

# Idaptive Next-Gen Access

---

JANUARY 2019

# Agenda

---

About Idaptive

---

Joint Use Cases

---

Next Steps

---

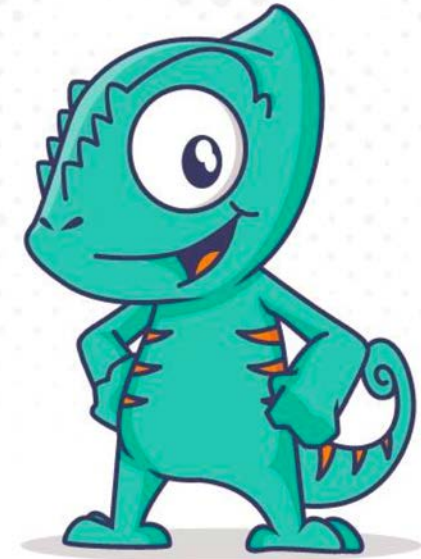
---



# About Idaptive

# About Idaptive

- Born of out Centrify, a leader in the Infrastructure Services Security space and recently spun out as an independent cloud company
- Cloud First, Next-Gen Identity as a Service vendor
- Owned by Thoma Bravo, one of the largest Private Equity firms in the world with over \$30B in investments
- Empower companies with **Next-Gen Access** so they can securely and confidently build their business
- Trusted by over 2000+ customers with over 95% retention
- HQ in Santa Clara, CA with development and sales offices across the world



idaptive   
NEXT-GEN ACCESS

# Over 2000 customers across all verticals

## BANKING, FINANCE, INSURANCE



## TECHNOLOGY, MEDIA & TELECOM



## GOVERNMENT, STATE, LOCAL, EDUCATION



## RETAIL, MANUFACTURING, PHARMA



## CONSUMER, WEB





# Clear Market Leadership in Cloud *Identity & Authentication* for Enterprise *Workforce, Partners* and *Consumers*

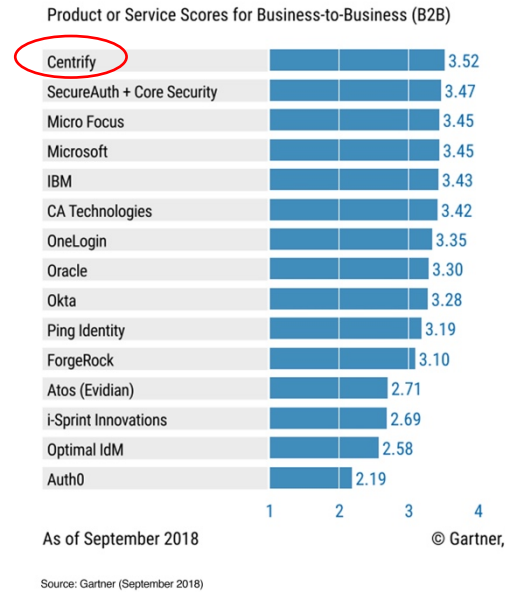
## LEADER FORRESTER IDAAS WAVE



## LEADER GARTNER CRITICAL CAPABILITIES WORKFORCE TO SAAS



## LEADER GARTNER CRITICAL CAPABILITIES B2B



## LEADER KUPPINGCOLE CLOUD MFA

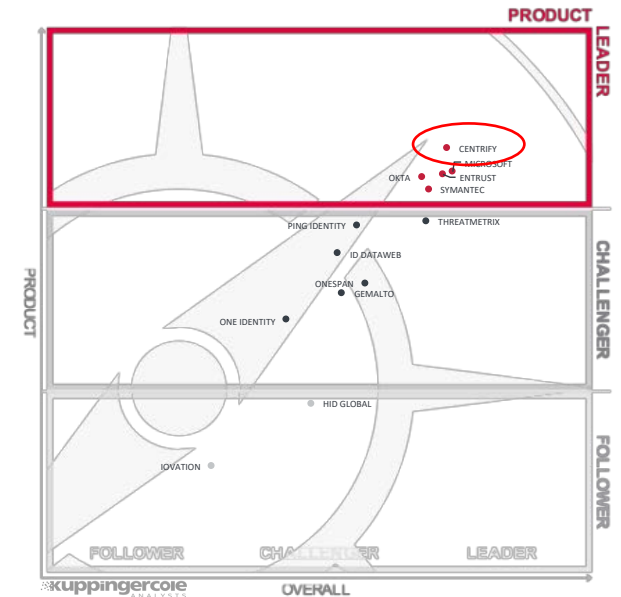


Figure 1: Product leaders in the Cloud-based MFA market segment

LEADERS IN IDENTITY AS A SERVICE AND CLOUD BASED MULTI-FACTOR AUTHENTICATION

# High Praise from Customers



**4.5** out of 5.0  
in 88 customer reviews

**“Everything we had hoped for in a new solutions partner”**

— Director of IT in Finance Industry



**8.8** out of 10.0  
in 66 customer reviews

**“My IT team took to the product very easily. The end users love it!”**

— Director of IT in Manufacturing Industry



**4.4** out of 5.0  
in 85 customer reviews

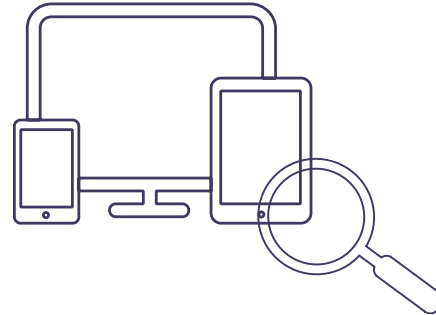
**"Great Identity Provider + outstanding technical support"**

— IT Administrator

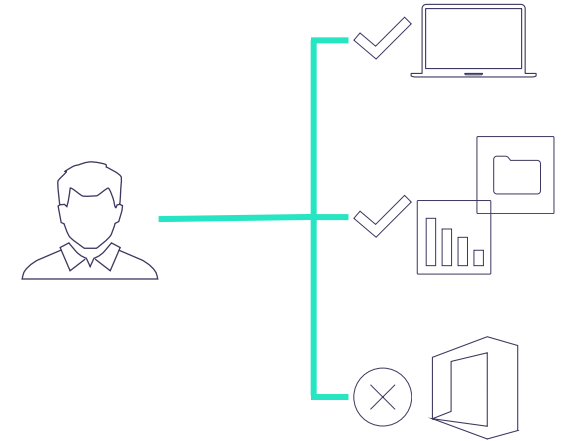
# Next-Gen Access Powers Zero Trust



**1** VERIFY EVERY USER



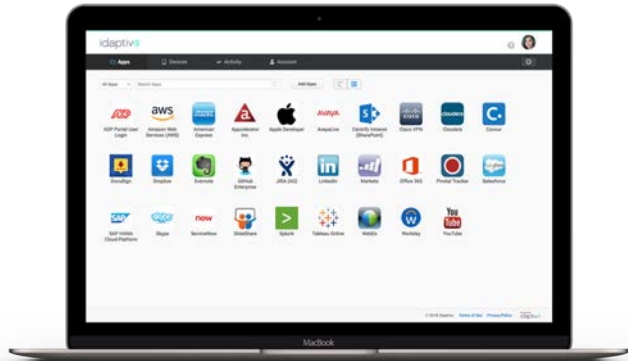
**2** VALIDATE THEIR DEVICES



**3** INTELLIGENTLY LIMIT THEIR ACCESS



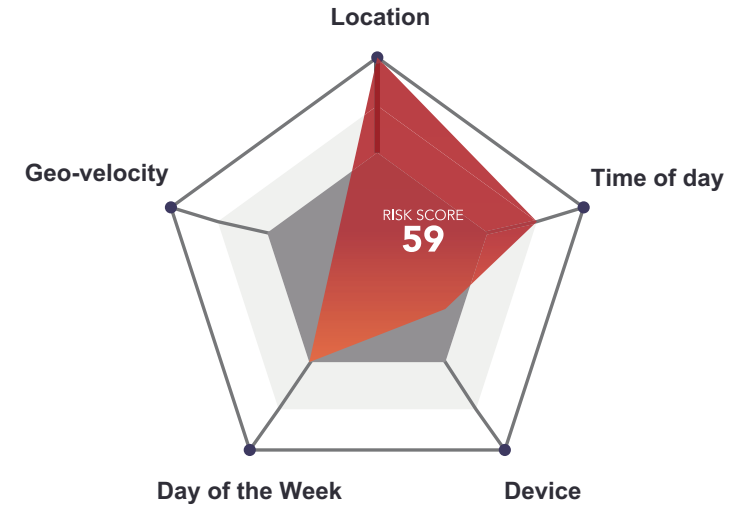
# Zero Trust Security: Verify the User



**SINGLE SIGN-ON**

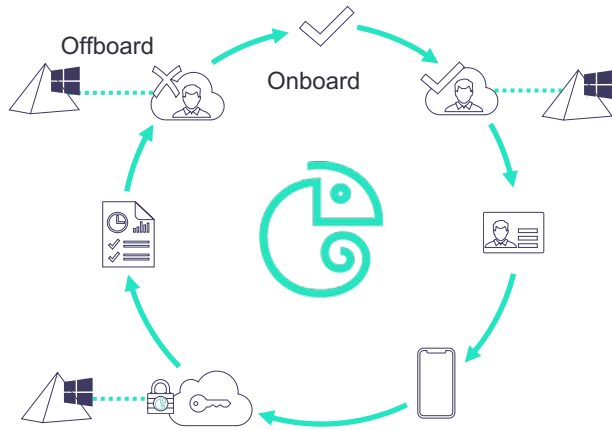


**MFA EVERYWHERE**



**BEHAVIOR-BASED ACCESS**

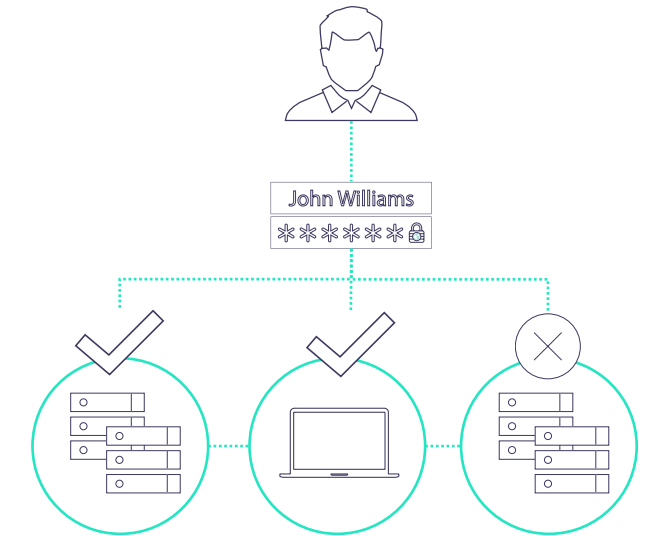
# Zero Trust Security: Intelligently Limit Their Access



**LIFECYCLE  
MANAGEMENT**

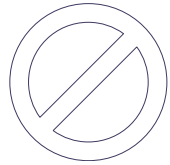


**ACCESS REQUEST  
WORKFLOW**



**APP GATEWAY WO/VPN**

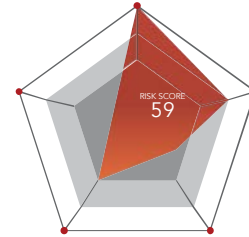
# Intelligent Access



**BLOCK ACCESS**



**ADAPTIVE MULTI-FACTOR AUTHENTICATION**

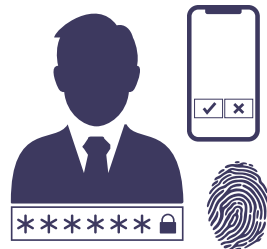


**CONDITIONAL ACCESS**

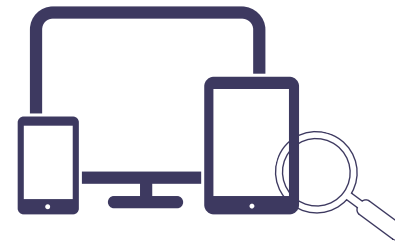


**INSIGHT AND FORENSICS**

## MACHINE LEARNING



**VERIFY THE USER**



**VALIDATE THEIR DEVICE**

# Next-Gen Access Platform

## User Risk and Behavior Analytics

---

### SECURE ACCESS TO APPLICATIONS

Single Sign-On to Apps  
Provisioning & Lifecycle Management  
App Access Gateway

### SECURE ACCESS TO & FROM ENDPOINTS

Mobile Con  
Adaptive MFA for Endpoint Login  
Conditional Access

---

## Adaptive Multi-factor Authentication



# F5 Networks and Idaptive – Joint Use Cases

# F5 Big-IP + Idaptive = Secure Zero Trust Access

## Zero Trust External Access to On-Prem Apps

- Enable secure single-sign on through an integration between Big-IP's Service provider and Idaptive's Identity Provider
- Enable SSO to legacy on-prem apps using header based authentication using Big-IP's Reverse Proxy

## Multi-Factor Authentication

- Drive superior identity and authentication assurance levels by leveraging Idaptive's Adaptive MFA capabilities

## Continuous Fine Grained Access Control

- URL based MFA based on custom iRules?

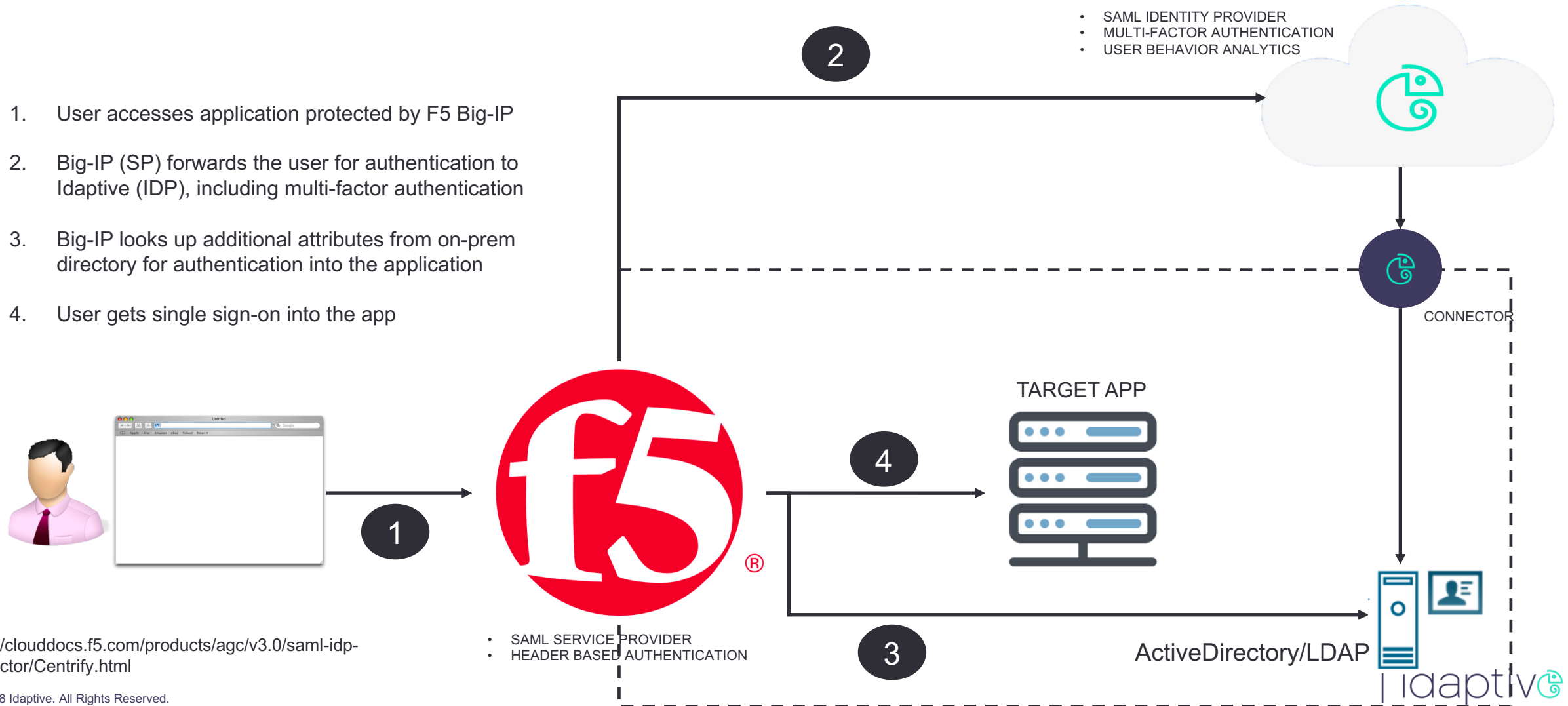
## Single End User Portal for All Apps

- Provide a single-pane of glass to all end users to access all their apps, cloud and on-prem protected by Big-IP



# Zero Trust External Access to On-Prem Apps Protected by Big-IP

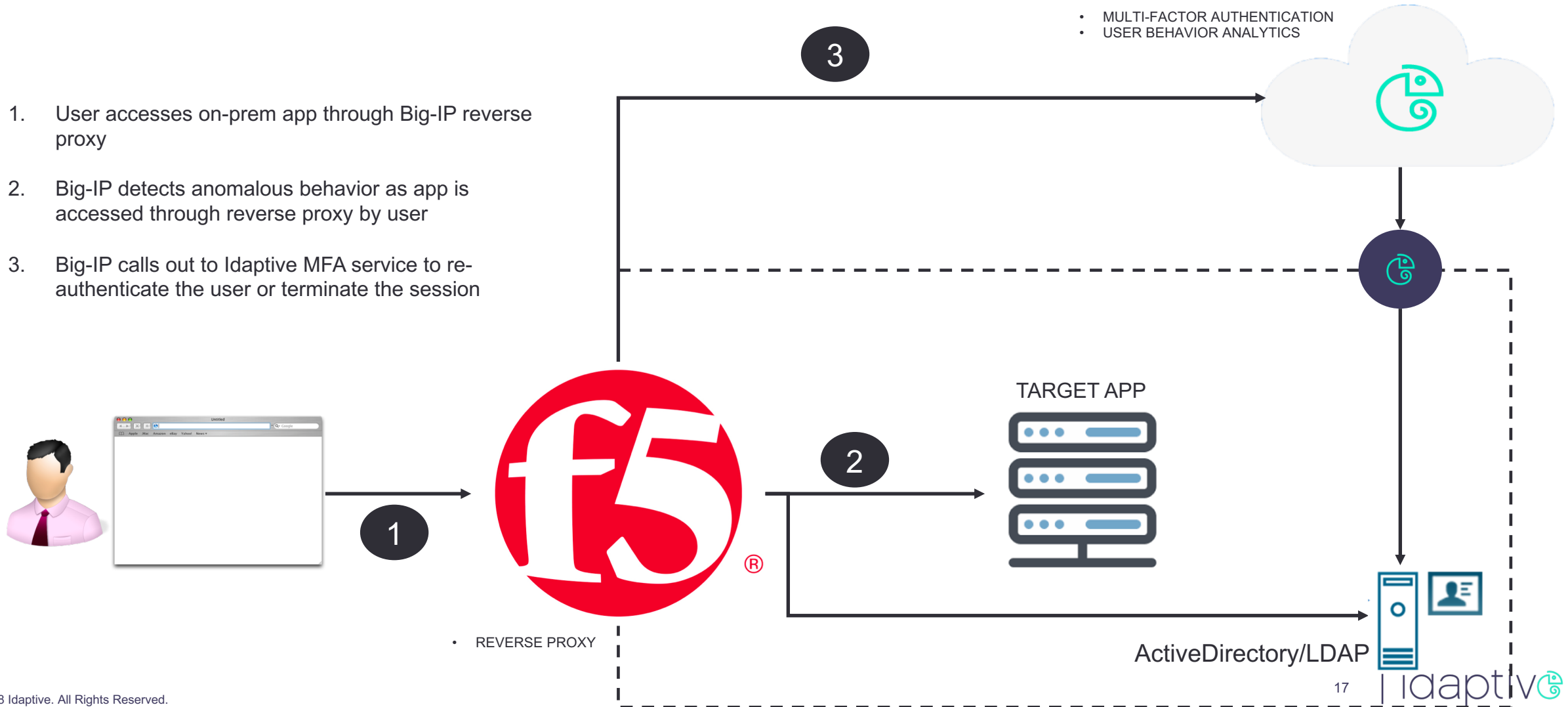
1. User accesses application protected by F5 Big-IP
2. Big-IP (SP) forwards the user for authentication to Idaptive (IDP), including multi-factor authentication
3. Big-IP looks up additional attributes from on-prem directory for authentication into the application
4. User gets single sign-on into the app



<https://clouddocs.f5.com/products/agc/v3.0/saml-idp-connector/Centrify.html>

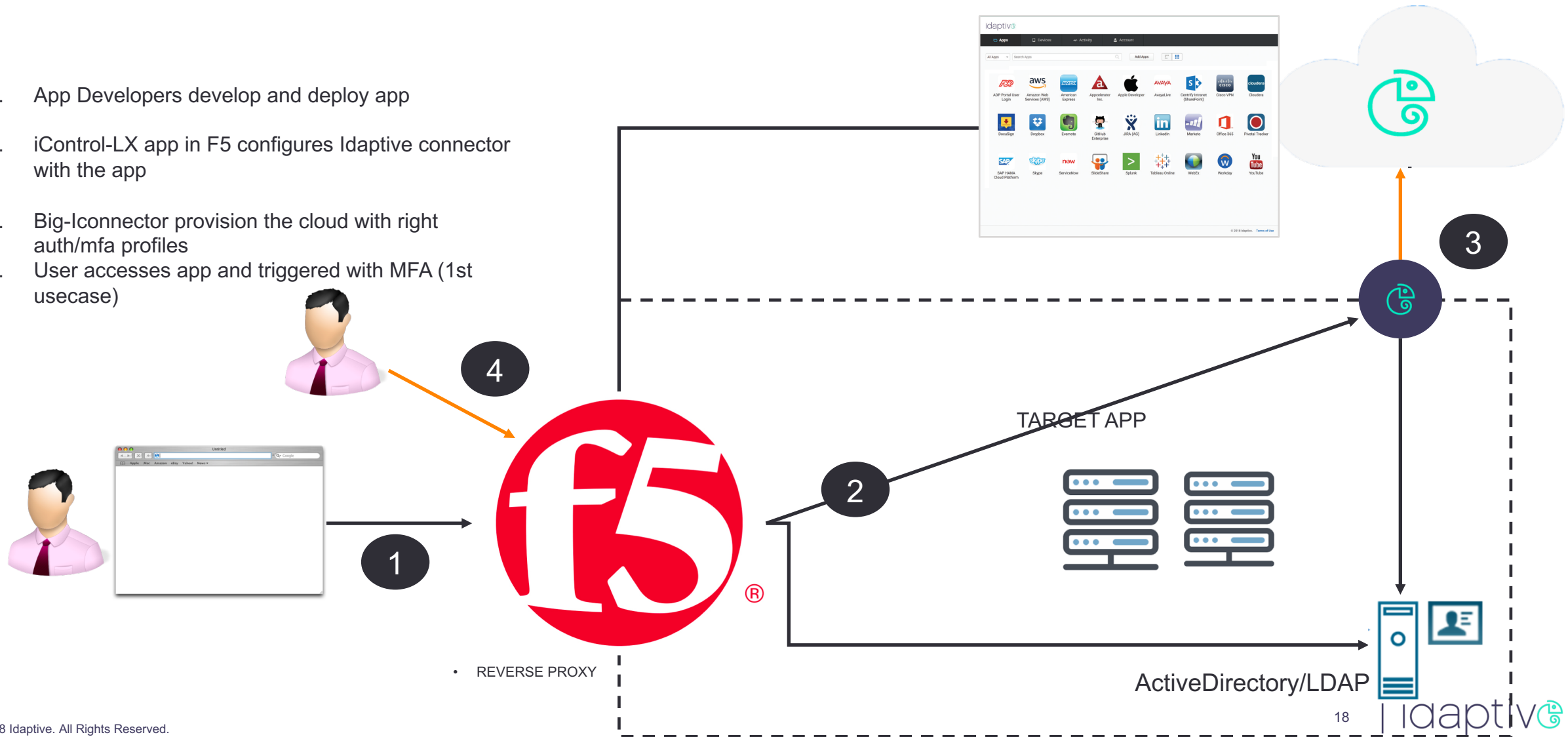
# Continuous, Fine-Grained Access Control for Apps protected by Big-IP

1. User accesses on-prem app through Big-IP reverse proxy
2. Big-IP detects anomalous behavior as app is accessed through reverse proxy by user
3. Big-IP calls out to Idaptive MFA service to re-authenticate the user or terminate the session



# Seamlessly Deploying App with Access/MFA Policies

1. App Developers develop and deploy app
2. iControl-LX app in F5 configures Idaptive connector with the app
3. Big-Iconnector provision the cloud with right auth/mfa profiles
4. User accesses app and triggered with MFA (1st usecase)



# F5+Idaptive Joint Use Cases

- App Lifecycle Mgmt
  - Deploy with F5 policies
  - Idaptive discovers and applies access/MFA policies
  - Provisioning etc.
- Reverse proxy use case for on-prem/cloud apps.
  - Idaptive as IDP for SAML.. Custom iRule
  - SSO by looking at the header for authenticated user.
- F5 Firewall data ingested into the analytics engine.
- MDM synergy.



# Next Steps

# Next Steps

- Identify 4-5 key joint customers
- Discuss joint go to market possibilities
- Discussion proof of concept/technology for joint use cases





# Thank You

---