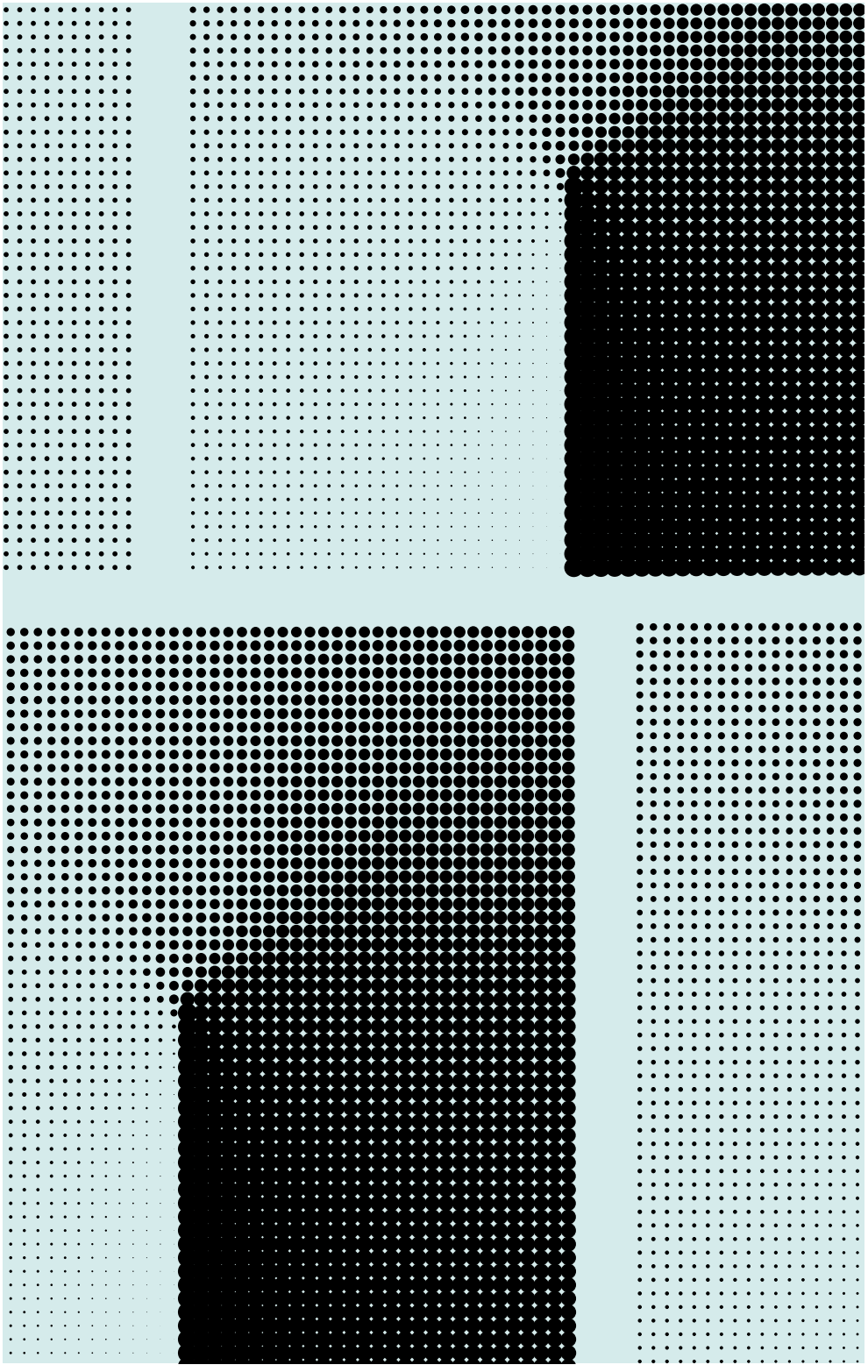
Whitepaper

November 2020

# Securing Cloud Access in Healthcare



Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871

okta

# Securing Cloud Access in Healthcare

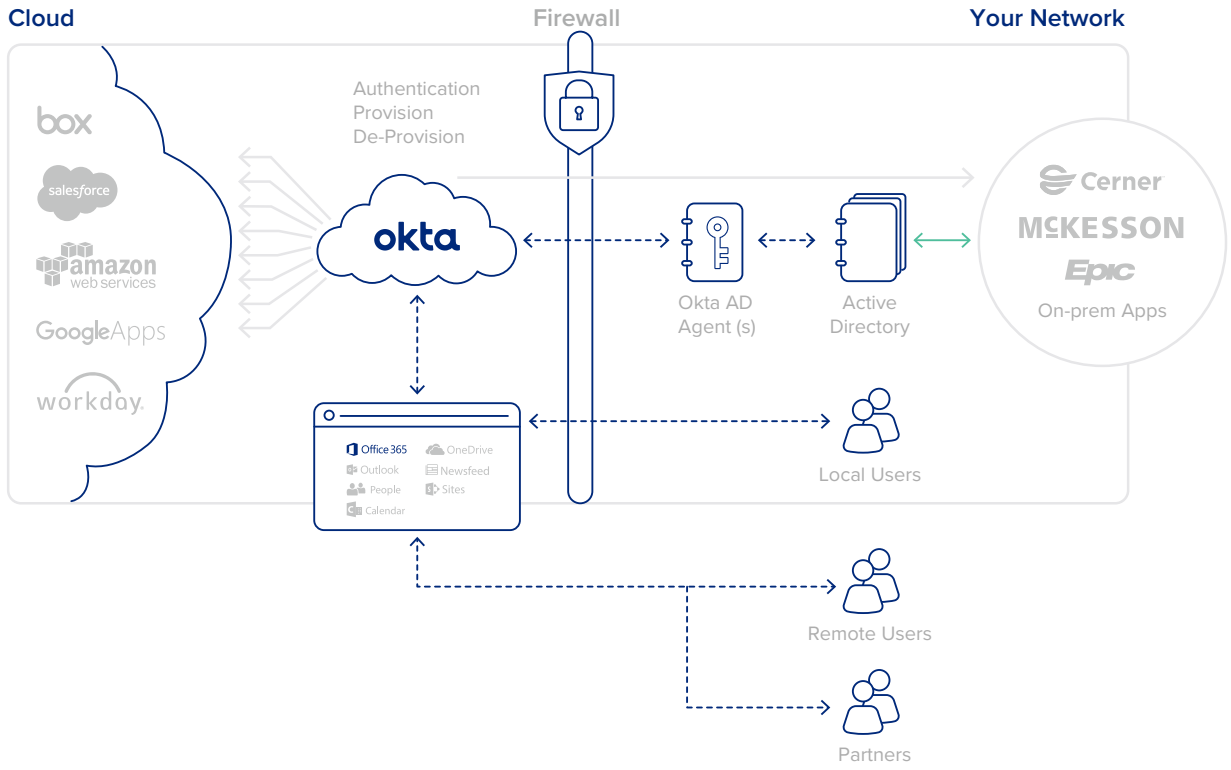
According to Gartner Research, by 2021, public cloud service providers will process over 35% of a healthcare provider's IT workloads1. A recent survey conducted by HiMSS Analytics indicates that this move to the cloud is well underway. Many healthcare organizations already use cloud apps; those that don't indicated short term plans to do so. Nearly 47% of organizations from this survey said they plan to use cloud apps for back office use in 2016, up from 22% in 2014. Over 37% plan to use cloud apps for HR and/or financial apps (up from ~17% in 2014), 41% for health information exchange (up from 20% in 2014), and over 46% for business continuity and disaster recovery (compared to 13% in 2014). As healthcare organizations increasingly adopt cloud apps, cloud identity and access management will provide a critical foundation benefiting both IT departments and their users.

With the proliferation of cloud apps in healthcare organizations, legacy identity and access management (IAM) solutions are becoming less desirable. On-prem products lack the visibility, speed and agility that today's IT environment demands. Setting up and maintaining a legacy IAM solution is time consuming and cumbersome. The average organization spends up to 50% more on deploying an on-prem IAM solution versus a cloud identity solution. And, the average on-prem deployment takes up to eight times longer. The additional time and expense doesn't end once a system is deployed either. Organizations tend to adopt new cloud apps as they grow. With legacy IAM solutions, this is challenging. Every time a new cloud app is added to an on-prem identity solution, a connector has to be built. This is time consuming and costs between $15,000 and $25,000 on average (with costs up to $100,000 per connector). With on-prem systems, apps themselves need to be updated regularly and app integrations also need ongoing maintenance. This means more expense to organizations and often results in taking the service offline for periods of time.

On-prem identity management solutions don't adequately support today's modern infrastructure. Cloud identity is an agile, scalable, and reliable alternative. It's fast and easy to deploy, with no ongoing maintenance for organizations. Cloud identity enables CIOs to have a complete, 360-degree view of all apps, users and devices in their environment. It also enables the creation of an app catalogue with pre-integrated applications. Each cloud identity solution maintains the apps in its catalogue (and the connectors) to make managing authentication simple for organizations. Cloud services never have to be taken offline for upgrades or maintenance. And, with a robust app catalogue, organizations can easily adopt new apps as needed.

[1] Gartner, Inc., Challenges on the Healthcare Provider Journey to the Cloud, Gregg Pessin, 9 Nov 2016.

Single sign-on is a central component of cloud identity. With SSO, clinicians, staff, employees, and partners can access Box, Salesforce, AWS, Google Apps, Workday, and any other browser-based app with just one username, one password and one session. Some single sign-on solutions also work in parallel with vendors like Imprivata and Caradigm, who provide SSO to essential thick client apps including EPIC, Cerner, and McKesson.



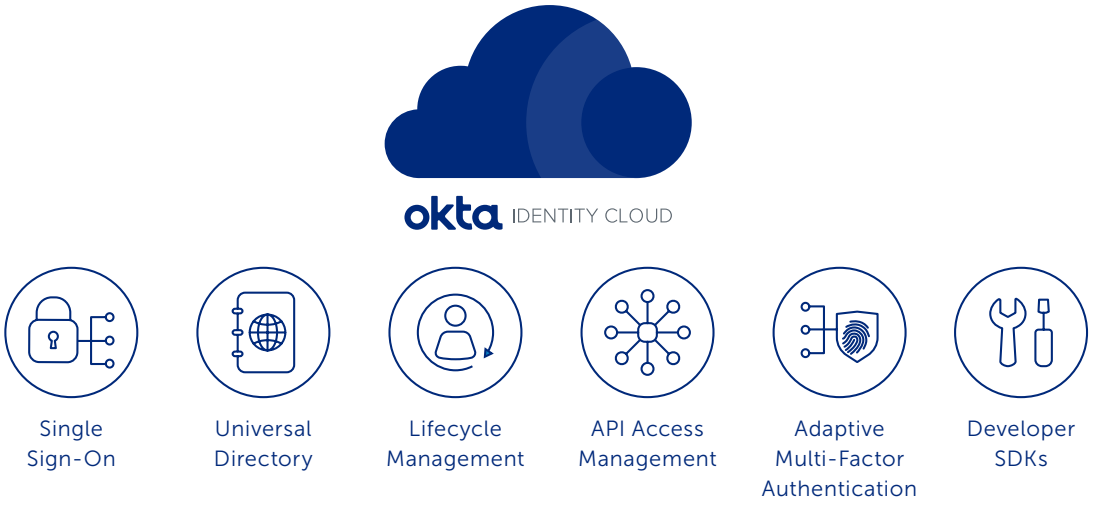

SSO has many benefits to end users and IT. It enables clinicians and staff to be more efficient because they don't waste time logging in to each individual application. SSO also secures environments. Without it, users often get password fatigue and use the same, easy to remember password for multiple apps. If one application is compromised, all applications are at risk of being compromised. Single sign-on also benefits IT departments by significantly reducing the number of password reset requests they receive. With Okta SSO, for example, the average organization sees a 50% reduction in helpdesk calls related to logging in.

SSO solutions can extend beyond staff and clinicians; this is critical as relationships between healthcare organizations and external physicians, insurance companies and suppliers become more intertwined. Federated single sign-on allows organization partners to sign in with their existing identity provider credentials, as opposed to using a new username and password. This greatly simplifies the login process.

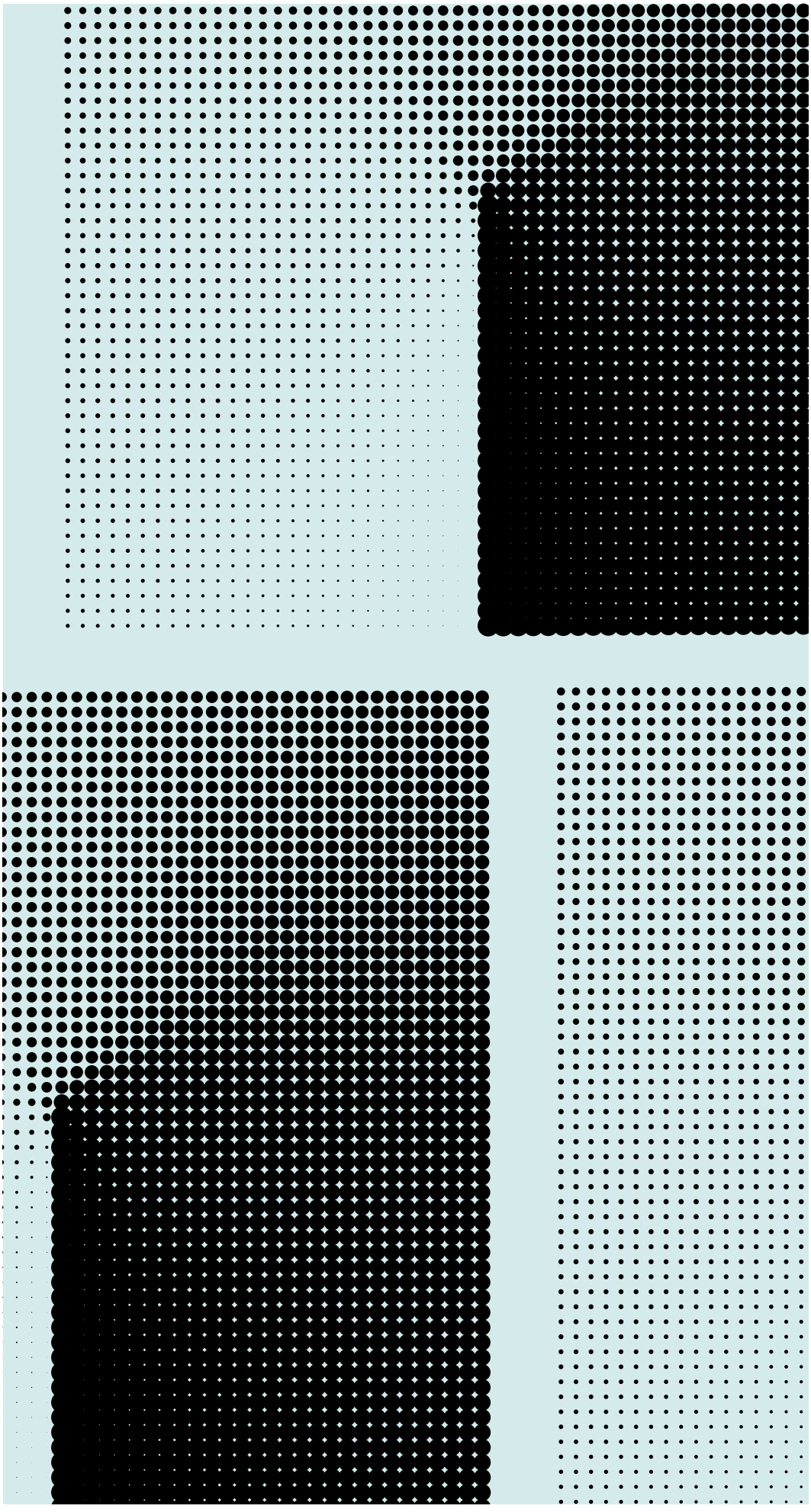
As healthcare organizations move to the cloud, they need to know their information (PHI, medical records, etc.) is safe. Multi-factor authentication (MFA) does just that by increasing the assurance of every identity connecting to your applications. MFA verifies that a person or device is who they claim to be by requiring an additional authenticator before they can access corporate information. MFA can connect to cloud applications as well as VPNs so organizations can grant clinicians and staff access to on-prem apps that don't natively support MFA.

While organizations want (and need) to protect their data, MFA can't be a burden to end users or it will inhibit their productivity and encourage the use of shadow IT. It's important to provide clinicians and staff with a comprehensive set of easy-to-use authentication factors that they can choose from. Organizations also don't want to unnecessarily prompt users for a second factor. When cloud identity and MFA are tied together, not only are apps and data more secure, but the user experience is also far superior. With cloud identity, MFA can be adaptive, meaning users are only prompted to enter a second factor when suspicious or atypical activity is detected. IT can also apply contextual access policies. IT may choose to prompt users for a second factor when they are accessing certain applications with highly sensitive patient information, for example.

If cloud apps are the future of healthcare, the future is here. Cloud identity is the foundation healthcare organizations need as they adopt more cloud apps. CIOs need a secure, scalable, reliable, and unified approach to successfully manage the cloud app explosion.




## The Industry's Most Reliable and Secure Platform, Period.



okta