

How to let the good guys in and keep the bad guys out?

In the first of a three-part series looking at aspects of defending your enterprise systems, at a time when cloud technologies are changing the concepts of application location, Decipher Works Principal Consultant Michael Leonard discusses security access management challenges.

The advent of cloud applications has changed the IT landscape. Traditional models of purchasing, building and deploying applications into production have been transformed. Many organisations are now using applications to conduct transactions with their partners, suppliers and customers across multiple domains. At the same time, business stakeholders now frequently subscribe to cloud services for departmental use, sometimes with little or no recourse to IT. Anecdotally, it is estimated that two-thirds of applications now operate 'outside' the enterprise IT organisation.

Information security professionals and others responsible for compliance with internal and regulatory standards have always faced significant challenges in maintaining control over access to enterprise applications. Let's examine some of the new hurdles that have been raised, and how to clear them.

Managing access to different kinds of applications

Most enterprise users access a wide range of applications to perform their job. This frequently results in the need for multiple usernames and passwords with all the attendant productivity, security management and IT support implications:

- Users forget how to access each application (especially those irregularly accessed), resulting in lost productivity and frustration – especially when trying to work from home or on the road.
- This results in calls on IT – with unnecessary support resources expended on assisting 'locked-out' users and resetting/reissuing application passwords.
- Potentially more serious, users record their unique application access credentials on Post-It notes or other aides-de-memoire that could compromise enterprise security should they lose or misplace their access device, wallet or briefcase.

In response, many IT organisations have adopted a Single Sign On (SSO) solution that addresses these issues by:

- Centralising control over enterprise user accounts to reduce management effort
- Reducing the burden of supporting users who need to remember (but inevitably forget) multiple usernames and passwords

In this White Paper...

- Limits of Single Sign On in the cloud era
- Managing access to SaaS applications
- Overcoming multiple passwords and usernames
- Bringing external applications into SSO
- Minimising access management costs, resources and risks

- Eliminating the risk of users writing multiple passwords down, or storing them insecurely on laptops and mobile devices
- Delivering visibility over access to enable management of potential risk

If you've already implemented SSO to manage access to your internally-hosted applications, you'll have overcome these issues – but for those applications only!

Corporate web applications

These include your own web servers, web applications and portals – such as your intranet and applications used by remote workers – which are hosted within your own domain.

Cross-domain applications

Many enterprises now use web-based applications that seamlessly access resources from a partner, or between different lines of business within your organisation. These cross-domain applications include web servers, web applications and portals involving cross-domain exchanges.

Cloud services and Software as a Service (SaaS)

Operated by external parties – such as SaaS providers or e-commerce hubs – via the internet, these applications may become increasingly critical to your operations. Whether the business has sought the assistance of IT in deploying them, and whether or not they are integrated with your own enterprise systems, they still provide access to valuable corporate data that must be protected.

Support for cloud services that require little or no input from IT can still raise support and security questions. For example:

- When users forget passwords, how are they reset? Will the user or IT need to call a contact centre on the other side of the planet for assistance? What kind of controls are there in place to ensure that the person makes that call is actually who they say they are?
- When someone leaves your company, how easy is it to remove their access to these applications and can this be performed quickly?

Extending SSO to the cloud

So how can you include cloud-based applications within your existing enterprise SSO access technology and processes? One reason for line-of-business managers not wanting to engage IT in cloud application deployment is the fear that such engagement will become onerous. Offering simple, effective ways of delivering access to new applications the business wants to use – without compromising corporate security standards – makes it more likely the business will involve IT in future SaaS decisions.

The perils of Post-Its

One of our clients, a professional services firm, has consultants that travel widely throughout the region, using the firm's VPN to access a range of applications to support their work as well as several partner portals. This meant they had numerous accounts and passwords, and many of the consultants recorded them on Post-It notes stuck to their keyboard or lists slipped into their laptop carry bag.

When a consultant mislaid a laptop and its accompanying list of systems, usernames and passwords on an international trip, the firm sought our help. We devised a solution based on IBM Security Access Manager Enterprise Single Sign On. Now the firm's consultants only need remember a single username and password to log onto the firm's VPN via their laptop or tablet. From there, they can access all the systems they need for their work, wherever the applications – and the consultants themselves – are physically located.

Web applications

For your own web applications, domain-based Kerberos authentication may supply a solution that allows for SSO to some applications, while security access management (SAM) solutions that integrate with web-based applications are also available.

Cross-domain applications

For cross-domain applications, a federated access model is a highly effective method of connecting partners and suppliers in your business ecosystem. It is also a way to quickly incorporate new acquisitions, or bridge different divisions within your organisation that might have different security implementations. Integrating these applications with a federated identity management solution (FIM) can allow for SSO.

Many applications are able to integrate with FIM, which delivers a central, internally managed and strong authentication and authorisation point that brings cloud application access back under control. Password resets are not required, as users do not log into these cloud applications directly. Plus, removing access when users leave or change roles can be performed under your own internal authentication and authorisation policies.

But what about those applications that either don't or can't integrate with FIM? For example, web applications that are hosted in DMZs may not be allowed to synchronise data from your protected network, which means that passwords cannot be kept in sync.

Automating passwords

You can overcome this challenge with a solution that enables login to applications via SSO, rather than the actual application itself, allowing users to access these applications transparently. The user only needs to log into a device as themselves, then they are given access to the applications and the range of transactions they are authorised to perform within them.

The benefits of such a solution include the ability to handle periodic password changes automatically, and the inability of people to share passwords with others – because at no time do users actually know their username or password to the particular application! Thus the identity of the user accessing applications is assured and the need for users to remember multiple credentials and change their passwords according to the schedules of each application provider is removed. Automated password changing also enables extended complexity for application passwords, since end users don't need to enter or remember them – further reducing the possibility of brute force password cracking or password guessing. Additionally, as users are much less inclined to supply their device logins to their colleagues, it is significantly less likely that others will be able to access their applications.

Bringing SaaS into the fold

Our client, a national distribution business, selected several cloud application providers to deliver their CRM and HR systems. The IT team wanted to ensure that employees could only log into these applications from work, to ascertain the computer used is free of viruses and spyware. They also needed to meet internal processes and policies for removing access from all applications immediately an employee leaves. However, the SaaS applications chosen by the business for their operational functionality didn't allow for provisioning an API to the company's access security systems. This would have meant additional manual processes to remove users from multiple cloud applications, with the risk that removal of access to confidential or valuable commercial information might be missed.

The company approached us about increasing security over these critical systems. We devised and implemented a federated SSO solution based on IBM Federated Identity Manager. There is no longer a need for users to provide username/password to access the cloud applications – in fact, the users don't even know their username and/or password for these SaaS applications. As FIM is only made available to computers connected to the internal company network, only managed corporate devices can access them. Also, as soon as an employee leaves, they can be denied access to these externally-available applications in the same operation that removes their internal logins.

How will your business benefit?

Greater flexibility in application delivery does not necessarily mean compromising your security policies and standards. Implementing a comprehensive SSO regime to cover all the applications your users access – regardless of where they are hosted and their in-built access provisions – improves security and reduces business costs. Benefits can include:

- Reduced costs from retiring discrete and custom access administration solutions across your software and web infrastructure
- Reduced IT support resources by reducing the need to reset passwords
- Improved staff productivity resulting from fewer employee logins and credentials required when moving between applications
- Improved IT productivity by significantly simplifying administrative effort involved in adding new users and removing redundant ones, as well as reducing calls to the help desk from users having difficulties accessing the applications they need, when they need them
- Increased user satisfaction – whether employee, partner and/or customer – through standardising the SSO experience to eliminate multiple ‘roadblocks’ to performing different transactions
- Improved business flexibility and faster time to market with on-demand provisioning of appropriate access to new applications from a centralised, standardised enterprise security infrastructure
- Reduced risk with centralised auditing of runtime authorisation events enabling easier detection of malicious behaviour
- Stronger security easily achieved by adding multifactor authentication for higher risk applications.

How to get started

The implementation of a comprehensive SSO solution that effectively covers all of the applications your users need to access is best run iteratively, so that benefits can be realised quickly and value directly seen by the business, thus demonstrating the validity of the IT decision. The process begins with a review of your existing access security policies and processes. Potential challenges – such as the deployment of existing or planned cloud- or web-based applications – are assessed and factored into design of an access security architecture. Once the appropriate solution is deployed, you can then concentrate on monitoring and preventing the ever-present threats of unauthorised access from within or outside your organisation: the subjects of the next two papers in this series:

- > *Who's having an identity crisis?*
- > *Real time threat intelligence, PCI compliance and reporting*



Michael Leonard is Principal Consultant at Decipher Works specialising in ISAM and FIM, and is the firm's Infrastructure and Virtualisation subject matter expert. He previously worked with Fujitsu/RailCorp, Leighton Contractors and IBM Global Business Services, when he designed and deployed a new Identity and Access Management framework for the Australian Department of Immigration and Citizenship (DIAC). At Allianz Australia, he delivered Identity and Access Management for online insurance and claims services. Recently, he has led Decipher Works' deployment of Global Access and Federated Identity Management for a large Australian investment bank.

About Decipher Works

Decipher Works specialises in helping medium-to-large organisations enhance their information security infrastructure to reduce risk, cost and maximise return on their IT investment.

A certified IBM Security Systems business partner with a strong focus on solving our client's specific business issues, we draw on our deep industry experience to design, deliver and manage customised IT security solutions offering rapid ROI. Our team of consultants has an extensive track record in successfully implementing business-driven security, identity and access management systems and complementary application integration and software development services.

Phone 1300 724 880

Email services@decipherworks.com.au

Web www.decipherworks.com.au