Market Guide for SaaS Management Platforms

Published 10 February 2021 - ID G00722449 - 17 min read

By Analysts Chris Silva, Manjunath Bhat, Dan Wilson, Ryan Stefani

Initiatives: Digital Workplace Infrastructure and Operations

Managing SaaS applications with disparate admin controls decreases IT’s ability to track usage, automate management tasks and establish consistent security posture across the portfolio. Scalable SaaS portfolio management requires I&O leaders to adopt SMP tools.

Overview

Key Findings

- The market for SaaS management platforms (SMPs) has matured, with core capabilities to discover SaaS applications, manage their use, automate workflows, and establish consistent identity, access and data governance controls across SaaS applications.

- Gartner defines SMPs as tools that provide the ability to centrally manage and operate multiple SaaS applications, offering a single point of management for multiple apps.

- SMPs vary in the depth of function offered in the three functional areas of an SMP: discovery of apps, management and automation of administrative functions, and provision of a central point for enforcing app and data security for the SaaS portfolio.

Recommendations

Infrastructure and operations (I&O) leaders focused on digital workplace infrastructure and operations must:

- Increase visibility into SaaS usage, improve manageability and automate repetitive SaaS administration tasks, while improving consistency of securing identities and data across SaaS applications by adopting an SMP.

- Achieve the greatest efficiency benefits for IT by choosing the SMP that can support the majority of SaaS apps in use and that offers the greatest number of integration points in the functional pillars of greatest importance.

- Drive continuous improvement by leveraging the SMP to monitor and optimize SaaS license entitlements based on consumption and drive adoption of SaaS apps, and measure the performance
Strategic Planning Assumption
By 2026, 50% of organizations using multiple SaaS applications will centralize management and usage metrics of these apps using an SMP tool, an increase from less than 20% in 2021.

Market Definition
Gartner defines SMPs as stand-alone tools that can discover, manage and secure multiple SaaS applications from a central admin dashboard, delivered as a turnkey service. SMP tools are offered by pure-play vendors whose business is focused on this offer, as well as by traditional software asset management (SAM) vendors, cloud platform management and cloud migration vendors, cloud security offerings such as cloud access security brokers (CASBs) and, more recently, some IT service management (ITSM) vendors. Gartner views these as partially competitive with the pure-play SMP vendors, as they don’t fully address all three pillars of SMP.

Market Description
The main functions of SMP tools are (see Figure 1):

Figure 1: What Is a SaaS Management Platform?

What Is a SaaS Management Platform

Discover
Manage
Secure

Source: Gartner 722449_C
Discovery: SMPs ingest information from various other infrastructure, such as identity federation services, expense management tools and client-side browser extensions, to create a central repository of data on all SaaS apps in use.

Management/automation: SMPs centralize SaaS applications’ management controls and role-based control sets in a single, central location. These capabilities include automation of common SaaS management tasks, such as user onboarding and offboarding, entitlement management, migration, and reassignment of application data.

Security: SMPs provide a central place to harmonize data protection policies, entitlements and access controls for multiple SaaS applications, or to centralize controls and establish a parity of security and control across disparate SaaS applications. The level of control and interactivity will vary depending on the SMP's integration; tools that have a one-way “read only” relationship with the SaaS tool will be able to identify, but not actively remediate, issues. Tools with bidirectional integration "read/write" for a given SaaS app will be able to actively take steps to remediate issues.

It is imperative to gauge the level of interaction an SMP offers with the SaaS apps it can manage. Gartner has noted that, even within a single SMP, integration types can vary by app supported. Some SMPs will offer bidirectional read/write integration for some apps, allowing reporting of information and the ability to take actions or change settings in the SaaS app's management console. Other integrations may only be one-way, “read only” integrations, where the ingestion and reporting of data from the SaaS app's console is possible.

This distinction is important, SaaS apps integrated with the SMP in a one-way fashion can only identify issues, whereas bidirectional integrations will identify issues and can take action based on those identified. Not all tools will offer bidirectional integration with all relevant SaaS apps, and a mix of one-way and bidirectional integrations with the SMP across the SaaS portfolio is common.

The tools, through their security capabilities, are critical to establish consistent security policy and compliance across multiple SaaS vendors or tenants, and to provide visibility into sensitive data context for adaptive access decision making within secure access service edge (SASE) and CASB architectures.

Gartner believes that the tools in the SMP market can deliver value today. We expect to see continued, modest growth in this market, influenced by the growth in procurement and consumption of SaaS applications due to remote and hybrid work; Gartner has observed a shift toward multi-SaaS management in tools that initially focused on single-SaaS management.

Organizations can expect the following outcomes from adopting an SMP:

Visibility and cost control:

Better visibility leads to a clearer and more complete picture of the SaaS app mix and identifies any application or license redundancies.
The market for SMP consists of both pure-play SaaS-only management tools and SAM tools that have extended their software license and operational management to SaaS-based applications. Traditional SAM tools are still largely focused on the management of non-SaaS applications where an installation is present. However, leading SAM vendors are increasingly adding capabilities natively, or through acquisition, to support the discovery of SaaS applications and manage licenses. Additionally, Gartner has identified new and emerging SAM vendors that focus solely on the management of SaaS applications. These new SAM for SaaS vendors emphasize their ability to discover SaaS, manage contracts and optimize SaaS spend. In some cases, these SAM for SaaS vendors also provide workflow automation to improve the allocation of licenses, approvals to provision and notifications to drive actions to stakeholders involved in managing SaaS applications.

In similar fashion to the limited role SAM tools play in managing SaaS, SMPs also offer limited, if any, functionality to manage other cloud workloads. Management of PaaS and IaaS environments, often considered a capability of cloud management platforms (CMPs), is not included in the scope of SMPs by Gartner’s definition, and based on the in-market capabilities from the sample vendors outlined in this research.

**Market Direction**

- Identify consumption of SaaS services by providing dynamic data useful in opportunities to optimize SaaS investments based on actual consumption.

**Management and automation:**

- Create and automate workflows for common, repetitive processes such as employee onboarding, license assignment and license revocation, and offboarding,
- Create and modify groups or workstream collaboration spaces.
- Provide visibility into usage and patterns of use across SaaS apps to contribute to continuous improvements in employee experience.

**Security and access:**

- Integrate with data governance, endpoint management, endpoint security, and identity access management (IAM) tools and processes to gain a complete picture of SaaS app usage and integrations.
- Improve security posture and provide context for CASB/SASE.
- Manage, automate and enforce configuration policies consistently across the SaaS application portfolio.

The market for SMP consists of both pure-play SaaS-only management tools and SAM tools that have extended their software license and operational management to SaaS-based applications.

Traditional SAM tools are still largely focused on the management of non-SaaS applications where an installation is present. However, leading SAM vendors are increasingly adding capabilities natively, or through acquisition, to support the discovery of SaaS applications and manage licenses. Additionally, Gartner has identified new and emerging SAM vendors that focus solely on the management of SaaS applications. These new SAM for SaaS vendors emphasize their ability to discover SaaS, manage contracts and optimize SaaS spend. In some cases, these SAM for SaaS vendors also provide workflow automation to improve the allocation of licenses, approvals to provision and notifications to drive actions to stakeholders involved in managing SaaS applications.

In similar fashion to the limited role SAM tools play in managing SaaS, SMPs also offer limited, if any, functionality to manage other cloud workloads. Management of PaaS and IaaS environments, often considered a capability of cloud management platforms (CMPs), is not included in the scope of SMPs by Gartner’s definition, and based on the in-market capabilities from the sample vendors outlined in this research.
As organizations' SaaS portfolios grow, so does the need for a single orchestration point for visibility and control. Gartner has witnessed continued, modest growth in client interest in 2020 that began in late 2019. The market remains lucrative for platform-specific SaaS management tools, which are intended to manage only a single environment such as Microsoft 365 or Google Workspace. They fulfill many of the same functions as an SMP, but are excluded from this research due to the lack of multi-SaaS capabilities.

**SMP Market Growth**

Growth has been strongest among small to midsize businesses (SMBs). Large enterprises, by comparison, have been slow to adopt these tools. While businesses with a complex SaaS profile of any size are likely to benefit from SMP adoption, they often lack centralized ownership of SaaS applications. This insulates these organizations from feeling the inefficiencies of manually managing SaaS applications.

Gartner witnessed slow growth in buyer interest in the SMP space from 2018 through 2020, with a slight acceleration in awareness and inbound interest beginning in late 2019, as indicated by client inquiry volume. Buyer awareness continues to grow incrementally, although many buyers approach SMPs with a specific pain in mind, seeking to determine whether a solution exists. Given the rise in attention being paid to SaaS apps and the role these platform-agnostic tools play in fostering remote and hybrid work, Gartner expects to see both awareness and demand increase in 2021.

Portfolio investors have taken note of the SMP market and demonstrated a positive view of the space through investments that range from small, seed investments to 8- and 10-figure funding commitments to vendors raising capital in later-stage rounds. ¹

**Market Analysis**

Often adopted to reduce capital costs and operational complexity, a large and diverse portfolio of SaaS applications can ultimately contribute to operational complexity for IT. While the responsibility for provisioning and maintaining application infrastructure is largely mitigated through the adoption of SaaS, the one-off nature of each ecosystem's administration console creates duplicate, isolated workflows and reporting. Add to this the repetitive nature of user-generated requests for applications, and compliance and security requests for consistent, auditable controls, and SaaS administrative staff are quickly mired in low-value tasks. Gartner hypothesizes that this pain is beginning to be felt by organizations of all sizes as their SaaS portfolio grows. Many organizations, especially midsize enterprises that have migrated the majority of core applications to SaaS, have begun to address this pain through adoption of SMPs.

In contrast to the adoption observed in the SMB space, Gartner sees larger enterprises focusing on adding tools to address pain points with SaaS applications in broad use. Taking on a specialized tool that can address specific issues, such as data governance in cloud office suites, is sometimes preferred over the broader capabilities of an SMP. This dichotomy of needs and pain points may drive different tool selections that correlate to company size, with large enterprises preferring tools that target specific
issues with a single SaaS app or app family, while SMBs prefer tools with a broader reach across the spectrum of SaaS apps.

Gartner believes this difference in adoption is attributable to the distributed decision making and ownership of large enterprise SaaS portfolios. These distributed centers of ownership and control can mask the true complexity being undertaken to manage SaaS at an organizational level.

Gartner predicts these three forces will influence the trajectory of the SMP market, vendors and products over the next 24 months:

- **Hybrid management need**: The reality of the app mix in many businesses requires a tool that can span management of traditional and SaaS apps, a differentiator touted by the SAM vendors making investments in their product portfolio around SMP features.

- **Competitive interest**: Gartner sees identity, ITSM and cloud migration vendors adding features to compete with SMPs. Partnerships and interoperability will be impacted as these vendors begin to compete with the SMPs.

- **SaaS platform pressure**: SaaS application and platform vendors continue to add management capabilities that include automated workflows, improved discovery and analysis of telemetry data. Vendors continue to invest in improved security capabilities. This will strain some SMPs as they try to compete with the much larger SaaS vendors.

**SMPs Ingest Information to Drive Discovery**

SMPs integrate with various infrastructure components to ingest information on SaaS application use. Ingestion of expense data from financial systems and federated identity information from IAM infrastructure provides a comprehensive picture of the SaaS apps in use, spanning those integrated by IT into the identity system as well as those in use but adopted outside of IT’s control. SMPs can also integrate with network infrastructure and endpoint management infrastructure (via unified endpoint management integration). Some SMPs offer browser extensions to dive deeper into the discovery of apps that are not visible from IAM or expense management integrations, to identify user-sourced apps in use of which IT is not aware.

In this way, the SMP’s initial deliverable is the inventory and baseline of SaaS apps in use, by whom, and how frequently. Some SMPs offer this discovery as part of the presales process or proof of concept. Organizations using SMPs regularly report finding a significant delta between SaaS apps identified during discovery and their official list of “approved” applications (see Figure 2).
Figure 2: SMPs’ Role in Discovering SaaS Apps

SMPs' Role in Discovering SaaS Apps

SMPs Centralize Controls and Automate Manual Processes

As SaaS usage grows, so does the number of disparate SaaS administrative consoles and associated open browser tabs that IT administrators must traverse to remain abreast of the settings, status and usage of each SaaS app. This manual process is highly error-prone. It renders administrative tasks, such as license or entitlement assignment for new users, and revocation for those leaving the organization or changing roles, as well as creation/modification of security groups and workstream collaboration spaces, inefficient and cumbersome.

Gartner’s 2020 I&O Leaders Survey data shows that 70% of organizations are currently investing in SaaS and public cloud offerings and will continue to do so. This will lead to a proliferation of these administrative interfaces and repeat tasks, further burdening IT administrators who already spend too much time on technical tasks that do not directly add business value and should be handled autonomously (see Figure 3).
SMPs Enhance Security Posture of SaaS Apps Through Consistent Controls

A common question is whether SMPs replace or obviate the need for other infrastructure, such as CASBs. CASBs do possess the ability to connect to SaaS applications via APIs for scanning content and user activity, but most CASB solutions are positioned and consumed as a control point for SaaS application data flow. These tools differ from the central administrative clearinghouse role that SMPs play, front-ending the native controls of various SaaS apps. Rather than competing offerings, tools like CASBs will work in conjunction with SMPs.

SMPs integrate with CASB infrastructure both to ingest information and contribute data to build a richer picture of app usage, scope and access. CASBs can work independently or using a workflow trigger from an SMP to undertake enforcement actions initiated in the SMP tool’s workflow.

For example, control schemes that span an SMP and other tools could offer the removal of sensitive data stored in a SaaS app through: removal of the local apps and data on endpoint devices (via UEM or UES integration); remediation of app data from a device and blocking further access (CASB); or creation of alerts or kickoff workflows in other security tools (data loss prevention [DLP], security information and event management [SIEM]; see Figure 4).
The role of an SMP can look similar to that of a SaaS security posture management (SSPM) tool or a cloud security posture management (CSPM) tool, but SMPs offer capabilities that expand to functions and capabilities that go beyond assessing and improving the security of SaaS apps or cloud infrastructure alone. While offering overlap with the security functions of an SMP, SSPM and CSPM tools do not offer functionality to offer management automation workflows or improve discovery of SaaS apps, respectively.

The broad reach of SMPs positions them as ideal choices for broad, operational support of SaaS application portfolio management, including some security functionality. Tools such as SSPM and CSPM, by contrast, are focused on providing rich, centralized security controls for SaaS apps and cloud workloads, expanding beyond the charter of an SMP. These more narrowly focused tools are a good choice for organizations that do not require the full breadth of an SMP tool. Neither CSPM nor SSPM tools are profiled in this research, as Gartner considers CSPMs, SSPMs and SMPs as separate, if closely related, markets.

Representative Vendors

Market Introduction
There are a number of vendors participating in the SMP market, each with varying degrees of functionality in each of the three functional pillars of SMP. It is important to note that these differences in features or support are also exhibited across the support offered for various SaaS applications in a given SMP tool. It is critical for buyers to understand the breadth and depth offered by an SMP, in terms of app support and feature depth across functional areas and apps, chosen for evaluation.

Table 1 offers a sampling of vendors that meet Gartner’s definition of an SMP today (see Note 1). This is not intended to be a complete or exhaustive list, and representative vendors offering deep integrations with a SaaS platform, but that do not offer multi-SaaS integration, are also profiled.

Table 1: Representative Vendors in SaaS Management Platforms

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product, Service or Solution Name</th>
<th>Number of SaaS Applications Supported*</th>
<th>Key Infrastructure Integration** Points: Discover</th>
<th>Key Infrastructure Integration** Points: Manage</th>
<th>Key Infrastructure Integration** Points: Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>AvePoint</td>
<td>AvePoint Online Services</td>
<td>2 to 4</td>
<td>ITAM/SAM</td>
<td>ITSM, ITAM/SAM</td>
<td>DLP, SIEM</td>
</tr>
<tr>
<td>BetterCloud</td>
<td>BetterCloud</td>
<td>5-plus</td>
<td>IAM, Network,**** Expense, ITAM/SAM</td>
<td>IAM, ITSM, Endpoint,*** ITAM/SAM</td>
<td>IAM, Network,**** Endpoint,*** DLP, SIEM</td>
</tr>
<tr>
<td>CloudM</td>
<td>CloudM</td>
<td>2 to 4</td>
<td>IAM, Expense, ITAM</td>
<td>IAM, ITSM, Endpoint,*** ITAM</td>
<td>IAM, GRC, Endpoint,*** DLP, SIEM</td>
</tr>
<tr>
<td>CoreView</td>
<td>CoreView</td>
<td>5-plus</td>
<td>IAM, ITSM, Endpoint,*** Expense, ITAM, DLP, SIEM</td>
<td>IAM, ITSM, Endpoint,*** Expense, ITAM, DLP, SIEM</td>
<td>IAM, ITSM, Endpoint,*** Expense, ITAM, DLP, SIEM</td>
</tr>
<tr>
<td>Quest-Nova</td>
<td>Nova</td>
<td>2 to 4</td>
<td>SAM</td>
<td>ITSM, Endpoint,**</td>
<td>**</td>
</tr>
</tbody>
</table>

Source: Gartner (February 2021)

Other Notable Vendors
The following vendors have made investments in SMP technology, but lack key capabilities of the representative vendors discussed previously, including a lack of multi-SaaS management capabilities or a focus on an audience other than end-user IT buyers:

- **Kaseya 365 Command**: Kaseya offers 365 Command, a management and migration tool for the Microsoft 365 environment, to managed service providers (MSPs) and end-user IT buyers.

- **Nuvolex**: Nuvolex’s ManageX offers management focused on supporting the Microsoft 365 suite of products

*The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.*

**Market Recommendations**

- Stay informed regarding SaaS vendor roadmaps to determine if your required capabilities will be added to the native administrative consoles.

- Utilize connectors and APIs to ingest as much relevant information as possible to enable SMPs to provide greater benefit. Do not be afraid of too much data.

- Use SMPs to overcome limitations of native SaaS application administrator consoles and leverage more robust capabilities such as role-based access controls, adoption and cost reporting, anomaly detection and remediation, workflow-based orchestration, artificial intelligence (AI)/machine learning (ML)-based automation, data governance, and migration.

- Organizations with multiple tenants of a single SaaS application should investigate SMPs to potentially offer similar benefits of managing multiple SaaS apps.

- Consider vendors in the SMP market today, as the aforementioned prediction of market consolidation is unlikely to occur in the next two budgeting/buying cycles, nor should it significantly disrupt the availability of offerings.

- If the organization's requirements are only security-related, evaluate CASB and dedicated SSPM offerings.

**Evidence**

1. The following are featured vendors’ major transactions in 2020:

- **AvePoint Announces $200 Million Equity Investment Led by TPG Sixth Street Partners**, AvePoint.

Note 1: Representative Vendor Selection

The representative vendors listed in this research are a subset of the total market. The vendors included here are ones that offer a majority of the most important capabilities of an SMP, and that we have seen clients include in their own vendor evaluations.

Document Revision History

Market Guide for SaaS Management Platforms - 26 November 2018
Market Guide for Cloud Office Management Tools - 14 September 2017

Recommended by the Authors

Embrace Vendor and Asset Management to Effectively Manage SaaS Applications
Hype Cycle for the Digital Workplace, 2020
Predicts 2021: Crisis Will Force Changes to Software and Cloud SaaS Contract Negotiation
Optimize Cost and Risk as These Software and SaaS Pricing Metrics Emerge to Enable Digital Business
Hype Cycle for I&O Automation, 2020

© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."