AppOmni

TECHNICAL WHITEPAPER

HOW SAAS IS CHANGING SECURITY OPERATIONS

©APRIL 2019 APPOMNI, ALL RIGHTS RESERVED

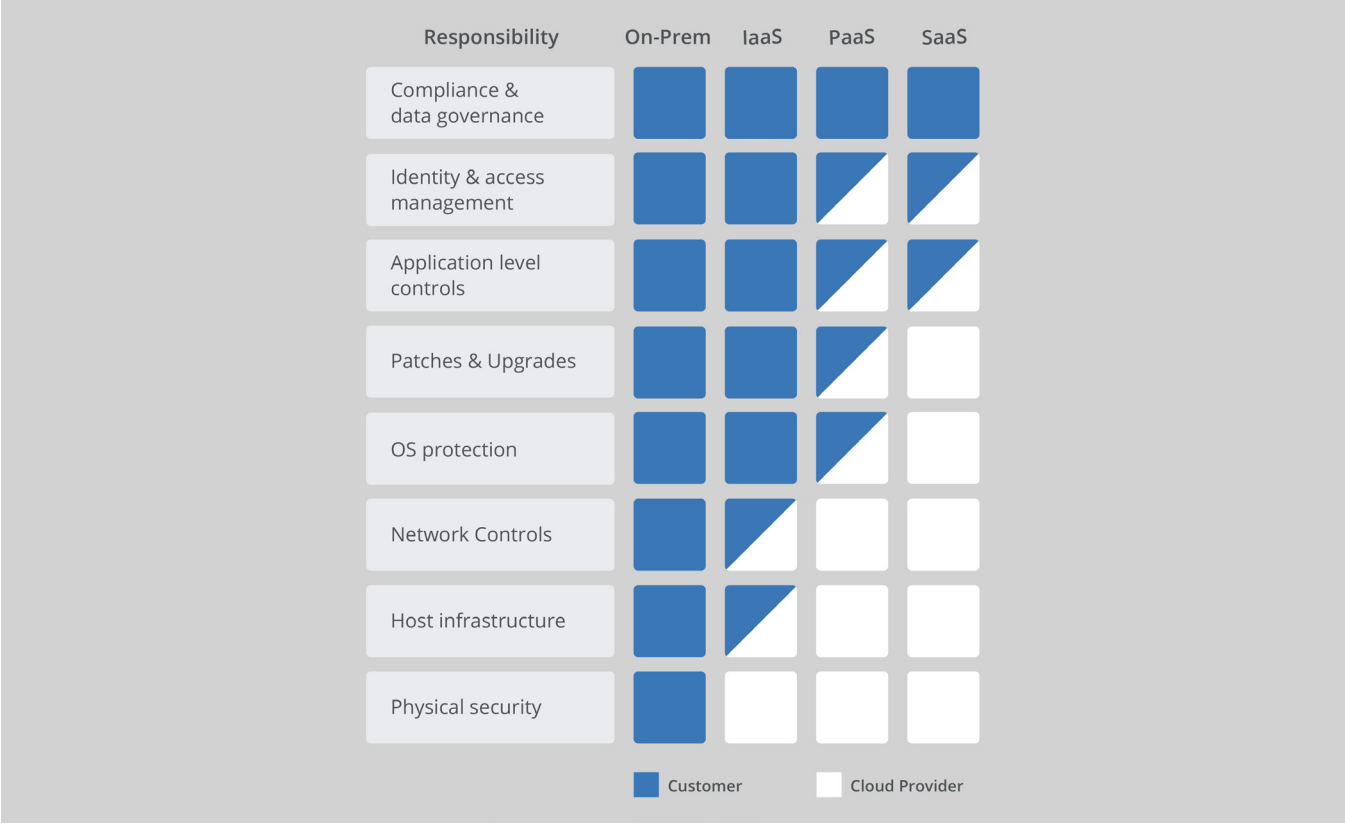
TABLE OF CONTENTS

HOW SOFTWARE AS A SERVICE IS CHANGING SECURITY OPERATIONS

Software as a Service has become the de-facto standard for application delivery across the enterprise. Every year, more and more desktop applications are moving to the cloud, and new native SaaS applications emerge on the market. In this model, the application code, configuration, security access control, and database now exist completely within the SaaS provider's environment. The benefits of SaaS are many. Reduced time to value for users, lower up-front costs, ease of delivery and scalability, and continuous upgrades and new functionality. However, SaaS also presents new challenges in the realms of cybersecurity, data governance, and compliance.

SHARED RESPONSIBILITY IN THE CLOUD

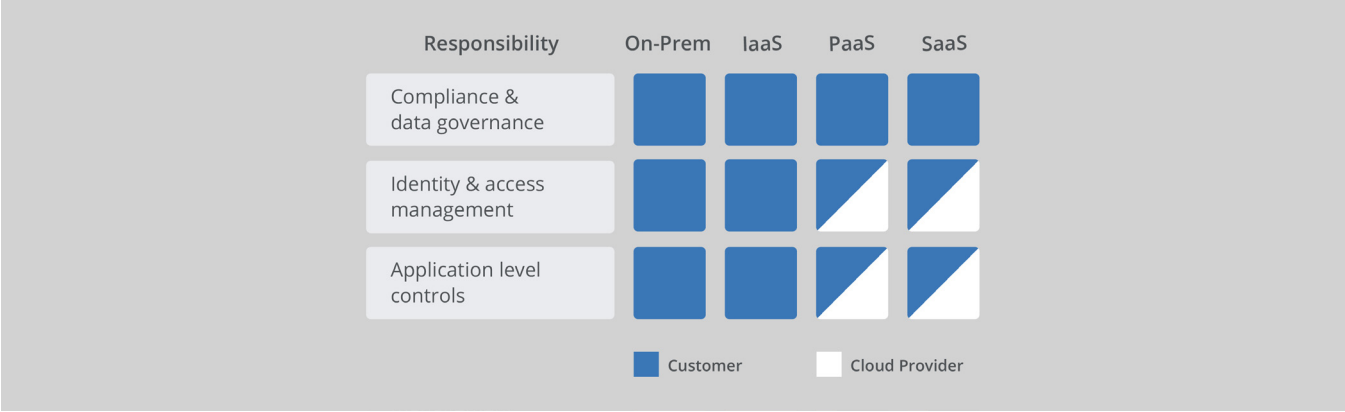
By now most security organizations have heard of the Shared Responsibility Model in Cloud Computing. It delineates which responsibilities fall upon the cloud provider, and which remain with the customer. The Shared Responsibility Model can be divided into 3 categories: IaaS, Paas, and SaaS.



Of these 3 categories Software as a Service (SaaS) is the most widely used,v and the least understood. The Global **SaaS Market size** is expected to reach **$185.8 billion** by 2024, and rising at a compound annual **growth rate of 21.4%**.

vMost security controls are deployed in two logical places: on the corporate network, or host operating systems. When it comes to SaaS, this approach doesn't quite fit. The cloud provider owns both the network and the underlying operating systems that power their applications. They handle firewall and network monitoring, OS hardening, and patch management on behalf of their customers. When it comes to application security, SaaS companies are often very good at preventing common flaws such as SQL Injection and Cross Site Scripting. With all those things covered, what's left for security teams to do?

Take another look at the Shared Responsibility Model. Customers maintain responsibility for configuring the application and its security controls, identity and access management, and data governance / compliance.



SAAS IS COMPLEX

There is a trend across enterprise IT toward slimmer endpoint operating systems. Tasks that once required bulky workstations on the desktop have moved to smartphones, tablets, Chromebooks, and IoT devices. At the same time, more and more application and business logic is moving into the cloud. Customers can now run almost any conceivable business process within a SaaS application. Software as a Service applications are flexible, powerful, and extremely customizable. They are also complex and this leaves companies at major risk of data breaches and security exposure. Not because the Cloud provider is insecure, but because the customer is unintentionally leaking their data through user error.

ATTACKERS DON'T NEED SQL INJECTION WHEN THE DATA IS ALREADY EXPOSED.

Each Cloud provider has a variety of capabilities and controls for customers to secure access to their information. However, the data access and security models are unique to each SaaS application

and ecosystem. Cloud applications natively support a variety of identities and user types, including enterprise users, customers, partners, contractors, application integrations, and devices. This creates a complex web of settings, permissions, identities, and access methods for organizations to manage that current tools are ill-equipped to properly interrogate or monitor. Most SaaS applications are managed by users with limited security expertise and are unaware of the unintentional leakage of sensitive data. It should not come as a surprise to learn that AppOmni has found extremely sensitive data exposed across hundreds of SaaS applications.

Since 2018, AppOmni has found:

```
drivers licenses            passports
medical records             patient prescriptions
financial transactions      invoices
social security numbers     encryption keys
passwords                   emails
contracts                   legal communications
revenue forecasts           customer lists
HR records                  sales quotes
```

WHY TRADITIONAL SECURITY APPROACHES DON'T WORK FOR SAAS

Today companies use a variety of tools deployed on the server and endpoint OS to help manage security. Centralized management tools for data protection, standardization, and detecting security anomalies and events are common place in the enterprise. But for SaaS applications, these OS-based tools simply don't provide the same value. In the past, applications ran on the local OS and accessed data stored on the hard drive or across the LAN. OS based tools could effectively monitor these applications and processes and provide a layer of protection to sensitive data. With SaaS, endpoint tools only see that the browser is running. They do not have the ability to monitor the applications, processes, or data within the cloud provider's environment.

NETWORKS ARE EVOLVING

There are two major shifts happening in networking technology that will drastically change the way organizations protect their users and data. TLS 1.3 and the reality of 5G wireless networks.

Transport Layer Security version 1.3 is a major revision to the protocol and provides a new set of capabilities to ensure the privacy and security of network communications. As a design goal, TLS 1.3 attempts to make inspection of encrypted traffic exceedingly difficult. As browsers and cloud providers adopt support for TLS 1.3, traditional security controls that rely upon intercepting and decrypting network traffic will stop working the way they do today. Additionally, the move to 5th Generation (5G) networks will allow for data rates up to 10 Gbps. This will empower users to truly work from anywhere, and Internet of Things (IoT) devices to send and receive vast amounts of data to the cloud. The old architecture of centralizing security controls around LAN-based egress to the Internet will become less and less effective.

SECURITY BUILT FOR SAAS

A new approach is needed to secure and monitor data access in SaaS applications. At AppOmni, we see three major gaps in security capabilities:

- **First and foremost, security teams need Visibility. Visibility into what data their organization has in the Cloud, and who has access to it. The ability to scan their cloud applications and identify data leaks and security exposures.**
- **The ability to apply security and data access policies consistently across their cloud applications. Whether it's multiple instances and applications from a single provider, or multiple applications across multiple cloud providers, security teams need assurance that appropriate access controls are in place.**
- **Continuous monitoring for data leaks and security exposures, integrated into their current workflow. Most security teams already suffer from "alert fatigue." They don't need more noise or more false positives. Instead, they need actionable alerts for security events in cloud applications, integrated with existing tools and workflows.**

HELP IS HERE

AppOmni helps security teams Scan, Secure, and Monitor their SaaS applications. Our patented technology deeply scans SaaS APIs and configurations, identifying data leaks in minutes. Apply consistent access controls and data governance across your cloud applications with our policy engine. Continuously monitor your SaaS applications for security events, and integrate detection and response capabilities with your existing workflow.