastructure-as-a-service

When you hear the word "cloud" in an IT context, it usually brings to mind infrastructure-as-a-service (IaaS), provided by the likes of Amazon Web Services (AWS), Microsoft Azure, or Google Cloud. The size of the global IaaS market was estimated at $68.91 billion in 2023, and it is expected to increase at a compound annual growth rate (CAGR) of 18.19% to reach $222.12 billion by 2030.

IaaS providers offer storage, networking, servers, and virtualization on a pay-as-you-go basis. IaaS avoids investment in and administration of infrastructure. It also enables organizations to scale their data volumes and leverage high-performance computing for less cost than they would incur with an on-premises data center. Thanks to IaaS, cutting-edge technologies like artificial intelligence (AI) and machine learning (ML) are available to anyone with Internet access and a credit card, though they are primarily used by developers.

Platform-as-a-service

The popularity of IaaS often overshadows platform-as-a-service (PaaS). PaaS vendors provide a complete development and deployment environment in the cloud. It includes the hardware and software required to provision, instantiate, run, and manage a cloud-based application. As with IaaS, developers are the typical users of PaaS.

The PaaS market, estimated at $17.23 billion in 2023, is the smallest of the three categories of cloud computing. While Research and Markets forecasts the global PaaS market will grow by a whopping 35.3% through 2030, that rate will only expand the market to $142.87 billion by 2030.

Software-as-a-service

And that brings us to SaaS—software applications that are fully cloud-based. SaaS applications are available for virtually every function in the enterprise and thus have a much larger user base than IaaS and PaaS. In fact, end users are just as likely to use SaaS applications in their personal life as in their work life.

For years, SaaS applications have been the leading driver of cloud adoption. Although this trend was well underway prior to the COVID-19 pandemic, the rapid shift to hybrid and remote work models since 2020 has further accelerated SaaS adoption. Today, SaaS applications are ubiquitous. They've made their way into highly regulated industries like healthcare and financial services, and address business-critical use cases such as email, customer relationship management, HR management, and even finance.

There's no indication that the rapid acceleration to a SaaS-centric operating model will slow anytime soon. SaaS continues to be the primary way organizations consume cloud services. They have little choice. Legacy software companies are building SaaS versions of their existing products and, in some cases, forcing their customers to migrate. Meanwhile, new software companies are SaaS-first or SaaS-only. If an organization wants access to the latest and greatest innovations, then it must adopt SaaS.

All these factors contribute to a global market for SaaS that is bigger than IaaS and PaaS combined. According to Fortune Business Insights, in 2024, the global software-as-a-service (SaaS) market is projected to grow from $318 billion in 2024 to $1.23 trillion by 2032, a CAGR of 18.4%. That's a staggering $911 billion increase.

The View from the Ground

Claiming the lion's share of the cloud market is one thing, but what does SaaS usage look like in the typical business? Let's get our heads out of the clouds and our feet on the ground.

SaaS, by the numbers

Let's start with a look at sanctioned SaaS applications—in other words, the SaaS applications that are within IT's and security's purview. In 2024, AppOmni surveyed more than 600 security practitioners around the world to understand their SaaS cybersecurity requirements. Here's what they found:

- ☑ 34% of companies declared that they didn't know how many SaaS applications were deployed in their organization.
- ☑ 31% experienced SaaS incidents resulting in data breaches in the past 12 months.
- ☑ 34% were most concerned about SaaS data exposure and loss of intellectual property.

Remember, these numbers reflect only the SaaS applications that respondents were aware of. Chances are, the actual numbers are much higher, given how easily users can adopt SaaS applications without IT's or security's oversight.

In most organizations, there's nothing to prevent users from adopting SaaS applications at will. And that is exactly what users are doing. In a survey, BetterCloud discovered 65% of all SaaS apps aren't approved by IT. Additionally, 68% of IT professionals mentioned they removed unnecessary apps within the last year.

It's also not unusual to have multiple instances of the same SaaS application deployed in an organization. Departments may independently spin up unsanctioned instances, unaware that there's a sanctioned instance available to them.

But wait... there's more

SaaS proliferation doesn't stop there. SaaS environments have a way of sprawling thanks to third-party integrations, which introduce other SaaS applications to the environment. Third-party integrations enable users to connect different applications to share data and automate business processes. And they're easy for any authorized user of a SaaS platform to set up.

On average, organizations have 256 third-party applications connected to other apps, also known as SaaS-to-SaaS connections. Since they address unique use cases, there is little overlap among the top 10 third-party applications for each SaaS solution. So, for example, the most popular third-party application for GitHub is not the most popular third-party application for Salesforce. Nor is the most popular application for Salesforce the most popular application for Microsoft. The result is the exponential growth of the SaaS environment, much of it operating in the shadows.

78% of organizations are storing sensitive data in SaaS apps. So, ask yourself, where is the majority of your sensitive data stored? Is it in your PaaS? Your IaaS? Or your SaaS environment? Answering this question should help guide your security priorities.

Chapter 2

Setting the Record Straight

In this chapter

- Grasp why organizations think their SaaS environment is secure
- Learn why many are underestimating their risks
- Understand why much of the business-critical data could be SaaS data, which must be protected

SaaS applications pose a significant security risk for two reasons: they touch every aspect of the modern enterprise, including financial data, and they are a growing target for cybercriminals. Threat researchers from Mandiant have noted an increase in threat actors targeting SaaS, as breaches from Snowflake to Midnight-Blizzard continue to impact organizations globally. Yet, organizations at best are oblivious to SaaS risks or, at worst, think their deployments are secure.

In a survey by AppOmni, 85% of respondents indicated they were confident that company and customer data stored in their SaaS applications is secure. But don't be misled. This confidence in SaaS cybersecurity is misguided and is putting SaaS applications and data at increasing risk.

An Expanding Attack Surface

As SaaS increasingly dominates the enterprise, SaaS security risks are expanding as well. Not only is SaaS the biggest cloud attack surface, it's also the fastest growing. The most critical SaaS business applications, Microsoft, Salesforce, and Workday software products, account for 60% of enterprise attack surfaces—making them an attractive target for cyberattackers.

Attack incidence is growing

As the SaaS attack surface grows, so too does the number of attacks—both in quantity and scale. A single misconfiguration or vulnerability in a major SaaS platform like Salesforce can have a widespread impact. For example, AO Labs noted an increase of over 300% in threat-related SaaS activity, coinciding with a Krebs on Security report on misconfigurations in Salesforce sites that were leaking private data. Several organizations, including those in government, healthcare, and financial services, were exposing private and sensitive data via their public Salesforce Community websites. Let's take a quick look at some of the breaches.

- ☑ In September 2023, MGM Resorts and Caesars Entertainment were compromised when attackers gained entry to employee accounts via phishing. The attackers then gained admin rights in Okta and deployed a ransomware attack that resulted in widespread outages across internal networks, ATMs, slot machines, digital key cards for room entry, and electronic payment systems.
- ☑ In October 2023, threat actors used stolen credentials to access Okta's support case management system (likely a SaaS platform), where files containing sensitive session cookies and tokens are stored. Attackers were able to use this data to target Okta's customers and gain control of their identity instances and associated applications.
- ☑ Also in October 2023, Equifax was fined $13.4 million for a preventable data breach in 2017, which affected nearly 147.9 million customers, after hackers exploited a flaw in an open web application.

- ☑ In January 2024, the Midnight Blizzard attack, attributed to the Russian state-sponsored group known as Nobelium, targeted Microsoft. The attackers used a password spray attack to compromise a legacy, non-production test tenant account without multifactor authentication (MFA). This breach allowed them to access Microsoft's internal systems and source code repositories. The attackers moved laterally within Microsoft's network, targeting corporate email accounts, including those of senior leadership.
- ☑ In June 2024, Snowflake experienced a significant data breach when the threat actor group UNC5537 targeted its customers using stolen credentials. This group leveraged weak authentication methods and VPN IPs to access over 165 customer accounts. The compromised accounts often lacked MFA and proper network allow-lists, making them vulnerable to exploitation.

Any data can be SaaS data

As the de facto operating system for the modern enterprise, SaaS applications host a variety of data and workflows, including those deemed business critical. Because of the diversity of SaaS use cases, the impact of a breach varies, depending on:

- ☑ the nature of the business or industry (e.g., financial services, healthcare, or legal)
- ☑ the type of application—such as security, payroll, or people management
- ☑ the nature of the data—such as personally identifiable data (PII), intellectual property, etc.

The consequences of a SaaS breach can be significant, typically resulting in financial and reputational damage. Most applications contain a treasure trove of sensitive data that, if exposed, can result in long-term organizational damage greater than the initial fallout from the breach. In addition to the loss of data, a breach can erode customer trust, leading to a lasting impact on the organization's reputation and financial stability.

B2B SaaS apps can host multitudes of data and business process categories, such as:

- ☑ User and account information
  - User profiles and records—including names, email addresses, phone numbers, PII, and patient health information (PHI)
  - Authentication and authorization data—such as passwords, access tokens, and permissions
- ☑ Customer and client data
  - Customer profiles—such as company names, addresses, and contact details
  - Interaction/communication history—including emails, transcriptions, video recordings, and meeting notes
  - Sales opportunities and pipeline data—such as competitive intelligence, leads, prospects, and deals
- ☑ Business and financial data
  - Product or service data
  - Billing and subscription details—such as payment methods, invoice history, and plan details
  - Order history—including purchase orders, invoices, and shipping details
  - Financial operations data
- ☑ Business process data
  - Project management information—such as tasks, deadlines, resources, and progress
  - Document and file management—may include contracts, proposals, and marketing materials
  - Collaboration data—such as chat messages, comments, and files shared between internal and external users
- ☑ Reporting and analytics
  - Custom reports and dashboards
  - Data integrations with third-party services—think CRM, ERP, and marketing automation tools
- ☑ Security and compliance data
  - Audit logs—including login attempts, data access, and changes made to application configurations
  - Data backups and recovery information
  - Compliance documentation—such as for GDPR and HIPAA, regulations and the SOC 2 framework
  - Security settings and configurations

A False Sense of Security

As we mentioned at the beginning of this chapter, despite the prevalence of SaaS security breaches, the vast majority of organizations feel their SaaS data is secure.

Clearly, there is a disconnect between reality and perception. So, what gives? Early SaaS solutions were simple web applications that users accessed primarily through the enterprise network. Over the past 14 years, SaaS applications have grown into complex platforms with an unlimited number of access points. And as often happens in the enterprise, adoption has outpaced the development of security controls and best practices.

Limited visibility skews perceptions

Security teams can't protect what they can't see, and their visibility into SaaS applications is limited. Because SaaS monitoring and attack surface management remain blind spots, many organizations focus only on initial risk assessments and outside-in audits, as opposed to examining how their SaaS applications are actually implemented and operationalized at scale.

Lack of visibility in cloud environments also affects the efficacy of SaaS risk assessments. Incomplete information about the asset(s), the perceived risks, and the severity of those risks skews the results. Businesses get an inaccurate and incomplete picture of the security issues that are increasing their cyber risk. They therefore are unable to implement the appropriate security and risk controls to address high-impact issues that have the potential to disrupt business operations and expose data.

A lack of visibility also reduces an organization's ability to govern and manage the SaaS environment, which is anything but static. In addition to adopting SaaS applications, organizations often discontinue their use or retain orphaned credentials of former employees. Discontinued applications or inactive but valid identities remain a very real risk, as their third-party integrations with other SaaS applications remain active, effectively presenting attackers with an entry point.

No one is taking responsibility

Security and IT teams understand that they're fully responsible for securing the systems and data running on premises. However, in the cloud, security responsibilities are not so clear. They are shared by the provider and the customer to varying degrees, based on the type of cloud service. The diagram below describes typical SaaS application responsibilities.

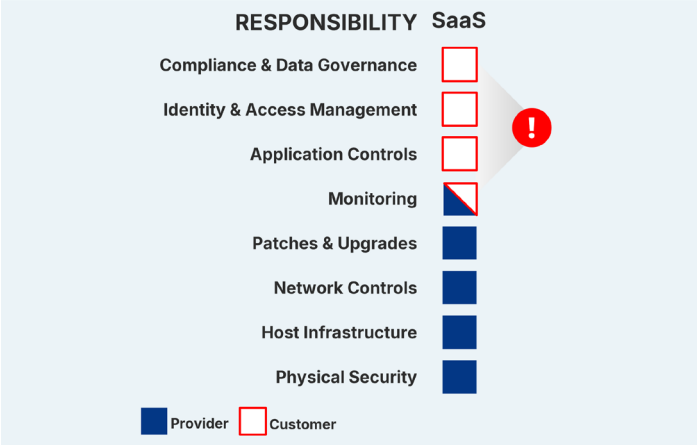

Figure 2-1: The shared responsibility for SaaS.

To help organizations grasp the security risks in their cloud environments, the UK's National Cyber Security Center developed the shared responsibility model, shown in Figure 2-1. At first glance, SaaS appears to require relatively little work from the customer. However, organizations may not realize that the safety of their data relies heavily on upholding their end of the model, which assigns the customer full responsibility for securing SaaS application configuration. Responsibility for securing SaaS identities and access controls is borne by the customer.

Current tools provide security 'to' SaaS – not 'of' SaaS

Many organizations are under the false impression that their existing cloud security tooling provides the protection needed to prevent a SaaS application compromise or data breach. Unfortunately, this is not the case. Because endpoints are increasingly based in the cloud, SaaS security does not lend itself well to legacy network-based solutions or tools that only focus on on-premises or network-edge identity and access management (IAM).

Consider cloud access security brokers (CASBs) and secure access service edge (SASE) solutions. They were intended to stand between the network and the Internet and broker access to cloud applications. In the early days of SaaS, when users accessed these simple web applications primarily through the enterprise network, CASBs provided some—albeit limited—protection.

But modern SaaS applications are anything but simple, and modern workforces connect to corporate resources from virtually anywhere, without having to access the corporate network. In addition, as SaaS has evolved and the interface to these systems has grown to include many external use cases, external users comprise the vast majority of users in many systems, rendering CASB and SASE ineffective.

Even SaaS users on the corporate network can easily bypass a CASB or SASE solution. These tools are only effective if they are the single access mechanism available to users. Side-loaded accounts or accounts with optional MFA/single sign-on will go unnoticed by the CASB or SASE solution.

The complexity of SaaS platforms introduces new security risks that CASBs and legacy software aren't designed to address. Legacy CASB and secure web gateway (SWG) solutions generally only provide an outside-in view of a SaaS application. In other words, they don't provide visibility inside the application, such as how it's configured or how it's being used. SaaS-to-SaaS and third-party connections are also invisible to these legacy cloud security solutions.

Conventional approaches to securing cloud network access are no longer sufficient for protecting the numerous ways SaaS apps are accessed and used across corporate and remote work environments.

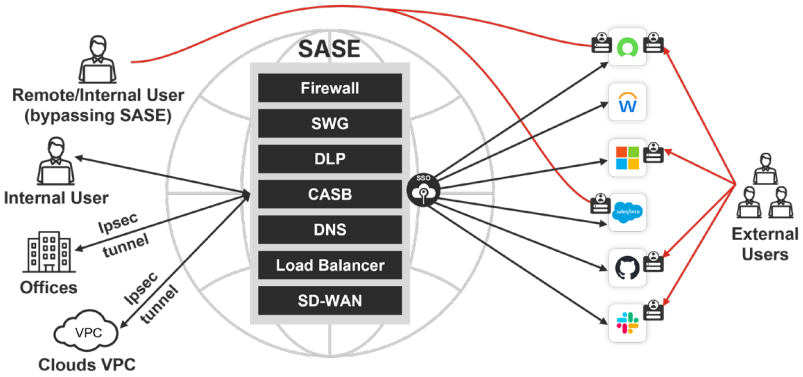

Figure 2-2: SASE can provide security TO SaaS, but users can bypass these controls.

There is good news. Awareness of SaaS cybersecurity risk is growing, with 67% of organizations reporting that SaaS cybersecurity would be a top three security initiative within the next one to three years. First, they need to overcome a number of challenges. We'll explore those next.

Chapter 3

Exposing SaaS Security Risks and Threats

In this chapter

- Learn the major sources of SaaS security risks
- Understand how data in SaaS applications can be exposed
- Explore common SaaS security threats

Despite the confidence many organizations have in their SaaS security, the truth is often troubling. Let's take a closer look at how attackers are compromising SaaS applications.

SaaS Risks

Many SaaS application security risks fall into three categories: misconfigurations, excessive permissions, and limited insight into suspicious activities because of incomplete and inconsistent log data.

Misconfigurations

Once a SaaS application is deployed, it is often left to groups with limited security expertise, like business or application owners, to ensure the solution is configured and functioning correctly. Due to their lack of security knowledge, application owners may grant end users excessive permissions or misconfigure security settings. For example, they might set multifactor authentication (MFA) to optional or leave secrets stored insecurely. These mistakes increase the enterprise's exposure to the risk of a data breach, and also represent a compliance violation.

In every other area of technology, robust security tools are available to stop people from making changes that can impact the organization's security posture. But, until recently, nothing existed for SaaS. As a result, mistakes and configuration drift have gone largely unchecked.

Configuration drift occurs when gradual changes to SaaS applications make them inconsistent with an organization's business intent. This process can disrupt established security standards and introduce security threats.

It's not uncommon to have tens or hundreds of IT users with admin access, all developing new apps or extensions to SaaS apps. Often, business owners, developers, and security teams might not coordinate or collaborate as they move as quickly as possible. The combination of SaaS's many moving parts, tremendous pressure from the organization to move faster, and a lack of security focus continue to create issues, security risks, and incidents.

Inconsistent settings across different applications make it impossible for security teams to master each application and enforce security policies. As a result, misconfiguration-related vulnerabilities frequently occur and recur across the SaaS environment.

Without the proper SaaS security tooling to detect configuration drift on a continuous basis, organizations are unable to address the dynamic and ongoing nature of SaaS cyber risk in their environments.

Permission drift and excessive access

Permission drift and excessive access, including allowing access by human and non-human identities or third-party applications when they should not, poses significant risks. For example, a customer support portal may have access controls set incorrectly, confusing UI visibility with actual access control. This can lead to customers accessing restricted data via the API. Without proper security change management processes and SaaS-specific expertise available, these access control issues can remain undetected and unresolved.

A Common Misconfiguration Leads to Data Exposure

A corporate marketing team is working with a group of contractors on a landing page for a custom website. The marketing team creates a folder in Google Drive and shares it publicly with anyone who is given the link. In addition to various project deliverables, a Google sheet that has credentials to log into the WordPress account is added to the drive. Over time, the group adds more credentials to the spreadsheet.

What the team doesn't realize is that the publicly accessible link is also discoverable. Databases of these public links are available on the dark web. With a simple click, an attacker can access the Google Drive folder—and everything in it— establishing initial access. With unchecked access they can establish persistence and compromise other connected systems, as well as exfiltrate data.

The risk is further amplified when non-human identities, such as service accounts and automated processes, are granted excessive permissions. These non-human identities often operate with elevated privileges to perform their tasks, and if they are compromised, attackers can gain significant control over the SaaS environment. Automated processes, when not adequately monitored, can inadvertently introduce security vulnerabilities by interacting with other applications and systems in unexpected ways.

The interconnectedness of SaaS applications exacerbates these issues. Modern SaaS environments often involve numerous third-party applications that integrate seamlessly with core business systems. Each of these integrations represents a potential point of vulnerability. If a third-party application is granted more access than necessary, or if its security is not robust, it can serve as an entry point for attackers to infiltrate the primary SaaS environment. This interconnectedness makes it challenging to maintain a consistent security posture, as each application can introduce its own set of security risks and requirements.

SaaS apps, by their very nature, are designed to integrate with other SaaS apps. Integrations can be facilitated by browsing specific sites or by shopping for integrations in SaaS application marketplaces.

Limited insights into SaaS

Effective threat detection in SaaS environments involves continuously analyzing logs for unusual activity that could indicate a security breach. This process includes monitoring user behavior analytics (UEBA) to detect anomalies, such as an employee accessing data at odd hours or from unexpected locations, which could suggest compromised credentials or insider threats. But the question remains: who is doing this user behavior monitoring and how is it being done in the case of SaaS applications?

Despite the clear need for SaaS monitoring, there is a lack of consistency in SaaS events and audit logs, which makes it difficult to monitor for cyber threats. Log formats vary from one application to another and are inconsistent across data structure, context, and metadata. This lack of unity and consistency complicates security because it leaves gaps in threat detection and forces teams to waste valuable time evaluating applications.

This inconsistency in log data not only hampers the ability to detect threats but also increases the risk of missing critical security events. Without standardized logging, or standardized rulesets, security teams may overlook subtle signs of an attack, allowing cybercriminals to exploit vulnerabilities and cause significant damage before being detected.

SaaS Security Threats

The cybersecurity industry likes to focus on complex attacks that take down massive targets. Interestingly, in the world of SaaS, big breaches don't require a series of complicated zero-day exploits and advanced persistent threats. More often, successful SaaS attacks are "one-click" attacks, where a threat actor exploits a misconfiguration or misuses the system.

These attacks are simple in that they require minimal technical skills. However, that doesn't prevent them from doing a tremendous amount of damage. Here are some of the attack methods cybercriminals use to get in, get the data, and get out, using the Snowflake breach as an example.

Profile of a SaaS Security Risk

Let's take a look at how easily data can be exposed in a SaaS application. In this scenario, a customer support portal with a knowledge base is accessible from the Internet, allowing users to find answers to frequently asked questions and obtain technical support. Users must register to log a support ticket or schedule a service appointment.

Behind the support portal sits a SaaS system used for customer support and other use cases. A dedicated role is created for customers, rather than reusing an internal profile. Access control has been set to expose customer support information only to customers and internal employees. Customers have limited access to the database tables and limited privileges.

Only a small part of the SaaS application is exposed through the support portal. Further, customers can't access data or functionality within the SaaS application except for what is delivered via the portal.

Unfortunately, the support portal's admins have confused UI visibility with access control. They mistakenly assumed users do not have access to restricted data. But this simple mistake means customers do have access to what was intended to be restricted data via the API.

To make matters worse, there is no security change management process and the security team has no idea the portal was built and rolled out. Even if the team had known, they lacked the SaaS-specific expertise to correctly configure access control and appropriate permissions for the SaaS platform.

These issues could be resolved with:

- SaaS-specific configuration baselines on how to properly harden the portal and application
- Continuous monitoring enabled access control review for all SaaS identities, including external users
- Visibility and drift detection to configuration changes, changes to security settings, data access, and user-based permissions

Access

Threat actors can leverage misconfigurations and vulnerabilities within a SaaS application to gain unauthorized access and obtain all the permissions associated with that account. Take, for example, the Snowflake breach. Attackers used stolen credentials to log in, exploiting misconfigured permissions that allowed them to gain access to critical data.

Attack methods related to SaaS application access include:

- ☑ Credential exposure or attack
- ☑ Compromised or over-provisioned third-party access

Persistence

When we talk about persistence in cybersecurity, we're referring to an attacker's ability to maintain long-term access, even if there's a change to the application, such as a password reset.

Attackers can maintain persistence in a SaaS application by taking advantage of:

- ☑ Unused API keys and tokens left in production
- ☑ Webhooks
- ☑ SSO set to optional

In the Snowflake breach, the attackers maintained persistence by leveraging existing integrations and misconfigurations that allowed them to bypass security measures.

Defense evasion

In the SaaS world, attackers evade security defenses by:

- ☑ Deleting audit logs
- ☑ Disabling security controls

Specific to Snowflake, attackers could have used such methods to remain undetected while accessing and exfiltrating data.

Lateral movement

Attackers can access additional accounts after breaching the initial one, often with the same permissions, by moving laterally. In SaaS applications, lateral movement can involve these methods:

- ☑ Shared credentials: If the compromised user has shared credentials for another account, the attacker can access that account too.
- ☑ Access to account creation: Attackers create new accounts that they can control.
- ☑ Cloud-to-cloud pivoting: Attackers use access from one SaaS application to gain entry to another cloud service—whether PaaS, IaaS, or container-as-a-service.
- ☑ Discovered credentials, tokens, or keys: Attackers use these to access other systems.

In the Snowflake breach, the attackers could have used compromised credentials to access other integrated systems, further expanding their reach and potential damage.

Privilege escalation

Attackers also look for ways to expand their access to sensitive data and systems by compromising user credentials with privileged access. Privilege escalation can occur through:

- ☑ Permission issues such as over-provisioning
- ☑ Internal API key/configuration exposure
- ☑ User accounts with elevated permissions that are no longer needed and have not been decommissioned

Data exfiltration

Attackers can also transfer data out of a SaaS application by:

- ☑ Exporting the data directly from the application
- ☑ Using APIs
- ☑ Leveraging the application's built-in messaging to send data
- ☑ Setting up reports to be delivered to a server or email under the attacker's control
- ☑ Reconfiguring the application's share settings

In the Snowflake breach, the attackers exfiltrated data by exploiting API vulnerabilities and misconfigured sharing settings, which allowed them to transfer sensitive data without detection.

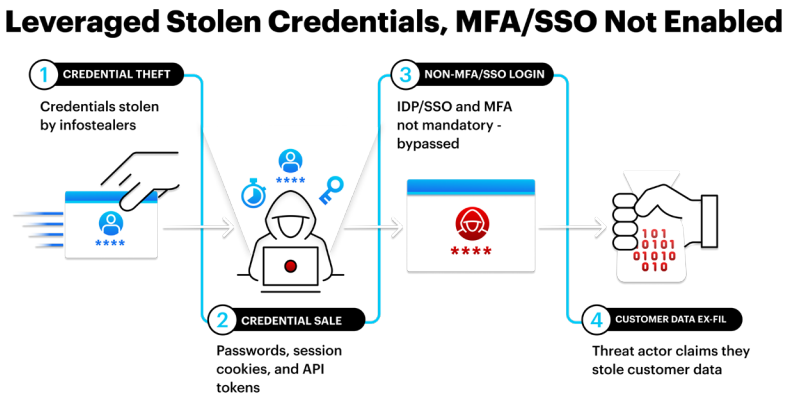

Figure 3-1: Snowflake breach tactics, leveraging stolen credentials and misconfigured settings.

Now that we've uncovered how key risks are exploited in SaaS environments, it's clear that understanding these vulnerabilities is crucial. Misconfigurations, identities, and limited insights into SaaS present major exposure points for attackers. In the next chapter, we'll tackle the broader challenges of SaaS security, including scalability limits, decentralized ownership, and the complexities of securing SaaS applications.

Chapter 4

Understanding SaaS Security Challenges

In this chapter

- Read how the complexity of SaaS applications limits scalability
- Understand how decentralized application ownership impacts SaaS security
- Learn how protecting identities complicates SaaS security

By now, you hopefully have a good sense of the scale and scope of the SaaS environment and the risks it poses. Despite the desire to secure their SaaS environments, organizations encounter numerous challenges including lack of scalability, decentralized application ownership, and limited visibility and access. Let's explore those further.

Lack of Scalability

Securing a diverse SaaS environment can overwhelm the most seasoned cybersecurity team. The depth of expertise required for each application makes it impossible to manually verify overall SaaS security posture. But it also makes it incredibly difficult to scale security efforts across the hundreds of SaaS applications used in a typical enterprise.

SaaS solutions continue to grow more complex as providers offer tremendous customization to appeal to large enterprise customers. This customization adds a high degree of flexibility and granularity to permission models. But it also means there is no one-size-fits-all approach to enforcing configuration policies.

Figure 4-1: SaaS is complex: all of the applications are connected, making it difficult to understand the impacts of a misconfiguration, let alone quantify the risk.

For some perspective, consider this: the scope of configuration changes in a large-scale enterprise deployment can easily exceed 50,000 modifications in a single month on a single SaaS application instance.

It would be one thing if organizations had only a couple of SaaS applications to properly configure. But we're not talking about one or two unique applications. Most enterprises are using hundreds of SaaS applications, while others are using thousands—and each has its own unique permission models, some of which may have been used by the organization for over a decade. However, most cyber risk is concentrated in a handful of core enterprise applications such as Salesforce, Microsoft 365, Workday, and ServiceNow.

This brings us to the issue with instances. The configuration problem becomes even more significant for organizations that have multiple instances of a SaaS application. It's not unusual for a large enterprise to have dozens of instances of Salesforce alone—each of which must be individually configured.

Rapid growth of the SaaS environment, combined with thousands of configuration changes and faster release cycles, makes manual security management an impossible task. As a result, solutions are needed to keep pace with both the growth of SaaS instances and increasing rate of change. With new product updates, these cloud environments are dynamic, and there is no guarantee that today's secure configuration will remain secure after an update is rolled out. For this reason, configurations must be continuously monitored to ensure the environment evolves securely and to provide the necessary visibility.

Decentralized Application Ownership

The Shared Responsibility Model in SaaS environments often masks the true extent of risks associated with SaaS applications. While the SaaS provider is responsible for the infrastructure and the application, the customer is responsible for data, access management, and proper configurations.

On top of that, SaaS adoption and management are no longer an IT function. Instead, they are decentralized across the business. Unfortunately, a lot of the risks associated with SaaS applications are due to the divide that naturally exists between SaaS application owners and security teams. This gap leaves little visibility into what is happening across an entire SaaS ecosystem.

For proper configuration, the owners/administrators must have a comprehensive understanding of the applications themselves, including how they handle permissions, as well as the know-how to configure them correctly. Application owners typically understand the application and may even have earned vendor-specific certifications as a result of training. However, vendor training rarely dives into how to effectively secure and apply permissions for an application.

The security team, on the other hand, understands security principles and how to apply them in most situations. But SaaS applications do not fit into the category of "most situations." Each is a unique security challenge, in and of itself.

If we take a step back, you can see that one side understands the application and the ecosystem, and the other side understands security—but there's no overlap between the two that would allow them to share an understanding of the application's management and security. In addition, there's no single "source of truth" to ensure that application and security teams are looking at the same data versus discussing perceptions. They lack a centralized location to consume, review, and analyze SaaS security settings and findings, risks, etc.

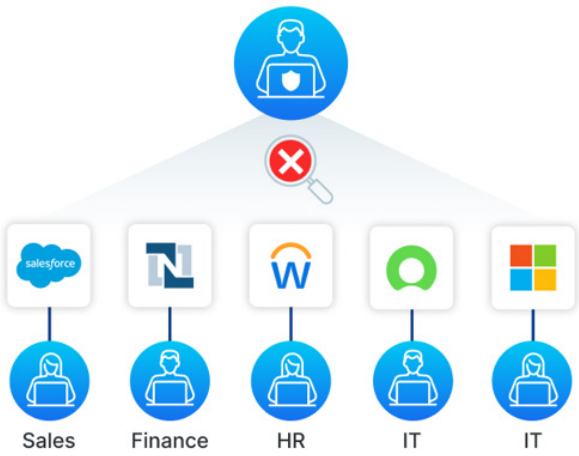

Figure 4-2: Security for SaaS is decentralized because ownership of each application varies, limiting visibility and understanding of risk.

Lack of Visibility and Access

Security teams are accountable for protecting the organization's data, but they often lack visibility into the SaaS applications that store and process this data. This lack of visibility creates significant challenges in identifying and mitigating data risks, access issues, and threats that bypass traditional security controls.

If we were to introduce a Zero Trust architecture, identity would serve as the cornerstone of security, underpinning all access decisions and interactions within the digital ecosystem.

However, ensuring that identity and access policies are correctly implemented and maintained across a diverse set of SaaS applications is complex. Drift in these configurations can occur, and security teams must work continuously to prevent it.

Zero Trust Network Access (ZTNA) tools like CASBs and secure service edge (SSE) solutions sound like they provide visibility and access control for SaaS. However, in reality, they only secure access to SaaS applications and do not provide security beyond the network to SaaS applications and data. Thus, remote users or third-party app connections can easily bypass ZTNA controls.

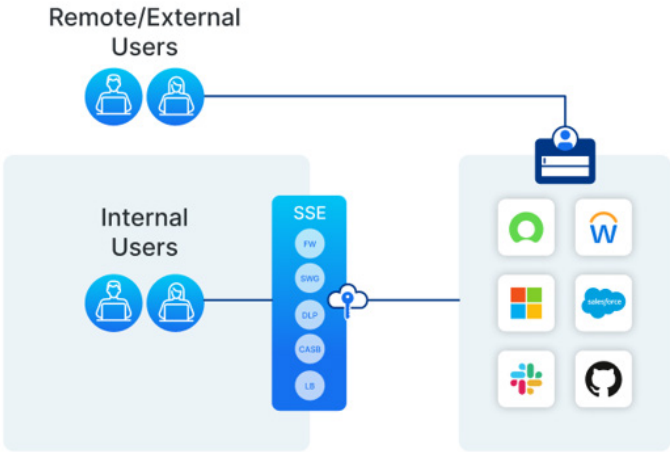

Figure 4-3: To access SaaS environments, traditional controls can be bypassed, limiting insight into what is happening in these SaaS applications.

By integrating identity and policy information across all components of a Zero Trust architecture, organizations can ensure unified and consistent application of security policies. This integration enhances the ability to detect, respond to, and adapt to threats in real time. Identity as a central reference point simplifies security management, ensuring policies are universally applied and reducing gaps that attackers could exploit.

Chapter 5

Reducing the SaaS Attack Surface

In this chapter

- Learn how to reduce the attack surface with a risk-based approach to SaaS security
- Understand the core components of a SaaS security platform
- Read about the benefits of a robust SaaS security solution

SaaS security platforms enable organizations to take a risk-based approach to prioritizing SaaS security alongside other cyber risks in the environment. Thanks to modern SaaS security solutions which include capabilities like SaaS security posture management (SSPM), threat detection, and identity and access management, the extent of risk that SaaS represents is, for the first time, observable and quantifiable. An effective SaaS security solution that provides security risk observability and control is fast becoming critical to bolstering cybersecurity resilience.

Enabling Risk-based SaaS Security

A SaaS security platform is designed to holistically address the security challenges and risks unique to SaaS applications. These centralized platforms enable observability, continuous monitoring, and control for the entire SaaS environment. In addition to detecting vulnerabilities, a SaaS security solution provides the visibility security teams need to detect an attack—ideally in real time—and trace back the activity to find out what was accessed, by whom, and how.

A SaaS security platform gives security leadership and app owners a consolidated view of the enterprise's entire SaaS environment and proactively identify and mitigate SaaS security risks and threats.

The Pareto principle — i.e., 80% of consequences come from 20% of causes — drives the concept of SaaS security and illustrates how enterprises must safeguard their most critical apps. Because an enterprise's SaaS-associated risks are concentrated in the core SaaS apps that its employees use on a daily basis, securing those apps with a SaaS security management tool is the most efficient way to reduce the SaaS attack surface.

There are five core facets of a SaaS security management solution:

Posture and configuration management

Posture and configuration management is crucial to maintaining the security and integrity of SaaS applications, especially as organizations scale. A SaaS security management platform ensures configurations are consistently monitored and managed while enforcing strong identity controls.

Posture and configuration management are important to:

- ☑ **Prevent data breaches and unauthorized access:** Proper configuration and identity management make it difficult for attackers to exploit vulnerabilities. By controlling configurations, identities, and drift, you minimize the risk of unauthorized access and potential data breaches.
- ☑ **Improve compliance:** Many regulations require specific security controls. Ensuring configurations and identities are managed correctly helps meet these requirements and avoid hefty fines.
- ☑ **Foster scalability:** Efficiently managing security across numerous SaaS applications and instances helps ensure consistency in security policies and configurations as the organization grows.

Key capabilities to look for:

- ☑ **Continuous monitoring:** Automatically check configurations to detect and remediate misconfigurations and drift.
- ☑ **Policy enforcement:** Implement and enforce security policies across all SaaS applications.
- ☑ **Identity management:** Enforce the principle of least privilege, ensuring users have only the access they need.
- ☑ **Automated alerts:** Receive notifications for configuration drift, potential security issues, and identity anomalies.
- ☑ **Guided remediation:** Provide step-by-step instructions to fix detected issues, ensuring full control while maintaining security.

Some solutions offer automated remediation. To deploy this capability, the platform must be intricately embedded in the inner workings of the SaaS applications, generally via read/write access. However, permitting that level of access isn't recommended and may violate security best practices such as the principle of least privilege. Guided remediation provides a higher level of security by giving users full control while ensuring the SaaS security management platform remains securely connected to SaaS applications.

Identity and access controls

Traditional identity and access management (IAM) tools primarily focus on controlling access at the authentication stage, or "gate." However, the real concern for businesses is what happens after an identity gains access – specifically, how that access is used and what data can be accessed within the SaaS application. This oversight means that applying Zero Trust concepts to identity security in SaaS is incomplete without tools that monitor and manage activities within the applications themselves. This is where SaaS-specific tools can help.

Identity and access controls address these challenges:

- ☑ **SaaS misconfigurations:** Security teams may think their environment is protected due to their IAM policies, but SaaS misconfigurations can bypass these policies. For instance, an enabled local login setting can ignore SSO requirements. Additionally, complex role-based access control models in SaaS applications can be overlooked by IAM teams. Think back to Chapter 4.
- ☑ **Limited visibility in SaaS:** Identity providers (IdPs) lack comprehensive visibility into SaaS activities. Traditional IAM tools miss critical aspects like local users, non-human identities, and risky access combinations within SaaS platforms.
- ☑ **Insufficient threat response:** Traditional zero trust and conditional access focus on static gate policies. However, threats often emerge after access is granted, based on how identities use their permissions. IAM tools struggle to dynamically address insider and persistent threats within SaaS environments.

Key capabilities to look for:

- ☑ **Identity and access management:** Ensure that users have appropriate access levels, enforce multifactor authentication (MFA), and apply the principle of least privilege to minimize risk.
- ☑ **Data access monitoring:** Track who accesses what data and how it is used.
- ☑ **Remediation suggestions:** Offer actionable insights to remediate data exposure risks.
- ☑ **Access control:** Enforce strict access controls to ensure only authorized users can access sensitive data.

By closely monitoring data access and applying robust security measures, organizations can minimize the risk of data breaches, ensure data integrity and confidentiality, and meet regulatory compliance standards.

Threat and anomaly detection

Effective threat detection involves identifying and responding to potential security threats in real time. This includes monitoring user activities, detecting anomalies, and managing identities. A SaaS security platform excels in these areas.

Effective threat detection helps to achieve:

- ☑ **Proactive threat management:** Early detection of anomalies and potential threats allows for timely intervention, reducing the risk of breaches.
- ☑ **Enhanced security posture:** Continuous monitoring and detection improve overall security posture by addressing issues before they escalate.
- ☑ **Streamlined response:** Integration with SIEM and SOAR systems ensures a swift and coordinated response to threats.

Key capabilities to look for:

- ☑ **Anomaly detection:** Identify unusual user behavior, such as multiple failed login attempts or access from unknown locations.
- ☑ **Integrated threat intelligence:** Utilize threat intelligence to stay ahead of emerging threats.
- ☑ **Integrations:** Standardize and export analysis in SIEM and SOAR systems to enhance and automate current workflows.

By leveraging advanced threat detection and anomaly management, organizations can enhance their ability to detect and respond to security threats in a timely manner .

Security of connected apps

Managing third-party integrations is essential to secure the entire SaaS ecosystem. Connected apps can introduce vulnerabilities if not properly monitored and controlled. A SaaS security platform provides comprehensive tools for managing these integrations.

Why it's important:

- ☑ **Reduce the attack surface:** Monitoring and controlling third-party integrations help minimize vulnerabilities and potential entry points for attackers.
- ☑ **Ensure data security:** Proper management of connected apps reduces the risk of data leakage through unauthorized third-party access.
- ☑ **Maintain compliance:** Monitoring and controlling third-party apps strengthen compliance with regulatory requirements regarding data access and security.

Key capabilities to look for:

- ☑ **SaaS-to-SaaS monitoring:** Track and manage all third-party applications connected to your SaaS environment.
- ☑ **Access control:** Define and enforce access policies for third-party integrations.
- ☑ **Risk assessment:** Continuously assess the security posture of connected apps.
- ☑ **Automated discovery:** Identify all third-party connections and evaluate their security implications.

Securing connected apps ensures that third-party integrations do not become a weak link in your organization's security posture.

Governance, risk, and compliance (GRC)

Maintaining compliance with industry standards and regulatory requirements is critical for any organization. A SaaS security management platform helps ensure adherence to best practices and avoids potential legal and financial repercussions.

Benefits include:

- ☑ **Streamlined audits:** Efficiently manage audits with readily available logs and reports, reducing the time and effort needed to demonstrate compliance.
- ☑ **Enhanced security posture:** Continuously monitoring and managing compliance help maintain a robust security posture and reduce the risk of breaches.
- ☑ **Scalability:** Ensure that compliance requirements are consistently met across all environments as the organization grows and adopts more SaaS applications.

Key capabilities to look for:

- ☑ **Compliance mapping:** Map SaaS applications to internal policies.
- ☑ **User access visibility:** Maintain clear visibility into user access and permissions.
- ☑ **Centralized GRC view:** Provide a centralized governance, risk, and compliance view for SaaS estate configuration review and reporting.
- ☑ **Audit reporting:** Generate detailed reports for audits and regulatory reviews.

Key Features of a SaaS Security Solution

A SaaS security solution reduces complexity with management from a single pane of glass. At a glance, security teams can answer questions like what settings are on or off for a specific instance of a specific SaaS application, or who has access to what. In addition, SaaS security solution vendors provide default policies, out-of-the-box detections, universal insights, and standard reports that help organizations make decisions that lower SaaS risk.

Additional features of a SaaS security solution include:

- ☑ Discovery of and visibility into SaaS security vulnerabilities through continuous monitoring
- ☑ Alerting on potential SaaS misconfigurations and data risk exposure events
- ☑ Threat detection and prevention of suspicious user activity, plus critical unsanctioned change activities
- ☑ Regular audits of end-user privilege access and permissions, including for third-party vendors and applications
- ☑ Enforcement of strong IAM and password management policies, including implementation of MFA and SSO

An ideal SaaS security solution encompasses robust configuration and identity management, data exposure and access modeling, threat and anomalies detection, security for connected apps, and GRC capabilities. This holistic approach not only protects sensitive data but also improves operational efficiency, compliance with industry standards, and scalability as organizations expand their SaaS environment.

In the next chapter, we will explain how to implement a SaaS security program, including resource requirements, a three-phase process, and an implementation timeline.

Zero Trust principles don't always encompass SaaS applications. Even the U.S. National Security Agency (NSA) is noting this issue. But SaaS security solutions can provide continuous authorization and granular access needed to extend Zero Trust to SaaS applications.

Chapter 6

Implementing a SaaS Security Program

In this chapter

- Read about the resource requirements for a SaaS security program
- Explore the three-phase process of implementing a program
- Understand the program implementation timeline

SaaS security teams and business stakeholders should collaborate on developing an effective SaaS security program. This entails a multi-phased approach that includes allocating the necessary resources (personnel and time) for developing and executing the SaaS security program, as well as onboarding and implementing an SSPM solution.

Gather Your Resources

When starting any security program, it's important to take a proper accounting of the resource commitments needed for successful execution. For a high-level assessment of the resources required for your SaaS security program, consider the following.

People

Stakeholder identification is an important first step in collecting the resources for your program. Strive to achieve a breadth of representation while avoiding creating a group so big that you lose the ability to be nimble and act quickly. Core stakeholder groups should include but are not limited to:

- ☑ Cloud security staff
- ☑ Security operations teams
- ☑ Governance, risk, and compliance (GRC) staff
- ☑ SaaS application teams
- ☑ Internal and/or external implementation teams

Next, it is important to designate ownership of the program's management function. An owner must be nominated to conceptualize, architect, standardize, and scale the program. Since this is a security-focused program, it makes sense to house it within the security function. As such, the CISO often designates a program owner and manager. External implementation consultants, if appropriate, can assist in designing and architecting the program, with feedback from stakeholders also playing an essential role during the conceptualization phase.

Process

Implementing a robust SaaS security program to address all SaaS risks takes thoughtful prioritization and time. However, most organizations often see value immediately upon deploying a SaaS security program, as the solution can identify critical SaaS vulnerabilities, including data exposures.

The timeline for enterprise SaaS security (encompassing SSPM, threat detection, and identity security) implementations can range anywhere from six to 12 months, depending on the scope and complexity of the SaaS environment and the size of the organization. Some enterprises with a very large SaaS footprint and a high degree of complexity can expect implementation phases to exceed 12 months.

Technology

The technology aspect is a relatively simple component of a SaaS security program. SaaS security solutions were covered in depth in Chapter 5. The nature of the deployment, the initial findings derived from the SaaS security solution, and

the availability of dedicated resources will all impact the technology onboarding process.

In addition to the SaaS security solution, other technology aspects to consider include the support for third-party and your custom, domain-specific applications. Some SaaS security providers can provide protection for custom SaaS applications as well as well-known, off-the-shelf SaaS applications.

Implement Your Program

It's easy to think that when building a program, you need to know all of the applications. However, a risk-based approach provides better threat mitigation to the business. Identifying and prioritizing SaaS apps with the highest attack risks, based on the potential impact and likelihood of an incident, allow organizations to allocate resources efficiently and mitigate the most critical risks first.

We talked earlier about the Pareto principle (the 80/20 rule) as it applies to SaaS: 80% of your sensitive data lives in 20% of your applications. Start there. Prioritize securing and building your program around those apps to protect business-critical data first!

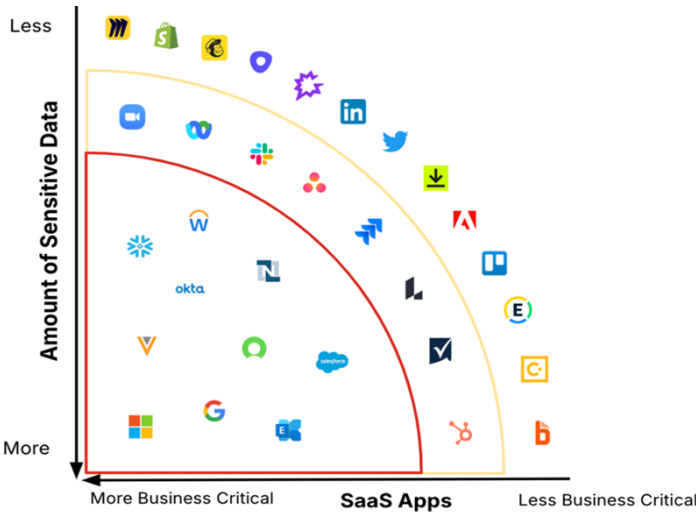

Figure 6-1: A few applications are critical to running a modern business. Securing these first can help reduce risk.

Following is a recommended three-phased approach to creating the program.

Phase 1: Initialization

- ☑ **Form a cross-functional SaaS security team.** As mentioned earlier, the organization identifies key stakeholders and assigns responsibility across different departments and levels of the organization.
- ☑ **Onboard a SaaS security platform.** Select a SaaS security solution which addresses SSPM, SaaS threat detection, and identity security capabilities. During this time, the implementation team identifies use cases, analyzes the results of the initial scan from the SaaS security solution, identifies security gaps and critical vulnerabilities, and evaluates the organization's security posture against industry best practices and standards.
- ☑ **Define current state and remediate.** The program implementation team develops a baseline of the organization's SaaS security posture using initial scan findings plotted on a cybersecurity maturity model. The team remediates critical vulnerabilities.

Phase 2: Adoption

- ☑ **Determine a timeline.** The implementation team defines realistic milestones and develops specific, measurable, achievable, relevant, and time-bound (SMART) goals.
- ☑ **Establish policies and procedures.** The security team reviews and updates its initial policies and procedures, including guidelines for SaaS procurement and vendor management. The team communicates policies and procedures to all employees.

- ☑ **Create an enterprise architecture roadmap.** The implementation team develops an enterprise architecture roadmap that incorporates SaaS adoption into the program and is aligned with the maturity model and business strategy.
- ☑ **Integrate with workflows.** The SaaS security product is integrated with existing security flows, including SIEM, SOAR, ticketing, and escalation procedures.
- ☑ **Metrics and reporting criteria.** The implementation team identifies key performance indicators (KPIs) and develops a reporting framework.

Phase 3: Formalization

- ☑ **The SaaS security program is deployed at scale.** The SaaS security platform serves as a single source of truth.
- ☑ **Roadmap for the program and maturity model.** They are based on current and future needs and priorities and include a realistic timeline.
- ☑ **Education and awareness program.** The organization implements a plan to provide ongoing education and awareness training about the security of? SaaS apps to all employees.
- ☑ **Testing and auditing.** The security team performs ongoing vulnerability assessments and audits to identify risks and ensure the SaaS security program remains aligned with business strategy and objectives.

Moving Forward

We hope at this point you have a good understanding of the risk SaaS applications pose to your organization and are ready to secure your SaaS environment. With a fully implemented SaaS security program, your organization can continue its adoption of SaaS solutions with the confidence that cloud security risks are being properly prioritized and managed.

What's Next?

Evaluate SaaS Security Solutions

- 5 Key Considerations
- Checklist
- RFP Template

Get Your Copy

appomni.com/buyers-guide

Defend your SaaS estate. Stay ahead of threats with proactive, comprehensive, and resilient SaaS security.

Adoption of SaaS has outpaced IaaS and PaaS combined, making it the largest—and least protected—cloud computing surface. As the de facto operating system for the modern organization, SaaS platforms and applications store sensitive and private data. And attackers have taken notice. It's time to prioritize SaaS security. This book will show you how.

- **Understanding the scale of SaaS adoption —** explore the cloud computing landscape and SaaS adoption trends
- **Learning the truth about SaaS security —** understand why many organizations mistakenly believe their SaaS applications are secure
- **Exploring SaaS security risks —** learn about the issues and threats that put sensitive data at risk
- **Introducing SaaS security challenges —** examine the hurdles organizations encounter when addressing SaaS risk
- **Reduce the attack surface —** understand how to reduce your attack surface with a risk-based approach
- **Implementing a SaaS security program —** learn how to get your SaaS security program started

About the Author

A former editor of SearchSecurity.com, Crystal Bedell is a senior marketing consultant specializing in cybersecurity. She's been helping technology providers create engaging content since 2000.

CYBEREDGE PRESS™

Not for resale

ISBN 978-1-948939-42-3