Case Project: Comparison of IAS Cloud Providers

Divya Aradhya

Saint Leo University

Author Note

Contact: divya.aradhya@saintleo.edu

October 30, 2017

Table of Contents

Abstract

This paper compares and contrasts three enterprise Identity and Access Management cloud providers and analyses their cloud services, security measures, and their vision for adapting to future needs in the challenging niche of cloud-based IAM. This paper is intended to aid the management of ABC University in weighing the advantages and shortcomings of each provider and facilitate the decision on choosing one of them as the Identity and Access Management solution for the organization.

Keywords: *Identity and Access Management, cloud services, IDaaS, Okta, Ping Identity, OneLogin, information security*

Defining IDaaS

Security researchers and consultants, Gartner, defines an enterprise-level Identity and Access Management (IAM) solution as one that has basic identity administration, automated self-service password reset, multi-factor authentication, role-based provisioning of access, single sign-on (SSO), and session management, and clean account termination and revocation features. Identity and Access Management as a Service (IDaaS) is a solution suite offered by cloud-based IAM solution providers who build the solution based on recognition of the challenges of handling critical identity data of clients from a remote cloud (Cser, A., & Maxim, M., 2015).

IDaaS industry leaders

The 2017 Gartner report that was released to the industry pitches Okta, Ping Identity, and OneLogin as the leading IDaaS providers for organizations ("Gartner Magic Quadrant for Access Management", 2017).

Organizational Mission

Chief Marketing Officer Ryan Carlson, declares that Okta's mission is to "improve the connections between people and tools to make companies more productive and secure" (Carlson, 2016).

Ping Identity claims their mission is to "simplify how enterprises provide secure and seamless digital experiences" ("Ping Identity: Our Company", 2017).

Al Sargent, Director at OneLogin is quoted as saying that their mission is to "enhance the security of the modern enterprise." (Sargent, 2016)

Given that ABC University's IAM requirements are to align and streamline identity creation and access provisioning between student, staff, and faculty, Okta's mission comes closest to defining what the University is expecting in an IDaaS.

Analysis of IAM Services Offered

The services offered by the IDaaS providers are compared over the following essential enterprise IAM features-

Identity Administration

Okta uses features of pre-integrated provisioning, a universal directory, orchestrated policies and APIs, and a simplified access governance, with reporting, to deliver identity lifecycle management. Okta incorporates a multitenant model to provide its services, and requires a couple of lightweight connection components to reside on the client's premises ("Lifecycle Management", 2017).

Ping Identity works on a multitenant IDaaS model as well. It uses an in-house developed PingDirectory for identity administration that promises a robust and adaptive solution to storing identity and profile data. It offers REST APIs and the XML-based LDAP for clients to connect with them programmatically ("Ping Identity Directory", 2017).

OneLogin provides IDaaS on a multitenant model, while also requiring lightweight on-premises components for connection. It offers identity governance, reporting, and identity management through a secure unified directory to digitalize an organization's hierarchy tree and synchronize in real time.

In terms of providing basic identity administration and governance, all three providers are well matched, with Okta having a slight edge in being able to incorporate policies into digital controls.

Automated Self-Service Password Reset and Multi-factor Authentication

Having an Identity and Access system that can automatically allow users to reset their passwords safely and securely is a boon, as it can drastically cut down help desk calls, support tickets, and save time and resources.

Okta offers a multi-factor authentication feature that is integrated into their automated password reset functionality. This allows device specific security policies to be adaptively invoked and executed when a user attempts to reset their password. They further offer protection against brute-force attacks, proxy detection, and dynamic IP blacklisting. ("Adaptive Multi-Factor Authentication", 2017).

Ping Identity uses MFA as well, independently, and in tandem, with their self-service password reset feature. They use a contextual MFA that is capable of drawing input from smart devices (watches and other wearables), along with smart phones ("Securing Your Enterprise Credentials", 2017).

OneLogin uses a regular straightforward OTP (one-time-password) implementation of MFA to secure their password reset as well as their authentication process.

While Ping Identity's contextual sensory-based MFA is powerful, it may not be as necessary a feature as Okta's adaptive MFA. Okta's ability to draw in device-specific policies for authentication makes it a winner in this module ("Multi-Factor Authentication Solutions", 2017).

Role-based Provisioning of Access and Single Sign On

Okta helps to automate the error-prone process of role-based provisioning by utilizing pre-integrated provisioning that is based on the organization's own custom policies on identity and role definition. It further integrates with various meta-directories and pre-built applications.

Ping Identity allows for the automation of provisioning and sign on processes. It further integrates various custom applications into a single sign-on model ("Ping Single Sign On", 2017).

OneLogin provides an automated onboarding, off boarding, and access provisioning experience. It enrolls the services of Microsoft Active Directory and dynamically synchronizes all changes ("Cloud Directory Services - Active Directory as a Service", 2017).

Again, all the three service providers offer robust and competitive features. However, Okta, yet again, with its intuitive provision for adapting to the client's niche policies, gains a slight, but important, lead. ("Security And Compliance", 2017).

Service Providers Measures to Protect Consumers

Okta claims that they understand the unique security risks and threats to cloud providers, and the importance of the confidential data entrusted to them. They further state that the factor of security seeps into all their processes – hiring, architecture, development, strategies, operations, and practices. All their web access pipes through ***https*** and each client has their own individual domain, directory, sub-domain session management, and cookies. All data access requests are revalidated in case of triggered alert – even if they are benign and are false positives. They partner with Amazon Web Services for their infrastructure needs. Okta's SSO meets and is compliant with the SAML (Security Assertion Markup Language) standards. Further, Okta take careful measures to address all of OWASP's web application threats (like XSS, SQL injections) and has controls in place. Third-part penetration teams are hired to audit and test Okta annually. All physical resources are periodically inspected for physical health, and all staff access is logged and monitored. New employees are hired after strict security clearances. ("Okta's Approach To Security", 2017).

Ping Identity, akin to Okta, take their security seriously. They have a responsible disclosure program that promises clients that they will be informed of any security breaches in time. Further Ping Identity boasts of being certified by, and affiliated with Information Systems Security Association (ISSA), Cloud Security Alliance (CSA) Registry, FBI InfraGard, and OWASP. They, however, want their association with these organization speak for their security rather than breaking down the measures they take internally to provide security to clients ("Security at Ping Identity", 2017).

OneLogin, like Ping Identity, has a responsible disclosure program to assure their clients. They also have a bug bounty program that invites security freelance researchers to find bugs in their system and be rewarded. They display an up-time map on their website to show that that clients can trust their services to be available "99.9970%" of the time ("Cloud Directory Services", 2017). However, the recent OneLogin breach is a huge black mark against their reputation and security practices.

By transparently and systematically spelling out their security policies and practices, Okta gives prospective, and current, clients a clear view of how important security is to Okta's management team. This helps build trust as well as give tangible evidence of their security measures for protecting their customers.

IDaaS Providers' Clarity and Current Implementation of IAM

Okta views Single Sign-On, Muti-Factor Authentication, Universal Directory Mobility Management, and Lifecycle Management as core features in their understanding of IDaaS services.

Ping Identity recognizes Single Sign-On, Multi-Factor Authentication, Access Security, Directory, and Data Governance as essential IDaaS components.

Single Sign-On, Unified Directory, User Provisioning, Adaptive Authentication, and Mobile Identity are on the lists of the IDaaS implementation of OneLogin.

All the features of the three providers overlap, and are in line with Gartner's expectations on an enterprise-level IDaaS provider. However, as seen in earlier sections, the granularity, depth, and width of implementation of these features varies across the three of them, and Okta was seen to have an edge over the other two.

Cloud Providers vision for Technological Evolution and Next Generation of Services

Okta's vision is to "enable any company to use any technology" (Okta – Vision, 2017), and in line with this vision Okta labs is experimenting with machine learning, adaptive authentications, and advancements in cloud technologies to deliver the next generation IDaaS solutions.

Ping Identity's vision is for an "identity centric future", and having effectively pitched this, they have raised $44 million in investments to build the Next-Gen IDaaS platform. They are looking at scaling identity management to massive numbers that can serve "billions of users, device, and services", according to a media statement released by their CEO, Andre Durand.

While OneLogin does not clearly spell out their vision for the future, earlier this year they acquired the contextual authentication provider ThisData (Sargent, A., 2016). By making significant investments in the space of IDaaS, OneLogin shows that they are focused on the future and in retaining their position on one of the leaders of this market space.

By attracting investor by-in, Ping Identity has proved, on record and in numbers, that their vision for the future of IDaaS is clear. However, by spelling out the organization vision and investing in-house labs, Okta proves that they mean serious business and are invested in innovation as well.

Known Dangers

Gartner, in their 2017 report, on IDaaS providers, lists the following cautions against each of the three providers.

Okta decision to go public and enter the IPO space resulted in significant expenditures and losses, and this caused them to drastically increase their prices in the last few months.

Ping Identity's focus remains mainly on large and very large enterprises, and they don't cater well to small and medium-sized organizations. Additionally, their event reporting is very basic and not as detailed and granular as an enterprise-level IDaaS should ideally offer.

OneLogin, having already suffered a security breach, has a tarnish on its reputation in providing secure services.

Conclusion

Gartner and Forrestor reports have rightly recognized Okta, Ping Identity, and One Login to be head over shoulders than the other players in the Identity and Access Management as a Service niche. While all three offer competitive and excellent solutions – in terms of functionality and security – in every scenario of comparison and contrast, Okta has consistently retained a lead. Okta's clarity of vison, of its mission in this space, its transparency of disclosing their own security practices, their understanding of the client's needs for adapting individual and unique company policies into digital translations, and finally delivering all innovations and technology advancements in simple clean interfaces and UIs, to hundreds of satisfied customers, make them an obvious choice for ABC University.

References

Adaptive Multi-Factor Authentication. (2017, September 05). Retrieved from https://www.okta.com/products/adaptive-multi-factor-authentication/

Carlson, R. (2016, July 15). Onward: Telling the Okta Story. Retrieved from https://www.okta.com/blog/2015/11/onward-telling-the-okta-story/

Cloud Directory Service - Active Directory as a Service - Cloud Active Directory. (2017). Retrieved from https://www.onelogin.com/product/directory

Cser, A., & Maxim, M. (2015, June 29). The Forrester Wave™: B2E Cloud IAM, Q2 2015. Retrieved from https://kloudrydermcaasicmforrester.s3.amazonaws.com/mcaas/Reprints/RES113063.pdf

Durand, A. (2013, July 16). Ping Identity Raises $44 Million for Next-Gen Identity Management. Retrieved from https://www.pingidentity.com/en/company/press-releases-folder/2013/ping-identity-raises-44-million-for-next-gen-identity-management.html

Gartner Magic Quadrant for Access Management, Worldwide. (2017, June). Retrieved from https://www.ca.com/gb/collateral/industry-analyst-report/gartner-magic-quadrant-for-access-management-worldwide.html

Lifecycle Management. (2017, September 07). Retrieved from https://www.okta.com/products/lifecycle-management/

Multi-Factor Authentication Solutions - Multi Factor Auth Vendor - MFA Security Provider. (2017). Retrieved from https://www.onelogin.com/product/multi-factor-authentication

Okta's Approach To Security. (2017). Retrieved from https://support.okta.com/help/Documentation/Knowledge_Article/28503326-Oktas-Approach-to-Security

Okta - Vision. (2017, June 28). Retrieved from https://www.okta.com/company/vision/

Ping Identity Directory. (2017). Retrieved from https://www.pingidentity.com/en/platform/directory.html

Ping Identity: Our Company. (2017). Retrieved from https://www.pingidentity.com/en/company/our-company.html

Ping Single Sign On. Retrieved from https://docs.pingidentity.com/bundle/p1_overview_aps/page/apsAdminOverview.html

Sargent, A. (2016, June 21). OneLogin Study: Employees Exposing Employers to Security Risks. Retrieved from https://www.onelogin.com/company/press/press-releases/onelogin-study-employees-exposing-employers-to-security-risks

Securing Your Enterprise Credentials. (2017). Retrieved from https://www.pingidentity.com/content/dam/ping-6-2-assets/Assets/white-papers/en/3139-securing-your-enterprise.pdf

Security at Ping Identity. (2017). Retrieved from https://www.pingidentity.com/en/company/security-at-ping-identity.html

Security And Compliance - OneLogin Blog. (2017, October 17). Retrieved from https://www.onelogin.com/blog/categories/security-and-compliance

User Provisioning Software - Access Provisioning System - Active Directory Provisioning Tool. (2017). Retrieved from https://www.onelogin.com/product/user-provisioning