STACK ANALYSIS

RESEARCH BRIEF:

SSO vs. Directory Services from the Cloud

ONE OF THE MOST COMPELLING PARTS OF THE IT LANDSCAPE IN RECENT YEARS IS THE IDENTITY MANAGEMENT SECTOR. THERE MAY NOT BE ANYTHING MORE FOUNDATIONAL WITHIN AN ORGANIZATION THAN ITS CONTROL OVER ACCESS TO IT RESOURCES AND SYSTEMS.

Today, access and identity is accomplished by a cobbled-together combination of single sign-on (SSO) technologies and Microsoft's homogeneous Active Directory (AD). Of course, the landscape is very different today than in 1999 when AD was introduced. As a result, solutions based on these legacy technologies are highly dependent on Windows-based infrastructures.

> **A new generation of cloud directory services is emerging to solve the problem of mixed platform, multi-location architectures.**

With web application use exploding, a wave of vendors has tackled the problem of connecting Active Directory to web applications. Because Microsoft was slow to extend Active Directory to the cloud, a generation of web SSO players emerged. These solutions leveraged the core, on-prem directory (AD) and bridged user identities to web applications. This approach worked well, as did the AD-only approach, for a short period of time.

As the IT sector continued to evolve and innovate with microservices, heterogeneous platforms, new authentication approaches and protocols and updated security models, the idea of AD and SSO started to break down. An on-prem, single-vendor directory with a single protocol web authentication platform approach became too limiting.

A new generation of cloud directory services is emerging to solve the problem of mixed platform, multi-location architectures. These modern approaches to core authentication services are being driven by third-party vendors without ties to platforms (e.g. Windows), productivity platforms (G Suite and Office 365) or infrastructure services (e.g. AWS, Kubernetes). This neutral approach is imperative in a rapidly innovating environment, where new solutions are emerging from all corners of the globe and best of breed is changing constantly. IT, development and ops organizations must be enabled to leverage the best — and right — tools for their jobs in this new era.

With these significant shifts in the market and IT landscape, organizations have been wondering whether their focus should be on extending their current on-prem approach of Active Directory with web application single sign-on or shifting to a modern cloud directory service. This SSO-versus-cloud directory services question has significant long-term implications.

Does an organization evolve its legacy architecture because of the enormous amount of time and work already invested to integrate a solution into the existing IT environment, or does it make a break from the past to a modern, cross-platform solution? This decision is often epitomized by the direction IT organizations take when it comes to identity management.

THE STACK RANK

	Single Sign-on	Cloud Directory Services
REPLACES ACTIVE DIRECTORY	NO	YES
SYSTEM-LEVEL USER MANAGEMENT	NO	YES
CROSS-PLATFORM SYSTEM MANAGEMENT	NO	YES
MFA	YES	YES
WEB APPLICATION SSO	YES	PARTIAL
LEGACY APPLICATION SSO	PARTIAL	YES
WIFI / NETWORK INFRASTRUCTURE	NO	YES
FILE SERVER ACCESS	NO	YES
SSH KEY MANAGEMENT	NO	YES

The path of SSO starts with the understanding that Active Directory is a fixed variable in the discussion. An organization has made the decision that its directory solution should remain on-prem and continue to be built upon rather than replaced. In this approach, an SSO solution such as Okta, a market-leading web application SSO solution also often referred to as an IDaaS platform, is leveraged to extend AD identities outward to web applications. Because AD has been a core solution for many years, various segments have emerged to build upon this core, including single sign-on. Other segments include privileged identity management, identity bridges, and governance solutions. Even Microsoft has acknowledged this strategy of piecemeal parts with ADFS and Azure AD, the latter of which looks a great deal like a web application SSO platform (Okta competitor) rather than a core directory service, despite its name.

Web application SSO vendors are keenly aware of their precarious position in the market and are continuing to extend their visions. This may be nowhere more apparent than in trying to bring greater security to identities. For example, Okta's other capabilities include deep multi-factor authentication capabilities to help secure access to web applications. Adaptive MFA, as Okta refers to it, can help ensure that only an organization's users can access their web applications. Further, through its acquisition of StormPath, Okta has entered the developer space with an authentication solution for web applications. At its core, Okta is helping enterprise organizations connect to web applications, choosing to remain away from the fray of directory services and Active Directory.

Does an organization evolve its legacy architecture because of the enormous amount of time and work already invested to integrate a solution into the existing IT environment, or does it make a break from the past to a modern, cross-platform solution?

The other side is an approach to leverage a cloud directory service, such as the popular solution called Directory-as-a-Service® by JumpCloud. JumpCloud's focus is on being the cloud directory service for internal IT resources including laptops, desktops, servers, and applications. Through policy deployment, it has the ability to manage systems as well. User authentication to on-prem applications via LDAP and WiFi (RADIUS) is also a core part of JumpCloud's offering. A cloud directory services approach looks much like a cloud alternative to Active Directory rather than an extension, as web application SSO solutions are.

The core issue for IT organizations centers on whether to maintain an on-prem, legacy Active Directory architecture or shift to the cloud

While we have tried to make the discussion of SSO versus cloud directory services more cut and dry, of course, there are some nuances. The two spaces do overlap in some areas. For example, SSO providers are extending to on-prem applications via LDAP. Cloud directory services are including web applications within their authentication path for identities. Despite the overlap — which, by all accounts, seems minimal and hardly all that comparable — the core issue for IT organizations centers on whether to maintain an on-prem, legacy Active Directory architecture or shift to the cloud. Of course, like any other decision within IT, there are a tremendous number of trade-offs and issues. It is always best for IT organizations to understand deeply their existing infrastructure and their future goals to make the best trade-offs possible.

If you are tied to your on-prem Active Directory instance and are interested in extending to web applications, then an SSO solution can be ideal. If you are looking to shift to the cloud and bring your authentication needs under one SaaS platform, cloud directory services may be the right fit for you. Ultimately, if you know exactly what your needs are, there shouldn't be much confusion between these two cloud identity management spaces.

STACK
ANALYSIS

Stack Analysis is a leading analyst firm that is focused on the next generation of enterprise IT. With particular interest in DevOps, security, infrastructure tools, and next generation architectures, Stack Analysis has unique insight into how organizations can leverage their people, modern processes, and world class technology to drive their business forward through extensive research, surveys, and primary interviews. For more information, contact Stack Analysis at research@stackanalysis.io.