

# Secure sensitive cloud data for SaaS applications

## Key Benefits

- Gain visibility into access rights from all users and applications
- Continuously monitor privileges and permissions
- Receive guided remediation recommendations
- Compare changes to users and applications across time
- Confirm accurate access levels with 100 percent certainty

“No one has better security than the big public cloud providers. Almost all of the cloud security failures have been attributed to customer actions.”

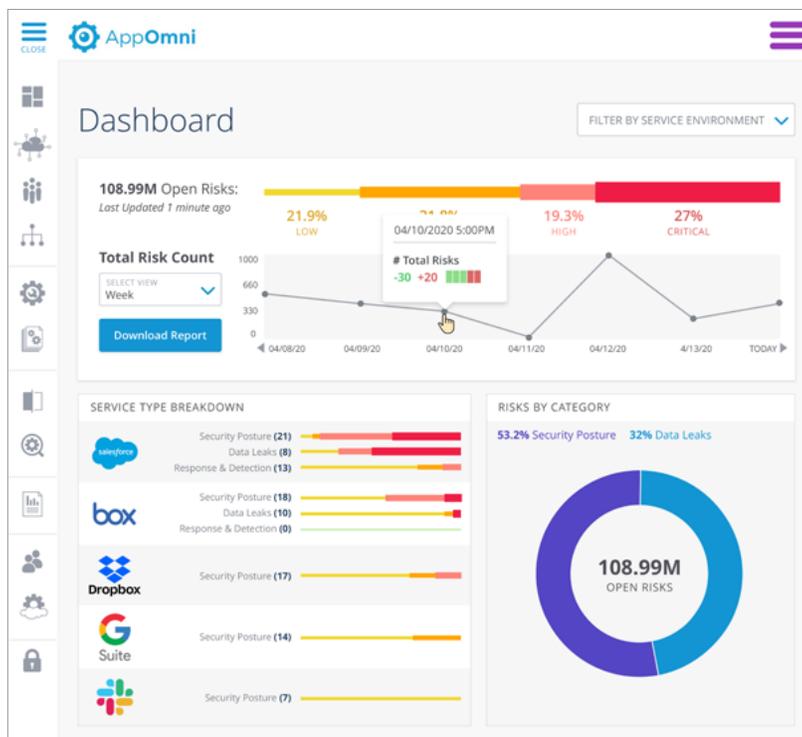
– Craig Lawson  
Gartner Research VP

As enterprise software as a service (SaaS) adoption hits double digit expected growth rates, high-profile SaaS application data breaches are rising too. Gateway architecture solutions dominate the market, but they lack visibility into the unique characteristics of each SaaS application. Keeping up with SaaS providers' security configurations can be overwhelming for an enterprise already facing cybersecurity staffing shortages. Unfortunately, as a result of these burdens, Gartner predicts that through 2025, 99% of cloud security failures will be the customer's fault.

Enterprises need a new approach that provides visibility into their many SaaS platforms including their configuration, data exposure, and regulatory risks. This solution must also leverage the latest controls and security features available from SaaS providers without requiring additional in-house expertise. An effective approach must also continuously enforce business policies and offer a quick and simple path to remediation that integrates with existing processes and technology.

## AppOmni Enterprise

AppOmni Enterprise is the first solution of its kind, streamlining the process of configuring and managing SaaS applications to meet the security needs of the enterprise. The platform offers unprecedented data access visibility, management, and security controls, seamlessly securing mission-critical and sensitive data. In addition to providing visibility into the SaaS applications that power the organization, AppOmni Enterprise provides continuous monitoring, enforcement, and guided remediation.



<sup>1</sup> Gartner Forecast Worldwide Public Cloud Apr 2019

<sup>2</sup> Brookes, J. (2018, August 20). Expect More Data Breaches But Don't Blame Cloud Providers: Gartner. Retrieved January 15, 2020, from <https://which-50.com/expect-more-data-breaches-but-dont-blame-cloud-providers-gartner/>

## Data Visibility

AppOmni Enterprise offers unparalleled visibility and insight into SaaS application data. A dashboard provides an at-a-glance summary of all alerts and policy violations requiring attention. The drilldown and filter capabilities allow for detailed investigation with just a few clicks, and administrators can also “snooze” the alert for future analysis.

Security, IT, and compliance teams can easily identify the effective access of any user or role. Rather than manually piecing together various settings and configurations to build a mental map of access, AppOmni’s **Access Explorer** gives administrators a direct view of what each user or role can see and do. **Mimic** allows administrators to interact with the enterprise’s platforms and tools as a certain user or role to definitively validate data access policies. With Access Explorer and Mimic, SaaS application administrators can operate with 100 percent certainty that users have correct access rights.

Users aren’t the only ones with access to sensitive data — SaaS applications are often connected to a host of third party cloud applications, all with varying degrees of permissions. AppOmni Enterprise provides visibility into all cloud-to-cloud integrations and the data to which these applications have access.

## Continuous Monitoring

AppOmni Enterprise continuously and automatically monitors who has access to data in your SaaS applications, ensuring that access levels always match business intent. The platform also monitors whether access adheres to regulatory requirements such as GDPR, PCI, and more.

With the proprietary technology behind AppOmni’s **Policy Engine**, Security, IT, and Compliance teams can design a wide range of policies to monitor SaaS applications. Administrators can also immediately deploy pre-built policies that support common use cases.

Policy Engine continuously monitors your SaaS applications and user roles for any changes in data access or configuration. If and when the Policy Engine detects changes, it ensures that no new access has been granted that violates your maximum allowed access settings. Conversely, functional policies ensure that changes to user roles don’t impact the minimum access required for people to perform their jobs.

The Policy Engine also ensures that all of your SaaS applications remain configured properly and as required by your business and compliance needs. Not only do these policies reduce trouble tickets, but they also can streamline deployments by allowing your team to validate functionality against policies prior to production releases.

## Guided Remediation

AppOmni Enterprise provides flexible workflows for remediation. Administrators can route policy violation alerts to an existing SEIM solution, work management solutions such as Jira, or collaboration applications such as Slack. AppOmni customers can also create internal and custom notifications via webhooks to systems they designate.

To remediate incidents, SaaS application administrators often require insight into not just a snapshot of user access today but also the history of how that access has evolved — in some cases, erroneously. **Time Travel** shows a comparison of user access between two points in time. The feature can also pinpoint when a particular third party application was installed or when a user was mistakenly granted a new access right. These capabilities empower security and IT teams to focus their investigation on what access has changed since their last audit or approved rollout, greatly reducing their time spent on investigation and remediation.

In addition, AppOmni’s built-in reporting features greatly aid administrators in troubleshooting and remediating incidents. Reports ranging from connected application details and access reports to changes in user types and high-level report cards are all readily available.

**ABOUT APPOMNI** AppOmni is the leading software as a service (SaaS) data security and management platform for the enterprise. AppOmni provides unprecedented data access visibility, management, and security of SaaS solutions, enabling organizations to secure mission-critical and sensitive data. AppOmni’s patent-pending technology comprehensively scans APIs, security controls, and configuration settings to evaluate the current state of SaaS deployments and compare against best practices and business intent. With AppOmni, organizations can establish rules for data access, data sharing, and third party applications that will be continuously and automatically validated. The company’s leadership team brings expertise and innovation from leading SaaS providers, high tech companies, and cybersecurity vendors.