SailPoint

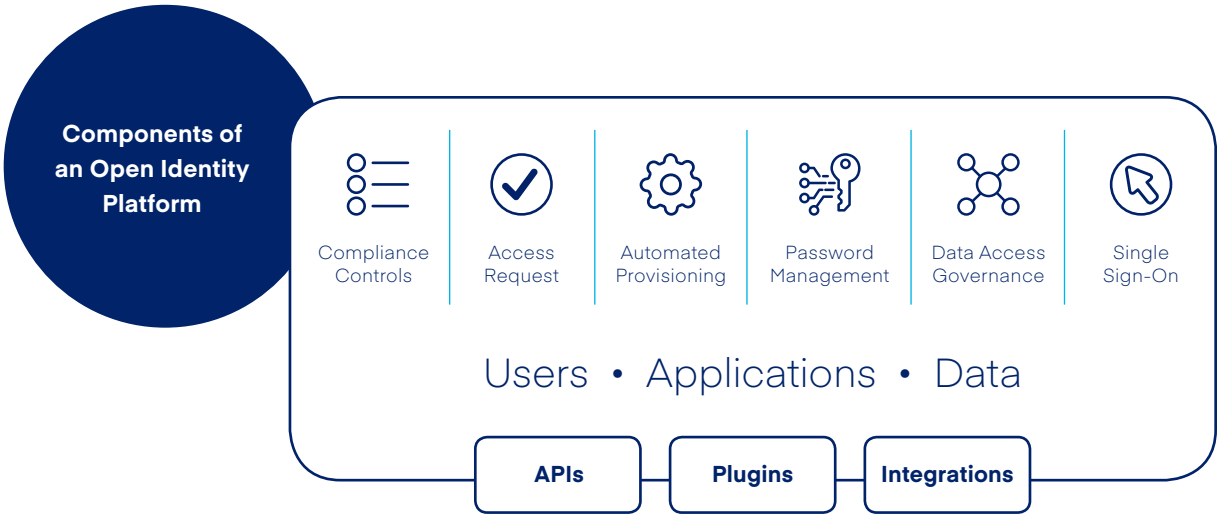
SOLUTION BRIEF

The Three Requirements of **an Open Identity Platform**

Today's enterprises are different. They're global forces with which to be reckoned, rapidly adopting (and creating) new technologies and enabling a new way of how we connect and collaborate with one another. But they have a weakness. All this advancement has created the reality that they will inevitably be the subject of a data breach. And more often than not, the attack vector is their most valuable asset: their people. Not just their employees, but also their suppliers, contractors – even their customers. And so they're finding themselves searching for a solution to help them secure that asset and their organization at large.

For these enterprises to be secure, they must put identity – the attack vector of choice by hackers – at the center of their security. By implementing an identity governance solution, they can better mitigate risk and answer the all-important question of "who has access to what," and then manage that access appropriately. But for this vision of a secure organization to be accomplished, identity must be pervasive. To be secure, organizations require an open identity platform.

But what is an open identity platform? In addition to everything that is entailed with provisioning, access certifications, lifecycle management, compliance control and automation of these processes in the basic foundations of an identity governance solution, an open identity platform must have three characteristics: it must be agile, unified and extensible.



Agility to Adapt to Any Situation

Enterprises, in their very nature are environments with a variety of applications and deployment models utilized to improve efficiency and serve business demands. The identity platform must be agile in that it connects to all portions of this infrastructure to create a consistent, enterprise-wide view of identity – and, in turn, enterprise-wide identity governance.

Structured & Unstructured Data

Organizations have long been aware of the need to govern sensitive data that exists in structured forms – mainframes, databases, business applications (e.g., SAP and Salesforce.com) and the like. However, they must now also wrangle with the fact that 80% of their enterprise data is unstructured: e-mails, presentations, documents and other such files that may be stored in a variety of locations. Every enterprise is different, and so the open identity platform must be agile enough to account for those different environments.

Mobile & the Cloud

The phenomenon of BYOD and cloud adoption is so pervasive that enterprises must be prepared for users to logon and work from their mobile devices as well as using applications from the cloud in conjunction with users within the network and uses on-premises systems. The open identity platform must be able to handle this hybrid environment – without breaking a sweat.

Unified with Every Aspect of the IT Environment

Without a unified foundation in the open identity platform, valuable time, effort and cost are all lost by administrating multiple solutions rather than enhancing the security stance of the organization. An open identity platform must understand several concepts:

Identity
This one may seem obvious, but it's important to specify how the open identity platform understands its core concept. Organizations must declare rules for how to identify what an identity is, as well as how that translates to the "real world." Without this knowledge and clarification, the context of who is doing what in the systems may be lost.

Resources
Once the concept of identity is established, then the platform needs to understand resources – any object that may be acted on by an identity, from data to applications and more. With the addition of resources to the open identity platform data sharing model, powerful policies may be put into place to establish compliance with regulation and thus enhance security.

Entitlements
With a shared understanding of identities and resources comes the potential for a coherent vision of what access should be permitted on a specific resource by a specific identity. This unique combination is the building block of enforcing identity governance policies.

Events
An event is the recording of a change that has taken place within the environment. Often, but not always, these are signified by an action taken on a resource by an identity (creation, delete, modification, access, etc.). The event may also include an assessment – whether or not the sending component believes the event to be a positive or negative occurrence.

While it's not a concept that an open identity platform must understand, a unified user experience is an important part of the platform. A consistent user experience across all devices – desktop, laptop or mobile device – for all users ultimately helps business users adopt the identity platform into their daily use, which is critical for the platform to succeed.

Build Upon the Base Functionality with Extensibility

An open identity platform is just that – a platform. This implies that not only does it provide a solution in and of itself, but it also allows for extension of that solution to address unique requirements of the environment in which it operates. This foundation broadens the reach of identity governance to all facets of the business – even to systems and applications that are proprietary, antiquated or brand new.

Formal Integrations
One aspect of this extensibility comes in the form of productized integrations with various other market-leading solutions in areas adjacent to the open identity platform.

These should be constructed in consultation with experts in their respective solution sets, and should seek to optimize the usage of the solutions based on previous real-world, production-based experiences.

Plugins

Much as many users have installed ad blockers and other modifications to internet browsers, the open identity platform also must be able to use community plugins. In this way, users at every level of the business, from the everyday to the administrative, can extend the identity solution to function how they need it. Not only do these plugins foster collaboration among the platform's users, they solidify best practices across the entire ecosystem and promote productivity.

APIs

A mature, open identity platform will provide an additional avenue for integration, as well. The needs of the organization are often best met using information disseminated from the open identity platform using a standards-based interface such as an API. This allows the organization to bring custom applications or other systems under the security purview, and further expand the security effectiveness of the existing solution.

Summary

Organizations seeking not just to survive the coming decade must avoid the "island-based" security mindset and instead embrace the idea that identity must be core of their security and operational infrastructures. Identity must inform and be informed by every action taken by the enterprise. Only a coherent, open identity platform-based approach can provide the required identity context – one that is agile, unified, and extensible so that the entire business is brought to understand identity governance and enhance the enterprise's overall security stance.

SB1091-1703