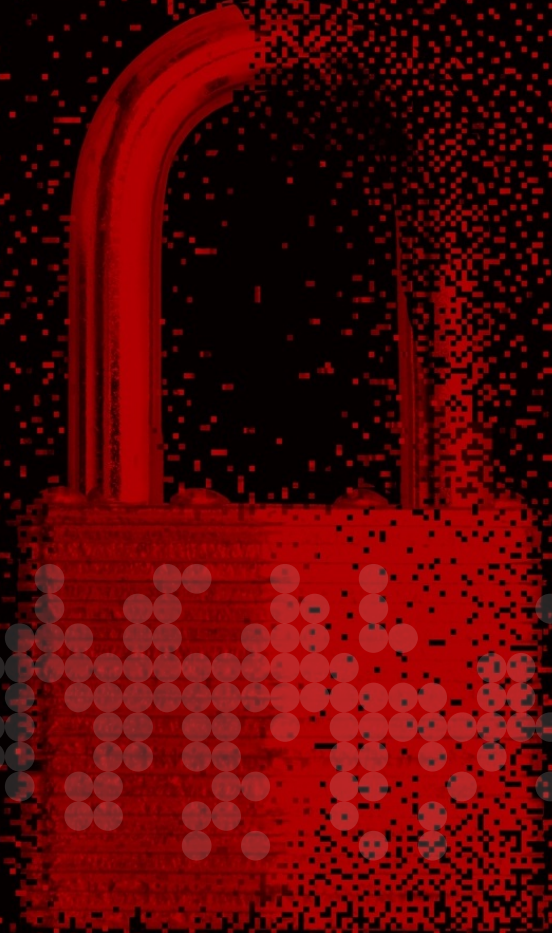




# The Anatomy of Securing the access perimeter

Matthieu DIERICK

*Specialist System Engineer - Security*



# Agenda

## Office 365 Modern Authentication

ADAL

Multi Factor Authentication

OAuth

## MDM integration

Device posture control


Per-App VPN

## Anti-Fraud

Credential grabbing protection

# Office 365 Modern Authentication

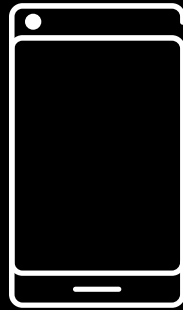




Office 365 is the #1 SaaS  
applications our customers use !

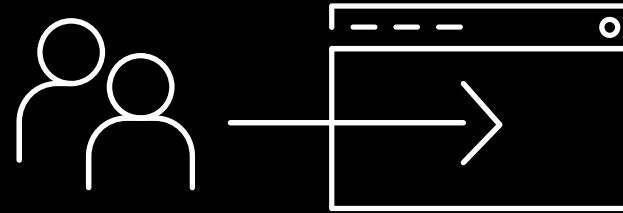
Okta – Ron Miller (@ron\_miller)

# Why does F5 care ?



**70%**

Fortune 500



**70%**

1Q16 growth

# Three identity models for Office 365

## Cloud Identity

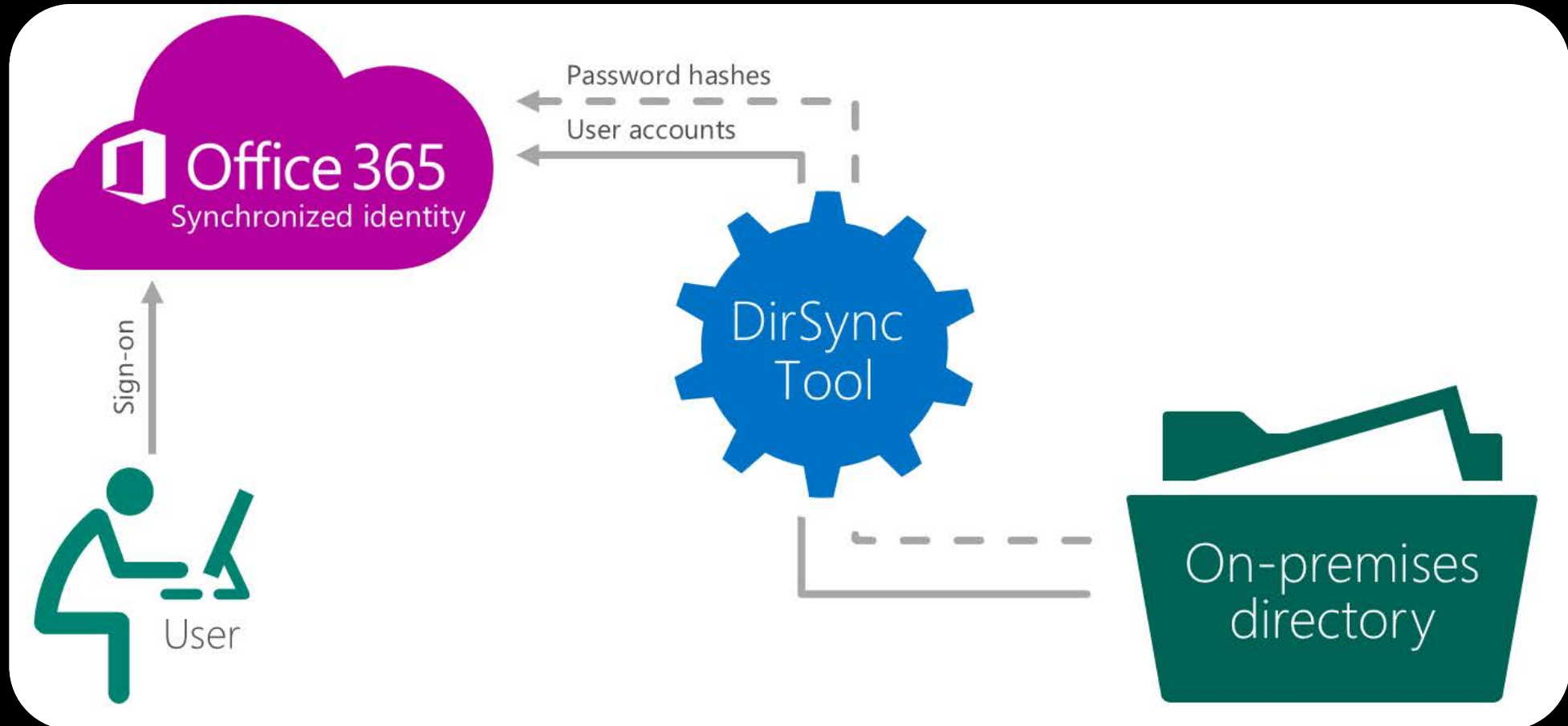


User accounts



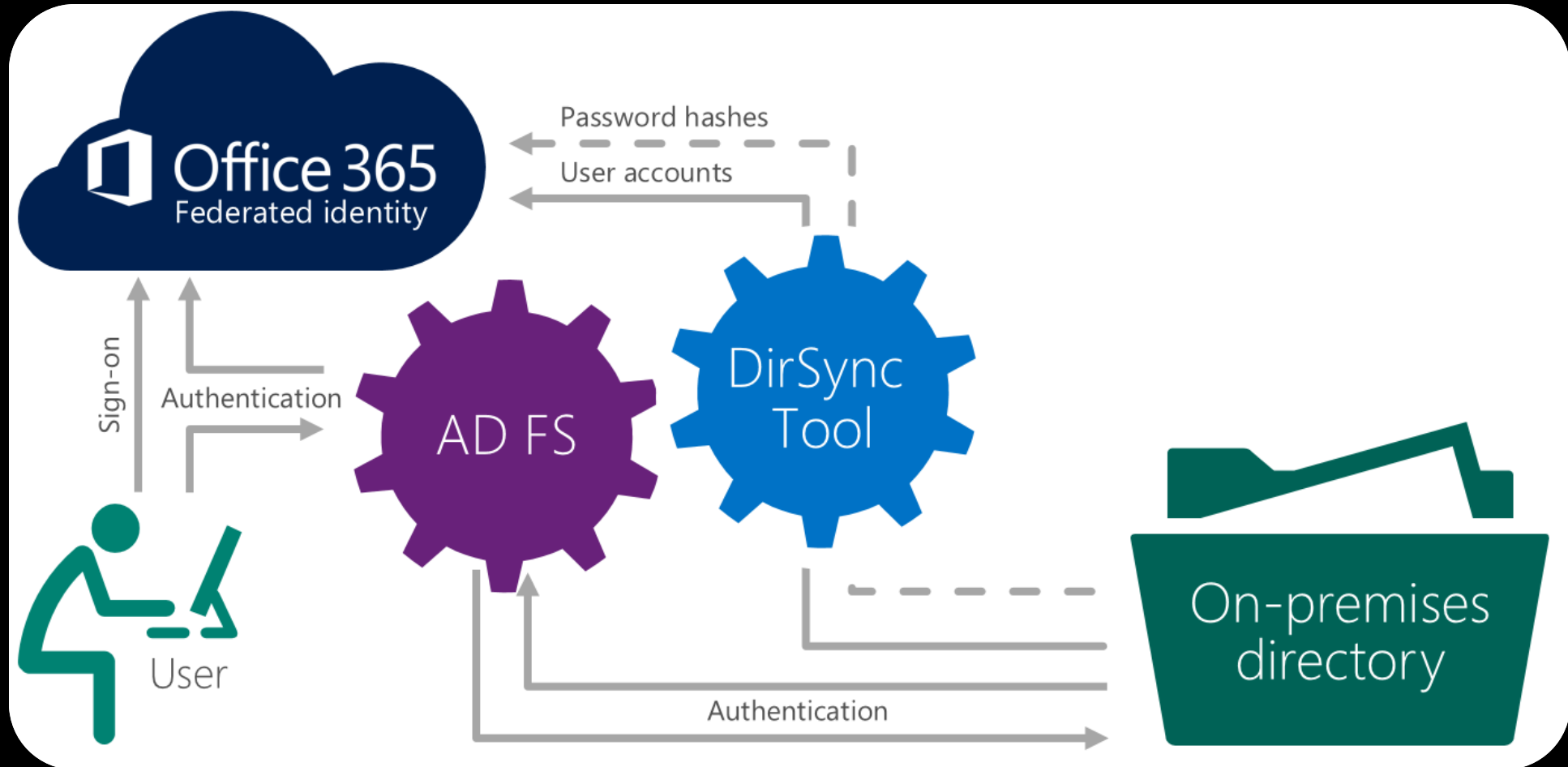
# Three identity models for Office 365

## Synchronized Identity



# Three identity models for Office 365

## Federated Identity





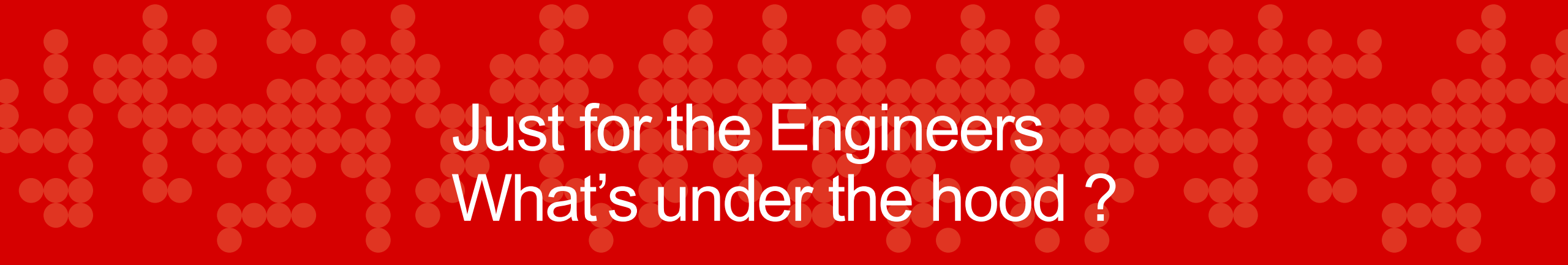
# What exactly did MSFT announce on Nov 19th, 2015?

This is key

- Modern authentication(ADAL) in the Office 2013 Windows client and in the Office 2016 Windows client are complete and at GA.
- All users of Office 365 modern authentication can now get production support through regular Microsoft support channels.
- Use of Office 365 modern authentication is now on by default for Office 2016.

# Current Modern Authentication Support Matrix from Microsoft(as of April 15th, 2016)

Office client application	Windows	Mac OS X	Windows Phone	iOS	Android
Office clients	Available now for Office 2013 and Office 2016.	Office 2016 Mac Preview supports ADAL including Word, Excel, PowerPoint and OneNote. OneNote was released with ADAL in 2014.	Coming soon.	Word, Excel and PowerPoint are available now.	For Android phones: Word, Excel and PowerPoint are available now. For Android tablets: Word, Excel and PowerPoint are coming soon.
Skype for Business (formerly Lync)	Included in Office client.	Coming soon	Coming soon.	Available now*.	Available now*.
Outlook	Included in Office client.	Available Now	Coming soon.	Available now.	Available now.
OneDrive for Business	Included in Office client.	Available now	Available now for Windows Phone 8.1.	OneDrive for Business is available now.	OneDrive for Business is available now.
Legacy clients	There are no plans for Office 2010 or Office 2007 to support ADAL-based authentication.	There are no plans for Office for Mac 2011 to support ADAL-based authentication.	There are no plans for Office on Windows Phone 7 to support ADAL-based authentication.	There are no plans to enable older Outlook iOS clients.	There are no plans to enable older Outlook Android clients.



Just for the Engineers  
What's under the hood ?

# Modern authentication (Federated Identities)

User

Word

Sharepoint O365

login.microsoftonline.com

F5 APM

Open a file

Request doc (no token)

401: need token from login.microsoft

GET login.microsoftonline.com/[authUrl] / 200: (show login page)

(enter username)

send

GET [on-prem authURL] / 200: (show login page)

(enter Username/password)

(verify

302 with SAML Assertion for login.microsoftonline.com)

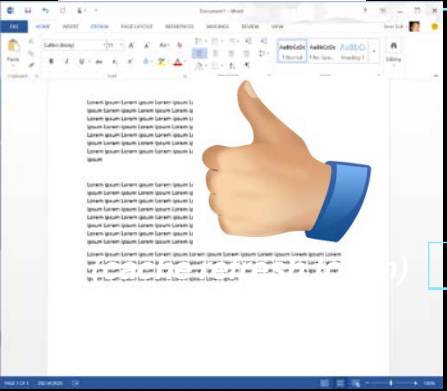
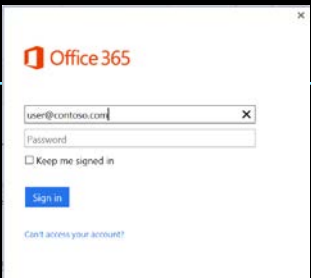
username/password)

POST SAML Assertion to login.microsoftonline.com

200: (return access/refresh token)

Request doc (access token)

200: return doc



# Office 365 ADAL Authentication uses OAuth 2.0 tokens for access control

## Access Token

- Issued based on valid credentials
- Valid for 1 hour
- Action required when access token expired

## Refresh Token

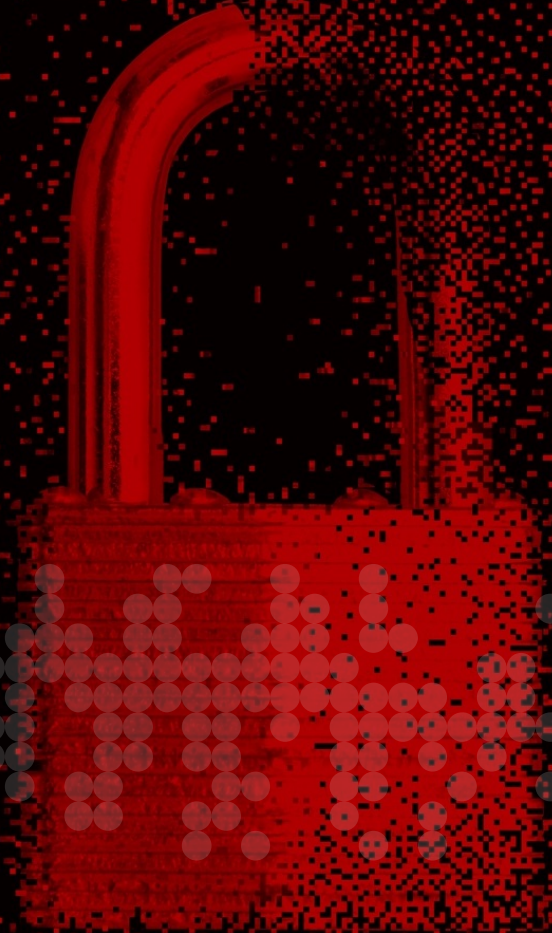
- Valid for 14d by default, up to 90d with use
- No credentials needed from the user as long as refresh token is valid

- When an Access Token expires, Office 365 client attempts to trade in Refresh Token for a new access token
- **Admins cannot control lifetime of tokens!**
  - Refresh/access token are invalidated only if user changes their password or if user is using Microsoft Intune MDM for conditional-based access



# Demonstration

Office 365 with thick client and 2 MFA





You said OAuth ???

“OAuth is an open standard for authorization.”

“OAuth gives applications secure, delegated access to server based resources given to them by a resource owner.”

“OAuth can authorize someone to use these resources without sharing their credentials by instead using a set of managed access tokens.”



# OAuth: What It Is & What It Isn't

## What OAuth IS

- OAuth is a manager of tokens
- OAuth is an open standard
- OAuth is primarily intended to authorize access to Web Services APIs

## What OAuth ISN'T

- OAuth is NOT an authentication standard
- OAuth does NOT inherently protect itself
- OAuth is NOT always compatible

# OAuth: Who Supports It?

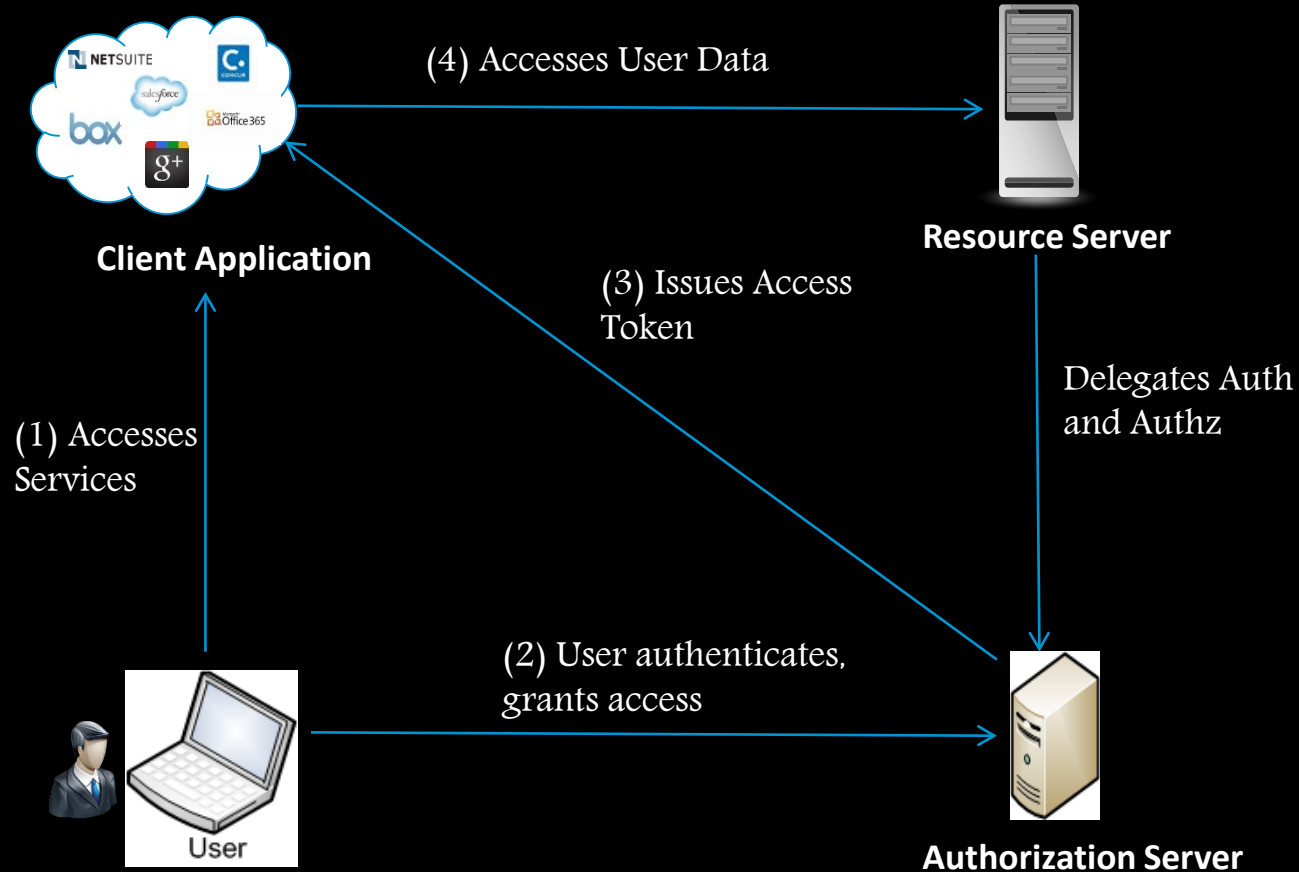
- Public Web Services



... and over 150 other public services.



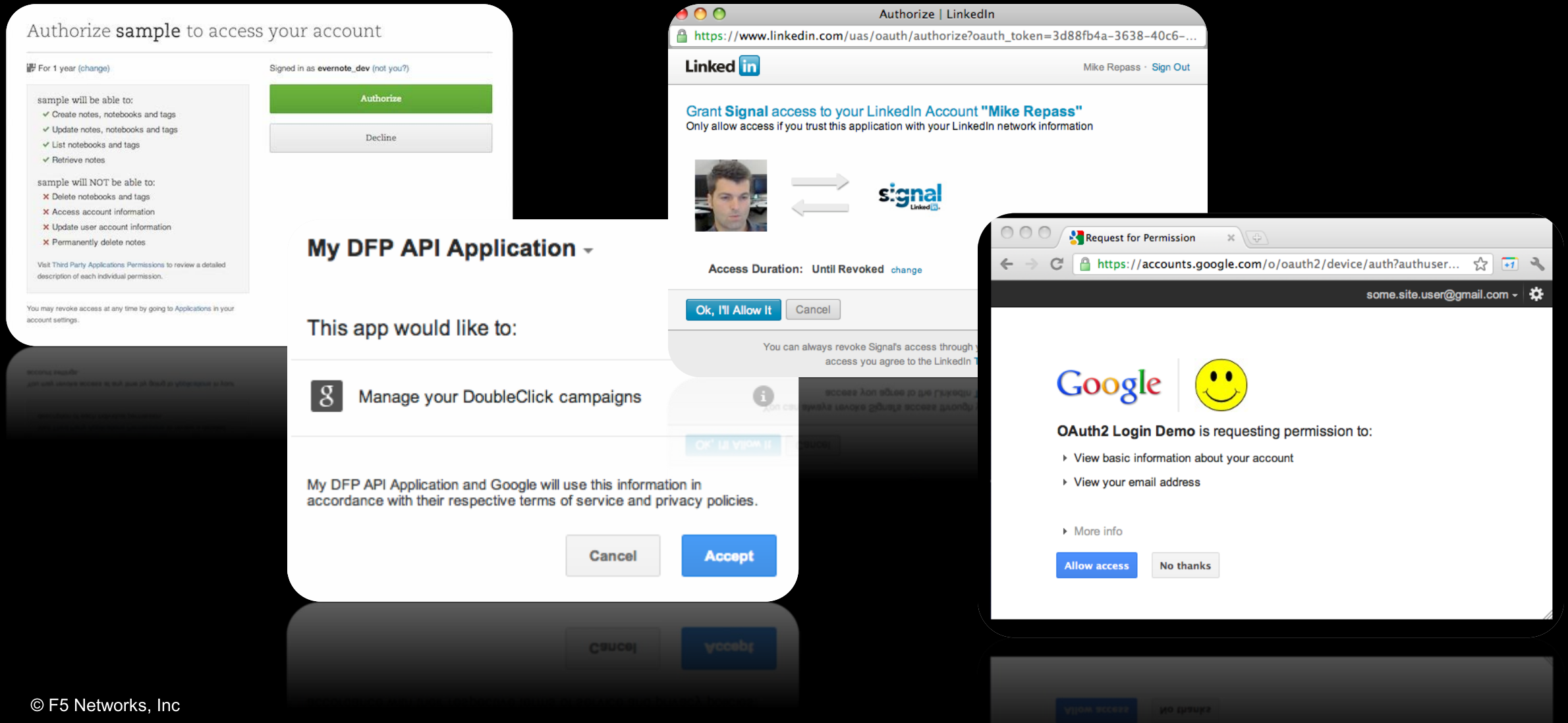
# OAuth: Authorization Flow



1. User accesses client application.
2. Application redirects the user to the AS for authentication. Upon authentication, the user is redirected back to the client application with an authorization grant.
3. Client retrieves access token from the AS by providing client id/secret and the authorization grant.
4. Client application accesses the user data on the resource server by providing the access token.

# OAuth: What Does it Look Like?

Here are a few examples of OAuth Authorization requests in some common services:



# OAuth: What Does it Look Like?

Client

Authorization  
Lifetime

Resource  
Owner

Authorization  
Decision

Scope

The screenshot shows an OAuth authorization interface. At the top, it says "Authorize sample to access your account". Below this, on the left, is a section for "sample will be able to:" with a list of permissions: "Create notes, notebooks and tags", "Update notes, notebooks and tags", "List notebooks and tags", and "Retrieve notes", all marked with green checkmarks. Below this is a section for "sample will NOT be able to:" with a list of permissions: "Delete notebooks and tags", "Access account information", "Update user account information", and "Permanently delete notes", all marked with red X's. At the bottom of this section is a link: "Visit Third Party Applications Permissions to review a detailed description of each individual permission." On the right side of the screen, it says "Signed in as evernote\_dev (not you?)". Below this are two buttons: a green "Authorize" button and a grey "Decline" button. At the very bottom, there is a note: "You may revoke access at any time by going to Applications in your account settings."

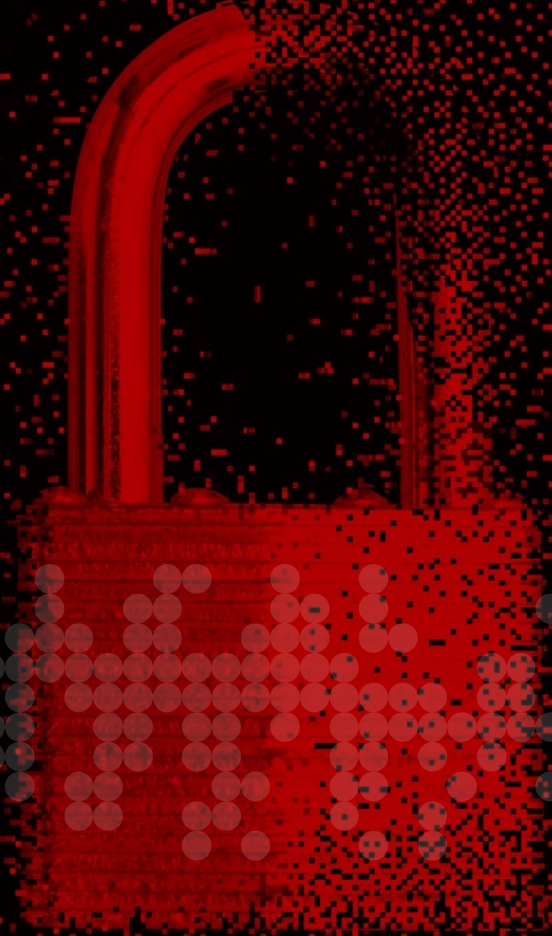


OAuth to be released on BIGIP  
Daytona v13.0



# Demonstration

OAuth beta release on v13.0





# Enterprise Mobility Management





# Magic Quadrant

- MobileIron
- AirWatch
- MaaS360
- XenMobile
- Good

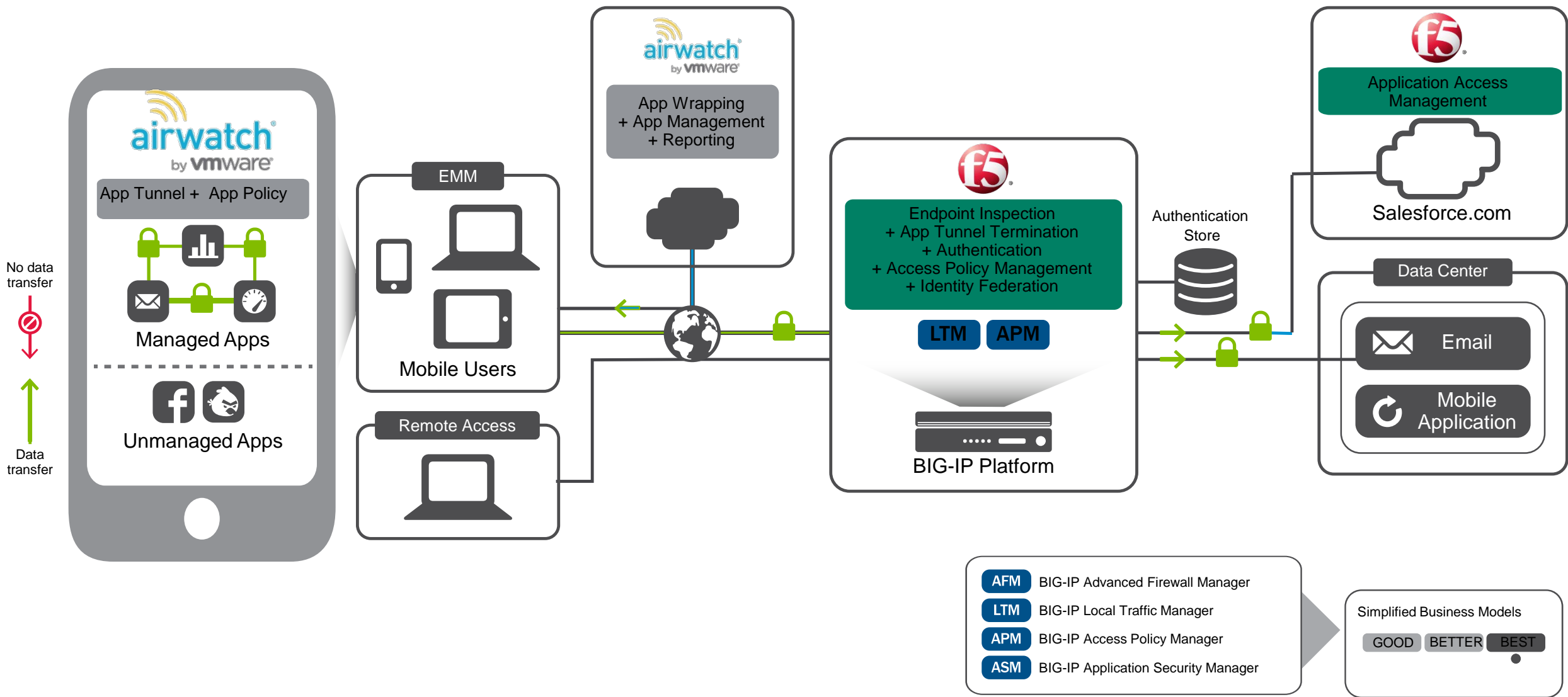
## Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Mobility Management Suites



Source: Gartner (June 2015)

# F5 and EMM



# How to communicate with EMM ?

## Retrieve Device Information

**Functionality** – Retrieves details of the device identified by device ID.

**HTTP Method** – GET

**API URI** – `https://host/api/mdm/devices/{id}`

You can obtain the device information using the following parameter:

- **Alternate device ID type** – `https://host/api/mdm/devices?searchby={searchby}&id={id}`

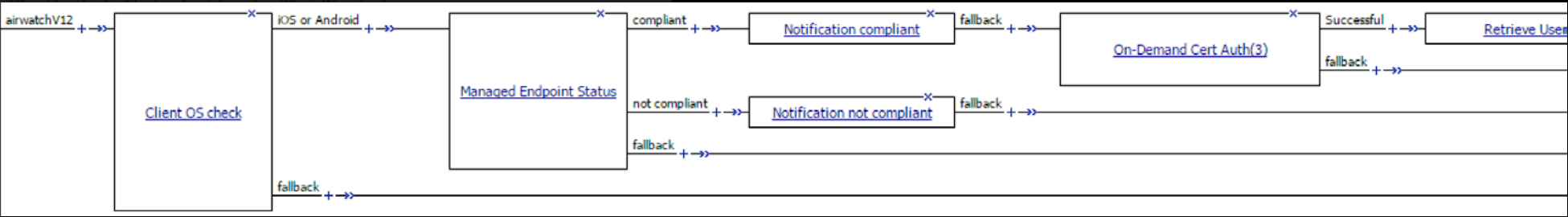
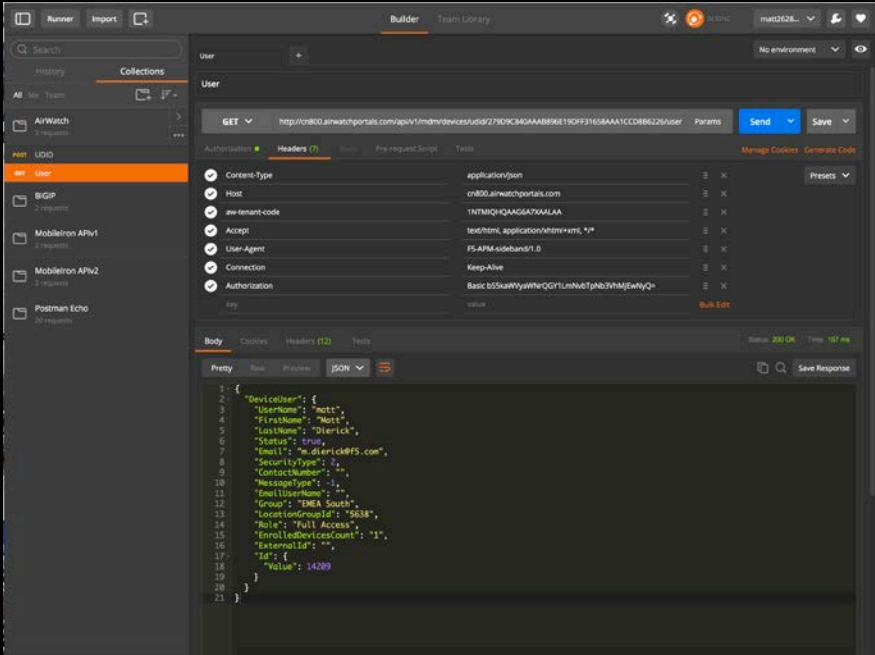
### URI Parameters

Tag	Description
searchby	The alternate id type (Macaddress, Udid, Serialnumber, ImeiNumber, Easid)

### Deprecated API URIs:

- **MAC Address** – `https://host/api/mdm/devices/macaddress/{macaddress}`
- **Serial Number** – `https://host/api/mdm/devices/serialnumber/{SerialNumber}`
- **UDID** – `https://host/api/mdm/devices/UDID/{UDID}`

**Request Body** – NA



# Full VPN, On-Demand, PerApp VPN

## When to use them ?

### Full VPN

- OS VPN SSL Tunnel
- Started manually
- All application can use it

### On-Demand VPN

- Started automatically
- Triggered on FQDN
- All applications can use it

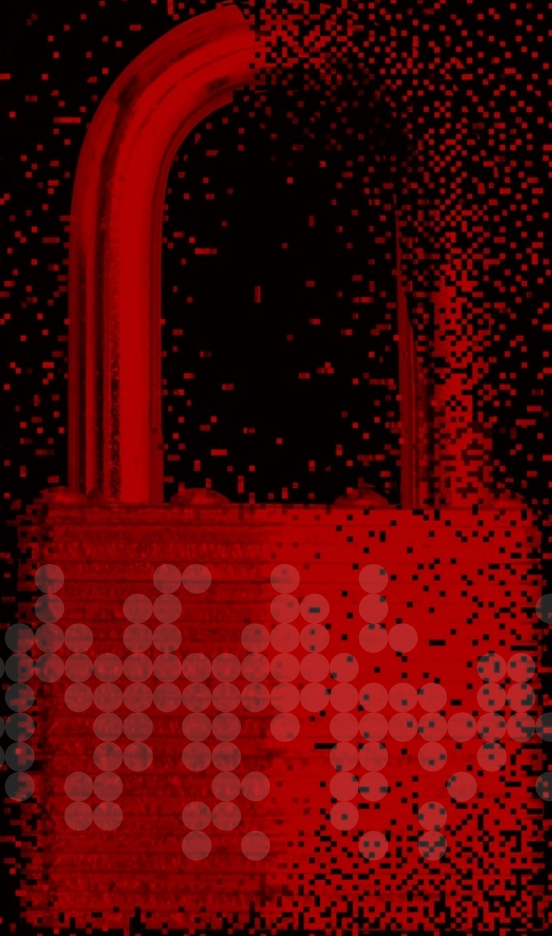
### Per-App VPN

- Started automatically
- Triggered on App starting
- Only apps allowed can use it
- EMM needed



# Demonstration

Device posture control via AirWatch



# How to protect credentials ?





# How to protect employees credentials ?

- Your employees have managed laptops
- Your employees connect to extranet / VPN gateway
- Your employees have AV installed
- But your employees have a MITB malware
- And this malware grabs credentials
- Let's have a look !!!!!



# How Malware Steals Bank Credentials

https://federate.f5.com

HTTPS REQUEST

HTTPS RESPONSE

Malware  
Infected Laptop



**f5**

for F5 Networks  
Having issues logging in?

Click [here](#) to submit a request to the IT HelpDesk

Username

Password

Logon

☐ Log me on automatically

This product is licensed from F5 Networks. © 1999-2015 F5 Networks. All rights reserved.

BIG-IP

**Web App**

**f5**

Secure Login  
for F5 Networks

Having issues logging in?

Click [here](#) to submit a request to the IT HelpDesk

Username

Password

Logon

☐ Log me on automatically



# How Malware Steals Bank Credentials

https://federate.f5.com



The screenshot shows the 'Secure Logon for F5 Networks' page. It includes a header with the F5 logo, a login form with fields for Username and Password, and a 'Logon' button. The Username field contains 'ericnelson' and the Password field contains 'pa55w0rd'. There is also a checkbox for 'Log me on automatically'.

Secure Logon  
for F5 Networks

Having issues logging in?

Click [here](#) to submit a request to the IT HelpDesk

Username  
ericnelson

Password  
\*\*\*\*\*

Logon

☐ Log me on automatically

This product is licensed from F5 Networks. © 1999-2015 F5 Networks. All rights reserved.

Malware  
Infected Laptop



ericnelson  
pa55w0rd

TO A DEN OF THIEVES



# FPS protected APM logon page

https://federate.f5.com

HTTPS REQUEST

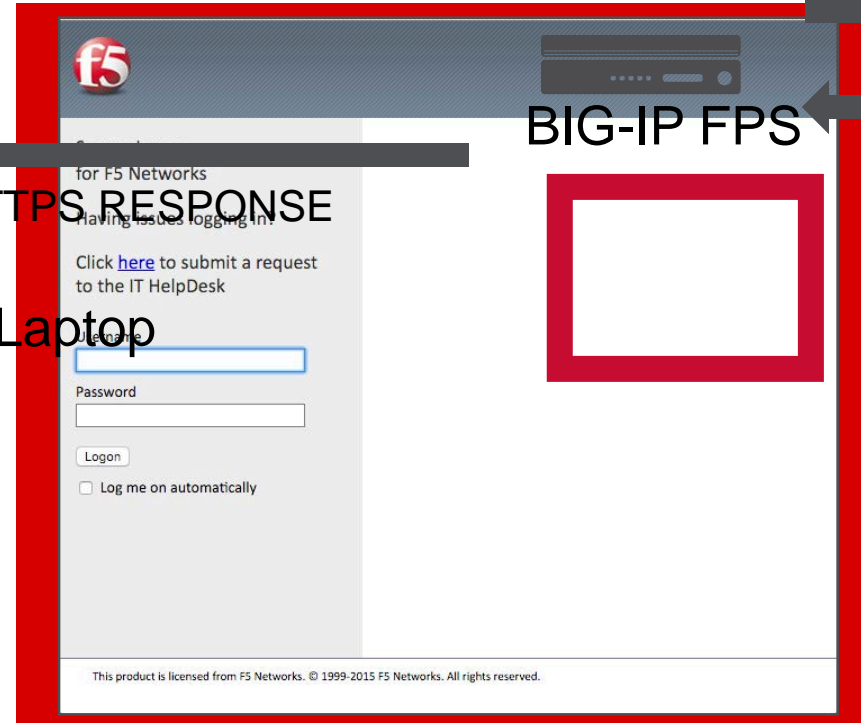
***FPS Module protects  
web page as it's  
delivered to user***

BIG-IP FPS

Web App

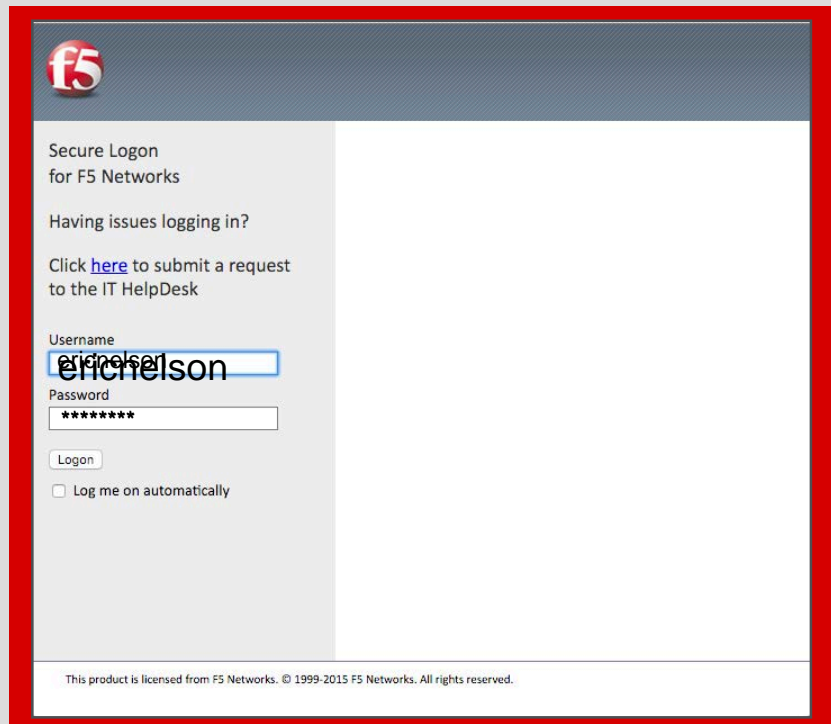
HTTPS RESPONSE

Malware  
Infected Laptop



# FPS protected APM logon page

https://federeate.f5.com



f5

Secure Logon  
for F5 Networks

Having issues logging in?

Click [here](#) to submit a request  
to the IT HelpDesk

Username  
ericnelson

Password  
\*\*\*\*\*

Logon

☐ Log me on automatically

This product is licensed from F5 Networks. © 1999-2015 F5 Networks. All rights reserved.

Malware  
Infected Laptop



STILL TO A DEN OF THIEVES

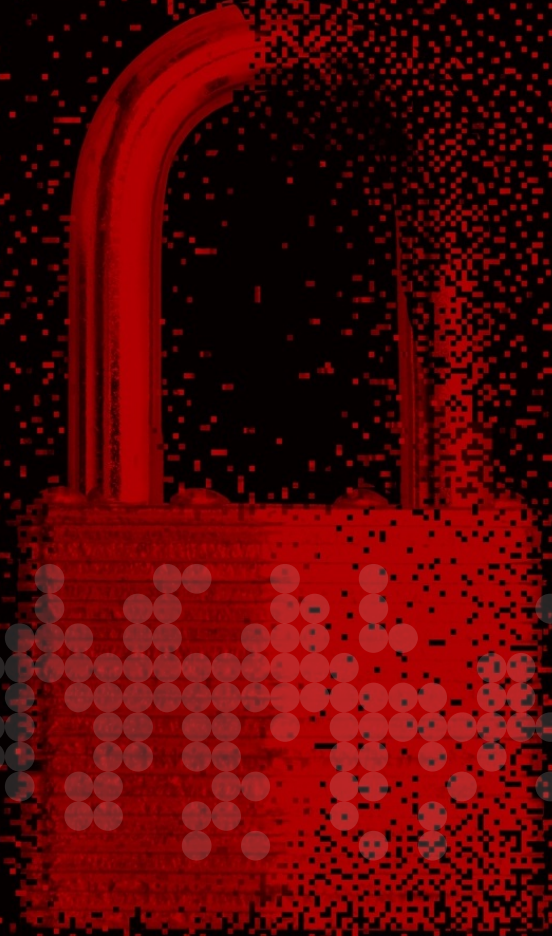
ericnelson  
a<iycQF"e[f|yU!18#fc\$yia

*But the data they get is  
useless!*



# Demonstration

Credentials encryption on top of APM



# To take away ...

- F5 solutions enable you to consolidate all your identity federation for on-premises and cloud applications
- With ADAL, O365 allows you to enable MFA on fat clients
- F5 solutions enable you to control device posture before granting an access to the applications
- F5 solutions enable you to protect users' credentials



**SOLUTIONS FOR AN APPLICATION WORLD**