SECUREAUTH®

WHITE PAPER

WHAT IS AN IDENTITY PROVIDER? WHY DOES MY COMPANY NEED TO BECOME ONE?

ASSERT YOUR IDENTITY

Tame Mobile and Cloud Security Risks: Become an IdP

Executive Overview

Enterprises face security threats from all directions. According to the Identity Theft Resource Center, there were 189 known breaches from January 1 of this year through the beginning of June. Those breaches exposed approximately 13.7 million records. Meanwhile, trends intended to benefit the enterprise, such as cloud computing and mobility, often introduce unintended risks.

The weak link in our online economy is trust. If you boil that down further, much of the lack of trust stems from the inability to verify online identities. It is increasingly difficult to know whether people (or companies) on the Internet are who they say they are.

To address today's security risks and to embrace new technology trends such as cloud, mobility and SaaS, enterprises must rethink how they handled their employees' identities. Fortunately, the industry has been moving towards federated Single Sign On (SSO) solutions, and has been standardizing building blocks like SAML and OpenID.

Enterprises should build on these standards in order to become Identity Providers (IdP). By becoming an IdP, companies can better control, enforce and extend security standards to all on-premise and cloud-based applications in their organizations, as well as to mobile devices.
This paper will discuss the reasons enterprises should become IdPs, what becoming an IdP involves, and why you should automate as much of this process as possible.

Introduction: New Security Risks Undermine Online Business

In August 2012, a hacker crafted a wickedly specific social engineering attack to target *Wired* writer Mat Honan. The hacker hijacked his credentials and then erased data on Honan's iPhone and iPad, completely deleted his Google account, commandeered his Twitter account, and went on to post a bunch of racists and homophobic diatribes.

When Honan figured out he'd been hacked, he took a smart counter-measure: he engaged the hacker in a conversation. He offered to refrain from pressing charges if the hacker, Phobia, would detail his attack methods. Those methods, which Honan delves into here, show that online businesses of all stripes are at serious risk. Actually, it's not just online businesses, but rather any business or person who has any sort of online presence.

The saddest part of the Honan attack is that it was totally avoidable. Honan believes that if he had turned on 2-Factor authentication in his Google account, the hacker would have moved on. Perhaps. Hackers, after all, tend to go after low-hanging fruit.

But simply turning on 2-Factor authentication, while better, doesn't address the root problem: namely, the fact that user identities and identifying personal information (date of birth, hometown, mother's maiden name) are scattered across the Internet. Phobia used identity information that was poorly secured in one location to defeat security measures in others. To reestablish trust on the Internet, then, we must reclaim our identities.

What Are IdPs and Why Are They so Important?

Remember that old *New Yorker* cartoon, "On the Internet nobody knows you're a dog"? Well, nobody knows that you actually are who you say you are either – unless you prove it.

The trouble is that few businesses take the steps necessary to make people prove they are who they say they are. In the Honan attack, Apple didn't know the hacker wasn't really Honan, nor did Amazon. This isn't meant to rake those companies over the coals. The sad truth is that this is common.
We've known for ages that user names and passwords are weak tools to protect sensitive data; yet, we rely on these for everything from online banking to remote access into corporate applications. If this were a late-night infomercial, this is where the spokesperson would look to the sky and say, "There must be a better way."

There is. To fix the online identity problem, businesses must become Identity Providers, or IdPs. This may sound daunting and complicated, but it's not. Well, the truth is that it can be, but it doesn't have to be difficult if the proper steps are taken.

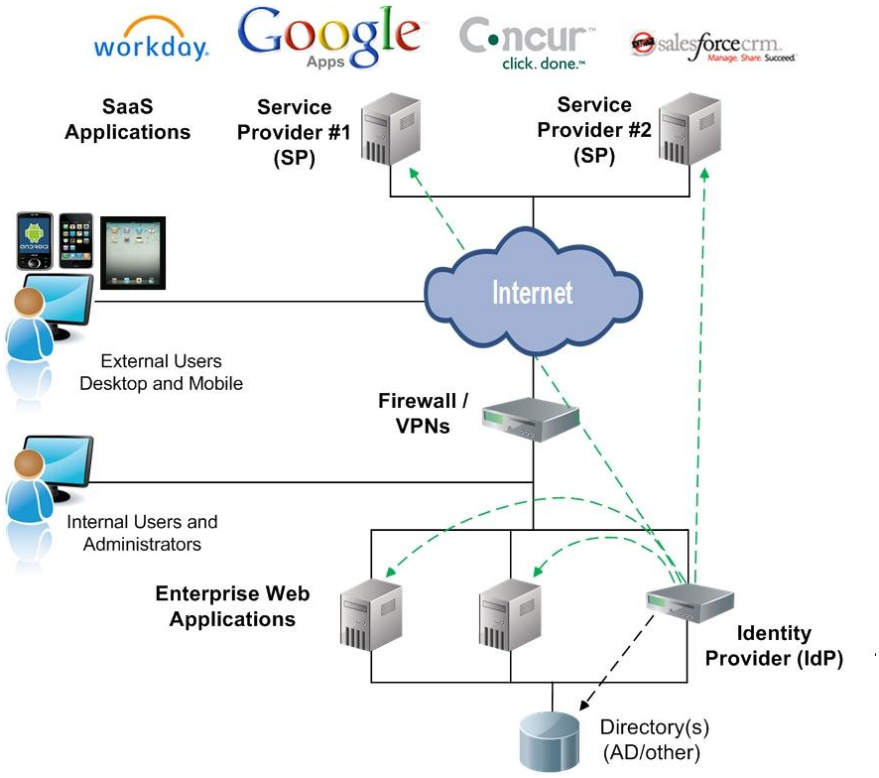
IdPs Defined

An IdP is the identity authentication component that serves identity details to a Service Provider for web or cloud-based applications. IdPs verify identities to a range of applications – in-house, in the cloud, or consumed as a service – in an agreed upon web-format, typically a layer 7 packet. Despite being called a "provider," an IdP is really just a tool. It's not a directory call. It's not a directory synch. Rather, it's just some form of agreed upon web ticket that both sides approve.

In the Honan hack, one of the security vulnerabilities was the fact that Honan daisy-chained accounts. Certain key details, such as email addresses and physical addresses were consistent among them, and one account (a Google email address, for instance), could help him (or an attacker) unlock other accounts (Amazon, Apple). Because user identities sprawl across the Internet, attackers have a much larger surface area to attack, which would point to the fact that if enterprises were to shrink that surface area, many attack strategies would be blocked.

For years, enterprises have been seeking single sign-on (SSO) solutions. Done right, SSO from a central identity provider, instead of daisy-chaining, greatly improve security. An IdP can provide SSO from a strong identity tool within the enterprise, the enterprise directory (Active Directory, LDAP, etc.), out to the cloud, SaaS applications; mobile apps, web resources and whatever else should be protected by strong authentication.

This may sound complicated, but it doesn't have to be. What an IdP does is obtain identity credentials from the enterprise, conduct an authentication session and then pass the trusted identity to the SP.



In specific, the IdP provides these functionalities:

1. Connects to an enterprise-held data store (AD, SQL, LDAP, etc.)
2. Accepts an identity from some mechanism (AD SSO, browser, portal, other app)
3. Authenticates the user is some fashion (ID/Password, IWA, 2-factor)
4. Asserts the user identity out to the SP in an agreed upon, universal way, typically through a federated token (SAML, OpenID)
5. Logs the authentication and session in some manner

Do I Have to Buy Yet another Security Product?

Believing that IdPs are products is one of the main misconceptions about them. There are indeed products you can buy, or service providers you can outsource to in order to handle this process, but even if you buy a product to help you manage the process, an IdP isn't a product you buy, but rather ability you acquire.

Is this just a matter of semantics? No. The IdP capabilities are too important and too fundamental to online trust to be considered a product.
Our online, connected world erodes trust. Much of that erosion occurs because. . . well, on the Internet nobody knows you're a dog, or a spammer, a scammer or a hacker. Until it's too late.

With a strong identity platform in place, you may still be any of those things, but the enterprise and Service Provider will know you are who you say you are. If Jack Smith happens to be a Jack Russell Terrier, you will know you have an HR problem, not a security one.

Even though an IdP should be thought of as an underlying security ability, most organizations will indeed purchase products to help them acquire that ability. It's not necessary to do so, but it's a long, cumbersome, error-prone process if you go it alone, and most organizations will find it more cost-effective to turn to market-tested solutions that streamline the process and strengthen the underlying identity foundation more than you could on your own.
Software exists to automate most of the IdP process, but before we look at an example of such software, let's look at why you'll want to have IdP abilities in the first place.

Why You Must Become an IdP Today: Five Reasons

1. Protect Yourself against the Risks You Know about. The most important reason to become an IdP is to start mitigating the many online risks that assault your organization each day. Phishing attacks, data loss, IP theft, cross-site scripting, buffer overflows, etc. We won't detail them all here, but let's just say that the Honan hack is the tip of the iceberg.

2. Prepare for Emerging Risks, especially Cloud and Mobile Ones. As businesses move to embrace cloud and mobile environments, identity becomes the linchpin of any security effort. If you think you can just avoid cloud products and enterprise mobility, you're deluding yourself. Many software providers are moving away from shrink-wrap software to SaaS and cloud models. Behemoths like Microsoft, Apple, Google and VMware are all heavily invested in cloud computing and mobility.

3. Protect Your Existing Identity Investments. Becoming an IdP helps you preserves your investment in existing identity tools like Active Directory. Most enterprises have sunk a lot of money into Active Directory, and they've spent a ton of time tailoring AD to fit their organizations' needs. In fact, most enterprises have structured their roles and policies according to AD concepts such as groups and attributes. Translating and migrating this lexicon of policies – is more than just synching identities. Any identity solution that requires that you abandon those investments should be looked upon skeptically.

4. Keep Your Identities Safe and In-House. You will hear various identity SPs telling you to outsource identity management to them. Chances are this will work out fine most of the time. There are major risks with this approach, though. If you are in a heavily regulated industry, outsourcing identities complicates compliance. If you lose the ability, over time, to manage identities, what happens if the third-party fails or, worse, is acquired by your main competitor? What if they experience a breach?

5. Guard against Expanding Insider Risks. If you outsource identities, you must now worry about insider threats from that Identity Service Provider too, because their insiders can do as much or arguably more damage than your insiders can, and you have no ability to train, monitor, manage, and if necessary, fire those third-party insiders.

Moreover, in this age of outsourcing and partnering, organizations of all sizes must grant access to enterprise resources to contractors, partners, guests and temporary employees. If you don't have strong identity management tools in place, insider threats grow exponentially.

Do Service Providers actually Support this Concept?

They do. In fact, one of the critical ingredients of the IdP is SAML (Security Assertion Markup Language)[1], which is backed by Salesforce.com, SuccessFactors, Oracle, Box, Google, and many others.

[1] ***SAML Defined.*** *Developed by OASIS (the Organization for the Advancement of Structured Information Standards), an organization that handles more than seventy other Web standards, SAML is an XML-based framework that allows for the exchange of security information. SAML enables different organizations (with different security domains) to securely exchange authentication and authorization information.*

Through SAML, your organization can deliver information about user identities and access privileges to a cloud provider in a safe, secure and standardized way. Many enterprises consider SAML the cornerstone of their SSO efforts.
OpenID is also an open standard. While SAML is an enterprise-focused standard, OpenID is more suited for consumer-facing apps. It allows users to be authenticated in a decentralized manner, saving the need for each and every SP to develop their own authentication systems.

When you log into some third-party application or site using your Google or Yahoo! credentials, you are leveraging OpenID. Of course, as the Honan hack proved, if you are going to daisy-chain accounts in this manner, your risks are equal to those of your most poorly secured account. In other words, without federated identity management, a weak link exposes all other related accounts. With federated security in place, on the other hand, identity management is consistent across all of your accounts.

How Do I Become an IdP?

As with so many things in life, there are two ways to become an IdP. There's the easy way or the hard way. Let's start with the hard way first.

How Do I Become an IdP on My Own?

For you Do It Yourself (DIY) enterprises out there, becoming an IdP on your own is certainly achievable. Here are the eight things you must do:

1. **Set up a secure web server.**
2. **Conduct secure data store connectivity**
3. **Conduct the proper authentication of the user**
4. **Construct the proper ID artifact (i.e., the match protocol of the SP)**
5. **Cryptographically sign the ID token**
6. **Construct distinct IdP URLs for each distinct SP**
7. **Log the user authentication and ID assertion**
8. **Manage the enterprise ID (used in federation steps above)**

At first glance, this doesn't look that complicated. But it gets more complicate the further along you get. Let's compare step one to, say, step six.

Step 1: Set up a secure web server. This means that if you are sending assets from your web server out in the world (to other apps, mobile apps, SaaS applications, etc.), you must ensure that the web server cannot be compromised. You must set up protections to prevent attackers from manipulating identities in order to gain access to sensitive data.
Even if you aren't an IdP, you must secure your web server assets, and your identities as well, and most enterprises have made significant investments that are intended to secure those things.

Now, let's look at **Step 6: Construct distinct IdP URLs for each distinct Service Provider.** Easier said than done. What exactly does it take to navigate this single step in the process?

The process starts by linking your in-house identity stores in a way to serve credentials to a service provider, such as Google. Realize, though, that once the first SP is worked out, various departments will clamor for the addition of other SPs, such as Salesforce.com, SuccessFactors, and Workday.

If you don't plan properly, each project will be a discrete one, requiring that you pretty much reinvent the wheel each time. How are you going to craft a new IdP for each of the resources your enterprise would like to federate to?

This is NOT trivial. It either requires that you: 1) Set up a completely new IdP server for every SP or 2) sub-divide your current IdP in a secure and well-articulated manner to befit multiple SP support.

Most enterprises who become IdPs via home-grown mechanisms choose the first approach, which then leaves them with serious maintenance and security issues. The maintenance issue should be obvious – because of the replication of servers across the enterprise. The security issue is a little less intuitive, but no less real. Enterprises often lose track of the proliferation of IdP servers. Thus, the servers fall out of scope of security reviews, maintenance and procedures.

Option two is the superior model for a number of factors, but it is often beyond the grasp of most DIY enterprises. What it requires is to securely subdivide each subset IdP in the master server to be its own distinct server by allowing it to:

- Configure its own data store selector
- Configure its own authentication and user workflow
- Configure its own identity assertion event
- Configure its own logging

In essence, the IdP solution should be crafted in a way to support almost infinite sub-IdPs – one for every SP. This "crafting" is beyond the scope of most, if not all, enterprises.

For an in-depth look at how to go it alone and become a DIY IdP, refer to "OK – So I'm Supposed to Become an Identity Provider (IdP) – What does this Mean?"

The Easy Way to Become an IdP: Automation

Technology tends to move towards automation and consolidation. Virtualization and cloud computing are both part of this trend. It's not as set in stone as Moore's Law, but everything from managing software patches to deploying servers to resetting passwords – tasks that used to be cumbersome and error-prone – can now be automated.

The trouble with this trend, though, is that IT shops struggle with the labor-intensive, error-prone processes for years before they turn to automation (or before automated solutions are even available).

Don't make this mistake as you attain IdP capabilities.

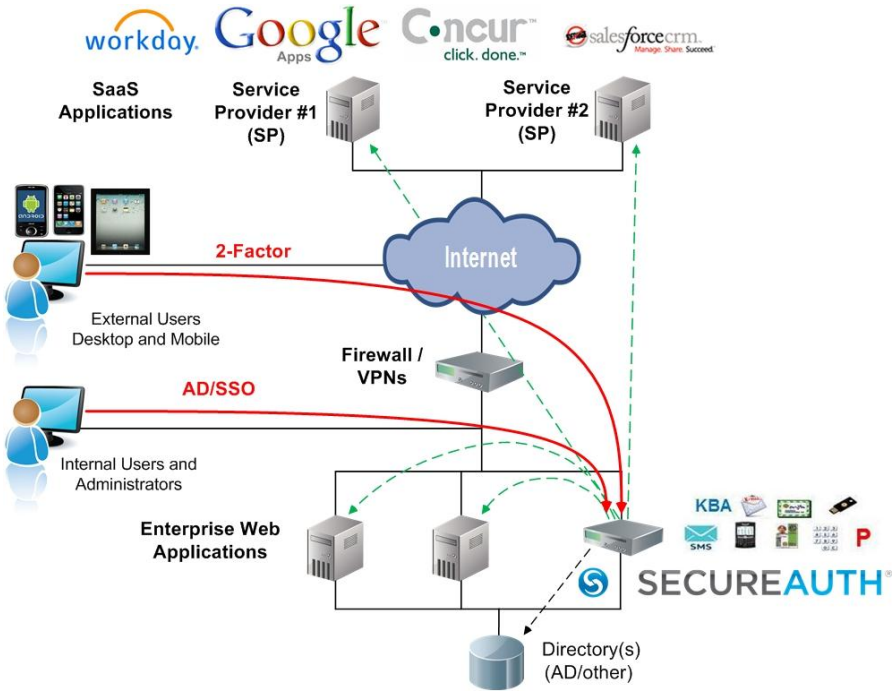
Automated IdP solutions have hit the marketplace recently, and they will simplify the process, save you money and help you avoid dangerous misconfigurations. Automated IdP solutions save you from the trouble of:

- Setting up and properly configuring secure web servers
- Setting up secure connections to enterprise data stores (AD, LDAP, etc.)
- Authenticating users to multiple third-party apps and services
- Sub-dividing the IdP to support multiple SPs
- Manually logging user authentication and ID assertions
- Enabling an SSO solution for on-premise, cloud and third-party apps

Why You Should Choose SecureAuth IdP – the World's First 2-Factor IdP

SecureAuth IdP is the only tool that delivers instant IdP capabilities for the enterprise, for SaaS, the web, VPN, cloud and mobile resources. SecureAuth IdP delivers instant IdP capabilities (on-premise, in the cloud or for mobile devices) with variable 2-Factor authentication built in. SecureAuth IdP is the only product that, in a single solution, provides:

- Two-factor authentication
- Identity Provider functionality



SecureAuth is currently the only solution that enables companies to become their own secure, auditable IdP. By becoming an IdP, companies can better control, enforce and extend security standards to all on-premise and cloud-based applications, as well as to any mobile devices supported by their organizations. It also enables single sign-on (SSO) without the need to synchronize to an enterprise directory or to send credentials to a third-party SSO provider, which dramatically increases IT security.

Find out for yourself with a 30-day free trial of SecureAuth IdP. See for yourself how straightforward and swift the process of enabling regulation-compliant single-sign-on (SSO) for all your cloud, mobile, and network/VPN applications can be. Start with the user directory you already have in place and you'll be connecting iPhone users to VPN applications and remote workers to SharePoint in short order.

Conclusion

As the social engineering attack on *Wired* writer Mat Honan proves, the proliferation of identity information used for authentication can be maliciously used against a user and an organization.To address these escalating risks and to adopt emerging technologies such as cloud-based infrastructures and mobile apps, enterprises should be Identity Providers (IdPs). An IdP is the identity authentication component that serves identity details to a Service Provider for web or cloud-based applications. IdPs verify identities to a range of applications – in house, in the cloud, or consumed as a service – in an agreed upon web-format, typically a layer 7 packet.

DIY enterprises can become IdPs on their own, but this is a complicated, expensive, error-prone process. Smart organizations will, instead, automate as much of this process as possible.

SecureAuth IdP is the only tool that automates the entire IdP process. SecureAuth IdP delivers instant IdP capabilities for the enterprise, for SaaS, the web, VPN, cloud and mobile resources. SecureAuth IdP is a shrink-wrapped IdP (on-premise or cloud) with variable two-factor built in.

See for yourself how straightforward and swift the process of enabling regulation-compliant single-sign-on (SSO) for all your cloud, mobile, and network/VPN applications can be. Sign up for a 30-day free trial of SecureAuth IdP now, and start eliminating identity related security risks today.

8965 Research Drive, Suite 200, Irvine, CA 92618

p: 1-949-777-6959 f: 1-949-743-5833 gosecureauth.com