WHITEPAPER

SAML ALONE IS NOT SECURE
- HERE’S HOW TO FIX IT

ASSERT YOUR IDENTITY
Executive Overview

SAML (Security Assertion Markup Language) is a standard that facilitates the exchange of security information. Developed by OASIS (the Organization for the Advancement of Structured Information Standards), SAML is an XML-based framework. SAML enables different organizations (with different security domains) to securely exchange authentication and authorization information.

In other words, through SAML, your organization can deliver information about user identities and access privileges to a service provider in a safe, secure and standardized way.

Most cloud and SaaS service providers, including Salesforce.com, WebEx and Google Apps, favor SAML; thus, the standard has emerged as the go-to SSO protocol for SaaS applications. Yet, a standard isn’t a solution, and many methods of integrating existing identity stores into cloud-based applications are riddled with flaws and vulnerabilities.

Many organizations believe, falsely, that with SAML in place their online activities are secure. It is true that they are more secure than with user names and passwords alone, but SAML does not solve the entire security puzzle. Without additional services, SAML leaves gaping security holes that attackers can easily exploit.

This paper will discuss why SAML is important; what it does to boost security and what it lacks. Finally, the paper will offer advice on how to augment SAML with an SecureAuth Identity Enforcement Platform to make your online activities every bit as secure – if not more so – as your on-premise ones.
Introduction: SAML Emerges as a Secure Cloud ID Standard

Today’s IT security professionals spend more and more time dealing with one cumbersome task: managing user identities. Even for organizations that have adopted advanced authentication mechanisms, identity management is still a time-consuming cost center. Password resets alone take up an undo amount of IT resources.

As more mission-critical applications migrate beyond the firewall and as SaaS, Web Services and cloud-based applications continue to rise; organizations are learning the hard way that their access and enforcement mechanisms aren’t ready for the Web 2.0 world.

To combat application sprawl and minimize the impact on end users, most organizations are moving towards single sign-on (SSO) solutions. However, legacy SSO solutions can’t stitch together the many on-premise applications with those beyond the firewall. Access-control platforms, two-factor authentication tools and identity federation all tackle parts of the problem, but unified solutions are elusive.

To prevent competing solutions from creating too much chaos, standards bodies have stepped in to propose underlying SSO and identity federation standards, such as SAML (Security Assertion Markup Language) and OpenID.

SAML caught on quickly with cloud-based providers, such as Google, Salesforce.com and WebEx, and once traditional companies such as IBM and Microsoft threw their support behind SAML, it became the go-to SSO protocol for SaaS applications.

What SAML Does

SAML is a framework that enables the exchange of security and identity information. It is not a solution that grants access or enforces identities. The main difference between SAML and other identity mechanisms is that SAML relies on “assertions” about identities. It is assumed that an Identity Provider (IdP) is making an assertion and that the IdP is responsible for maintaining user identities, authenticating users and determining privileges.

SAML enables enterprises to abstract authentication from applications. Rather than having to manage multiple credentials for a variety of apps, SAML allows organizations to extend identities from in-house resources to external service providers.
This one trait alone boosts security. When users have multiple credentials for various apps, they inevitably do one of two things (both of which erode security): they either repeat credentials from app to app, or they write them down.

If credentials are repeated, each resource that person uses is only as secure as the least secure one. If a hacker breaches one, he’s effectively breached them all. Writing down credentials is just as bad. Hackers have long known that if they find or steal someone’s laptop, they merely have to run a search for a file named “passwords” to dredge up a list of credentials.

**SAML allows enterprises to:**
- Standardize authentication assertions
- Retain identities in single repository
- Abstract authentication so that it is not tied to a specific application
- Extend identities from internal to external resources
- Log authentication locally

**What SAML Doesn’t Do**

The problem with SAML is that there are many myths circulating about what it is and what it does. The main myth that plagues SAML is that it is a complete identity management solution. It is not.

**5 Things SAML Does not Do:**
- Determine how secure the IdP webserver is
- Ensure that web forms are secure
- Standardize authentication mechanisms
- Determine where data is extracted from, and what ID is asserted
- Enforce how an event is logged

As mentioned above, SAML assumes that an IdP is making an accurate assertion and that the IdP is responsible for maintaining user identities, authenticating users and determining privileges.

**SAML does not determine how secure the IdP webserver is**

You know the old saying about “assume.” If you assume that your IdP executes all of these important security functions, you may well end up regretting that assumption.
SAML does nothing to verify the quality of the IdP, nothing to ensure that IdP is compliant with industry regulations, and nothing to determine how hardened the IdP’s web server is.

In other words, the IdP itself could be the weak link in your security chain, and SAML would have no way of knowing. You are assuming that you can – now and in the future – trust your IdP. Unfortunately, that assumed trust could come back to haunt you.

Another difference between SAML and other security mechanisms is how identities are enforced. Where other identity-enforcement approaches rely on central certificate authorities to issue certificates ensuring secure communications from point A to point B, SAML is designed in a more Web-friendly manner. Under SAML, any point within the network can make an assertion stating that it knows and has verified the identity of a user or data set. Then, the application being asked to accept a user (or data) must decide whether or not to trust that assertion.

As you can see, the weak link in the SAML identity chain is the integrity of users.

Without additional tools in place, SAML means you’ll be trading one headache – managing identities across multiple apps – for another – continuously vetting IdPs. Since so many cloud-based services emanate from virtualized infrastructures, you have no idea what other processes (or whose other processes) are residing on the authenticating server. What IP ports are open on the server? How is it configured?

**SAML does not ensure that web forms are secure**

Another issue is the page on which users enter their credentials. To ensure security, you need to know how the webpage is constructed. Since the SANS Institute has found that a majority of hacks target forms as the point of weakness, it’s important to know whether or not forms on the authenticating page have stood up to rigorous penetration testing. If they have not, all of your work to ensure strong authentication is in place could be undermined by a flawed website.

**SAML does not standardize authentication mechanisms**

While SAML standardizes the assertion of identities, it does not standardize authentication. It is up to the organization to choose what type of authentication (ID and password; two-factor with SMS, with telephony, with tokens, etc.) to use. It is also up to the enterprise to integrate authentication.
**SAML does not determine where data is extracted from or what ID is asserted**

The handoff from the authentication system to the SAML assertion, if not properly configured, opens the door to hackers. Moreover, if an assertion is invalid, you may not know it, since SAML doesn’t provide any standardization for signing XML assertions. This means you have no way of verifying where the certificate is coming from, where it is stored, who has access to it, and how access is monitored and logged. Moreover, you can’t be sure how the identity is stored, what database it is being extracted from and how secure that database is.

**SAML does not enforce how an event is logged**

The final thing that SAML does not do, but which is absolutely necessary for strong security and compliance, is standardize and enforce logging. If you don’t log events in a consistent fashion, there is no way you can audit them to prove compliance with industry regulations.

**Plugging the Holes in SAML with a Unified Identity Enforcement Platform**

There are many ways to fill the gaps around SAML, but most involve a patchwork of point products and homegrown solutions. Not only is this approach time consuming, but it requires a lot of roll-your-own coding and the extensive use of disparate APIs, both of which increase your attack surface.

A better way to tackle this problem is through a unified Identity Enforcement Platform. What IEPs do is step in and leverage SAML and other existing resources to provide a complete SSO solution. With SecureAuth Identity Enforcement Platform in place, a dynamic, two-factor user authentication into the cloud is a simple task. Without one, identities are the weak link in your security chain.

With an SecureAuth Identity Enforcement Platform, when a user clicks on an application, the application asks the user to authenticate him or herself. The SecureAuth Identity Enforcement Platform handles the authentication and converts the local identity into a SAML assertion, communicating that assertion to the service provider or, depending on application designs, the application itself. All of this is accomplished behind the scenes and in a manner that is invisible to end-users.
Why SecureAuth Is the Best Way to Secure SAML

The SecureAuth Identity Enforcement Platform is the industry’s first single platform to integrate strong authentication, SSO, access, and user management services for cloud, Web, and VPN applications. This unique approach ensures that any organization can easily adhere to security and compliance regulations with a single solution that is configurable to meet your specific security requirements.

Competing SSO, authentication and identity management products only provide one security function – such as authentication, SSO, access or user management – and can’t support cloud, Web, and VPN applications in a single platform.

Moreover, SecureAuth Identity Enforcement Platform requires only one instance of user authentication. From that point on, each successive application the user connects to is able to authenticate the user via the Identity Enforcement Platform behind the scenes. With SecureAuth Identity Enforcement Platform, authentication is configurable, and each application can be configured independently and to the appropriate level, as mandated by enterprise policies.

SecureAuth Identity Enforcement Platform reduces integration costs, increases security for multiple resources (cloud, VPNs, SaaS), speeds deployment times, and increases compliance rates.

The end result is that your organization is able to leverage the SecureAuth Identity Enforcement Platform to achieve in-house, cloud, SaaS and Web SSO in a safe, secure and centralized way. At the same time, your organization maintains complete control over your most sensitive information asset: your user identities.
How an Identity Enforcement Platform Works

- **Identity Enforcement Platform pulls the identity from the enterprise data store** (AD, LDAP, SQL, etc)
- **It then conducts either:**
  - Secure Desktop SSO (Intranet)
  - Secure 2-Factor Authentication (Extranet)
- **Identity Enforcement Platform passes the identity on to:**
  - Hosted Web Apps (Microsoft, IBM, J2EE)
  - VPNs
  - SaaS applications (salesforce.com, Google Apps, Postini, etc.)
- **And provides added security in the form of:**
  - SSO between resources
  - Policy-based group authorization
  - Unified SSO across apps both on-premise and in the cloud
Conclusion: You need to enforce Identity Governance to secure SAML – SecureAuth gets you there.

The bottom line is that to utilize SAML – in any form – your organization needs to become an IdP (Identity Provider). Just as individuals should never share sensitive personal information like their banking PIN, enterprises too should be wary of sharing critical data that could put them at risk if it fell into the wrong hands. Trusting user identities to third parties means that you will always have to keep your fingers crossed that those outside of your organization are following best practices and not degrading your organization’s security.

Granted, becoming and IdP sounds like a serious burden, especially for organization with limited IT resources. The good news, though, is that new cloud-grade security tools will help you become your own IdP in a few short days.

The quickest way to become your own IdP is to implement SecureAuth. With SecureAuth your organization evolves from simply “holding” identities (AD, LDAP, SQL) to becoming a full, secure, guidance-compliant, highly available identity provider. With SecureAuth, you will be able to serve up secure identities to on- and off-premise applications in a standardized, automated and auditable fashion.

SecureAuth meets these requirements by providing:
- A secure URL-based interface for the Service Providers
- Configurable 2-Factor for all your business needs
  - B2E (Employees)
  - B2B (Business Partners)
  - B2C (Customers)
- SSO:
  - Active Directory
  - On-Premise resources
  - SaaS resources
- Full logging

It is this pre-built, shrink-wrapped capability that allows you to become your own full-service IdP. This is the capability that enterprises require, and what Secure
Stop worrying about SAML and take the next step

With SecureAuth, you can solve your user access, authentication and logging and reporting problems in a matter of days, versus weeks or even months with competing solutions.

If you have unique SSO challenges that this white paper has not addressed, call us at 949-777-6959 or email us at ssoquestions@gosecureauth.com.

As with any new technology purchase, we encourage you to try before you buy. Visit: http://www.multifa.com/contact-multi-factor-authentication-company/trial-request.aspx to sign up for a free 30-day trial.