viewds identity solutions

White Paper:

4 Critical IAM Features for MSPs

As a Managed Service Provider, you have unique challenges that evolve every day. From the changing technology landscape, security threats, and the balancing act that comes with appropriate staffing, your plate is full. We've been there, which is why we developed solutions that help address unique needs for your organization.

Help Desk Verification

Whether you transact hundreds or thousands of service calls every year, it's important that you're able to verify all of your end users. How do you know that it's actually Mary, the managing partner at one of your biggest law firms or a bad actor looking to perform some social engineering?

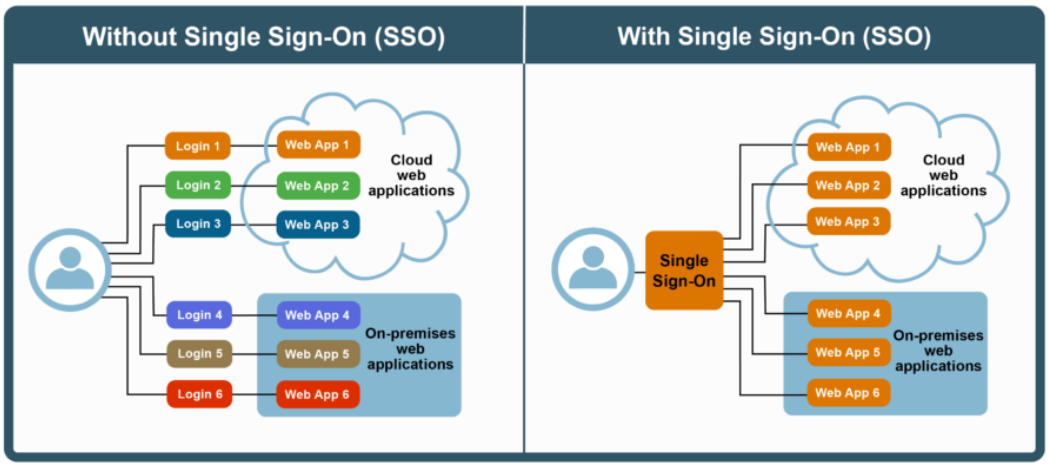
What if the attacker does gain access? What if they managed to escalate their privileges? How much damage would it cause? It's probably something that's crossed your mind so you went out and purchased an MFA solution to help mitigate your risk. But now you've added another challenge; are the users willing to embrace installing and maintaining the MFA application on their phones?

Cobalt's Help Desk Verification system allows a different approach:

- SMS challenges that most users are already familiar with
- Alternative email-based challenges for those without phones
- Low latency SMS response (sub 10s for each push)
- Flexible deployment options
- Continuous support

Single Sign-On (SSO)

How many passwords do you manage? On a personal level, probably a few. And you've probably used a derivative of that same password for many other platforms, right? What about your employees and customers? The perception is that SSO creates a single key to the castle, but the reality is that it provides the ability to harden security in a manner that people can easily get accustomed to. Instead of managing a complex password and incorporating MFA into each application, using a single password reduces the overall complexity of password management and the ease of use for the end user allows for a more secure way to access applications.



How does that translate into the MSP world? If you have 10 employees accessing 5 applications per employee and you require a password change every 90 days, that is 200 password rotations per year. Let's expand that to your customers. If you have:

- 50 customers, 15 users per customer
- 5 applications per customer

You're looking at 15,000 password changes per year. With SSO you reduce that to 3,000. But, that also assumes that you're doing the password resets yourself.

Cobalt's SSO solution provides:

- Single Sign-On to applications that have an open API
- Reduced password management
- An MFA vendor neutral approach (Google Authenticator, Authy, Microsoft Authenticator, and more)

Self Service Password Resets

Password resets are a mundane task, but a necessary one where your customers leverage your help desk for assistance. In recent studies, it can cost as much as $70 per help desk request for a password reset when you combine all of the factors associated with staffing, time, and lost opportunity costs.

Let's look back at our previous numbers and let's assume you won't really be servicing all of those password resets. In addition, let's also assume that the cost isn't nearly that high. At 50% across the board, you're still looking at over $260K in costs associated with scheduled password changes.

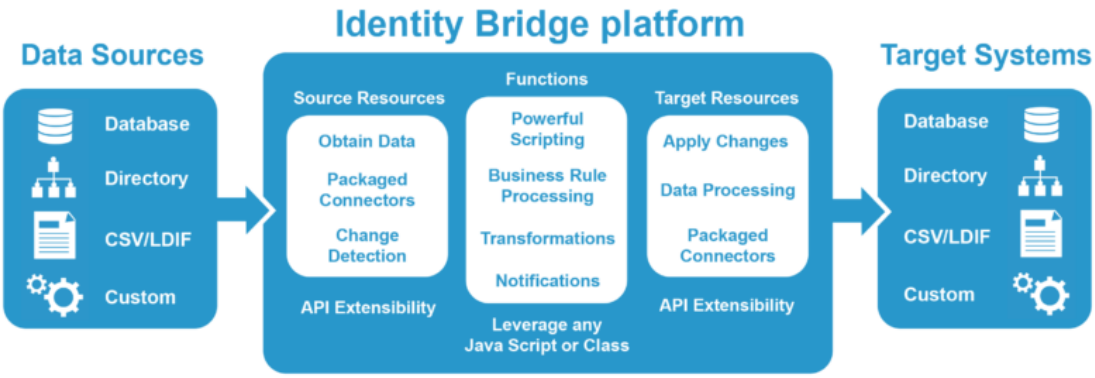
With SSO the costs dramatically decrease to just over $50K. A savings of over $210K annually. And, your organization can easily control the password policies through centralized management.

Cobalt's Password Resets allow:

- Users to change their passwords without contacting your help desk
- Reduce the complexity of password management
- Allow administrators to create policy-based password management unique to each tenant

Provisioning/Deprovisioning

Your staff and technicians have a tremendous amount of access to your internal platforms, and your customers share that same issue with access to their own platforms as well. Creating users can be tedious. Cobalt leverages our Identity Bridge platform to synchronize identities and allow centralized administration over the initial provisioning process.



But what about when the users leave? On average, it can take an organization 4 – 6 hours per employee to terminate access to various systems and platforms. It's even more costly during emergency situations. What if there was a system that was overlooked? What if the former employee still has access?

Our unique ability to synchronize identities also allows the process to happen in reverse. Providing administrators centralized control over the identities also allows a single "switch" to be flipped by disabling users in our administrative console and disabling their access to additional associated systems.

Cobalt's Provisioning and Deprovisioning allows the MSP to:

- Provision users across multiple systems with a single entry
- Easily disable access to multiple applications with a few clicks
- Increase overall security for employee terminations and resignations