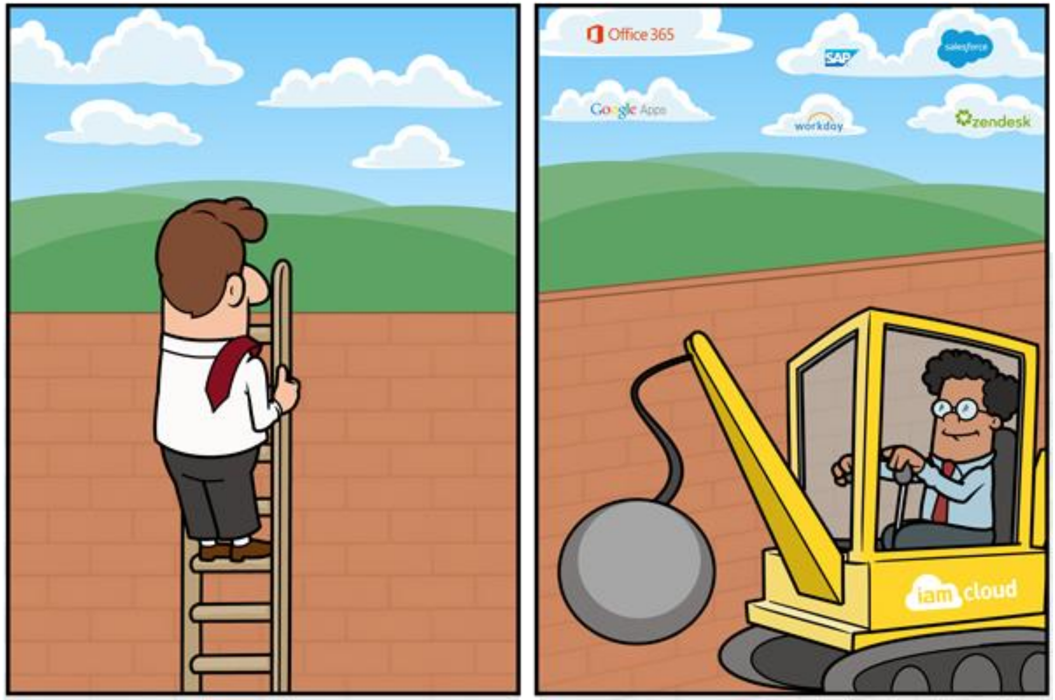
NO ONE EVER REGRETS KEEPING THINGS SIMPLE.

Simple Sign-On by IAM Cloud

CONTENTS

- SSO & The Cloud
- IAM Cloud: Simple Sign-On
- IAM Cloud: What's in the box?
- How IAM Cloud works
    - Identity management
    - Enterprise single sign-on
    - Off-site access
    - Self-service password reset
    - Multi-factor authentication
- Security & data protection
- Technical support & services
- FAQs
- How we compare
- Our customers
- Pricing



IAM Cloud, breaking down the barriers to the cloud

SSO & THE CLOUD: THE BACKSTORY

Single sign-on (SSO) has been around a long time, but for most its history it's just been considered a nice-to-have convenience.

That was until the meteoric rise of the cloud rocked the IT world. Now, SSO is one of the most critical technologies in IT - but why?

The thing you have to understand about the cloud is that it's all over the place – it's diverse and disparate. Different services, in different locations, with different login mechanisms and different security features, being used by different people, in different teams, who in turn – as we move into a more remote & flexible working culture – may be located in different parts of the world, using different login credentials, on different devices.

That's a lot of variables. It was difficult enough to efficiently and securely manage IT when it was all relatively uniform, physically clustered together, and used by people all in the same location. Now what?

The answer is SSO. Single sign-on systems route all of those disparate cloud applications, all of those security requirements, and all of those users (wherever they are), through a single centralized system. A system that you can control, and create rules and policies that governs: **"Who can access what, where and how."**

Single sign-on is really convenient for users, but in truth that's just a nice side-effect. The real benefit is in the control and security it can bring to organizations, like yours.

IAM CLOUD: SIMPLE SIGN-ON

Born in 2012, IAM Cloud was one of the first fully-cloud single sign-on providers in the world - in fact to this day IAM Cloud remains (to our knowledge) the only cloud-based identity federation solution that doesn't require any additional infrastructure at all on-premises to enable true desktop-based SSO.

Okta, OneLogin and other Identity-as-a-Service providers all require an IIS server to enable SSO. IAM Cloud does not.

After the initial explosion of demand for SSO, VC-funded Okta and OneLogin as well as IT-behemoth Microsoft all took the same strategy to SSO. They fought in an arms-race to out-do each other. More features here, more features there.

We just sat back and watched it all kick-off – including this moment in 2016 where Microsoft infamously disinvited Okta from a conference (news story).

Meanwhile, at IAM Cloud we realized that all our competitors were all doing the same thing. Stuffing their technology with features in order to command a premium price tag. But if a career in tech teaches you anything, it's that "less is more". Simplicity is a virtue, and we sensed an opportunity to provide a simple SSO solution that is uncompromising on security, reliability and performance – but that delivers critical SSO & MFA functionality for a much lower price than our competitors.

After all, SSO is SSO, MFA is MFA, password reset is… you get it. It doesn't really matter which brand's logo is on the box.

IAM CLOUD SSO: WHAT’S IN THE BOX?

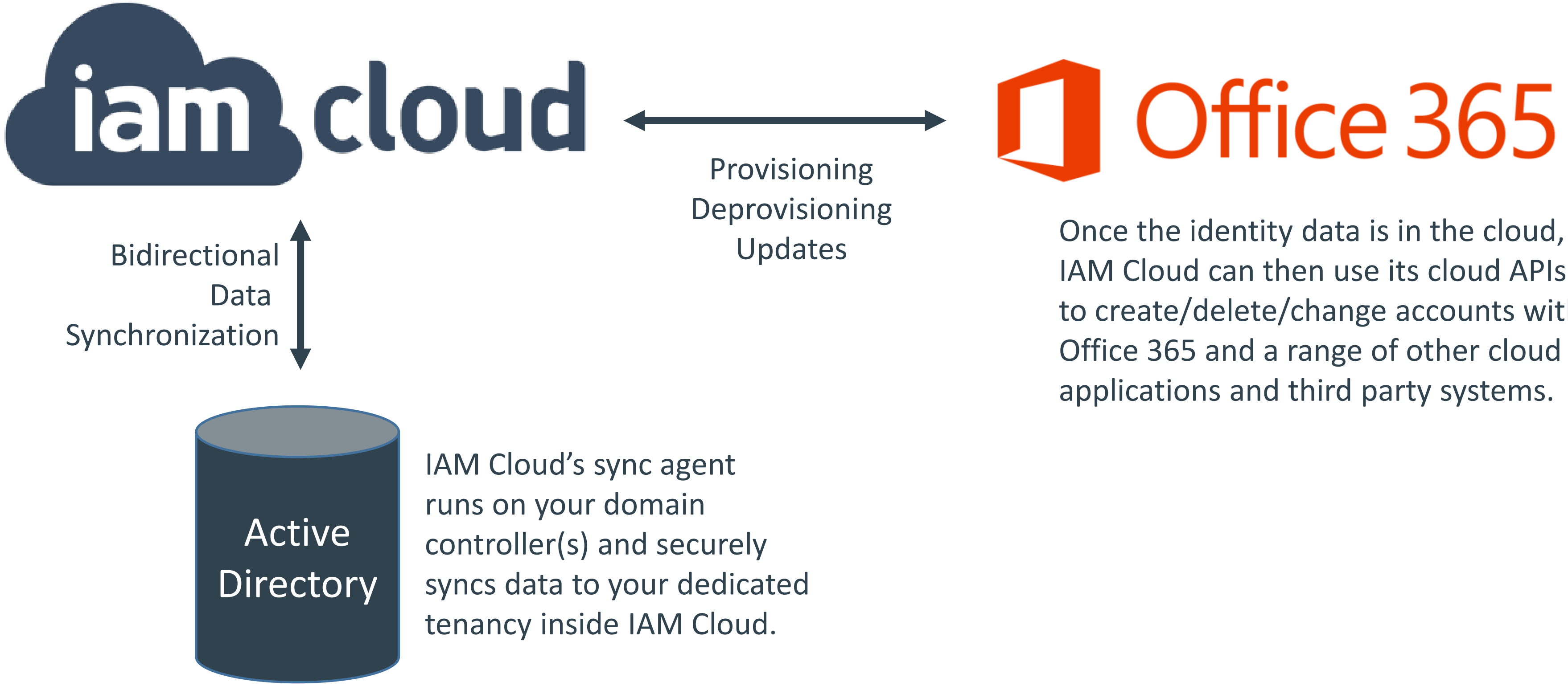
Single Sign-On (SSO)
SSO federates and centralizes user identities. It means that a single user credential can be used to access a wide range of SAML, WS-FED or LDAP applications securely. It means users can just log-in to their workstation and freely access all their applications without the need for further logins or passwords. It means fewer forgotten passwords. But most importantly, it means that you consolidate access to a single point of entry. A single point that you can control & secure.

Self-Service Password Reset (SSPR)
Passwords are still a core part of IT security, and when used properly and in conjunction with SSO & MFA, they can be very effective. But they can also pose some issues, particularly when forgotten. Our SSPR technology allows users to securely reset their own password if they forget it. This can reduce a significant burden from your IT support team, and at the same time provide greater convenience to users – especially out of business hours.

Multi-Factor Authentication (MFA)
MFA is one of the most impactful forms of IT security because it protects against the weakest link: the user. By centralizing the point of access and enforcing an additional factor of security for access outside of your Domain, you can add significant protections to your organization against credential phishing and other methods of identity theft and impersonation. MFA is simple (which is why we like it) but extremely effective.

Identity Management (IDM)
When we first created IAM Cloud, we focused strongly on its identity management capabilities. But we found relatively few customers needed advanced identity processes, and were happy with simple Dirsync-like cloud provisioning instead. Since then, we’ve simplified the IDM technology within IAM Cloud SSO to make it easier to deploy and manage as a customer. We’ve got other plans for the more advanced identity technology (watch this space).

HOW IAM CLOUD WORKS - 1. DATA SYNC



Provisioning
Deprovisioning
Updates

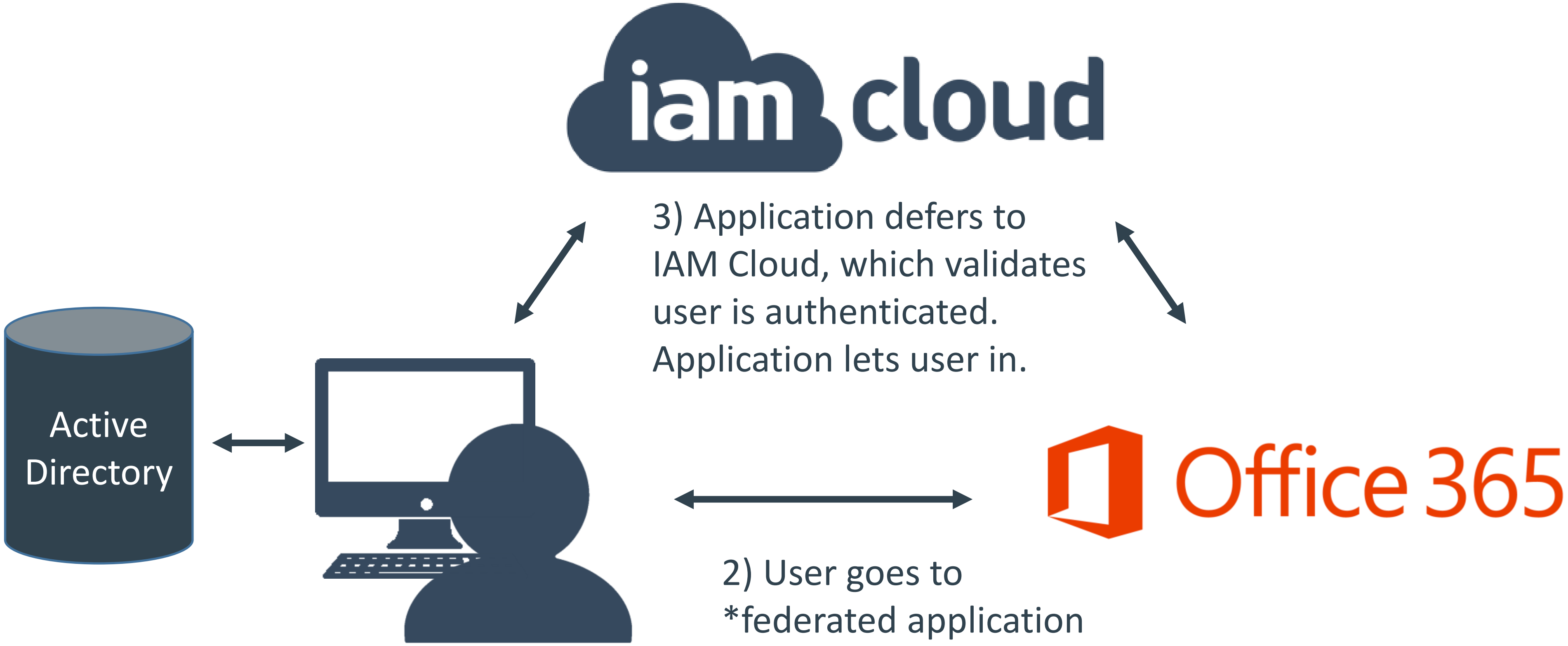
Once the identity data is in the cloud, IAM Cloud can then use its cloud APIs to create/delete/change accounts within Office 365 and a range of other cloud applications and third party systems.

Bidirectional
Data
Synchronization

Active
Directory

IAM Cloud’s sync agent runs on your domain controller(s) and securely syncs data to your dedicated tenancy inside IAM Cloud.

HOW IAM CLOUD WORKS - 2. ENTERPRISE SSO



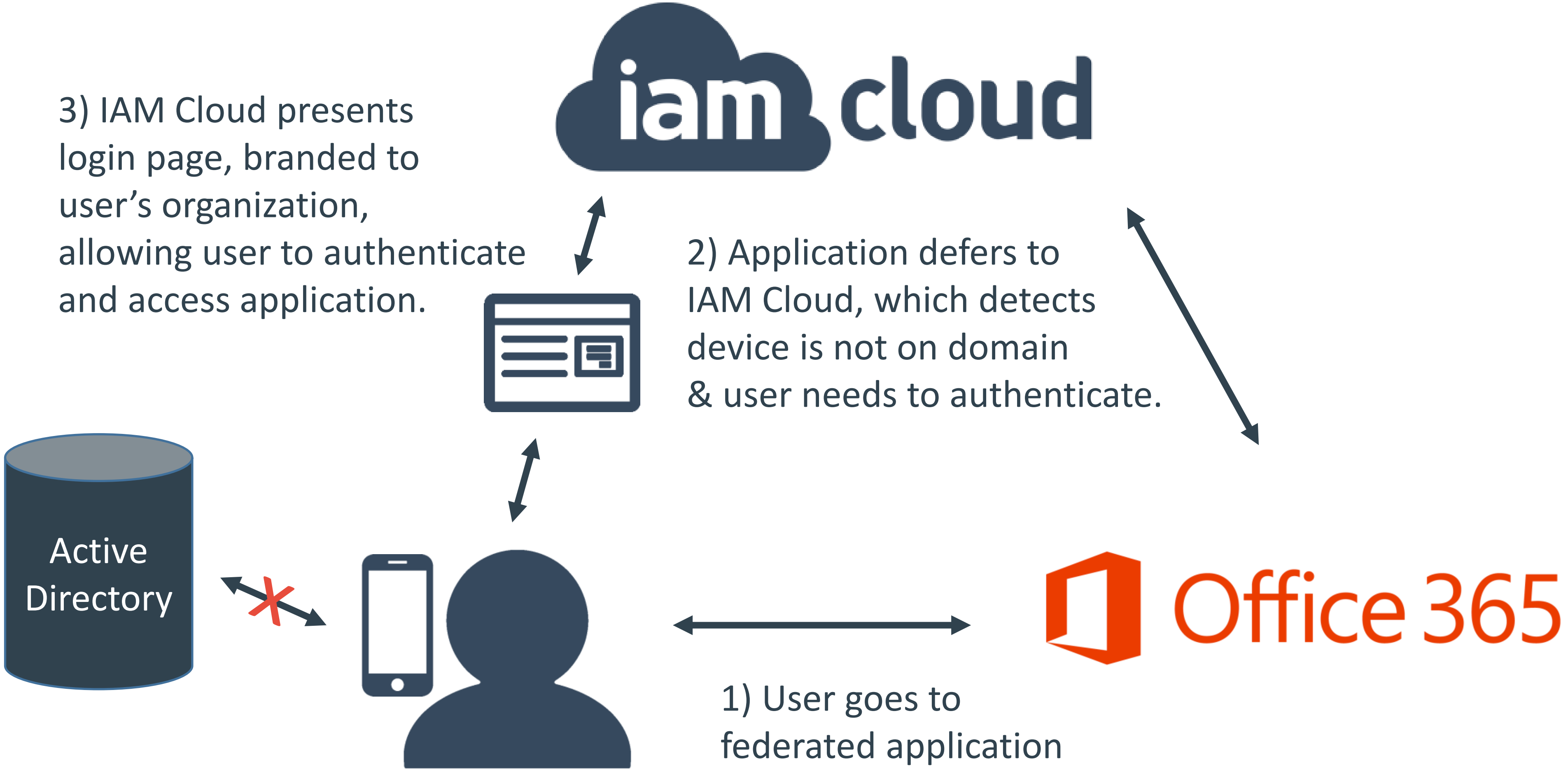
3) Application defers to IAM Cloud, which validates user is authenticated. Application lets user in.

2) User goes to *federated application e.g. Office 365

1) User logs into domain-joined PC.

* IAM Cloud SSO supports SAML, WS-FED & LDAP

HOW IAM CLOUD WORKS - 3. OFF-SITE ACCESS

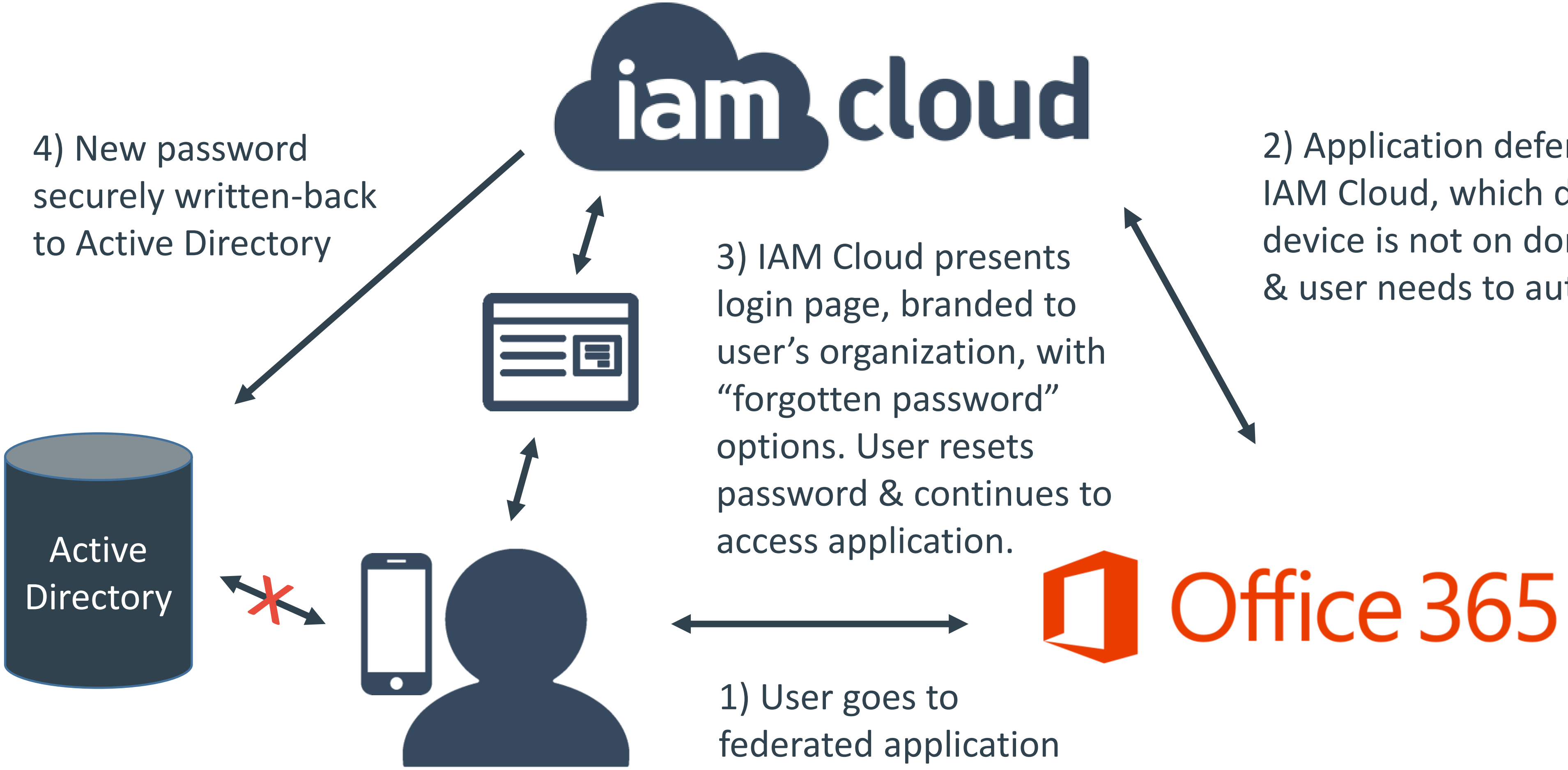


1) User goes to federated application on non-domain-joined PC or device

2) Application defers to IAM Cloud, which detects device is not on domain & user needs to authenticate.

3) IAM Cloud presents login page, branded to user’s organization, allowing user to authenticate and access application.

HOW IAM CLOUD WORKS - 4. SELF-SERVICE PASSWORD RESET



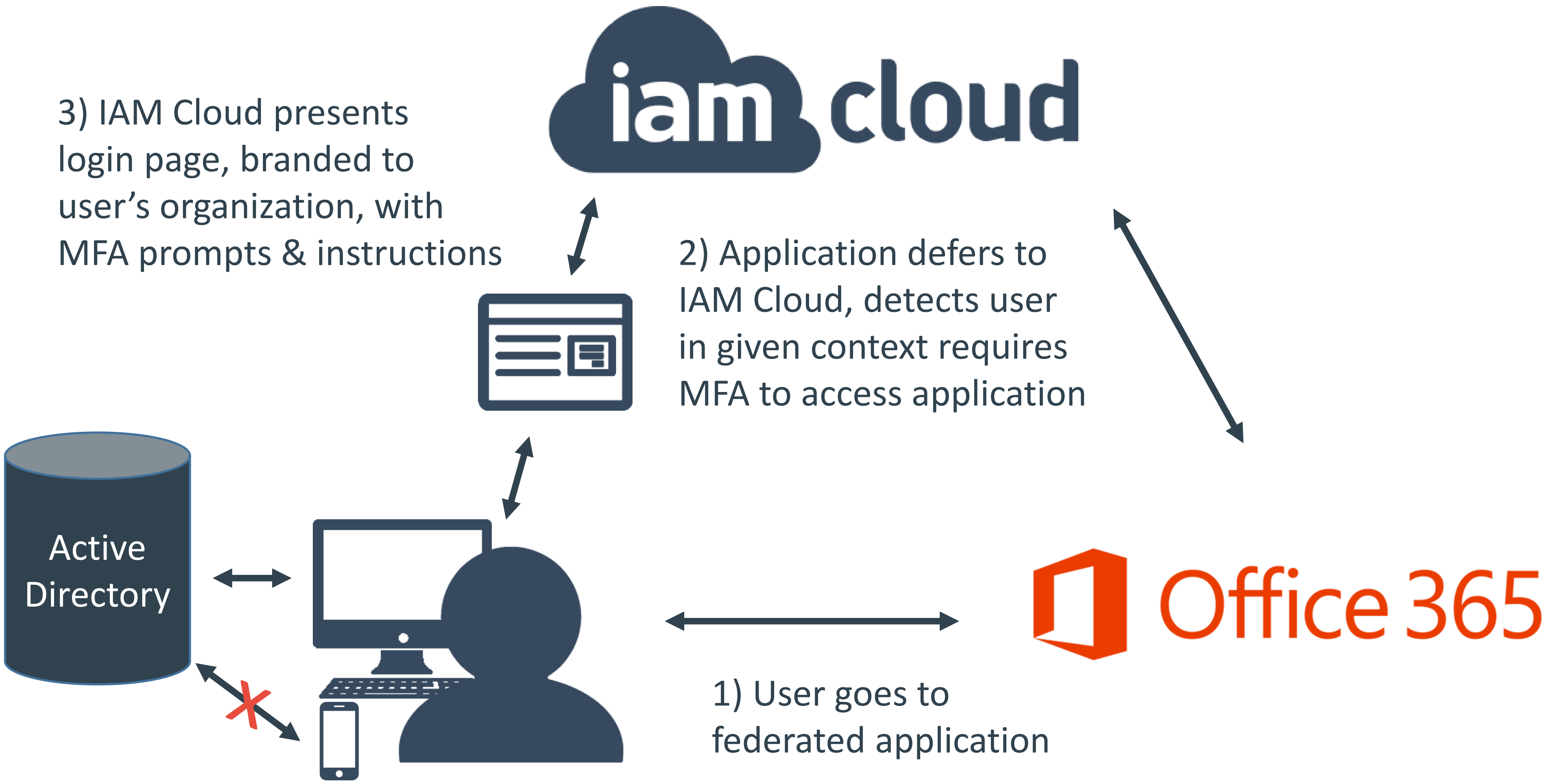
1) User goes to federated application on non-domain-joined PC or device

2) Application defers to IAM Cloud, which detects device is not on domain & user needs to authenticate.

3) IAM Cloud presents login page, branded to user’s organization, with “forgotten password” options. User resets password & continues to access application.

4) New password securely written-back to Active Directory

HOW IAM CLOUD WORKS - 5. MULTI-FACTOR AUTHENTICATION



3) IAM Cloud presents login page, branded to user's organization, with MFA prompts & instructions

2) Application defers to IAM Cloud, detects user in given context requires MFA to access application

1) User goes to federated application

END-TO-END SECURITY

IAM Cloud is a powerful IT tool to help save time, improve user experience, and significantly increase your organization's IT security.

- Identity federation and centralization effectively creates a single turnstile for your users to access all their business applications. This allows you to add security to all your federated applications – even the ones that don't have their own security features.
- Automated provisioning saves time and money. Automated deprovisioning does too, but it also substantially improves security by automatically removing access to users who've left the organization.
- IAM Cloud encrypts all data in transit (256bit HTTPS over TLS 1.2) and at rest in encrypted data storage, and only keep data physically located in data-centers appropriate to each customer's regional data residency laws. So all our EU-based customers have data stored exclusively in data centers physically located with in the European Union, all our North American customers are served by data centers in the USA.
- IAM Technology Group Ltd are ISO 27001 certified. ISO27001 is the global information security standard.

MORE THAN TECHNOLOGY

IAM Cloud is fully supported. For no extra charge, all our customers receive a 24*7*365 service, which includes:

- Full on-boarding support, including help with integration, configuration & federation.
- Access to our customer knowledgebase
- Access to our ticketing system
- Full extended business hours support
- Availability and support SLAs, including 99.9% service up-time
- Support by telephone, email, web tickets and web conference
- Quarterly service reviews
- Prioritized critical support for urgent issues

IAM CLOUD FAQ

What applications are supported by Simple Sign-On?

Simple Sign-On can federate and support any on-prem or cloud-based applications that support SAML, WS-FED or LDAP.

Is IAM Cloud GDPR compliant?

Yes, of course. We are also ISO27001 certified (the international equivalent to SOC 2 in the USA). We take data security and privacy seriously and undertake frequent security tests and audits to ensure our continued performance and compliance.

Do you have support SLAs?

Yes. Critical issues have a 1-hour response SLA. High = 4 hours. Medium = 8 hours. Low = 24 hours.

What support can we expect?

IAM Cloud SSO is a fully supported platform. Our team will help with the onboarding project, installation of our sync client, we'll collaborate with you on setting up the right configurations to meet your needs, we'll quickly build the connectors to new applications you want to provide SSO for, and provide ongoing support, guidance and troubleshooting. We provide full hands-on business hours support 7am-10pm (+0 UTC), and 24/7/365 critical support.

How quick is the onboarding process?

It depends. Typically from placing an order, we'll be able to start the process within 1-2 days, and complete it within a week. But for larger and more complex projects it may take longer.

IAM CLOUD SSO – HOW WE COMPARE

Where does Simple Sign-On fit into the SSO market?

Simple Sign-On is an intentionally lean SSO solution, that focuses on resilience, security and affordability.

Compared to Azure AD Premium, Okta, OneLogin (see next page for full breakdown)

Simple Sign-On has the same core features of all these services but does not have a user dashboard – we prefer to remain invisible and allow the users to choose whichever method they want to get to their applications – e.g. from a link on their Desktop.

Where IAM Cloud SSO wins versus these options is on price.

Simple Sign-On is $15 per user per year.
The Comparable Okta plan is: $132 per user per year
The Comparable OneLogin plan is: $120 per user per year, without Desktop sign-in, $192 with
The Comparable Azure AD plan (AAD Premium1) is: $72 per user per year

IAM CLOUD SSO – HOW WE COMPARE

Feature	IAM Cloud SSO	Comparable Okta, OneLogin, AAD Premium plans
Identity synchronization from AD and provisioning to other systems (e.g. Office 365)	Yes, included.	Yes, included.
Enterprise ("desktop") single sign-on	Yes, included. Full desktop-level SSO with no need for any extra infrastructure.	Yes, included. Primarily through a dashboard, but desktop possible but with added servers (Okta, OneLogin).
Self-service password reset & writeback, and password policies	Yes, included.	Yes, included.
Security & access policies, including user blocking, IP whitelisting, and other context-based access.	Yes, included.	Yes, included.
Multi-factor authentication (MFA)	Yes, included	Yes, included.
LDAP	Yes, included	Only as an extra add-on/upgrade
Application dashboard	No, not included.	Yes, included (Okta + OneLogin). Azure AD's dashboard is Office 365.
Customer support	Yes, full support included.	Basic support included, full support is a premium upgrade.
Typical price per user (volume & nonprofit discounts may apply). See our full pricing here	$15 per user per year	$72+ per user per year

IAM CLOUD SSO – HOW WE COMPARE

Compared to Azure AD Free / ADFS

Simple Sign-On is $15 per user per year. AAD Free is free. So what’s the difference between these two options?

If you need SAML federation (supported by ADFS) the AAD Free option is not free. Because you need to pay for several additional servers to run ADFS. With ADFS you also have maintenance, energy & housing costs, and most of all – you introduce a single point of failure. If your ADFS or AD servers become inaccessible for any reason (loss of internet connection, power failure, system crash) – no one can authenticate to Office 365 (or any other applications ADFS federates). This is a significant business risk. You also have no support, so if this happens it’s down to you or your local IT provider to try to figure this out as quickly as possible and restore access.

Simple Sign-On has been designed for resilience. We have only experienced 1 outage in the past 2 years, and it was due to an Azure data center outage. However, we run our service in multiple parallel Azure data centers, which meant that within 25 minutes of the Azure data center failing, we had switched our services over to a backup data center and were back online. Companies relying on Azure AD are locked to that data center, and they had outages for over 12 hours.

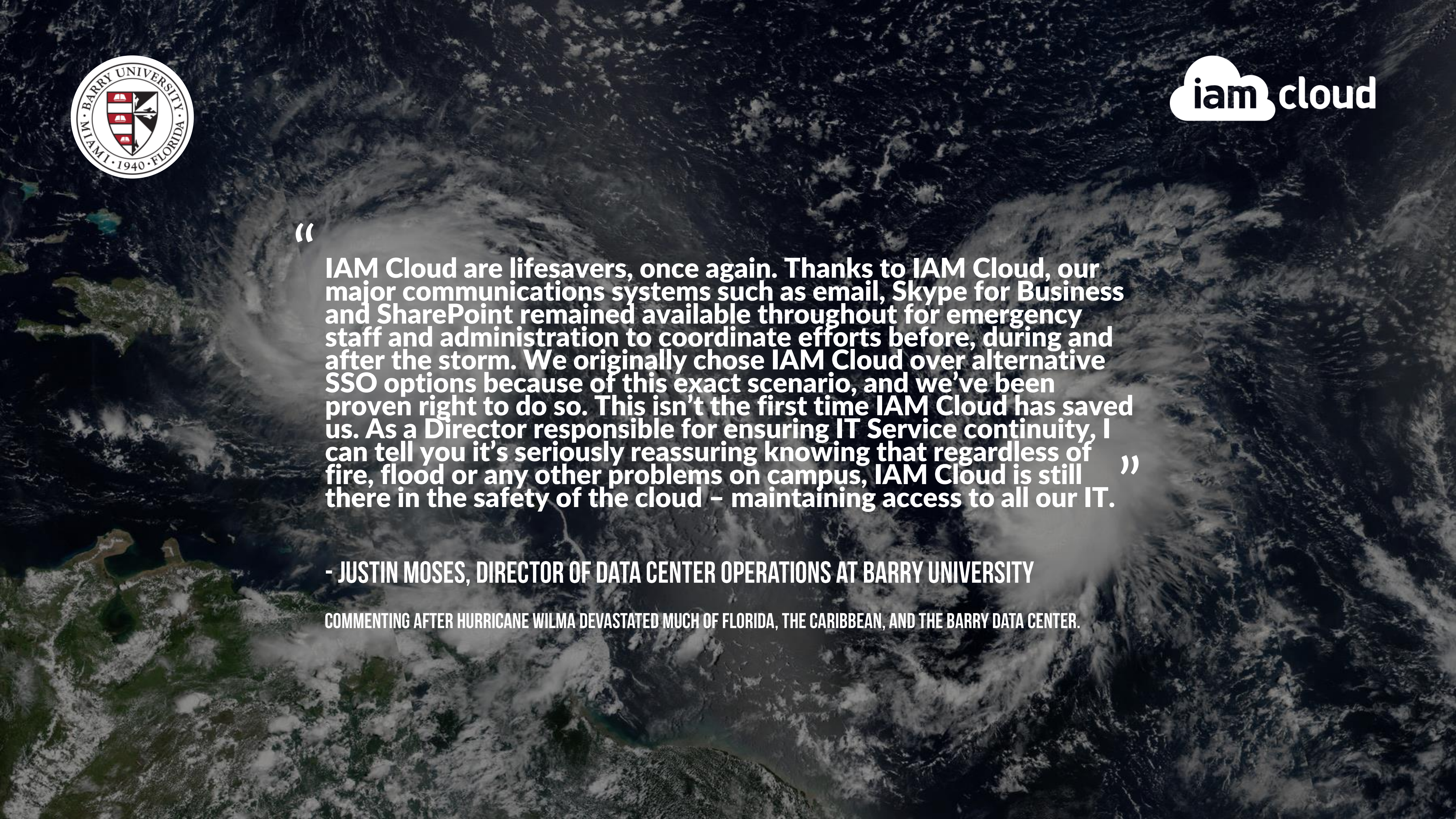
If you do not need federation, and are happy to run AAD Free without federation then you do not have the extra costs of servers to maintain and you remove 1 point of failure – although you are still locked to 1 data center, with the risk of prolonged outages if the data center fails. You also do not get a number of “core features” as part of the package, such as self-service password reset, conditional Multi-Factor Authentication, support for LDAP applications, and AAD SSO is limited to Windows 10 devices only. And again, AAD Free has no support, so if you have any issues you are unfortunately on your own.

IAM CLOUD
TRUSTED BY ORGANIZATIONS OF ALL SIZES AND SECTORS

>1 MILLION USERS

>1000 ORGANIZATIONS

GEELY
COMMONWEALTH ENGINEERS, INC. Celebrating 40 Years of Service Excellence
BACARDI
BAUSCH+LOMB See better. Live better.
United Learning The best in everyone
IMPAQ
The Royal Society of Medicine
coop
University of Bedfordshire
Save the Children
H&SA HEALTH AND SAFETY AUTHORITY
ANA AMERICAN NURSES ASSOCIATION
ROYAL VETERINARY COLLEGE
STARWOOD RETAIL PARTNERS
75 YEARS A Transformative Experience Barry University
MIAMI-DADE COUNTY
HRG Healthcare Resource Group
NHS
UNITED NATIONS UNIVERSITY
MAERSK
UMASS LOWELL
Berkshire Health Systems
SAFRAM
McWANE
SIERRA NEVADA
Mosaic
VISITING NURSE SERVICE OF NEW YORK VNSNY
müller
The Highland Council Comhairle na Gàidhealtachd SERVING The Highland Community
American Red Cross
engie
Virgin
StanleyBlack&Decker
PINE REST Foundation
WesBanco
GUILD HALL SCHOOL
Snohomish County Washington
The Growth Company
AUTOGLASS
alfa accountants en adviseurs



> “IAM Cloud are lifesavers, once again. Thanks to IAM Cloud, our major communications systems such as email, Skype for Business and SharePoint remained available throughout for emergency staff and administration to coordinate efforts before, during and after the storm. We originally chose IAM Cloud over alternative SSO options because of this exact scenario, and we’ve been proven right to do so. This isn’t the first time IAM Cloud has saved us. As a Director responsible for ensuring IT Service continuity, I can tell you it’s seriously reassuring knowing that regardless of fire, flood or any other problems on campus, IAM Cloud is still there in the safety of the cloud – maintaining access to all our IT.”

- JUSTIN MOSES, DIRECTOR OF DATA CENTER OPERATIONS AT BARRY UNIVERSITY

COMMENTING AFTER HURRICANE WILMA DEVASTATED MUCH OF FLORIDA, THE CARIBBEAN, AND THE BARRY DATA CENTER.

HOW MUCH DOES IT COST?

www.iamcloud.com/pricing

iam cloud

www.iamcloud.com/sso