The Mounting Case for Cloud Access Brokers

Lori MacVittie, 2013-06-02

#infosec #cloud #iam Addressing the need for flexible control of access to off-premise applications

Unifying identity and access management has been a stretch goal for IT for nearly a decade. At first it was merely the need to have a single, authoritative source of corporate identity such that risks like orphaned or unauthorized accounts could be addressed within the enterprise.

But with a growing number of applications - business applications - being deployed "in the cloud", it's practically a foregone conclusion that organizations are going to need similar capabilities for those applications, as well.

It's not easy, there are myriad reasons why unifying identity and access control is a stretch goal and not something easily addressed by simply deploying a solution. Federation of identity and access control requires integration. It may require modification of applications. It may require architectural changes.

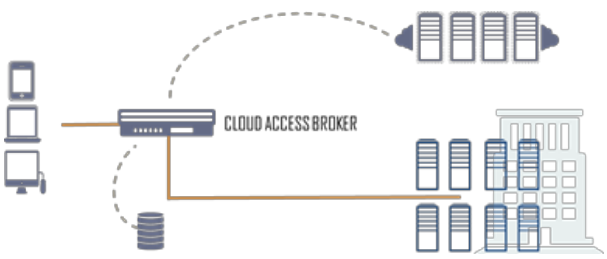
All of these are disruptive and, ultimately, costly. But the costs of not addressing the issue are likely higher.

> ## Security a Rising Concern for Cloud-Based Application Usage
>
> With access to these applications taking place from a variety of locations including smartphones (80 percent),tablets (71 percent) and non-company computers (80 percent) and with a large percentage of organizations (73 percent) needing to grant temporary access to cloud apps, respondents cited concerns around identity management, governance and complexity.
>
> ...
>
> Nearly three-quarters (72 percent) of the respondents said they have the need to provide external users, such as consultants, with temporary access to the company's cloud applications, while **just under half (48 percent) of respondents said they are still not able to sign in to cloud applications with a single set of credentials**. [emphasis mine]

There is a significant loss of control - in terms of governance - that's occurring, where the organization no longer has the means by which they can control who has access to applications, from what device or location, and when. That's the downside of cloud, of distributed systems that are not architected with security in mind.

Make no mistake, it's not just IT making a power grab for power's sake. This is a real, significant issue for the business side of the house, because it is their applications - and ultimately data - that is at risk by failing to properly address issues of access.

THE CASE FOR CLOUD ACCESS BROKERS



The least disruptive - and most efficient - means of addressing this disconnect is to insert into the data center architecture an access broker tier, a layer of dynamic access and identity management services designed to provide federation and unification of credentials across cloud and data center resources based on the organization's authoritative source of identity.

The advantages of such a tier are that they are less disruptive, it respects the authoritative source of identity and it is highly flexible. The same cloud access broker that provides authentication and authorization to internal resources can do so for cloud-based resources. The downside is integration with a growing variety of SaaS and custom cloud-deployed applications used by the enterprise. A standards-based way of integrating off-premise applications with a cloud access broker is needed, and we find such a standard in SAML 2.0, an increasingly popular means of integrating identity and access management services across the cloudosphere.

In addition to providing access control through such integration, a cloud access broker also provides the means for IT to address the issue of password security noted in "Security a Rising Concern for Cloud-Based Application Usage":

> The survey indicated unsafe password management continues to be a challenge, with 43 percent of respondents admitting that employees manage passwords in spreadsheets or on sticky notes and 34 percent share passwords with their co-workers for applications like FedEx, Twitter, Staples and LinkedIn. Twenty percent of respondents said they experienced an employee still being able to log in after leaving the company.

By enabling federation and single-sign on capabilities, organizations can mitigate this problem by ensuring users have fewer passwords to recall and that they do not share them with off-premise applications like FedEx. Because IT controls the authoritative source of identity, it also governs policies for those credentials, such as password length, history, interval of change, and composition.

FEDERATION MEANS HEIGHTENED (AND ENFORCEABLE) SECURITY

Federation of identity and access management through a cloud access broker can alleviate the loss of control - and thus expanding security threats.

By maintaining the authoritative source of identity on-premise, organizations can enforce security policies regarding password strength and length while improving the overall experience for end-users by reducing the number of credentials they must manage to conduct daily business operations. Issues such as orphaned or rogue accounts having access to critical business applications and data can be more easily - and quickly - addressed, and by using a flexible cloud access broker capable of transitioning security protocols, device incompatibility becomes a non-issue.

As more and more organizations recognize the ramifications of unfettered use of cloud services it is inevitable that cloud access brokers will become a critical component in the data center.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com