Identity as a Service (IDaaS)

Promising New Opportunity for MSPs

Brought to You By:

AVG Business

Abstract

Managed service providers are increasingly finding themselves in the role of "service brokers," reselling public cloud services and struggling to stay relevant as their clients turn to self-service SaaS and IaaS offerings from commodity cloud vendors. Not only is this a challenging, race-to-the-bottom approach with low margins and stiff competition, but it is a difficult model to sustain and grow. At the same time, end users increasingly expect to be able to access all of these enterprise cloud services from any device with minimal hassle. One option that allows MSPs, resellers and their clients to effectively address all of these challenges is through a so-called cloud service federation, a set of technologies that allows MSPs to refine their role as service brokers and add real value for customers. Also known as single sign-on or, more recently, Identity-as-a-Service, federation represents a unique opportunity for MSPs to increase revenue and remain critical partners for their clients.

Introduction

Two key phenomena are radically altering the role of the MSP and their relationships with their clients. The first is the mainstreaming of business-grade public cloud applications. Organizations can now rapidly provision everything from CRM to HR applications themselves without working through an "MSP middleman." The second is a shift in end-user autonomy and expectations. If IT (and the MSPs they utilize) can't provide the services they need to do their jobs efficiently and from any device, many are quite happy to simply use consumer cloud services and their own devices. The proliferation of these devices and the increasing mobility of the workforce compound the reliance on the cloud and the demand for ubiquitous access to corporate resources. Security, for the end user, too often takes a back seat to productivity.

If both businesses and users can provision their own services, bypassing normal IT channels and traditional service provider relationships, where does this leave the MSP? In actuality, this represents an opportunity for MSPs to shift toward service broker business models, particularly when they can add value and expertise to those services.

Many service providers have already gotten into the game of reselling commodity cloud services, but this is a low-margin proposition that doesn't get around the MSP middleman problem. Instead, when MSPs become cloud brokers, integrating services and connecting customers to the best platforms and services to meet their particular needs, service providers are able to deliver new layers of value and expertise that organizations often can't on their own.

> "Cloud services brokerage (CSB) is an IT role and business model in which a company or other entity adds value to one or more (public or private) cloud services… via…aggregation, integration and customization."
>
> – Gartner

In some ways, this harkens back to the VAR model from which many MSPs evolved. VARs assemble integrated solutions that are greater than the sum of their parts. They don't just sell hardware or software — top VARs design, deploy, and often maintain, complete hardware and software systems to meet a business need. For MSPs, this model usually involves adding layers of software, services and support to a variety of public or private cloud services. Gartner recently coined the term "cloud services brokerage" (CSB), recognizing this emerging role.

The Proliferation of Cloud Services

Many of the applications that once required either a desktop computer or on-premises client-server setups can now be delivered as a service via either public or private

> 81% of employees surveyed are using their own apps to improve their working productivity.
>
> – Globo

clouds. Overall, this has been a positive development for IT, businesses and even consumers. The cloud makes it easier, faster and cheaper to deploy applications and brings us closer to the ideal of "anytime, anywhere" productivity.

This same initial ease of deployment, though, has given rise to management and security nightmares for IT departments. When HR users can subscribe to a new payroll service as easily as sales can buy a new CRM application, proliferation of new applications leaves IT struggling to integrate and secure disparate systems while users manage increasing numbers of usernames, passwords and profiles.

Simultaneously, end users can simply provision their own consumer-grade cloud services for file sync and share, contact management, communication, collaboration, and more, all without any visibility from IT. Even small businesses frequently don't have a good handle on the number of cloud applications (whether consumer services or business-grade apps purchased by individual departments) that might be storing corporate data. Traditionally, IT was able to exercise fairly tight control over data security or build relationships with trusted service providers whose security was equally tight. As those capabilities have eroded in the face of BYOA and self-service business apps, savvy MSPs are finding ways to help organizations better manage this changing environment.

Making IT the Enabler Rather Than the Enemy

Ultimately, most employees just want the best services to do their jobs well. If IT doesn't provide them, it's easy enough to just pay for whatever cloud application appears to meet the requirements.Unfortunately, end users and lines of business can often circumvent IT processes and procedures that were designed to maintain security and cross-application compatibility.

The solution, of course, is to leverage the myriad business-grade cloud services quickly and cost-effectively to meet the needs of users across the organization. If they already have access to applications and services sanctioned by IT that enable high levels of productivity and collaboration, then there is little need to "go rogue" and purchase their own services. Bottomline: it's OK for organizations to use a variety of cloud services, but not to leave those services unmanaged, unsecured, or worse, unknown to IT.

Again, MSPs can play a critical role as partners, changing the perception of IT as Draconian enemies of progress and innovation to enablers of new, efficient, cost-effective ways of doing business. By delivering the right combinations of cloud-based services and software, MSPs can provide the management glue to tie together and properly secure the SaaS applications and IaaS platforms that would otherwise proliferate unchecked.

BYOD is Here to Stay

Bring Your Own Device is a trend that many businesses resisted for years because of security and implementation challenges. Now, though, the tide has shifted and there is no denying that BYOD has moved from "trend" to "reality."

BYOD and mobility, in general, are inseparable from the cloud. The successful rollout of any mobility initiative relies on secure, anytime, anywhere access to an organization's data, resources and applications, and only cloud services can meet all of these criteria. At the same time, security is not just dependent on the SaaS applications themselves, but also on appropriate mobile device management (MDM).

> "Tablet adoption for business purposes among SMBs is gaining traction,with 97% saying any time, anywhere access to data and applications makes employees more effective."
>
> – Dimensional Research

Certain leading vendors have created unified platforms that integrate traditional MDMincluding device provisioning, remote lock and wipe, monitoring and imposition of security profiles) with so-called "cloud federation" which goes a long way toward completing the mobile security puzzle. Federation provides single sign-on (SSO), preferably with secure, multifactor authentication, for multiple applications; in the case of BYOD, it dramatically simplifies both mobile access to cloud apps and their security.

MSPs are uniquely poised to deliver comprehensive mobile security solutions with cloud-based MDM and federation services. Organizations are generally not up to the task of effectively and consistently securing mobile devices and applications, leaving a significant unmet need that service providers can fill.

SSO = Single Point of Management, Single Point of Security

Federation and single sign-on are more than just convenience factors for users (although they do substantially improve productivity and the ease with which users can access a variety of business applications). Rather, they eliminate critical security vulnerabilities, whether users are on a mobile device or at their desktop.

As more and more services and applications are introduced in an organization, users tend to become even more lax than usual about password security, duplicating easy passwords across apps to make them easier to remember. Even under the best of circumstances, passwords are the weak link in endpoint security. When an MSP delivers federation services to an organization, multiple weak passwords can be replaced with a single strong password and/or multifactor authentication with centrally managed requirements.

This issue of centralized management also extends beyond passwords. With the right federation services, organizations can easily and securely onboard or terminate employees without needing to provision or deprovision every federated application separately. Before an employee has packed up his office, access to every cloud or locally hosted application can now be terminated from a single pane of glass, most often using existing MS Active Directory implementations. Organizations also gain high-level visibility into utilization across all of these applications, further enhancing the MSP relationship as they help their partners establish ROI for the apps they deploy.

Delivering Identity as a Service

The natural progression of SSO, federation and end user security is a relatively new approach referred to as Identity-as-a-Service (IDaaS). IDaaS is especially attractive for SMBs who want to eliminate the challenges of managing both on-premises and cloud-based system security.

But what exactly is IDaaS? The Cloud Security Alliance defines Identity-as-a-Service as "the management of identities in the cloud, apart from the applications and providers that use them. IDaaS is an extremely broad term, including services for software, platform and infrastructure services in both the private and public cloud."

In reality, IDaaS is not just another acronym, but something here to stay. What

> "By the end of 2015, Identity and Access as a Service (IDaaS) will account for 25% of all new identity and access management sales, compared with 5% in 2012."
>
> – Gartner

used to require several platforms, leading vendors have now combined SSO and EMM into systems and true managed services that unify access and end user security across a wide range of cloud services and device platforms including mobile, server and desktop. When MSPs can deliver unified platforms that simplify management and access for their customers, they add far more value than they can by simply reselling cloud services. For MSPs, this is about monetizing commodity cloud services, gaining control of mobile devices and ensuring their ongoing relevance with their customers. For businesses, it's about smart, secure access and enabling the Holy Grail for end users: simple connections, anytime, anywhere, to the services and applications that make them more productive.

Conclusion

Whether cloud app proliferation is a function of shadow IT, more formal BYOA programs, or even distinct IT initiatives to migrate to the cloud, we know that organizations are adopting cloud services in droves. Yet as organizations add more and more services, both users and IT frequently struggle with

everything from user provisioning and billing to password management and authentication. These problems are compounded by BYOD and mobility initiatives that rely on cloud services to connect employees to corporate data and applications.

While the cloud is essential tomobility, security and management of both the devices and the services they use, it has introduced real challenges, especially for SMBs where dedicated IT resources are often scarce. Herein lies the opportunity for MSPs, where unified delivery and management of mobile and cloud solutions represent a value-add that can't be had from any commodity cloud vendor. With the recent emergence of IDaaS, this represents a true managed services opportunity. ■

About AVG

AVG is the online security company providing leading software and services to secure devices, data and people. AVG has over 200 million active users, as of March 4, 2015, using AVG´s products and services including Internet security, performance optimization, and personal privacy and identity protection. By choosing AVG´s products, users become part of a trusted global community that engages directly with AVG to provide feedback and offer mutual support to other customers.

AVG Partners, Authorized Distributors, and Authorized Resellers comprise a distribution network in over 150 countries and are a major contributor to the awareness of AVG Anti-Virus around the world. We also provide other ways for business cooperation such as Affiliate and OEM programs. The growing success of AVG and our business partners is a testament to our strategic business partner programs.