The SSO/Rest
Transformation Process

Data Center

Application
SSO integration requests
to SSO/Rest (optional)

External Firewall

Application
in the
Cloud

IDF Connect
SSO/Rest
Plugin

IDF Connect
SSO/Rest
Gateway

SSO/Rest Plugin
(JSON over HTTPS)

Internal Firewall

Browser
HTTP(s) requests
to application

PEP to PDP
Traffic

Browser AJAX
SSO integration requests
to SSO/Rest (optional)

- SSO/Rest w/
  XACML engine
- CA SSO
- Oracle AM
- OpenAM
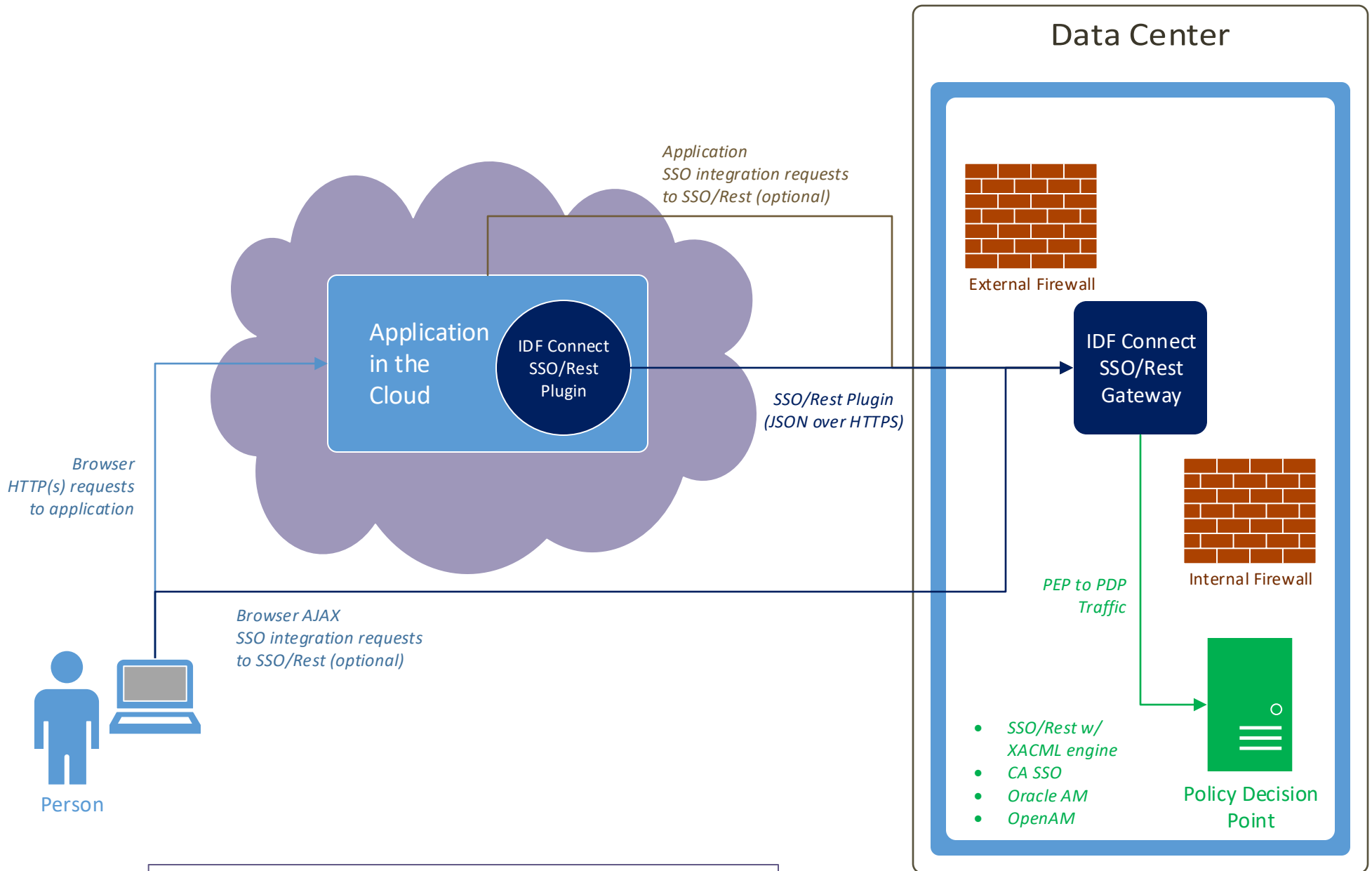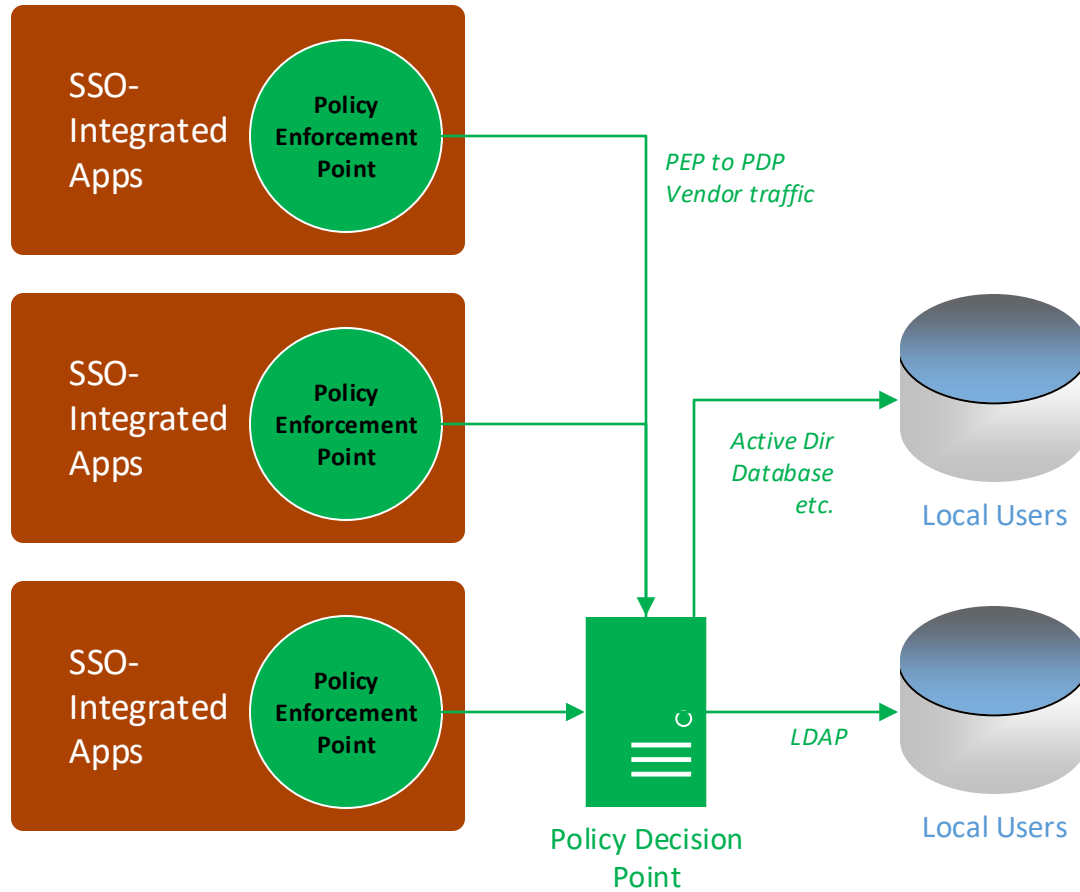
Policy Decision
Point

Person

Diagram shows where SSO/Rest resides,
and 3 different flows:
        - SSO/Rest Plugin
        - Client API support (AJAX, mobile)
        - Server-side API support

Data Center

SSO-Integrated Apps — Policy Enforcement Point

SSO-Integrated Apps — Policy Enforcement Point

SSO-Integrated Apps — Policy Enforcement Point

PEP to PDP Vendor traffic

Active Dir Database etc.

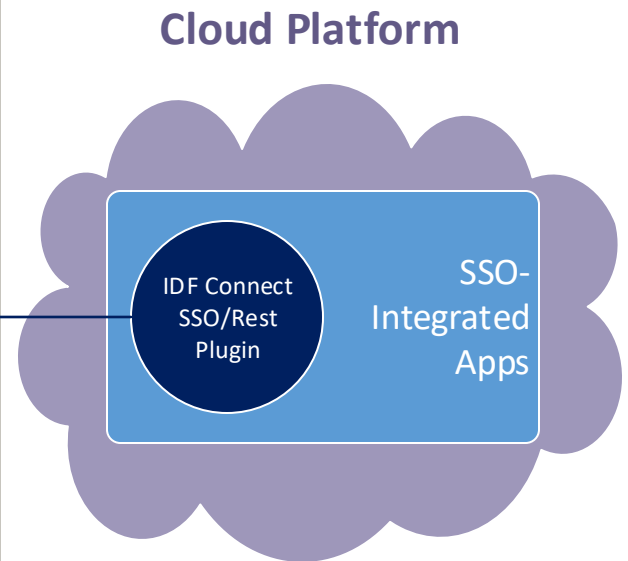Local Users
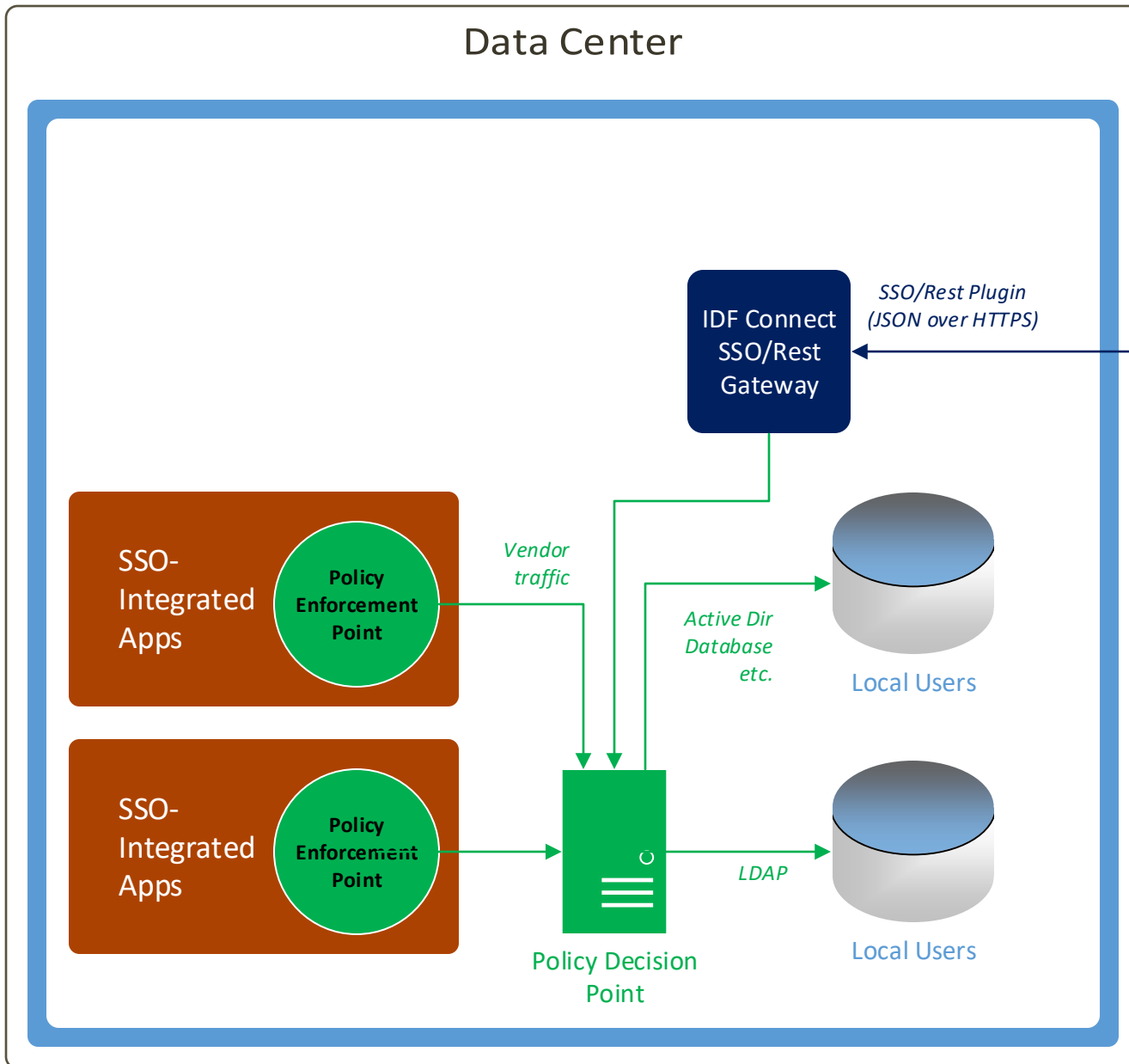
Policy Decision Point

LDAP

Local Users

Starting point – an on-premises Web Access Manager, and several integrated apps. Typical integrations could be based upon HTTP request headers, J2EE principals, etc.

Data Center

SSO-Integrated Apps

IDF Connect SSO/Rest Plugin

SSO/Rest Plugin (JSON over HTTPS)

IDF Connect SSO/Rest Gateway

SSO-Integrated Apps

Policy Enforcement Point

Vendor traffic

Active Dir Database etc.

Local Users

SSO-Integrated Apps
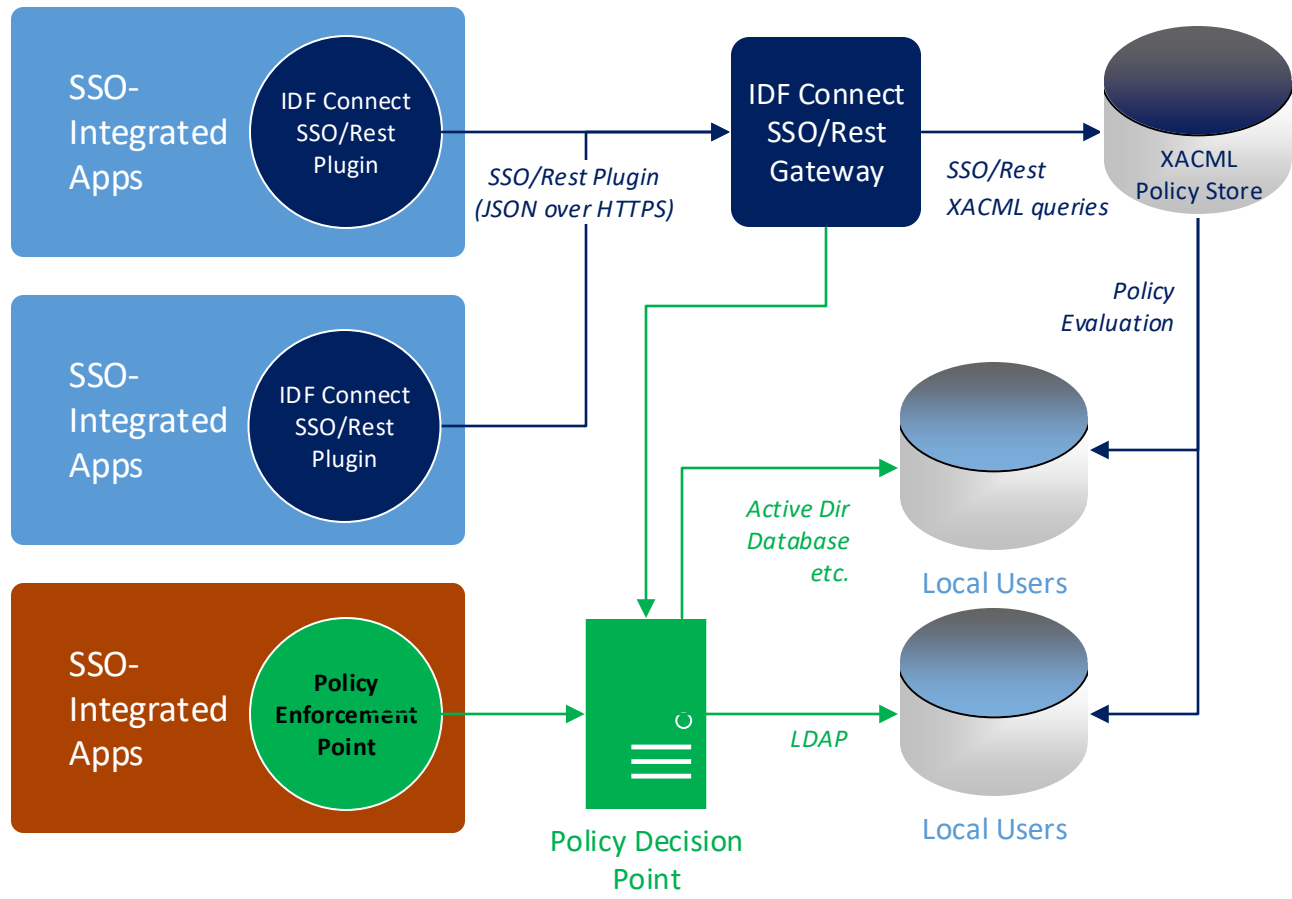
Policy Enforcement Point

Policy Decision Point

LDAP

Local Users
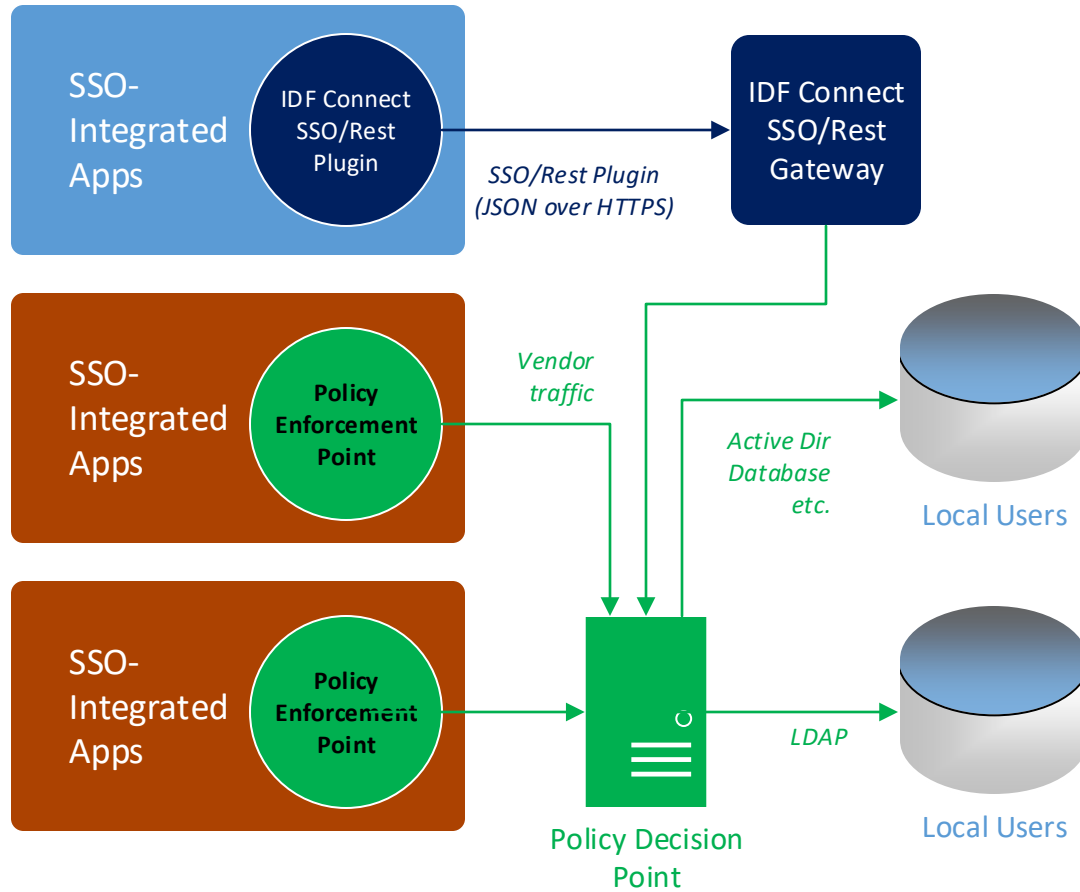
Now we add SSO/Rest to the mix, enabling applications to invisibly transition off of the direct WAM integrations

Data Center

Cloud Platform

IDF Connect SSO/Rest Gateway

SSO/Rest Plugin (JSON over HTTPS)

IDF Connect SSO/Rest Plugin

SSO-Integrated Apps

SSO-Integrated Apps

Policy Enforcement Point

Vendor traffic

Active Dir Database etc.

Local Users

SSO-Integrated Apps

Policy Enforcement Point

Policy Decision Point

LDAP

Local Users

Can be any IaaS or PaaS provider: MS Azure, CloundFoundry, Google App Engine, Amazon Beanstalk, etc.
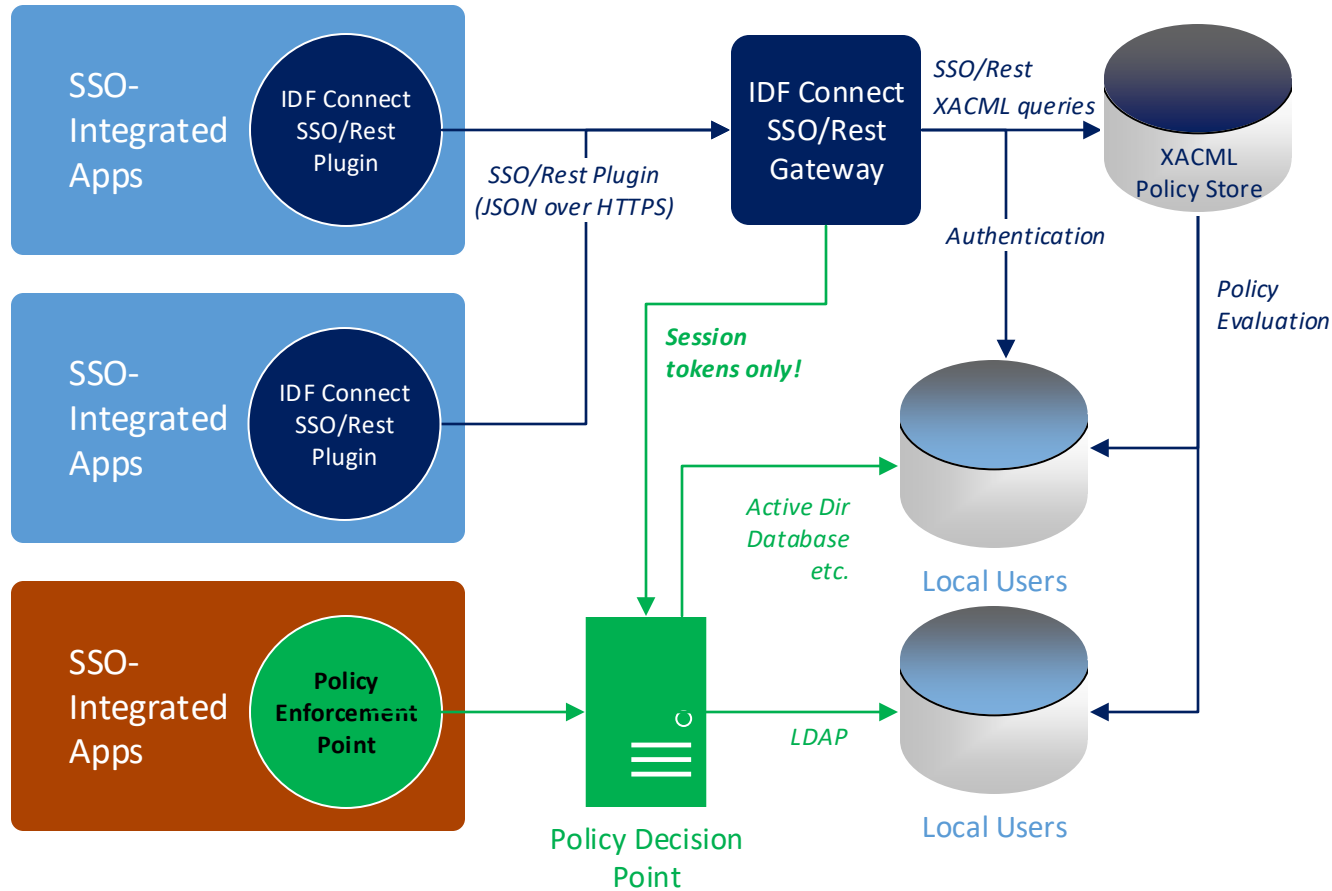
We can start lifting apps out of the data center and placing them directly into cloud Platform-as-a-Service providers. No application changes and no virtual machines required!
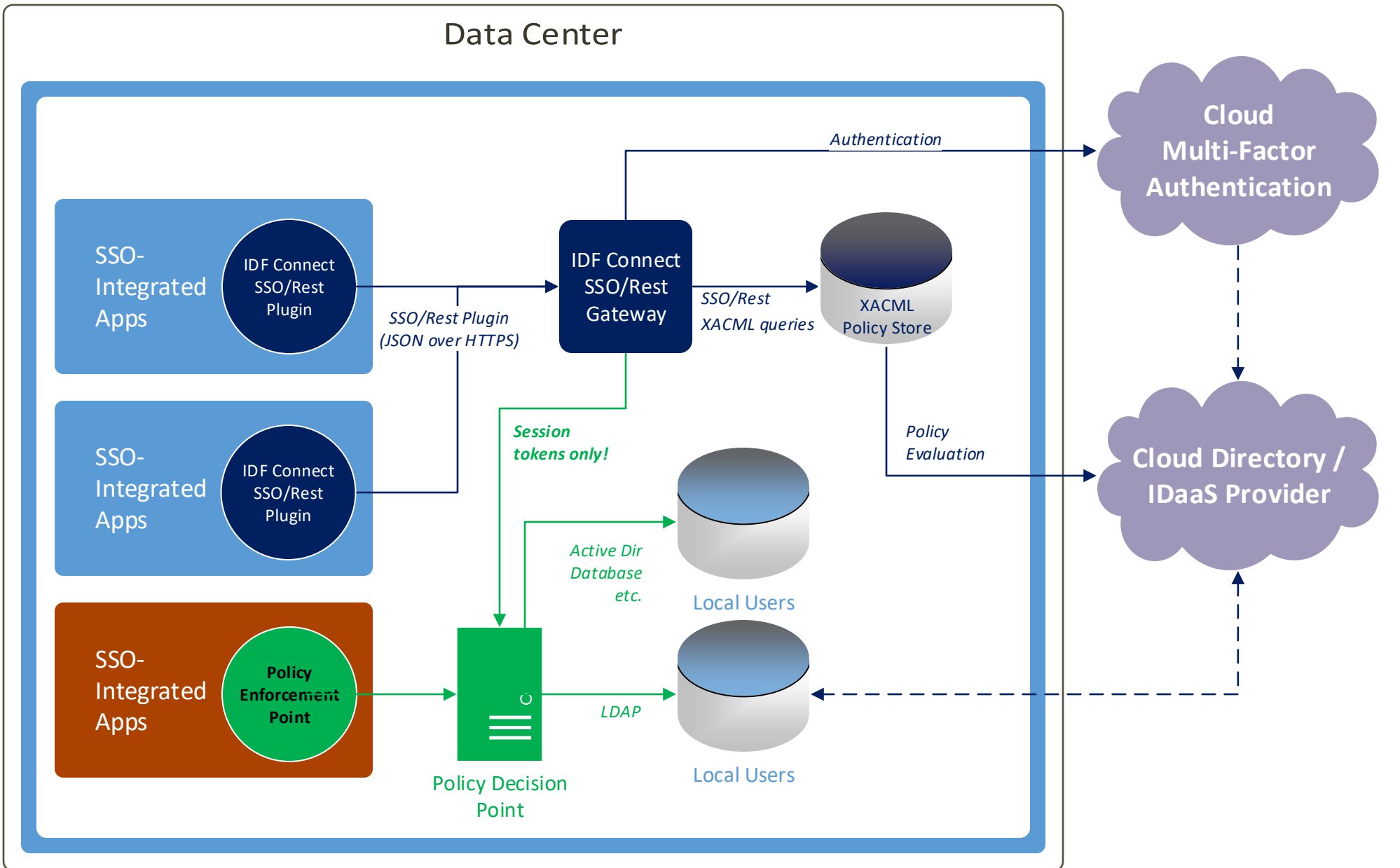
Data Center

SSO-Integrated Apps
IDF Connect SSO/Rest Plugin

SSO/Rest Plugin (JSON over HTTPS)

IDF Connect SSO/Rest Gateway

SSO/Rest XACML queries

XACML Policy Store

SSO-Integrated Apps
IDF Connect SSO/Rest Plugin

Policy Evaluation

Active Dir Database etc.

Local Users

SSO-Integrated Apps
Policy Enforcement Point

Policy Decision Point

LDAP

Local Users

Next we add a general-purpose access engine, based on XACML, to replace the vendor-proprietary policies. Also, we continue swapping out vendor agents for SSO/Rest plugins.

Data Center

SSO-Integrated Apps

IDF Connect SSO/Rest Plugin

SSO-Integrated Apps

IDF Connect SSO/Rest Plugin

SSO-Integrated Apps

Policy Enforcement Point

SSO/Rest Plugin (JSON over HTTPS)

IDF Connect SSO/Rest Gateway

SSO/Rest XACML queries

XACML Policy Store

Authentication

Policy Evaluation

Session tokens only!

Active Dir Database etc.

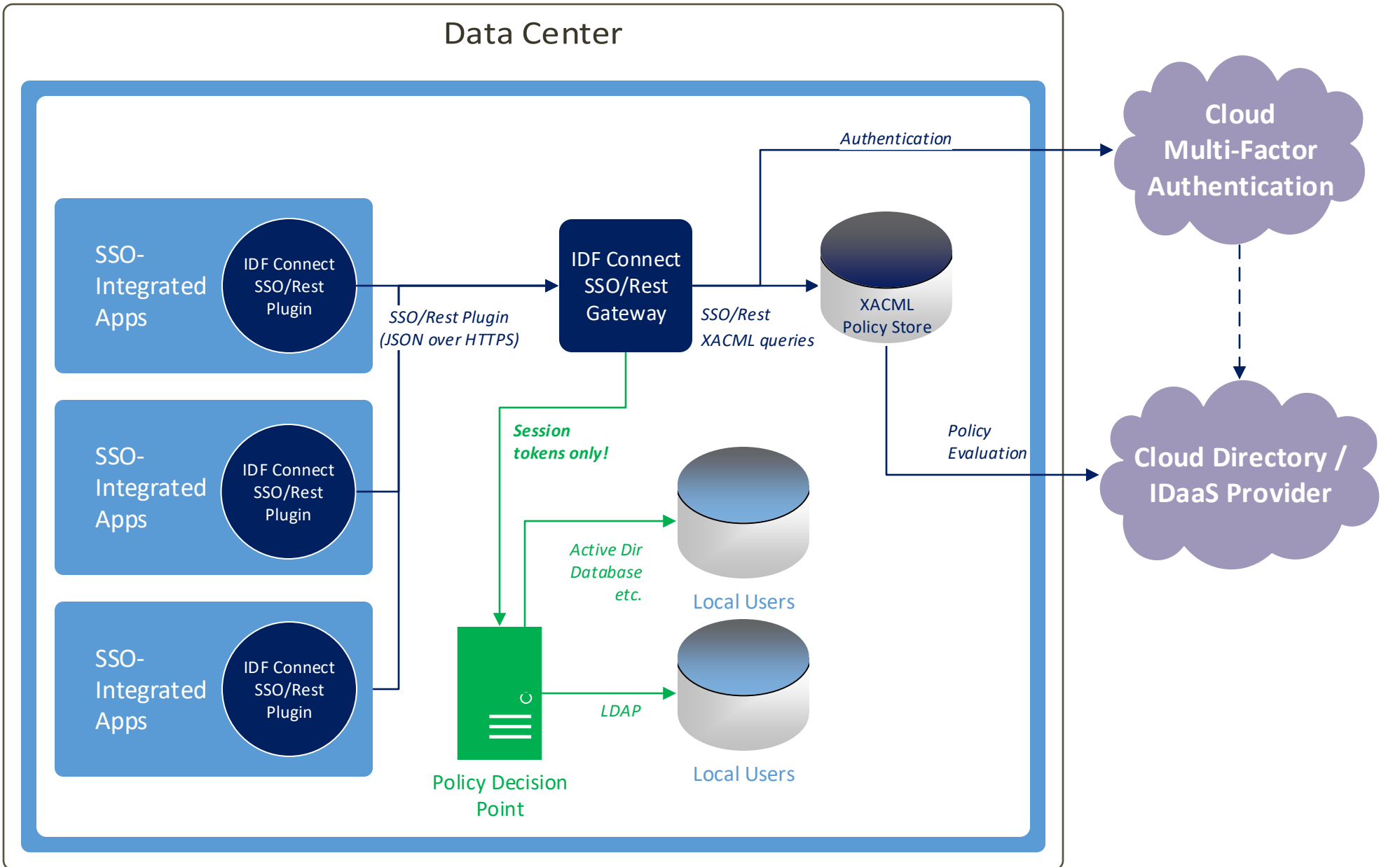Local Users

LDAP

Local Users

Policy Decision Point

Now SSO/Rest can authenticate users directly against the existing LDAP, AD, etc. The existing WAM vendor is still used for SSO token management, so SSO continuity is maintained
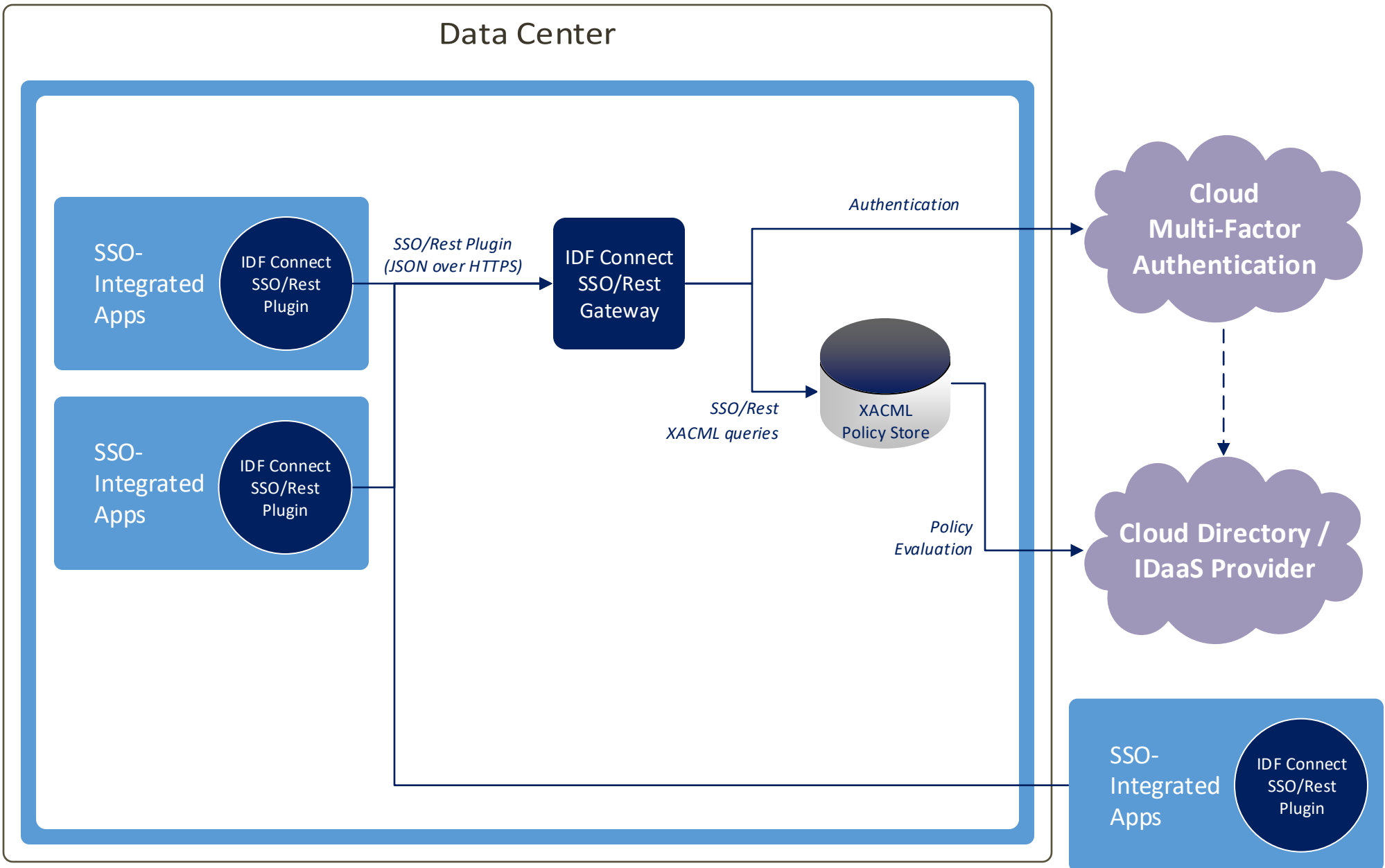
Data Center

SSO-Integrated Apps — IDF Connect SSO/Rest Plugin

SSO/Rest Plugin (JSON over HTTPS)

SSO-Integrated Apps — IDF Connect SSO/Rest Plugin

SSO-Integrated Apps — IDF Connect SSO/Rest Plugin

IDF Connect SSO/Rest Gateway

SSO/Rest XACML queries

XACML Policy Store

Authentication

Cloud Multi-Factor Authentication

Policy Evaluation

Cloud Directory / IDaaS Provider

Session tokens only!

Active Dir Database etc.

Local Users

LDAP
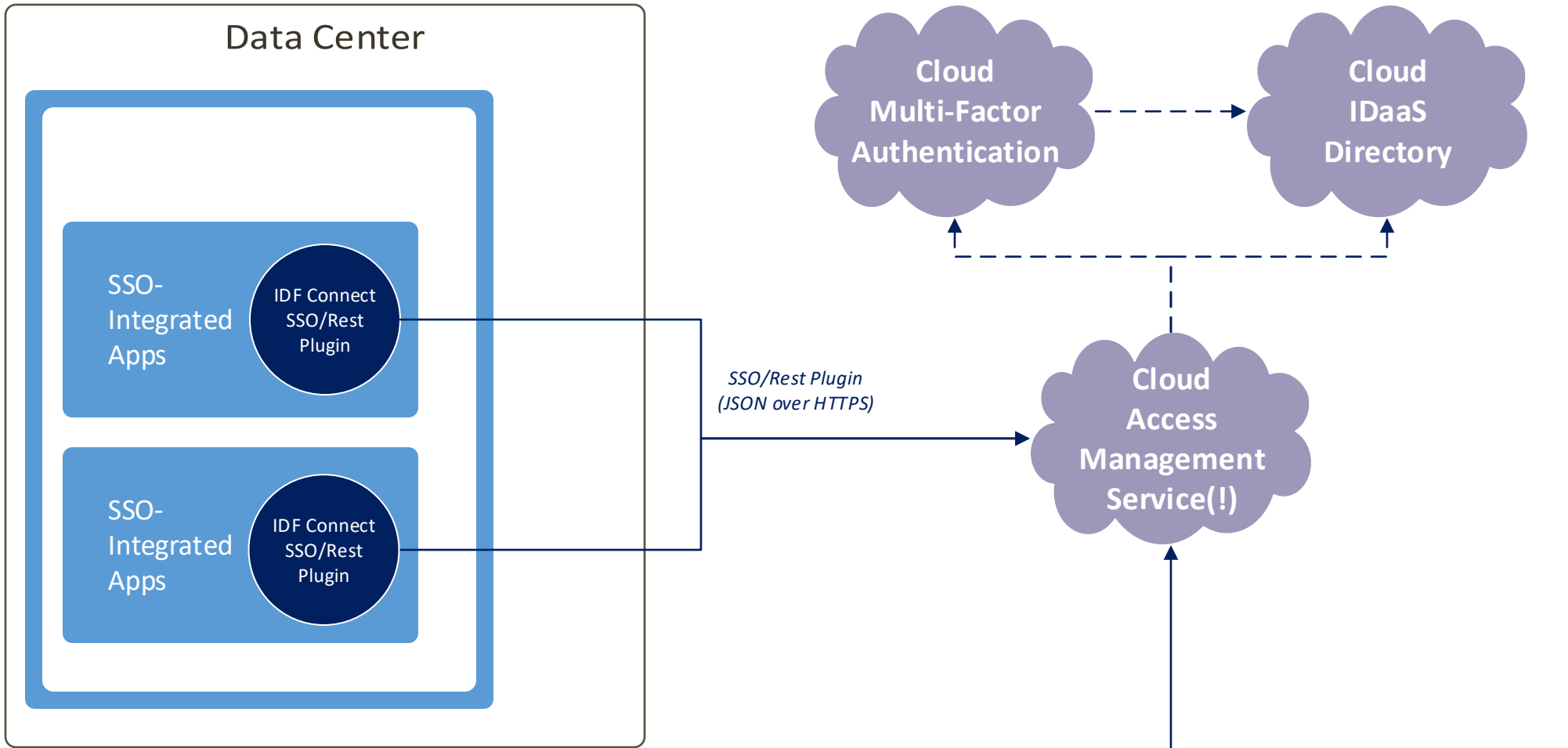
Local Users

Policy Decision Point

Finally, the legacy WAM solution is only used for token creation. It can now be safely decommissioned with the only side effect being that active user sessions will be logged out when the switch is thrown.

Data Center

SSO-Integrated Apps — IDF Connect SSO/Rest Plugin

SSO/Rest Plugin (JSON over HTTPS) →

IDF Connect SSO/Rest Gateway

Authentication →

Cloud Multi-Factor Authentication

SSO/Rest XACML queries

XACML Policy Store

Policy Evaluation →

Cloud Directory / IDaaS Provider

SSO-Integrated Apps — IDF Connect SSO/Rest Plugin

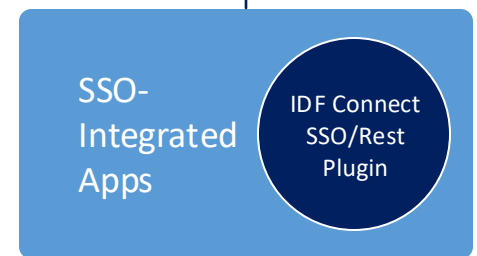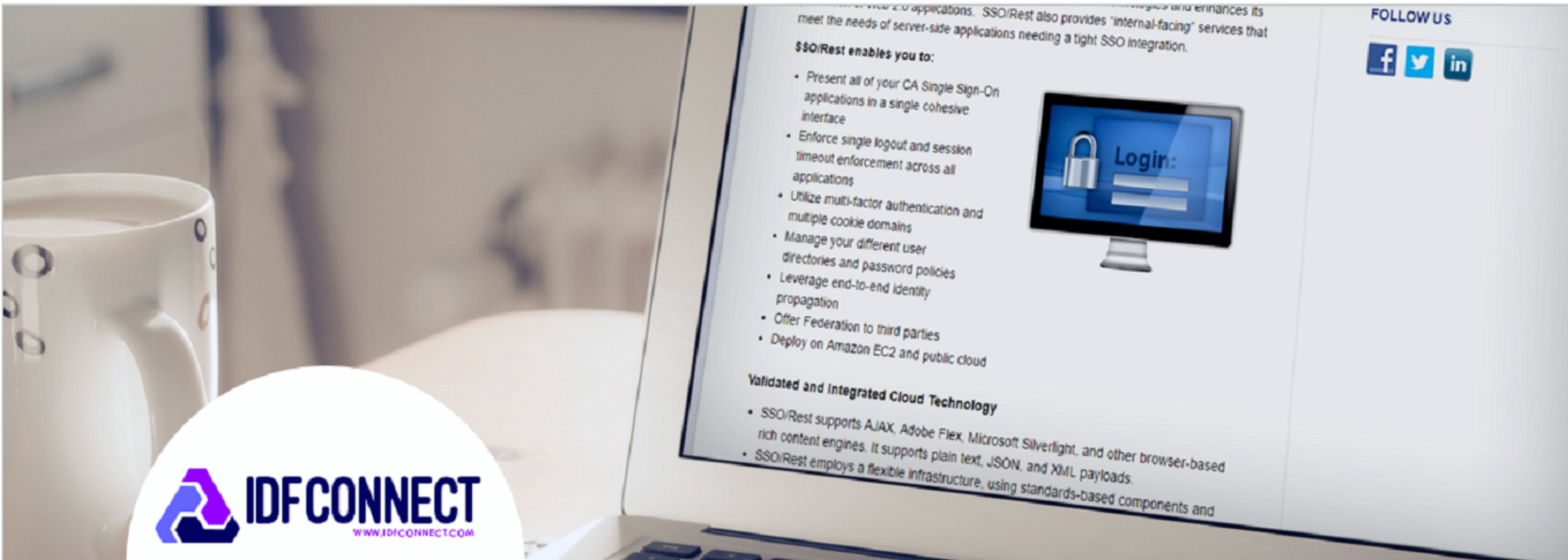SSO-Integrated Apps — IDF Connect SSO/Rest Plugin

A good end state:
– Managed MFA and IDM
– Apps may be in the cloud, apps may be on premises
– SSO/Rest Gateway + Policy Store may also be in the cloud or on-premises

Data Center

SSO-Integrated Apps

IDF Connect SSO/Rest Plugin

SSO-Integrated Apps

IDF Connect SSO/Rest Plugin

SSO/Rest Plugin (JSON over HTTPS)

Cloud Multi-Factor Authentication

Cloud IDaaS Directory

Cloud Access Management Service(!)

SSO-Integrated Apps

IDF Connect SSO/Rest Plugin

Complete enterprise-grade IAM-as-a-Service!
Access Management Service incorporates:

- *SSO/Rest Gateway*
- *Access Policy Engine*
- *Policy Management UI, APIs, import / migration tools*
- *Audit and compliance tools*

...on of Web 2.0 applications. SSO/Rest also provides "internal-facing" services that meet the needs of server-side applications needing a tight SSO integration.

SSO/Rest enables you to:

- Present all of your CA Single Sign-On applications in a single cohesive interface
- Enforce single logout and session timeout enforcement across all applications
- Utilize multi-factor authentication and multiple cookie domains
- Manage your different user directories and password policies
- Leverage end-to-end identity propagation
- Offer Federation to third parties
- Deploy on Amazon EC2 and public cloud

Validated and Integrated Cloud Technology

- SSO/Rest supports AJAX, Adobe Flex, Microsoft Silverlight, and other browser-based rich content engines. It supports plain text, JSON, and XML payloads.
- SSO/Rest employs a flexible infrastructure, using standards-based components and

IDF CONNECT
WWW.IDFCONNECT.COM

Also check out our other products:
www.idfconnect.com/products

Turn CA SSO into your Enterprise 2-Factor Auth Solution with SSO/MobileKey. For more details visit
www.idfconnect.com/products/sso-mobilekey/

THANK YOU!

For More Information, Please Visit

IDF Connect, Inc.
2207 Concord Pike #359
Wilmington, DE 19803
Phone: (888) 765-1611
Fax: (888) 765-7284

www.idfconnect.com

www.linkedin.com/in/rsand

@IDFConnect
@rsand2

www.facebook.com/IDFConnect