AppOmni
Secure Your SaaS Data

SaaS SECURITY RESEARCH BRIEF

A Risk-Based Approach to SaaS Security

By John Filitz, Sr. Tech Product Manager @ AppOmni &
Harold Byun, Chief Product Officer @ AppOmni

CONTENTS

Executive Summary 1
- Who Should Read This? 1
- Key Takeaways 2

Introduction 3

Overview 3
- Importance of SaaS 3
- Cloud Security Risk is Expanding 3
- SaaS Security is a Growing Challenge 4
- Legacy Tooling 4

SaaS Breach Vulnerability 5
- Attack Vectors 5
- Recent SaaS Breaches 5

SaaS Data Criticality 6
- SaaS Data 6

SaaS Cyber Risk Prioritization 7
- Cyber Risk Asymmetries 7
- Enabling Risk Based SaaS Security 7
- Risk-Based Cloud Security 7

Recommendations 8
- Shared Responsibility 8
- Implement Comprehensive Cloud Security 8
- Build a SaaS Security Program 8

Conclusion 9

References 10

Executive Summary

Who Should Read This?

This SaaS security research brief is intended for security and risk leaders concerned with keeping their organization's Software-as-a-Service (SaaS) estate and associated data safe and secure.

The research brief calls for a risk-based prioritization of SaaS security alongside other cloud security use cases – typically focused on public cloud infrastructure, platforms and workloads. The case for prioritizing SaaS security risk is underscored by the extent of current and expected SaaS adoption – with SaaS services being the leading driver of public cloud adoption since 2016. Not only is SaaS being adopted at an unprecedented pace, but it is fast becoming the de facto operating system for the modern enterprise.

Due to recent innovation in cybersecurity with the development of SaaS Security and Posture Management platforms, the extent of risk that SaaS represents is, for the first time, observable and quantifiable. These solutions enable unparalleled observability, continuous monitoring and control over the entire SaaS estate, and are quickly becoming an essential component to addressing SaaS security risk, comprehensively, and at scale.

Key Takeaways

The significant adoption of SaaS is set to continue over the medium term (3-5 years), and it is part of a longer digital transformation trend that will see SaaS-first strategies become the dominant business IT model in the enterprise within the next **two years**.

1. **Enterprise spend on SaaS** has consistently outpaced industry projections for the last five years, growing at a 29% Compound Annual Growth Rate (CAGR) in the 2017 to 2022 period – with enterprises spending an average of 50% more on SaaS services than Infrastructure-as-a-Service (IaaS) services (2022).
2. Of note is the nexus and growing importance of Platform-as-a-Service (PaaS) for SaaS app development and hosting, with enterprises increasingly building SaaS apps on top of PaaS providers. When looking at the spend of these two cloud services line items combined, the spend is over 2x the spend of IaaS (2022).
3. To place cloud security spend and prioritization into focus, the sector, which encompasses Cloud Access Security Brokers (CASB) and Cloud Workload Protection Platforms (CWPP) **registered a 77% CAGR** between 2018 to 2022, while application security spend registered a 17% CAGR during the same period.
4. The current concentration on conventional cloud security use cases in the enterprise fails to adequately account for the increasing and significant security risk associated with SaaS. SaaS security is starting to receive due attention, largely as a result of growing realization that SaaS is quickly becoming the de facto enterprise operating system, responsible for hosting business critical data and workflows.
5. Given the ever-expanding footprint and importance of SaaS, there is a need for a rebalancing of risk prioritization for cloud security to include SaaS security.
6. With increased size comes increased risk. SaaS represents a fast growing and poorly secured attack surface area. This is evidenced by a growing frequency of **SaaS breaches**.
7. SaaS-related breaches center on identity and permissions misconfigurations. Given that these human error-related risks cannot be comprehensively accounted for from a risk probability standpoint, every effort must be taken to address the risks from a proactive security control perspective.
8. Security and risk leaders will not effectively understand the extent of SaaS security risk faced, and the appropriate mitigation steps necessary to address it, until they establish visibility and control over the SaaS estate. It is imperative that organizations address this risk by utilizing a SaaS security solution as part of a broader SaaS security program.

Introduction

This SaaS Security Research Brief provides an overview of the current state of SaaS security, its growing importance from an attack surface perspective, and the need for a SaaS-inclusive, risk-based approach to addressing cloud security. The argument hinges on the increasingly significant role SaaS is playing in driving public cloud adoption and its growing importance within the enterprise. It also draws attention to the increasing frequency of SaaS breaches, the limitations of legacy cloud security tooling, and information asymmetries in cyber risk modeling. Finally, it underscores the need for a SaaS Security Posture Management Platform as part of a dedicated SaaS Security Program.

Overview

Importance of SaaS

Cloud computing has revolutionized the way organizations handle their data and applications. Gartner predicts that cloud computing will be the **dominant computing model** in the enterprise by 2025, rising from 41% in 2022 to 51% by 2025. Underpinning the shift to the cloud are **cloud related services**, with Gartner projecting 20.7% growth in cloud services for 2023, for a total market size of $591.8 billion – up from $490.3 billion (18.8%) in 2022.

The growth of SaaS has since 2016, been the primary driver of cloud, accounting for an average of 29% of the total spend on cloud services in the 2017 to 2022 period and is expected to continue to be the key driver of cloud for some time to come. When looking at the spend of these two cloud services line items combined, the spend is over 2x the spend of IaaS (2022).

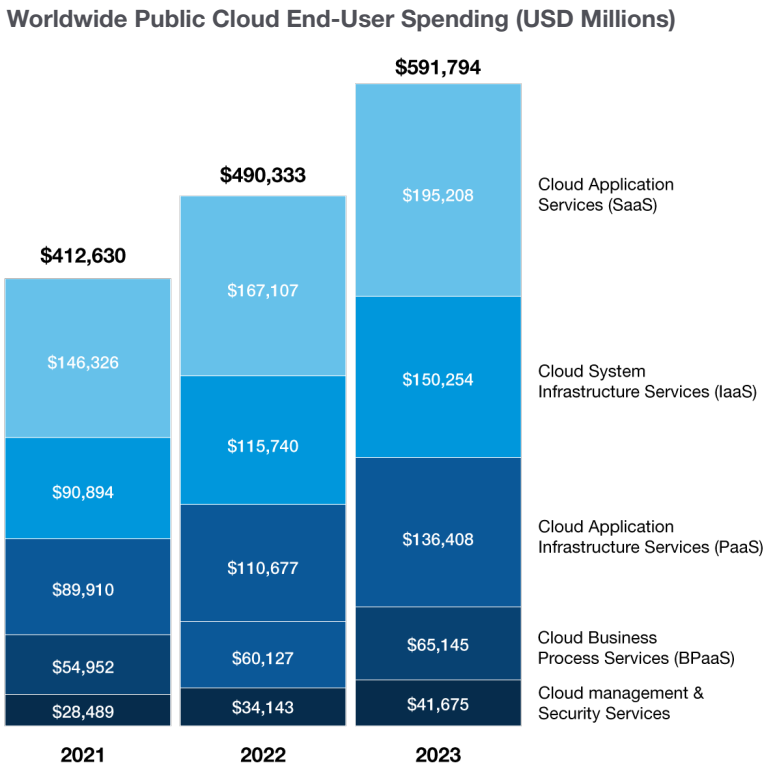

Fig. 1: Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 billion in 2023, Gartner (October 31, 2022)

Cloud Security Risk is Expanding

The adoption of cloud computing has brought with it the need for strong cybersecurity measures to protect organizations from cloud-related data breaches. Some of the early and noteworthy incidents revolved around cloud infrastructure being improperly orchestrated and provisioned, leading to data being inadvertently exposed. Although these incidents still take place, the cloud infrastructure security challenge is receiving its due attention both from a vendor and enterprise prioritization standpoint. For example, cloud security spending for **CASB and CWPP** has been the fastest-growing line item in security budgets since 2017, registering a 77% CAGR between 2018 and 2022. This is compared to a CAGR of 17% for application security during the same period.

Cloud infrastructure breach use cases include poorly configured Identity and Access Management (IAM), and over-privileged users. Additionally, one of the leading breach use cases is improperly configured data storage infrastructure that exposes data to the public internet, such as the misconfigured blob storage incident in 2022 by **Microsoft**, which exposed the data of 65,000 Microsoft customers.

Conversely, when it comes to the security of SaaS and the associated level of risk that poorly secured SaaS represents, prioritization, has until recently, been woefully inadequate. An analysis of Global 2000 companies shows that **95% have high impact security misconfigurations**; over 55% of companies have exposed data records in SaaS applications that can be retrieved without authentication, and thousands of SaaS-to-SaaS connections and third party plug-ins provide invisible, highly-permissioned access to core SaaS platforms.

SaaS Security is a Growing Challenge

SaaS is increasingly touching every aspect of the modern enterprise, from accounting to people management. It now represents the fastest-growing cloud attack surface. The average organization typically has anywhere from 500-1,000 apps deployed. Many of these apps are not in use after six months, yet they retain access and sensitive data. To further compound the challenge, the rate of configuration changes in a high-scale enterprise deployment can easily exceed 50,000 modifications in a single month on a single SaaS application instance. The challenge is more difficult when one considers SaaS-to-SaaS connectivity and tertiary cloud connections. This expands an organization's SaaS estate far beyond what most security professionals initially perceive it to be.

The number of SaaS solutions leveraged in the typical organization also does not stay static but grows each year. The combination of thousands of configuration changes and faster release cycles in SaaS environments makes manual security management an impossible task. As a result, configuration drift detection and continuous monitoring solutions are needed to keep pace with both the growth and increasing rate of change. More importantly, without centralization of visibility and control over the SaaS estate, security and risk leaders are effectively unable to assess the extent of attack surface risk their organizations face. This lack of visibility and controls creates the conditions for poor SaaS governance to manifest and consequently, increases a company's cyber risk profile.

As SaaS solutions increasingly expand within organizations, they become more vulnerable to multiple attack vectors. This includes threat actors targeting identity and permission misconfiguration risk, which can expose unauthorized access to sensitive data. SaaS solution providers themselves also appear in the cross hairs of threat actors, with numerous vendors having suffered breaches likely due to the significant breadth of attack access that these targets represent. Some compromised SaaS solutions are used by thousands of customer organizations. Notable **recent attacks** include GitHub, **Dropbox**, **CircleCI**, **Okta, and LastPass** to name a few, while a multitude of breach disclosures cite vague references to a "third party" as the source of a breach. These "third parties" are often actually SaaS applications that are operationalized for the affected company.

Legacy Tooling

A lack of awareness on the limitations of Cloud Access Security Brokers' (CASB) and Secure Web Gateways' (SWG) and their inability to protect SaaS applications is another contributing factor in the misprioritization of SaaS security risk. Legacy CASB and SWG solutions generally only provide an "outside in" view of a SaaS application, which offers limited visibility into security gaps, as opposed to SaaS security platforms that provide a much more in-depth and introspective view of SaaS misconfigurations and the effective risk. This is especially relevant considering the acceleration toward a decentralized computing model that sees end-users and third parties accessing SaaS apps directly, often without having to access the corporate network.

SaaS-to-SaaS and third-party connections are invisible to these legacy cloud security solutions. Conventional approaches to securing cloud network access are no longer sufficient for protecting the numerous ways SaaS is accessed and utilized across corporate and remote environments.

The complex nature of SaaS platforms has introduced new security risks that CASBs and legacy software can't address.

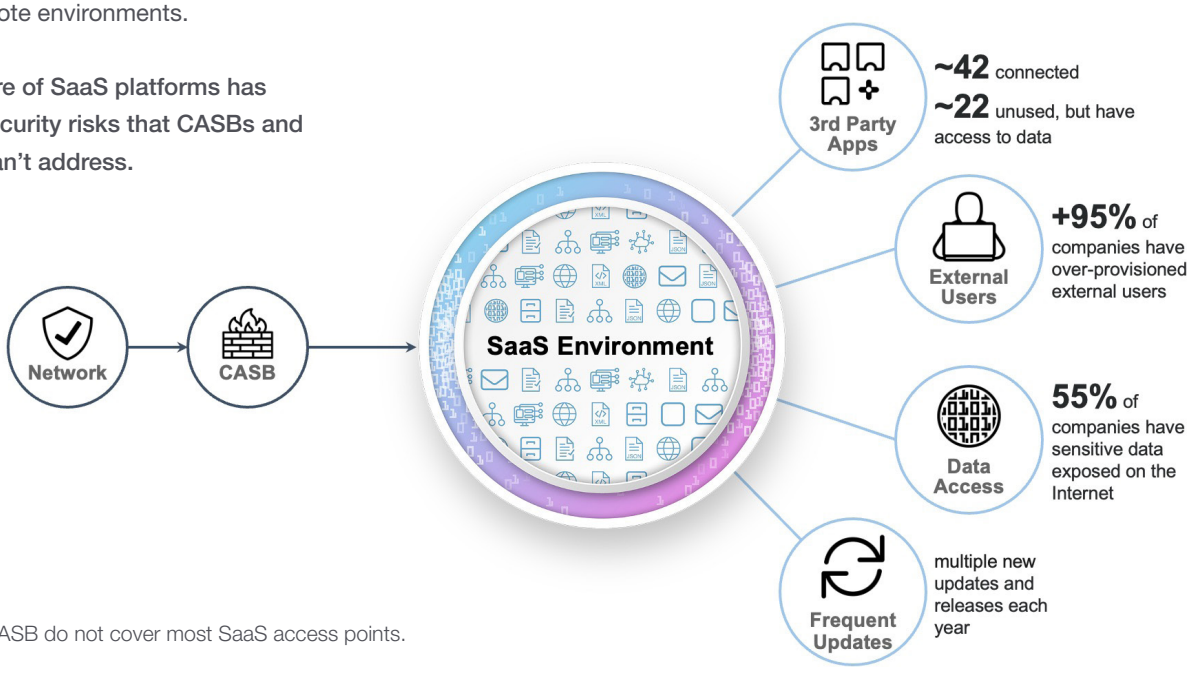

Fig. 2: Network and CASB do not cover most SaaS access points.

SaaS Breach Vulnerability

Attack Vectors

The threat model for SaaS and SaaS data breaches differs from traditional network and infrastructure attacks. Data theft in SaaS behaves much more like a "smash and grab" operation, so ensuring appropriate access control and configuration represents the most significant method for reducing risk. Addressing the attack surface and posture becomes more critical because there is no prolonged kill chain event for SaaS data breaches.

As organizations look to accelerate the release of services and new applications, many turned to utilization of the Platform-as-a-Service layer to develop and deploy SaaS on top of SaaS. While this greatly enables development teams to move faster, security teams often have little to no visibility into the release process and have limited ability to provide guard rails on the developers and their code. The lack of visibility and control over applications makes them appear secure on the surface, but the entire underlying data schema may be exposed through poor ACL definition or a lack of knowledge of best practices. This is a classic security dilemma where organizations try to move quickly while overlooking security implications.

End-users also represent another attack vector for SaaS since they directly access the applications often with elevated or administrative permissions scopes. This means that they have elevated privileges, making them susceptible to end-user targeted social engineering attacks such as phishing or malware-based attacks that enable remote access.

Some of the common SaaS attack vectors include:

- Phishing
- Account Takeover
- Credential stuffing and brute force attacks
- Man-in-the-middle attacks and multi-factor authentication compromise
- Data exposure through misconfiguration
- Supply chain/ third-party compromise
- Remote Access Trojan

Recent SaaS Breaches

The consequences of a SaaS breach can be significant, resulting in financial and reputational damage. Common negative impacts of SaaS breaches include the loss of customer data, intellectual property, or financial data. Besides the immediate negative impact arising from a breach, it can also have a lasting impact on the organization's reputation and financial stability, resulting from a loss of customer trust.

The interconnected nature of SaaS attacks often involve a trusted third-party, either up or downstream from the compromised entity. Below are some of the notable SaaS compromises in 2022 where the third-party developer platform GitHub was involved, hosting the source code for the majority of SaaS companies. Many of these companies were unaware that their systems had been compromised, but were instead informed by third-parties:

- **Microsoft:** In March 2022, Microsoft confirmed that it was breached hours after LAPSUS$, a cyber extortion group, conducted a phishing attack against an employee which resulted in the theft of source code on Github.
- **AstraZeneca:** A developer's credentials for an internal server was compromised via exposure on GitHub in 2021 for more than a year. The mistake resulted in exposed access to sensitive patient data.
- **CircleCI:** CircleCI was alerted to suspicious GitHub OAuth activity by one of its customers in early 2023, which resulted in the breach discovery with attribution to an earlier phishing attack and account compromise against its employees.
- **Dropbox:** The code that was accessed by threat actors on GitHub in late 2022 contained API keys used by Dropbox developers as well as employee and vendor names, modified third-party libraries, internal prototypes, security team tools, and configuration files. GitHub notified Dropbox of the breach compromising 130 Dropbox GitHub repos.

- **Toyota:** Threat actors obtained credentials for one of its servers by using the source code for a website published on GitHub by a subcontractor. The third-party had uploaded part of the source code to their GitHub account while it was set to be public, exposing 29,000 customers' data for five years. Toyota became aware of the breach in late 2022.
- **Travis CI & Heroku:** OAuth tokens were stolen to GitHub repositories that were attributed to an upstream supply chain attack. GitHub notified both customers of the breaches in early 2022.
- **Slack:** Threat actors gained access to Slack's GitHub repos via a limited number of stolen employee OAuth tokens.

SaaS Data Criticality

SaaS Data

Few organizations acknowledge the extent to which SaaS applications have become the de facto operating system, hosting critical business data and workflows. Depending on the nature of the business or industry (e.g. financial services, healthcare or legal) and the type of application (e.g. security, payroll, or people management), the nature of the data and associated fallout arising from a breach will vary. Most apps, especially those used in the enterprise, contain a trove of sensitive data that if exposed can result in the organization suffering damages in excess of the initial fallout from the breach. This can include the loss of intellectual property, incurring regulatory penalties, class action lawsuits, and the loss of customer trust.

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

1. User and account information:
    a. User profiles and records (names, email addresses, phone numbers, sensitive PII, PHI).
    b. Authentication and authorization data (passwords, access tokens, permissions).
2. Customer and client data:
    a. Customer profiles (company name, address, contact details).
    b. Interaction/communication history (emails, transcriptions, video recordings, meeting notes).
    c. Sales opportunities and pipeline data (competitive intelligence, leads, prospects, deals).
3. Product, service, and financial data:
    a. Product or service data.
    b. Billing and subscription details (payment methods, invoice history, plan details).
    c. Order history (purchase orders, invoices, shipping details).
    d. Financial operations data.
4. Business process data:
    a. Project management information (tasks, deadlines, resources, progress).
    b. Document and file management (contracts, proposals, marketing materials).
    c. Collaboration data (chat messages, comments, shared files).
5. Reporting and analytics:
    a. Custom reports and dashboards.
    b. Data integrations with third-party services (CRMs, ERPs, marketing automation tools).
6. Security and compliance data:
    a. Audit logs (login attempts, data access, changes made).
    b. Data backups and recovery information.
    c. Compliance documentation (e.g., GDPR, HIPAA, SOC 2).
    d. Security settings and configurations.

SaaS Cyber Risk Prioritization

Cyber Risk Asymmetries

Risk assessments are limited by the scope of information that is available. This applies both to the asset as well as to the perceived risks and the severity of those risks. The adage of “unknown unknowns” applies here. For example, the lack of visibility in IT environments with reference to attack surface risk is a significant contributing factor to unreliable and incomplete cyber risk assessments. The failure to prioritize cybersecurity risk mitigation can have serious consequences, exposing an organization to significant risk of a data breach.

Without access to comprehensive data on the attack surface risk for SaaS, businesses may fail to address high-impact security findings that increase their cyber risk. The breach blast radius can be far-reaching, and disruption to business operations is likely, without the appropriate security and risk controls in place.

Before the advent of SaaS Security Posture Management solutions, security practitioners and IT teams had the arduous task of manually and retroactively enforcing some semblance of governance over an ever-increasing attack surface, that wasn’t fully visible. This approach proved ineffective given the high frequency of SaaS estate expansion and configuration changes. What was missing was a universal control plane that enabled visibility into configuration and data exposure risk across the entire SaaS estate.

Enabling Risk Based SaaS Security

The development of SaaS Security Posture Management Platforms (or SSPM), tasked to address SaaS security risk at scale, now offer enterprises a way to address SaaS security concerns.

Core capabilities of this SaaS security tooling depend on enabling:

- Visibility and control over the SaaS estate at scale, preventing data exposure and critical misconfigurations.
- Continuous monitoring to alert on configuration drift and ensure adherence to a best practices baseline.
- Comprehensive user activity and threat monitoring.

Risk-Based Cloud Security

Leveraging SaaS Security and Posture Management tooling now enables risk practitioners to undertake a risk-based approach of prioritizing SaaS security alongside other cyber risks in the environment.

The standard approach to cybersecurity risk prioritization modeling detailed below can serve as a starting point for undertaking such an assessment:

- **Asset identification:** The functional role of the asset to the organization.
- **Criticality:** The value of the information/data that is processed or stored by the asset.
- **Impact:** The likely impact of a breach, the impact of the asset and its data being compromised (aka the blast radius and business impact).
- **Resource allocation:** Prioritizing security resources based on the value of assets, ensuring that the cost of protection is proportional to the assets’ value.
- **Prioritization:** Prioritized security based on results of the risk assessment with a focus on protecting the most critical assets first. Assets deemed high value should be given a higher level of prioritization and protection.

Recommendations

Shared Responsibility

Although ungoverned SaaS apps are a serious security risk, they have not received due attention by security and risk leaders until recently. Much like the initial stages of cloud adoption, early cloud users failed to recognize that the safety of their data relied heavily on accepting the shared responsibility model. The responsibility for securing SaaS apps from a configuration standpoint rests solely with the customer, with IAM controls responsibility equally shared.

Fig. 3: Cloud Security Shared Responsibility Model, UK NCSC

Implement Comprehensive Cloud Security

Organizations must adopt a comprehensive approach to cloud security, one that accounts for known and unknown risks brought on by SaaS apps and SaaS-to-SaaS connections.

The key first step to creating a risk-based cloud security strategy is to adopt an SSPM solution that establishes visibility into risks and a baseline for configuration management of your SaaS environments.

Benefits of SSPM:

- Discovery and visibility into SaaS security vulnerabilities through continuous monitoring.
- Providing alerts to any potential SaaS misconfiguration and data risk exposure events in your system.
- Detecting threats and preventing suspicious end-user activity.
- Conducting regular end-user privilege access and permissions audits, including for third-party vendors and applications.
- Removing and decommissioning dormant and unauthorized apps and user accounts on a routine basis.
- Enforcing strong IAM and password management policies, including implementation of Multi Factor Authentication (MFA) and Single Sign On (SSO).

Build a SaaS Security Program

Beyond the tooling, SaaS security and business stakeholders should collaborate on developing an effective SaaS security program. This entails a multi-phased approach that includes education and awareness, as well as allocating the necessary resources (personnel and time) to develop and execute a SaaS security program as part of the organization's cloud security strategy. A risk-based approach to SaaS security allows organizations to mitigate the current and anticipated risks associated with SaaS solutions, especially as the SaaS footprint grows in prominence. It also enables organizations to more comprehensively address cloud security risk.

Conclusion

The goal of AppOmni SaaS Security Research Brief is to call for a comprehensive, risk-based approach to cloud security. One that sees SaaS security as a core component given the amount of budgetary spend on SaaS, the sensitivity of the data held in these environments, and an almost complete lack of compensating security controls.

The decentralization of IT and computing, combined with the continued acceleration of SaaS adoption will make the challenge of securing your SaaS estate and associated data footprint increasingly challenging. On this basis, having an effective SaaS security solution and the associated security risk observability and control that this enables is fast becoming integral to bolstering cybersecurity resilience.

By investing in SaaS-specific security tools, educating employees on the risks associated with SaaS solutions, and enhancing cloud security risk modeling techniques, organizations can improve their overall cybersecurity posture while protecting their end-users and their data from cyber threats.

At a more fundamental level, however, to address SaaS security risks comprehensively, organizations must adopt a risk-based approach to SaaS security. This approach executes SaaS security initiatives as part of a dedicated SaaS security program that is aligned with an organization's investment in, and operational leverage of SaaS, including the associated value of the data.

References

1. AppOmni. (2023). SaaS Breach Info Center [accessed 4/3/23]
2. Byun, H. (2022). LastPass and Okta Breaches: Security Steps to Take Right Now, AppOmni [accessed 4/3/23]
3. DarkReading. (2022). CircleCI, GitHub Users Targeted in Phishing Campaign [accessed 4/3/23]
4. Filitz, J. (2023). Just How Vulnerable is Your SaaS Supply Chain to Compromise? AppOmni [accessed 4/3/23]
5. Gatchell, D. (2023). Unpacking (and Preventing) the CircleCI Data Breach, AppOmni [accessed 4/3/23]
6. Gatlan, S. (2022). Dropbox discloses breach after hacker stole 130 GitHub repositories. BleepingComputer [accessed 4/3/23]
7. Gartner. (2022). Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025 [accessed 4/3/23]
8. Gartner. (2022). Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023 [accessed 4/3/23]
9. Gartner. (2022). Gartner Identifies Three Factors Influencing Growth in Security Spending [accessed 4/3/23]
10. Gartner. (2018). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019 [accessed 4/3/23]
11. Gartner. (2020). Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020 [accessed 4/3/23]
12. Gartner. (2017). Gartner Forecasts Worldwide Public Cloud Services Revenue to Reach $260 Billion in 2017 [accessed 4/3/23]
13. ISC2 and Cybersecurity Insiders. (2022). Cloud Security Report [accessed 4/3/23]
14. Microsoft. (2022). DEV-0537 criminal actor targeting organizations for data exfiltration and destruction [accessed 4/3/23]
15. National Cyber Security Centre. (2023). Cloud Security Shared Responsibility Model [accessed 4/3/23]
16. The Stack. (2022). GitHub hacked, npm data stolen after 0auth tokens stolen in upstream breach [accessed 4/3/23]
17. Wadhwani, S. (2022). Misconfigured Azure Blob Storage Exposed the Data of 65K Companies and 548K Users, Spiceworks [accessed 4/3/23]
18. Wadhwani, S. (2022). Toyota Suffers Data Breach from “Mistakenly” Exposed Access Key on GitHub, Spiceworks [accessed 4/3/23]
19. Wallarm, I. (2023). Slack GitHub Account Hacked via Stolen Employee API Token. Security Boulevard [accessed 4/3/23]
20. Whittaker, Z. (2022). AstraZeneca password lapse exposed patient data. TechCrunch [accessed 4/3/23]

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