i-Sprint
Trust without Boundaries

Simple, Strategic and One Login for Enterprise, Cloud and Mobile

i-Sprint's Secured Unified Single Sign-On Solution

Issue 1

Featuring research from Gartner

Introduction

The Gartner report, '**How to Get to Single Sign-On**' , provides industry insider facts, background and insightful analysis on the current industry climate, observing that "The quest for SSO is a symptom of a broader problem. It is a by-product of a build-up of systems that each requires stand-alone authentication and potentially stand-alone administration."[1]

Exploring this industry-wide issue and the enterprise solutions that are available to organisations, the report comments that the need for multiple authentication and log-in steps results in continuing user complaints about the inconvenience, which in turn drives up an organisation's customer support costs.

SSO provides immediate benefit to the end-user in terms of an improved user experience by streamlining logins to multiple applications with a single username and password.

However, this is really just the first layer of benefit provided through SSO implementation.

As users are required to authenticate to an increased number of applications, the likelihood that they will either use the same password across applications, write them down and even occasionally share with friends greatly increases. If the password to one of the applications is compromised, it can be used to attack other applications easily. This may be mitigated by enforcing strong password policies at each application.

If stronger passwords are required, users inevitably forget them more often – resulting in higher help desk costs.

Consider the significance of users only needing to remember and enter a single password. They would be less likely to forget or write down their password, stronger password complexity policies can be enforced, and have lower incidence of login difficulties. Thus, these improvements not only provide organizational benefits in the form of increased productivity, but also enhance security and reduce support costs.

Source : i-Sprint Innovations

[1]Gartner Inc. , How to Get to Single Sign-On, 21 January 2013, G00247863

Assess the Current Environment and Drivers for An SSO Solution

A well-executed SSO strategy reduces password-related support incidents and provides users with improved convenience and more efficient authentication processes. But SSO has been around for the last number of years. Some companies seem to have survived so far without it; those who have implemented it seemed to have gone through some efforts to keep up with it. Do you need SSO in your organization? Gartner advised "a best practice is to identify the tactical and strategic approaches that reduce enough of the problem space over time and within budget."[1] You will need to assess the current environment and identify the business drivers relevant to the organization.

Some of the business drivers are:

- Provide a seamless user experience in accessing various types of applications
- Enhance security with strong authentication for the master login
- Cater for the new computing initiatives such as Cloud applications, Mobile applications, etc
- Reduce support call for password related issues
- Comply with the user access governance and policies

Source: i-Sprint Innovations

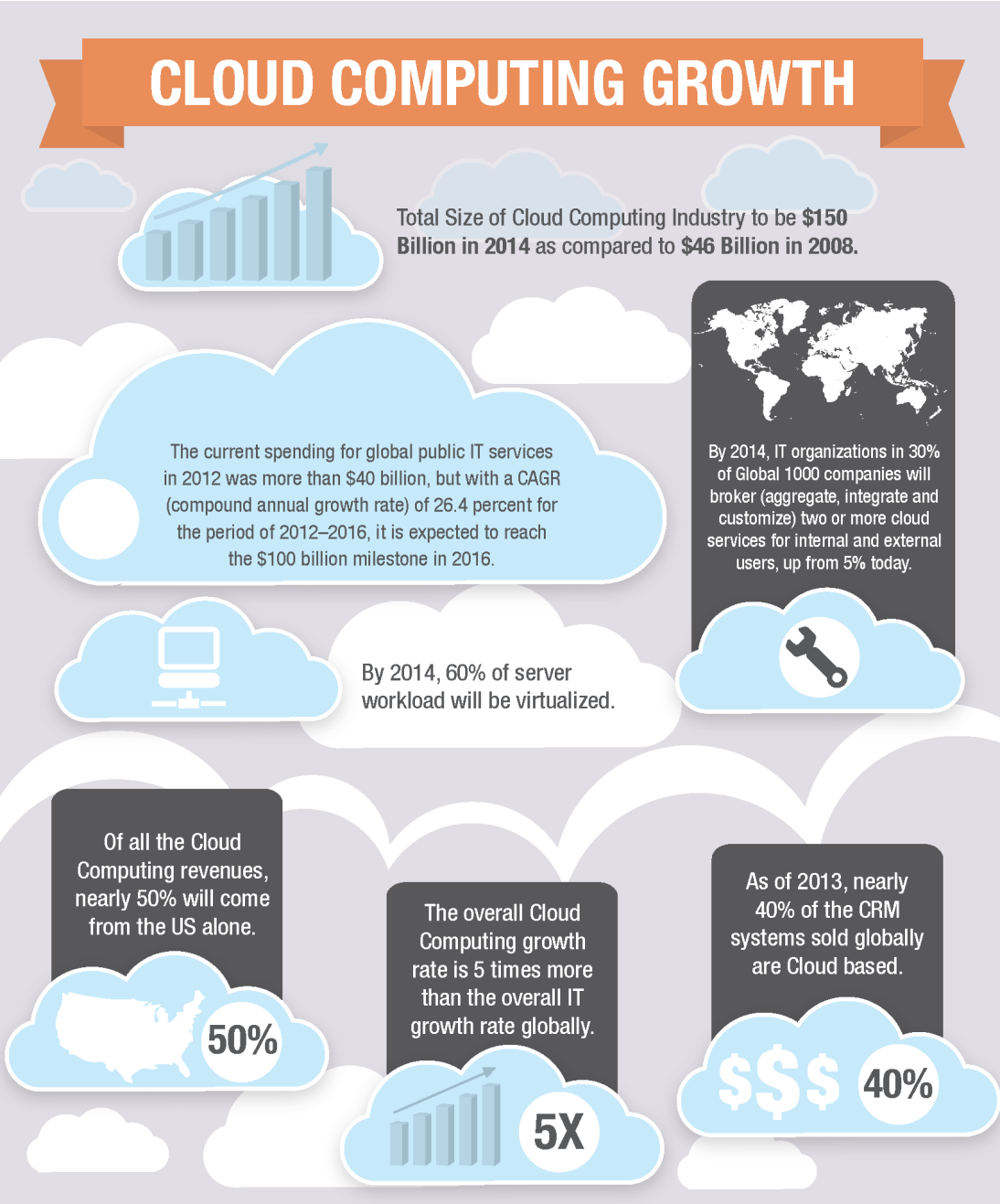
[1]Gartner Inc. , How to Get to Single Sign-On, 21 January 2013, G00247863

Today's Single Sign-On (SSO) Landscape

Cloud Computing

Technology innovation and business disruption are changing the software market today. The adoption rates of software-as-a-service (SaaS) for different software applications by enterprises have grown and are growing at a remarkable rate. Today, it is common to have 10 or more SaaS applications used across an organization and within departments. "Gartner's forecast for estimated SaaS total software revenue within the enterprise application software markets is a 17.2% overall CAGR from 2010 through 2015, or more than $22 billion to SaaS at the end of the forecast period."[1]

This evolution has created a complex environment that requires employees to remember multiple usernames and passwords for different system, application or service that they access. Users in these organizations are struggling to keep up with the increased new passwords and accounts that each application brings.



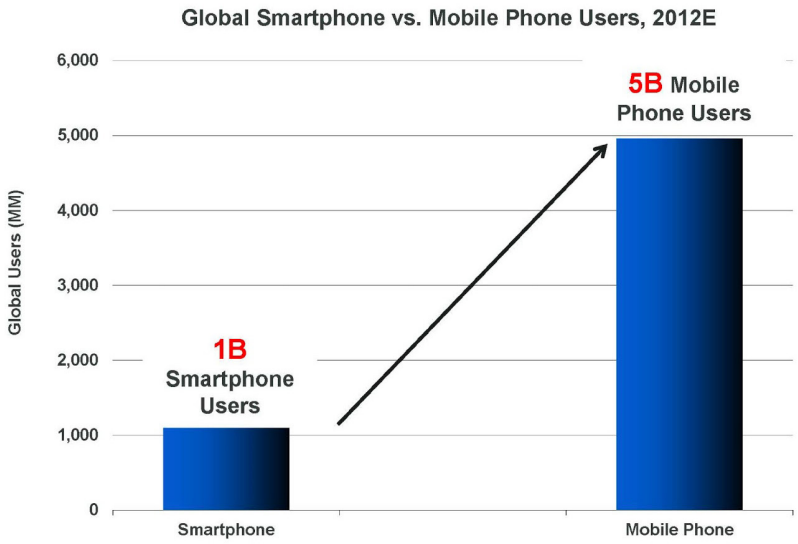
Source: Cloud Computing Infographic, August 2013[2]

Mobile Computing

The consumerization of IT trend has exploded over the past few years and is tightly coupled with the growth of the mobile economy and cloud based services. This trend has brought more applications and services which require the users to remember more user ids and passwords.

In an enterprise context, a trend that has evolved in mobile computing is Bring Your Own Device (BYOD). Companies now find themselves embracing enterprise mobility and balance the surge of BYOD with company security. Gartner predicts that "by 2017, half of all employers will require employees to supply their own device for work purposes."[3] Forward thinking enterprises are balancing the needs of a highly-mobile workforce with the security and manageability requirements of SSO, with identity and access management.

FIGURE 1 Despite Tremendous Ramp So Far, Smartphone user Adoption Has Huge Upside



KPCB

Source: Morgan Stanley Research estimates.
Note: One user may have multiple devices. Therefore the number of actual smartphone and mobile phone devices in use is likely higher than the user data shown here. 11

Source : i-Sprint Innovations

[1]Gartner Inc., Forecast: Software as a Service, All Regions, 2010-2015, 1H12 Update, G00228690, 13 March 2012
[2]http://www.prweb.com/releases/2013/9/prweb11121596.htm
[3]Gartner Inc., Gartner Press Release, http://www.gartner.com/newsroom/id/2466615, 21 January 2013

Can Your Enterprise Meet the Growing Demands?

One thing is certain: if an enterprise has any interest in increasing productivity, enhancing security, or reducing support costs in today's business landscape, a serious evaluation of SSO solutions is absolutely essential. What is needed is an approach that creates a seamless platform spanning the enterprise, SaaS and mobile world.

Some of the questions that you need to ask:

1. How many applications are your users accessing in a typical work-day?
2. How often do these passwords change? Every 90 days? 60days? 30 days?
3. Is there any Password Policy in effect today? Who enforces compliance?
4. Is there any incidence of passwords being exposed (e.g. Post-It notes, Smart-Phones)?
5. Is employee productivity/performance important to your enterprise?
6. Is there any incidence of fraud caused by password-sharing?

"Our original goal when we embarked on this project was to independently price 600,000 deals. We are now doing more than two million deals in the same timeframe."

Alberto Ricciotti
Head of Group Pricing,
Capital Allocation Unit
UniCredit

Based on market requirements, i-Sprint Innovations, a premier Credential and Access Management Solutions provider, has developed AccessMatrix™ Unified Single Sign-On (SSO) Platform to address the SSO challenges faced by organizations.

AccessMatrix™ Unified SSO platform covers Enterprise SSO, Web SSO, Federated SSO and Mobile SSO, and it is one of the leading products within their AccessMatrix™ integrated suite of Identity, Credential and Access Management solutions. AccessMatrix™ Federated SSO module provides identity federation platform that supports popular identity protocols such as SAML and OAuth to provide SSO capabilities for Cloud and mobile applications. It is also extensible to embedded strong authentication solutions on the same platform.

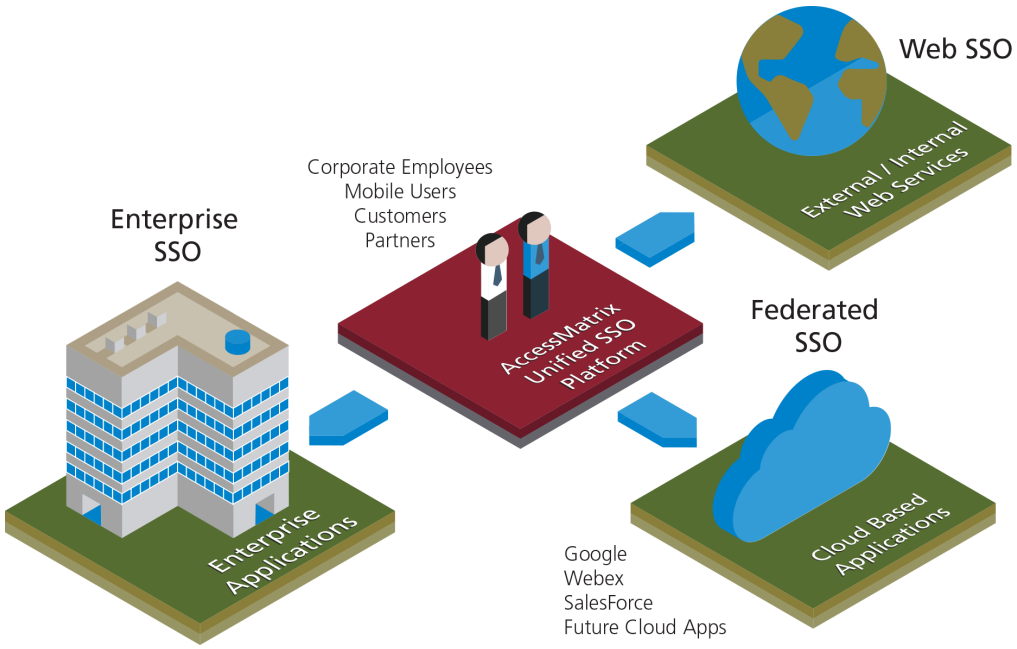
Using an incremental, evolutionary and strategic security consolidation approach based on a common security infrastructure, i-Sprint has deployed their solutions in more than 150 financial institutions, government agencies and high security-sensitive customers globally.

Source : i-Sprint Innovations

AccessMatrix™ Unified SSO Platform

AccessMatrix™ Unified SSO platform enables employees, consumers, customers and partners to access corporate and Cloud applications using a single login process across multiple operating platforms including mobile devices. *The combination of Enterprise Single Sign-On, Web Single Sign-On, Federated Single Sign-On and Mobile Single Sign-On supports SSO* to a wide range of web, non-web and cloud based applications in a single deployment.

FIGURE 1 AccessMatrix™ Unified SSO Platform



Source : i-Sprint Innovations

This platform allows users using different authentication methods to access additional applications and services. For security-sensitive environments, the initial sign-on can be fortified using the organization's preferred multi-factor authentication methods. Re-authentication using different authentication methods can also be enforced before the users can access the target applications.

The platform also provides a web interface with a personalized application list and this allows a user logging into the web portal to access various SSO enabled applications. When a user launches an application from the web interface, the platform provides the SSO function to sign-on to the application on the user's behalf.

Key AccessMatrix™ Unified SSO Platform Benefits:

- **A unified platform** that covers Enterprise SSO, Web SSO, Federated SSO and Mobile SSO
- **Create user convenience and improve productivity** via faster access to applications/ information - users only need to remember one set of credentials
- **Strengthen security** with flexible authentication to improve identity proofing supporting strong authentication methods and user-centric activity tracking
- **Ensure compliance** with powerful reporting capabilities to report user activities and security violations
- **Maximize ROI** by reducing help desk costs through reduction of password reset calls and consolidation
- **Unify SSO access platform** by providing SSO functions to Cloud applications, Web applications, desktop and mobile applications
- **Centralize authentication and management of user access information by** providing a single centralized authentication point for applying stronger policies and through integration with provisioning solutions
- **Lower integration and operational costs** with a common set of IAM services for custom enterprise and internet applications

Source : i-Sprint Innovations

A Comprehensive SSO Strategy

In a typical SSO environment, a user logs in just once, then is transparently granted access to a variety of permitted systems with no further log-in required.

With the diversity of applications and deployments, organizations need to develop and execute an SSO strategy to reduce password-related support incidents and provide users with improved convenience and more efficient authentication processes. A comprehensive SSO Strategy needs to address the following requirements:

- Enterprise Single Sign-On
- Web Single Sign-On
- Federated Single Sign-On
- Mobile Single Sign-On

Enterprise Single Sign-On (ESSO)

Often organizations do not have access to the source code so that they cannot modify applications to achieve their corporate single sign-on objective. Alternatively, they may have the source code, but modifying a working mission-critical application involves potential risks and unnecessary service disruptions.

An Enterprise SSO product enables a user to access multiple systems (web, Windows, terminal server/Citrix, terminal emulator/host, Java and applets-based applications) after being authenticated just one time, without any source code change of the target applications.

With only one primary log-in (which could be using a password, PKI smart card, USB token, biometric scan, proximity card or a combination of supported methods), users can achieve single sign-on to all the systems that they are authorized to use.

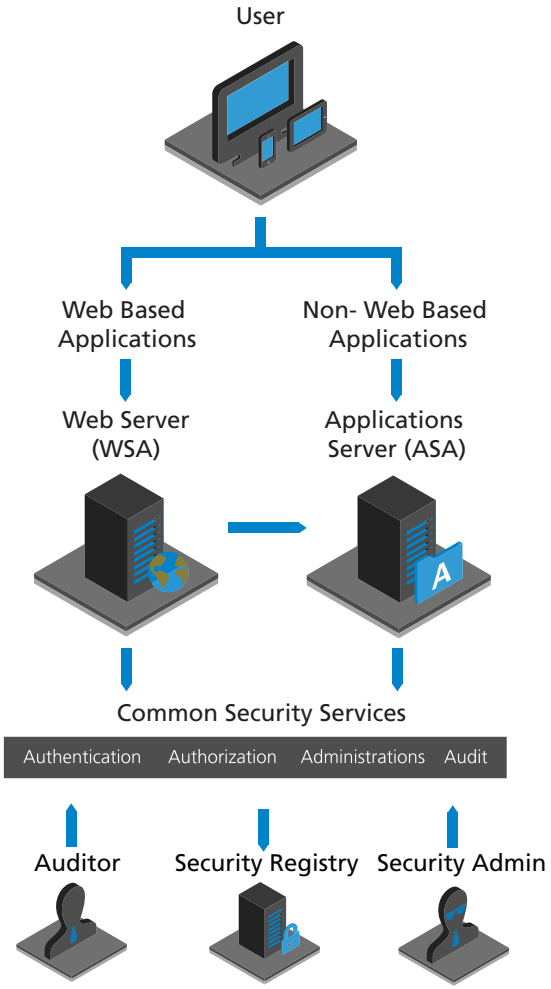
When the user attempts to log into an SSO-enabled business application, the ESSO product retrieves the user ID and password for that application from the password repository and performs the log-in to the target system. Behind the scenes in this "authenticate once, log-in everywhere" model, the system maintains a separate credential mapping (user ID, password and other optional attributes) for each target application.

AccessMatrix™ ESSO provides password vaulting and sign-on automation, enhances the authentication process and enforces consistent password management policies across applications. While ESSO enables single sign-on and follow-on automation for Windows, web, Java, Flash, Ajax, custom built, Unix telnet and mainframe applications without any code changes, it also improves user productivity by simplifying access to all applications while enhancing security by integrating strong authentication mechanisms and proven best security practices.

AccessMatrix™ ESSO for Mobile offers SSO capability for mobile devices providing a native App for Android and iOS. It also supports Citrix Receiver. Organizations now can leverage a common SSO platform for desktop and mobile devices and greatly simplify operational and support requirements.

AccessMatrix™ ESSO At-A-Glance

- Logon to any application: Enables single sign-on and follow-on automation for Windows, Web, Java, Flash, Ajax, custom built, Unix telnet and mainframe applications without any code changes
- Web interface for launching application: An optional web interface can integrate the SSO Client with an existing web portal to provide a common application access point for users
- Web based self-service facility: Enables users to perform application enrolment, password recovery and Windows Active Directory password reset
- Offline operations, auto-Sync and auto-connect: Provides an optional PSE feature (Personal Security Environment) to store the local cache on desktops or in secure storage devices to enable offline access and synchronize log-in information between the Server Password Vault and Local Cache. Configurable option to auto-switch to online mode when the connection to the server is available



AccessMatrix™ Web SSO At-A-Glance

- Web Security Agents (WSA) – With web security agents for all leading web and application servers, Web SSO supports URL level access control with ability to transparently push user information via standard HTTP request headers to assist web applications in establishing user identities and aggregate information from multiple directories.
- User Authorization Mapping – Supports mapping of different user IDs in different applications to a unique SSO ID. This is useful for co-existence strategy when existing applications wish to migrate to AccessMatrix™ Web SSO system. Such user information can again be transparently passed to applications protected by WSA or via web service integration.

Web Single Sign-On (Web SSO)

As web based applications are widely deployed, organizations require increasing support for both internal applications and external applications that service enterprises' customers, partners and other stakeholders. Emphasis is increasingly being placed on the use of Web Access Management (WAM) as a first-stage Cloud computing solution for SSO. Federation technology, included with or sold as an adjunct to WAM, provides the extension to SaaS applications.

AccessMatrix™ Web SSO provides a seamless, tight integration for the single sign-on of web based applications. It is designed to secure multi-tier applications (web based or non-web based) within an organization's data centre or within the Cloud. With use of web server plugins to intercept web requests, Web SSO is able to protect applications from threats identified by OWASP (Open Web Application Security Project). It increases productivity and reduces cost by relieving the business application developers from having to integrate into complex regulatory compliance. After the first deployment, subsequent applications can be easily implemented with minimal cost.

Cloud Single Sign-On (Federated SSO)

Convenience isn't the only driver for Cloud SSO. The rate of adoption of Cloud services is increasing so fast that different departments within an organization are using various Cloud applications without coordinating with each other and their corporate IT department.

It has become critical to find ways to securely manage identity across the increasingly interconnected web services and applications. Web portals are now a mix of services delivered across both on-premises and Cloud based applications.

AccessMatrix™ Federated SSO can act as a gateway or broker, allowing internal users to log-in with their corporate directory accounts, then seamlessly sign into cloud applications like SalesForce.com, Webex, or Google Apps. Business partners and customers have SSO for their corporate applications and are able to sign in with their corporate credentials or their social media identities like Google Apps, Facebook, Windows Live and Yahoo. AccessMatrix™ Federated SSO module can enhance authentication security by enforcing stronger authentication controls using biometrics, OTP tokens, PKI tokens and other multi-factor authentication solutions.

Mobile Single Sign-On (Mobile SSO)

As enterprises get comfortable with mobile devices, there is an increase of mobile enabled web and native applications. However, repetitive authentication on multiple mobile apps is still a major inconvenience for the users.

AccessMatrix™ Mobile Single Sign-On module enables organizations to achieve single sign-on on various mobile platforms extending the SSO experience from desktop to mobile.

For SSO across native applications, the module provides an SDK leveraging on standard protocols like OAuth while hiding the complexity of the protocols.

For browser based applications, a native SSO application is provided to perform SSO to applications using the ESSO approach.

Source: i-Sprint Innovations

Bridging Mobile and Cloud Security

Single Sign-On
to websites and applications

Encrypted data backup
to cloud storage

AES 256-bit encryption

AccessMatrix™ Federated SSO

- Standards-based: Supports all of the standard federation protocols such as OpenID, SAML and OAuth
- Supports a large number of Internet and Corporate Identity Providers including Active Directory, LDAP, Facebook, OpenID, Twitter, SalesForce.com, Google and Yahoo
- Supports the Federation roles of Identity Provider and Service Provider
- Built-in Identity Provider stores user identities in the AccessMatrix's internal and external directories

Mobile Devices Integration

- **Federated SSO for Mobile**: Provides a native application for iOS, Android and Windows mobile devices to perform single sign-on to applications by downloading the credential information from the Server Password Vault.
- **SDK for Mobile**: Enables native mobile applications to deliver the SSO function via OAuth integration while hiding the OAuth complexity.
- **Citrix Receiver**: Enables single sign-on to desktop applications which are delivered via the Citrix Receiver solution.

Case Study – CRM Project for the Most Profitable Bank in Singapore

i-Sprint was asked to undertake a Customer Relationship Management ('CRM') project for Singapore's then most profitable bank, addressing a number of CRM issues and priorities.

The bank wanted to provide an intelligent desktop for all front office staff and to respond rapidly to client inquiries, providing a level of customer service comparable to global benchmarks. It also wanted to manage the cost and complexity of multiple applications security silos rapidly, safely and efficiently in a non-intrusive, audit-compliant way; drastically reduce down-time caused by unnecessary 'password' resets due to misplaced or forgotten passwords/ IDs; and quickly deploy new applications to respond to fast changing customer attitudes and requirements.

i-Sprint's security consolidation methodology was applied throughout the project life-cycle, greatly helping the bank to implement and deploy AccessMatrix™ unified SSO platform, which quickly became the organisation's single sign-on platform.

AccessMatrix™ unified SSO platform enabled the bank to achieve the SSO objective in just weeks, as it did not require any source code changes. The SSO rapid deployment solution was implemented across the region, meeting project schedules and not requiring any on-site visits. Bank employees now only need to login to the USO using the primary login. After login, users do not need their ID or password again to log into the target business applications.

i-Sprint's SSO technology helps the bank improve application security policies and reduce both the number of password reset requests and user downtime due to account logout or invalid passwords. The methodology enabled the client to consolidate all user login processes and provided a consolidated view of application access information.

Source : i-Sprint Innovations

Case Study – One of the Most Progressive Financial Institutions in Asia

With 12,000 employees in Asia, one of the major financial institutions turned to i-Sprint to help its regional staff improve their user experience in accessing multiple applications and minimise human error in using more than six IDs and passwords.

The bank's employees were having to access anywhere from 3 to 32 applications, with some passwords having to be reset monthly. It also needed to mitigate the financial risks from human errors or mistakes arising from the complexity of managing multiple IDs and passwords.

i-Sprint was briefed that the solution must leverage the existing bank-wide web SSO infrastructure with a non-intrusive Enterprise SSO solution, while still being a seamless part of the bank's existing desktop operating environment. The cost of the solution and its deployment must pay for itself within a year and be measured against tangible ROI and against current OPEX.

Implementing our recommended solution, after a successful review by the Global Information Security Organisation, AccessMatrix™ unified SSO platform was cleared for a Proof-of-Concept (POC) project. The initial POC was for 15 applications, but after three months, 45 applications were trained and tested. i-Sprint's security consolidation methodology was applied throughout the project life-cycle.

i-Sprint AccessMatrix™ unified SSO platform enabled the bank to achieve the single sign-on objective in just weeks. The SSO rapid deployment solution was implemented across the region, meeting project schedules and with no need for on-site visits. Staff now only needs to log into their in-house developed authentication system, while AccessMatrix™ unified SSO platform has also been integrated to trust the same log-in information.

i-Sprint's SSO technology helps the Bank improve application security policies and avoids the need for having users to remember multiple user IDs and passwords.

Source: i-Sprint Innovations

Conclusion

So, does your organization need and will benefit from SSO? The answer is very likely a resounding "Yes!" But before we go any further, the point needs to be made that SSO is part of a larger access management infrastructure. Every SSO initiative should be coupled with an analysis of the organization's authorization / access control model to make sure that sensitive resources are in fact protected.

Single Sign-On solution provides end users with an improved user experience and helps IT staff reduce the cost of managing passwords for many applications. Still, a nagging concern persists. If the single credential is compromised, an attacker has free reign over all accessible resources. We need to ask ourselves, does the universal simple password, which can be easily cracked, provide adequate authentication in an SSO world.

The Need for Strong Authentication

With new threats, risk and vulnerabilities related to the usage of passwords, implementing Multi-factor Authentication to ensure that the user is who he claims to be, is an important focus for every business today.

Multi-factor authentication can be defined as requiring two or more of the following factors:

- What you know: such as a password
- What you have: like your ATM card / OTP token
- What you are: biometrics characteristics such as your fingerprint, voice or facial recognition
- Where you are

A new set of risk management techniques, called "contextual authentication", promises to request the proper level of authentication depending on what the user is trying to do. Contextual authentication requires the user to get used to exchanging a single credential for two or three more times, changing the user experience of today's SSO. You may require Level 1 authentication (simple password) to access the computer and network, while requiring Level 2 authentication (one-time password or smart card) to access human resources or financial data. For sensitive applications, you may add biometrics into the mix. The results are greatly enhanced security.

Through a single, unified framework, i-Sprint's AccessMatrix™ Universal Authentication Server (UAS) enables organizations to deploy a wide variety of authentication methods to achieve strong authentication and benefit from evolving authentication mechanisms.

A future-proof versatile authentication infrastructure, UAS supports multiple authentication mechanisms for strong authentication requirements, enabling organizations to rapidly deploy those selected authentication methods that address their specific requirements.

Watch out for i-Sprint's next newsletter featuring research from Gartner, looking more in-depth into the increasing business need for strong authentication.

Source: i-Sprint Innovatlions

From the Gartner Files:

How to Get to Single Sign-On

Enterprises can reduce time to value and limit costs for SSO solutions by properly scoping an SSO initiative, and by using owned tools to minimize project scope.

Key Challenges

- The requirements for single sign-on (SSO) are derived from a buildup of target application systems, which, by default, require their own authentication capabilities.
- An initial plan to provide SSO often does not adequately account for factors that may reduce the perceived problem's scope, and more time and resources than are needed may have been applied to solve the problem.
- Adoption of software as a service (SaaS) applications has become the most common driver for new SSO solutions.
- Mobile resident applications are problematic for SSO strategies.

Recommendations

Follow these four steps as a best practice to derive the right solutions:

- Assess the current environment and pain points.
- Evaluate anticipated changes to in-scope applications.
- Assess currently owned services or solutions that can be leveraged to reduce the in-scope applications.
- Select solutions to resolve the remaining requirements.

Strategic Planning Assumptions

Through 2016, federated SSO will be the predominant SSO technology needed by 80% of enterprises.

Through 2015, ease and simplicity and the lack of proven alternatives will perpetuate the use of only power-on passwords with X.509 device credentials for BYOD remote-access authentication in 50% of enterprises.

Introduction

The quest for SSO is a symptom of a broader problem. It is a byproduct of a buildup of systems that each require stand-alone authentication and, potentially, stand-alone administration. It comes from the recognition that groups of target applications will require separate authentication steps for users based on these systems' back-end technology (that is, Windows, database, proprietary applications and so on). This leads to users' complaints regarding inconvenience — that is, having to log in multiple times, having to remember multiple passwords and so on. It leads to unsecure password practices, such as writing down passwords. It also drives up support costs for managing passwords and authentication failures.

There are several common causes for the heterogeneous environment:

- Legacy custom or purchased applications were not designed to use standard, common authentication services, and altering these applications to use one of these services is not feasible.
- Mergers and acquisitions may lead to the inheritance of more nonstandard applications.
- Adoption of SaaS applications with their own identity and access management services leads to new identity silos and new passwords.
- Mobile devices that can't use legacy client applications and their associated authentication methods and services, or devices that have custom applications to access Web/SaaS applications, can leave portions of the user population without application access — or, at a minimum, can require more passwords.

A well-executed SSO strategy reduces password-related support incidents and provides users with improved convenience and more efficient authentication processes.

A sound SSO strategy will give users fewer reasons to write down passwords. However, SSO systems highlight a "keys to the kingdom" problem — that is, one password provides access to all in-scope systems, and therefore

a compromise of the initial sign-on password can lead to compromised access to all in-scope systems. Organizations implementing SSO, particularly to systems that hold sensitive data, should implement risk-appropriate authentication methods with the SSO system.

Solutions are not "one size fits all." Solutions that provide SSO to all target systems may be deemed too expensive. Therefore, a best practice is to identify the tactical and strategic approaches that reduce enough of the problem space over time and within budget. The following steps and framework should be used to appropriately scope the target solution set:

- Assess the current environment and pain points.
- Evaluate anticipated changes to in-scope applications.
- Leverage currently owned services or solutions to reduce the in-scope applications.
- Select solutions to resolve the remaining requirements.

Analysis

Assess the Current Environment and Pain Points

The first step is to scope the problem space by identifying the user population and use cases that require a solution, and to inventory the target systems, their architectures and anticipated lifetimes:

- **User population**: Identify whether a solution set should cover employees, contractors, external business partners or consumers/ constituents.
- **Use cases and applications**: Identify the logical location of users and the target systems that must be accessed — for example, internal users accessing internally managed applications and SaaS applications, or external consumers and business partners accessing internally managed applications. Identify the applications and use cases that are currently used the most and generating the most calls to the help desk for authentication-related issues.
- **Applications and their architectures**: Determine the application architecture for each application deemed to be in scope for an SSO initiative:
  - Client component, such as a browser, "thick client" on Windows, mobile resident application or terminal emulator.
  - Application server that communicates with the client (for example, Web server, Web application server, mainframe and database server).
  - Ability to abstract authentication from the current siloed methods and use a common infrastructure. Can the application support Lightweight Directory Access Protocol (LDAP) authentication or Active Directory/Kerberos? Can a Web application accept credentials through HTTP headers from an authentication product? Can the application support standard federated authentication protocols, such as SAML?
  - Authentication methods supported natively and through partnerships. Does the application vendor support native authentication method integration for a risk-appropriate authentication method you already own or are planning to use — for example, smart cards with X.509 credentials or one-time password tokens? Enterprises should also revisit application assurance requirements. This will help ensure that risk-appropriate authentication methods will be included in any SSO approach.

Evaluate Anticipated Changes to In-Scope Applications

Will the applications used today still be in scope in one year, two years or three years? If an application will be retired, replaced or have its user base significantly reduced within one to two years, then you may be able to remove it from consideration and, therefore, reduce the problem space. Approach commercial application vendors and ask whether there are any plans to provide authentication options that can leverage the enterprise standards:

- **Prepare a matrix with the inventory results**: Figure 1 depicts an example of an application inventory matrix. Look for common architecture and use case patterns.

FIGURE 1 Example of a Current Application Inventory

Application Name	Application Server Architecture	Application Client User Interface Architecture	Identity Repository	Current and Other Supported Authentication Methods	User Population and Use Cases	Estimated Application Lifetime
Finance	WebSphere/ Java	Windows thick client	DB2	One-time password tokens	Employees on-premises and remote	Replace in two years
Employee intranet	IIS	Web browser on desktops and mobile devices	Active Directory	Current password options: LDAP and Active Directory	Employees and contractors on-premises and remote	Greater than five years
• • •						
CRM	SaaS	Web browser on desktops and mobile app.	SaaS vendor's repository	Password	Employees	Greater than three years

IIS = Internet Information Services
Source: Gartner (January 2013)

Leverage Currently Owned Services or Solutions to Reduce the In-Scope Applications

What tools do you currently own that could help reduce the problem space? We often find that clients possess an infrastructure, such as Active Directory, a password management/ synchronization tool or a Web access management (WAM) tool, and these tools are just not being fully leveraged. Their use may be isolated to one business unit or application set when they could be more broadly deployed.

Applications that can use Kerberos authentication can be integrated with Active Directory.

Sometimes reduced sign-on (RSO), enabled by an established password synchronization tool or authentication to a common LDAP-accessible directory, will provide good-enough reduction in the problem space (see Note 1). When applications can have passwords synchronized, or when applications can point to a common LDAP-based directory for authentication, then users have the same password for those applications, but they must enter the password each time they access the system.

When multiple directories are used for authentication, directory synchronization or virtual directories may be brought to bear to join disparate identity sources, and to expose one standardized view of identity to multiple applications or authentication services, such as a WAM tool. This can provide RSO or SSO, depending on the configuration.

Select Solutions to Resolve the Remaining Requirements

The following section identifies the commercial offerings brought to bear most often for the most common sets of requirements identified by Gartner clients. If these solutions do not meet your requirements or seem like overkill for your environment, then contact Gartner to discuss your organization's needs.

Application designs have been moving inexorably toward Web architectures. The number of clients calling Gartner to discuss SSO needs for legacy "thick client" applications has been dwindling. As soon as currently owned directories, Kerberos and password synchronization tools have been leveraged, it is likely that tool or service selection will be based on the need to support SSO to Web-architected applications. Furthermore, SaaS adoption has been driving the need for federated Web SSO. Therefore, the solutions that support these needs are presented first, with less prevalently needed solutions following.

Solution Recommendation: WAM

When and why should an organization consider this tool?

- An organization needs support for Web-architected applications running on multiple, disparate Web application server versions in internally or externally facing use cases.

- An organization may require federated SSO to applications in another security domain (such as an external SaaS application), or it may need to allow federated SSO to applications from another security domain (such as a business partner). Roughly one-half of WAM tools support federation inherently, or vendors will sell a companion federation product that can work with the vendors' WAM tools. Stand-alone federation products from other vendors can often be integrated with WAM tools that don't inherently support federation.

- The organization may require support for multiple authentication methods for different applications.

- It may require support for coarse-grained, externalized application authorization — making authorization decisions to access application subcomponents that can be referenced by a URL.

- It may require agents to integrate packaged applications with Web interfaces, such as SAP or SharePoint.

Description/architectural approach:

- Combination reverse proxy and application target agents.

- Policy administration and decision points in the core access component.

- Directories or databases used to hold authentication attributes ("credentials") and attributes for rendering authorization decisions.

- May include federation components.

- May be delivered on-premises as software, in an appliance or as a service.

Common related solutions:

- Secure Sockets Layer (SSL) VPN: Provides reverse proxy authentication support to applications that can accept authentication information passed through HTTP headers. It has poor authorization support and no support for packaged applications that can't use HTTP headers. Generally, it is not used for high-volume extranet SSO needs.

- Versatile authentication servers or services (VASs): Preferred when multiple integrated authentication methods are required (instead of, or as well as, password authentication) and authorization support is not needed. These VAS tools increasingly offer federated SSO for integration with Web and cloud applications. However, WAM tools generally also have an advantage when target-application-specific agents are required.

Solution Recommendation: Stand-Alone Identity Federation

When and why should an organization consider this tool?

- The company requires SSO to applications in another security domain, or to allow federated SSO to applications from another security domain. Examples:

    - Employees authenticate to Active Directory or a WAM tool that does not have federation capability and needs SSO to SaaS applications.

    - Enterprise business partners manage their own users' identities; users authenticate locally to the business partner's infrastructure and are provided with SSO to your applications.

    - External users authenticate to a social networking site, and the enterprise wants to accept an authentication to that site to access its applications. This may support only RSO. Social networking sites and some major SaaS providers support variants of the newer RESTful identity federation protocols: OpenID with some variant of the OAuth authorization specification used for token handling. When users access an enterprise's site and the enterprise has federated with a social network, such as Facebook, then the user's browser is redirected to Facebook to sign on there. Then the user's browser is redirected back to the enterprise's relying application.

- An organization doesn't require the authorization policy management and enforcement functions, or the authentication methods support provided by WAM tools.

Description/architectural approach:

- Integrates with directories and WAM tools, leveraging an established, authenticated session token created by the identity provider,

and translates the local token to a standard security assertion trusted by the relying service provider.

- Requires partners to support federation. This is becoming more common; however, federation support for less prevalent, and perhaps industry-specific, SaaS applications is less common.

- May be delivered as software on-premises or SaaS.

Common related solution:

- We are increasingly seeing vendors of other product types adding federation support. VPN, authentication and virtual directory products are adding federation support to extend the reach of their products. Application vendors, such as SAP, and SaaS vendors are increasingly adding federation support as well.

Solution Recommendation: Enterprise Single Sign-On (ESSO)

When and why should an organization consider this tool?

- The organization requires SSO to all its applications, regardless of application architecture (including Windows "thick clients," applications with terminal emulators for user interfaces and Web applications).

- Need is accentuated when shared workstation support is required to allow rapid user switching and SSO on the same computer. We see this need often in clinical healthcare environments.

- The organization may need to integrate multiple authentication methods for front-end authentication to the ESSO tool, and to reauthenticate when accessing some applications.

Description/architectural approach:

- Generally requires endpoint device software agents that access encrypted, cached user IDs and passwords; decrypt the passwords; and transmit these credentials through application user interfaces.

- Some products are two-tiered, with the agent accessing a directory where access policy, automation profiles, and usernames and passwords are stored. Other products have a middle tier for these functions that can also synchronize identity attributes from directories.

- Can be used for Web applications, with caution regarding use with SaaS applications, because the SaaS provider can change the sign-on interface to its application without the enterprise's knowledge. This can break the SSO automation for that application until an ESSO administrator can reprofile the application.

Common related solutions:

- A few ESSO vendors sell ESSO as part of a multifunction product that includes WAM and federation.

- There are market solutions that provide SSO only to Web applications using the same "password stuffing" technique as ESSO. These tools generally lack other features, such as shared workstation support, multiple authentication method support, and enterprise policy and reporting management.

Solution Recommendation: Active Directory/Unix Bridge

When and why should an organization consider this tool?

- The organization requires Unix, Linux and Mac OS X systems to use Active Directory/Kerberos for SSO, and these Unix systems run different operating system versions from different vendors.

- The organization needs Windows users to have SSO to Kerberos-enabled applications running on Unix systems.

- The organization may need administration of Unix accounts and privileges using Active Directory.

Description/architectural approach:

- The agent runs on Unix systems and is joined to Windows domains.

- The administration console runs as a Windows service or may require an additional server.

Common related solution:

- Native Kerberos libraries for each Unix system can be used with Active Directory/Kerberos for the authentication function only. This is generally more complex to manage as the number of servers and variants of the Unix operating systems increases. Care may be needed to align the Kerberos libraries with Microsoft's Kerberos implementation.

The Mobile Device Problem

The proliferation of mobile phones and tablets with a variety of operating systems has created the latest and greatest challenges to authentication and SSO. Web-architected applications can often be supported with existing access management tools, such as WAM and federation, because smartphones and tablets have Web browsers.

Native mobile resident applications can create a gap in SSO support, and market offerings to resolve the issues are immature, proprietary, or not comprehensive enough to support multiple device and operating system variants. See the following research:

- "Supporting Mobile Device Authentication and Single Sign-On to the Enterprise and Cloud"
- "Market Trends: The Impact of Mobile Computing on User Authentication"
- "Good Authentication Choices: Evaluating Phone-as-a-Token Authentication Methods"
- "Predicts 2013: Mobile, Social and Federation Drive Identity and Access Management"

Mobile device authentication and SSO will be covered in upcoming Gartner research.

Acronym Key and Glossary Terms	
ESSO	enterprise single sign-on
LDAP	Lightweight Directory Access Protocol
RSO	reduced sign-on
SaaS	software as a service
SSO	single sign-on
VAS	versatile authentication server or service
WAM	Web access management

Evidence

The findings and recommendations in this research were derived from thousands of Gartner client interactions since 2002 on the topic of SSO.

Note 1

Definitions of SSO and RSO

Single sign-on generically refers to users' ability to authenticate once and then be subsequently and automatically authenticated to other target applications. The scope of these target systems may be limited to a particular subset of an enterprise's applications based on application architecture, use case or some other discretionary factors.

Reduced sign-on refers to the ability to use the same authentication method for a set of target systems, but it requires the user to use that authentication method each time one of those systems requires authentication.

Source: Gartner Research, G00247863, Gregg Kreizman, 21 January 2013

About i-Sprint Innovations

A leading IT services provider in the Asia Pacific region, i-Sprint Innovations is the premier Identity, Credential and Access Management Solutions provider for global financial institutions and high security sensitive environments and one of the most recognized names in the financial world.

i-Sprint's security products, intellectual properties and patents exceed global financial services regulatory requirements. Organizations of all sizes benefit from i-Sprint in their administration, access control and single sign-on requirements, using an incremental, evolutionary and strategic Security Consolidation approach based on a common security infrastructure.

Established in 2000 and based in Singapore, i-Sprint has offices in Malaysia, China, Hong Kong, Taiwan, Thailand, Japan and USA and has active authorized implementation and SI partners in many countries.

Over 100 global banks, financial institutions, government agencies and large enterprises rely on their solutions to protect over USD 10 trillion of valuable assets and important information.

i-Sprint's solutions are also deployed to protect mobile devices and cloud based applications. Their dedicated R&D team has their focus on providing an integrated platform to provide authentication solutions for cloud computing, mobile devices and biometrics. Some of the successful deployments include strong authentication for Internet banking applications and single sign-on for e-Government applications.

i-Sprint Trust without Boundaries

i-Sprint's unique world leading security solutions include:

- Proven Secure E2E Encryption (E2EE) Authentication and Data Protection for convenient (Single Sign-On) and securing access to internet banking applications. Their solution meets Internet Banking Security Guidelines from regulatory agencies in multiple countries; overcoming the security challenges of most internet and mobile banking solutions.
- Bank grade versatile strong authentication (biometrics, multi-factor authentication and more) and token management platform to secure multiple application delivery environments (web, mobile and cloud) based on a common security platform.

Global Headquarters
Blk 750A Chai Chee Road
#01-01 Technopark@Chai Chee
Singapore 469001
Global: +65 6244 3900
enquiry@i-sprint.com

For a complete list of our offices:
Malaysia, China, Hong Kong, Taiwan, Thailand, Japan and United States, please visit
www.i-sprint.com

©2000-14 i-Sprint Innovations Pte Ltd. All rights reserved.
A Hierarchy Model is a patent of i-Sprint Innovations Pte Ltd. i-Sprint, i-Sprint logo, AccessMatrix, AccessMatrix logo are registered trademarks of i-Sprint Innovations Pte Ltd. All other trademarks and registered trademarks are property of their respective owners. i-Sprint reserves the right to make changes to the specifications or other product information at any time and without prior notice.

Simple, Strategic and One Login for Enterprise, Cloud and Mobile is published by i-Sprint. Editorial content supplied by i-Sprint is independent of Gartner analysis. All Gartner research is used with Gartner's permission, and was originally published as part of Gartner's syndicated research service available to all entitled Gartner clients. © 2013 Gartner, Inc. and/or its affiliates. All rights reserved. The use of Gartner research in this publication does not indicate Gartner's endorsement of i-Sprint's products and/or strategies. Reproduction or distribution of this publication in any form without Gartner's prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.