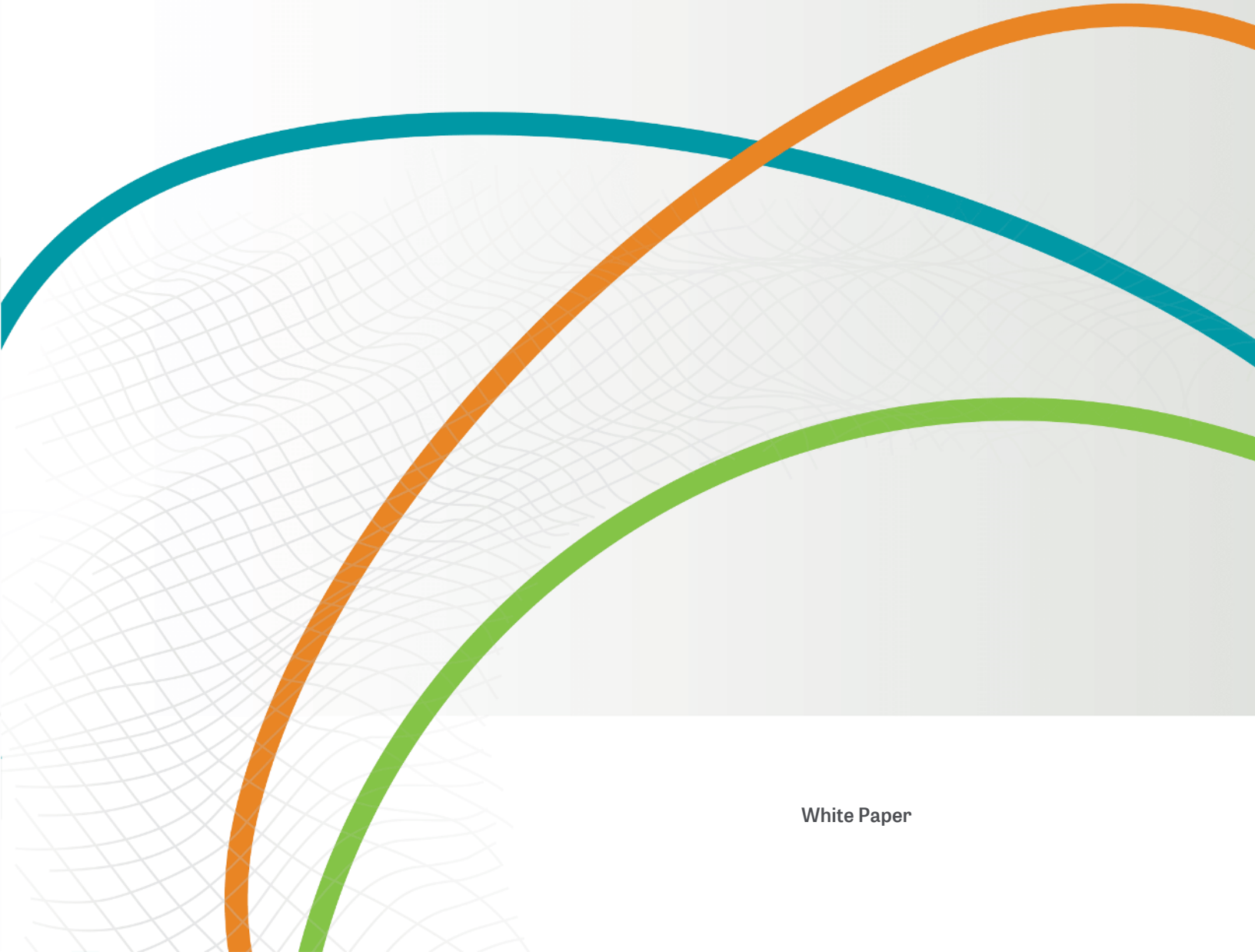
The F5 Access Federation Reference Architecture

Safely adopt an SaaS model by eliminating the drawbacks of distributed SaaS provider identity and access management systems and enhancing security.



White Paper

Introduction

Many organizations are realizing the benefits of adopting cloud-based services rather than deploying and maintaining in-house solutions. Software as a Service (SaaS) providers are able to deliver niche expertise in a cost-effective, multi-tenancy environment using a ready-to-consume, subscription-based model. The benefits of the SaaS option, however, often come at the cost of up-to-the-minute access control and reliable security policy enforcement. As with internally managed services, SaaS providers maintain their own identity and access management (IAM) systems for usernames, passwords, and access control enforcement—thus introducing IAM silos and the security management issues that result for organizations using multiple IAM systems void of synchronicity or any form of integration.

IAM siloing incurs both potential lapses in security and reduced productivity.

- The security risks are caused by password fatigue and, more importantly, delays in deleting expired accounts.
- The reduced productivity stems from delays in the creation of new user accounts for new employee or contractor access, as well as the management overhead demanded by numerous IAM systems.

F5 Access Federation eliminates these SaaS drawbacks by eliminating the disconnect between internally maintained IAM systems and services external to the enterprise, delivering consistent security everywhere.

Business Challenges

SaaS Adoption

The SaaS marketplace is ubiquitous and growing rapidly because it offers enterprises much to gain:

- SaaS is cloud-based, so there's no technology to acquire, install, and maintain.
- SaaS frees up IT resources to focus on more strategic projects.
- SaaS aids mobility, with services typically available on any device and from any location.
- SaaS is subscription-based, delivering simpler licensing costs than off-the-shelf software brought in-house.
- SaaS can be maintained with updates or upgrades that are transparent to the service consumer.

Nonetheless, SaaS is an additional service, external to an organization's privately maintained and secured resources, and with this additional service comes new and unique challenges.

Technology Silos

Any service delivered from outside an organization—outside of its private data centers— inherently represents a technology silo in respect to data management, application security, and identity and access management.

With SaaS, both data management and application security are in the hands of the SaaS provider, and this isn't something that can be easily changed. And for good reason: most of the benefits derived from SaaS come from the simple fact that the complexities of the service delivery are abstracted from the consumption of the service itself. Opening data management and application security to the subscriber, therefore, would transform the original SaaS to Infrastructure as a Service (IaaS) instead, bringing an immediate loss of all the benefits of the SaaS model by dropping management back into the hands of the service consumer. By definition, then, opting for SaaS means accepting the data management and application security policies of the provider and establishing trust in those policies.

When it comes to identity and access management, SaaS providers offer their own solutions, and it is up to the subscriber to populate and maintain them in addition to the subscriber's internal IAM systems, again creating isolated systems and IAM silos. With this increase in IAM silos come new risks to:

- Data protection
- Productivity
- Security integrity

Data protection

Data protection is important, and organizations greatly (and with good reason) fear the theft of data entrusted to an external provider, SaaS providers being no exception. But the risk is expanded when every IAM silo adds more passwords for employees to manage, because weak passwords make data theft attacks easier. Yet according to a 2012 report by online credit check provider Experian, "For an average of 26 different online accounts, users had only five different passwords."

"Using the same user ID and password exposes accounts to hacking, and developing complex choices makes it hard to remember them all. At some point it becomes too much to manage—that's password fatigue" explained Jon Brody, Vice President of Marketing at TriCipher in a 2009 issue of Forbes Magazine.

Password Fatigue

> "Using the same user ID and password exposes accounts to hacking, and developing complex choices makes it hard to remember them all. At some point it becomes too much to manage — that's password fatigue.
>
> —Jon Brody, Vice President of Marketing, TriCipher

Even more important than issues of password strength or hacking are the data-protection security implications that come with delays in decommissioning the user accounts of former employees and contractors. How often are HR systems cross-referenced across all IAM silos? The gap between a change in authorization and the time it takes to reflect that change across IAM silos risks serious security violations. Yet skilled IT resources are already in high demand and decommissioning delays can be inevitable.

Productivity

Any delay in getting new employees and contractors up and running with access to the necessary systems and tools is a measureable cost to productivity. And the time it takes to provision new personnel access is multiplied by the number of technology silos involved, so the more the organization takes advantage of SaaS benefits, the more access provisioning is required.

Security integrity

Organizations invest significant time and money researching access technologies and choosing appropriate authentication and authorization solutions for their privately maintained systems. A leading solution is multi-factor authentication, with the factors often comprising a username, a password, and another form of authentication challenge such as a one-time password or code. Examples of these solutions include:

- RSA SecureID
- Google Authenticator
- Entrust

This extra level of security, which is growing in popularity, assists in combatting the security flaws derived from password fatigue because a one-time password, for example, cannot be written down. It exists for one use only and then expires.

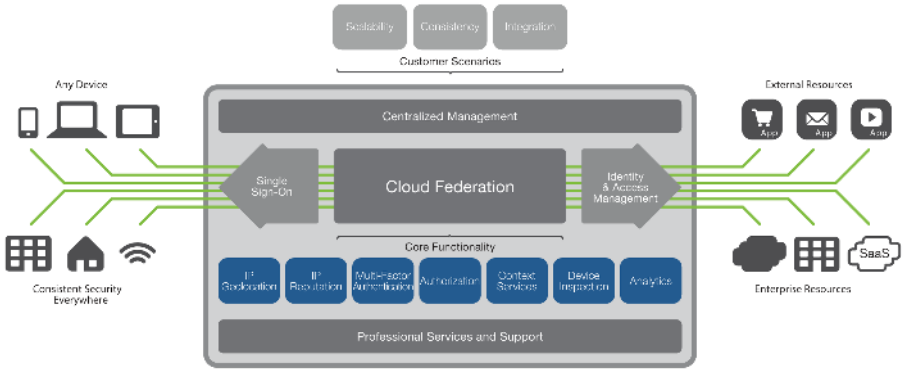
While such a solution might be implemented for internally managed systems, multi-factor authentication is not readily available from SaaS providers. If it were, it would be a separately managed two-factor authentication—stronger security but still an IAM silo.

Business Solution

SaaS subscribers have an alternative to adopting and managing the siloed IAM solutions of their SaaS providers. Instead, organizations can implement IAM federation, establishing a trust relationship between the SaaS provider's service and subscriber-owned and subscriber-managed IAM technology. For such a solution to be a reality, however, it must be achieved without adding architectural or management complexity and without the need to disruptively integrate technologies by building and maintaining a new network between those of the provider and the subscriber.

Forrester Research predicts that the IT department could disappear as soon as 2020.

A recent survey of 1,000 IT professionals by Forrester Research found that these professionals are turning to hosted (SaaS) products as a way to offload management of non-mission-critical applications such as those for HR and CRM. The subscription-based SaaS pricing model also can keep IT budget costs consistent with or lower than packaged or homegrown software.



The F5 Access Federation solution

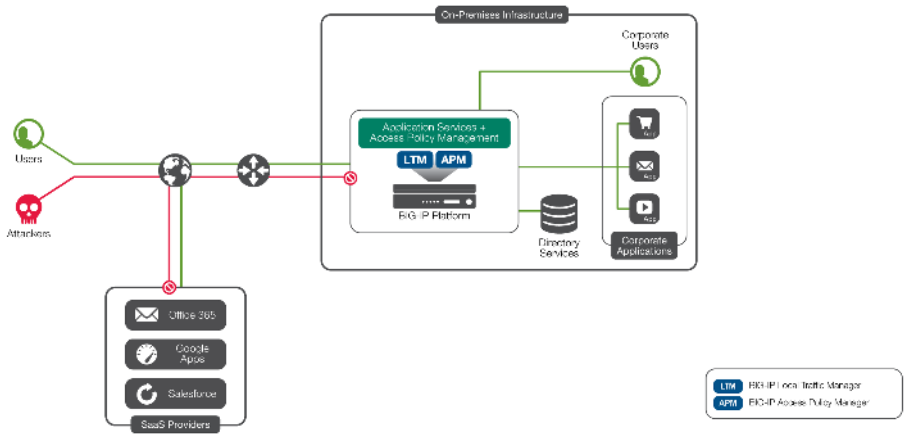
Technology Solution

F5 Access Federation architecture meets both requirements. It uses Security Assertion Markup Language (SAML), an XML-based, open standard data format for exchanging authentication and authorization data between parties. SAML technology eliminates the need to manage independent user accounts across SaaS providers. The most important element that SAML addresses is web browser single sign-on (SSO).

Furthermore, the F5 Access Federation architecture enables the deployment of stronger authorization solutions, including two-factor authentication, IP geolocation enforcement, and device inspection.

F5 BIG-IP Local Traffic Manager (LTM) and BIG-IP Access Policy Manager (APM) together provide the required platform for:

- SAML communication between an organization's private IAM system and external SaaS providers.
- Consistent, multi-factor authentication for all users across all systems accessed using the BIG-IP devices.



The F5 Access Federation architecture

Business Benefits

By implementing the F5 Access Federation architecture, organizations can:

- Implement SSO across SaaS applications to eliminate the cause of password fatigue.
- Enforce consistent security policy across all systems.
- Reduce management costs for access account commissioning and decommissioning.
- Reduce complexity and improve productivity.

- Capitalize on the benefits of SaaS while better managing security risks.

Conclusion

Isolated systems operating as technology silos are a significant inhibiter to productivity and security. They restrict an organization's ability to respond quickly to operational demands and they wreak havoc with proven and trusted security policies. The F5 Access Federation architecture eliminates SaaS access silos to enhance security, improve productivity, and enable safe adoption of an SaaS model.

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

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com