

BREAKING THE MOBILE MOLD



Mark Vondemkamp
VP Security Product Management

B.Y.O.D.

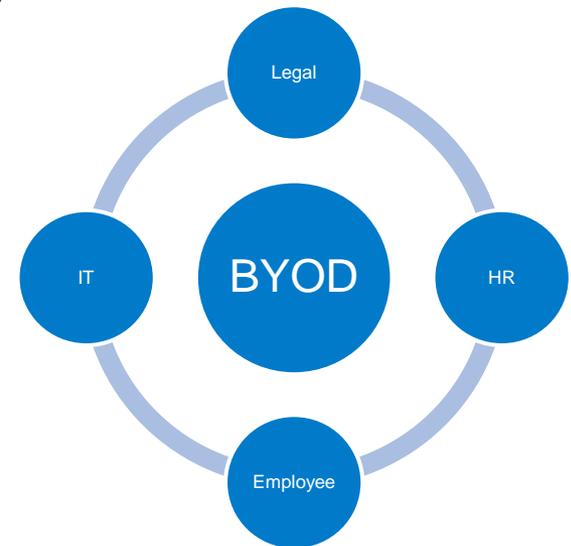
(Bring Your Own Device)



Bring-Your-Own-Device

Using personal devices for business

- Why implement BYOD?
 - Increase employee satisfaction, productivity
 - Reduce mobile infrastructure expenses
 - Reduce IT overhead
- Key issue areas
 - Protecting intellectual property
 - Controlling access to data and applications
 - Reporting



Critical Security Issue Then and Now

Top Security Concerns 2009

- **Mobility**
- Accidental or intentional unauthorized access to data especially sensitive data
- Compliance

“Network security continues to top the list of areas of concern”

THEINFOPRO
The Voice of the Customer



Top Security Concerns Today

- **BYOD**
- Unauthorized access to sensitive data
- Compliance

“BYOD Is Top Concern for Enterprise Mobile Security”
June 2012

Gartner.

BYOD 1.0: 2009-2012

Flaws in this approach:

- Imposes controls over user's personal device/experience
- Makes everything on the device an "enterprise" problem
- Difficult to VPN only corporate traffic



MDM: "Manage" the device

MDM Vendors

Access: "Connect" the device



BYOD 2.0: 2013+

**Builds on BYOD 1.0,
but evolves to:**

- Preserve user experience
- Secure/control enterprise data only
- Provides gateway tunnels data/apps (enterprise owned), NOT the device (user owned)



“Manage” *enterprise data and apps*

“Connect” *enterprise data and apps*

Mobile App & Device Management

Must-haves

Streamlined Admin Experience



Reporting

App
management

Intuitive End-user Experience



Secure PIM

App Store

Secure
Browser



App-level VPN

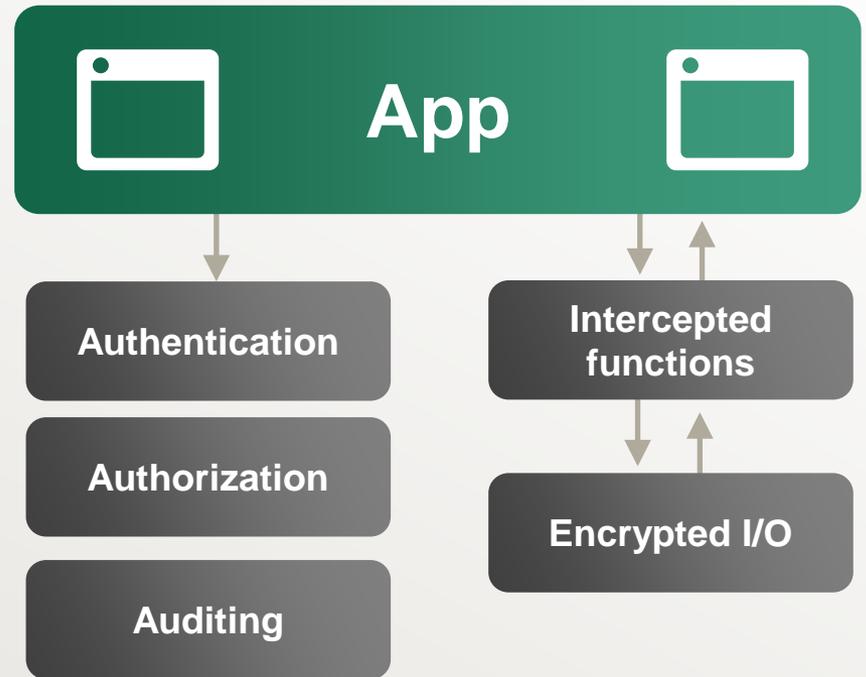
COMPLIANCE • SECURITY • MANAGEMENT

Application Wrapping

Adds app-level security

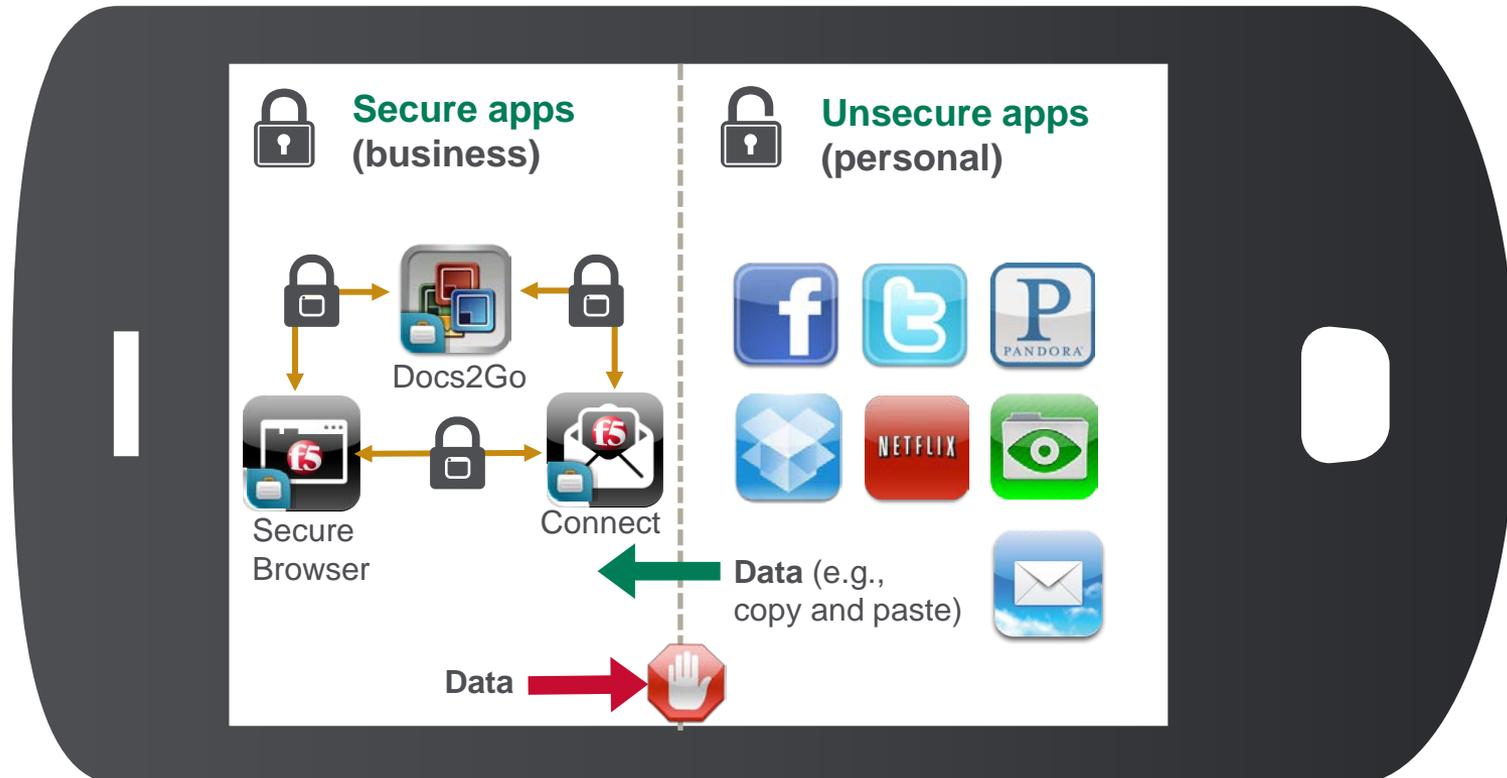


App wrappers can transform an app from an *unmanaged app* into a *secure, managed app*.



Creating a Secure Enterprise Workspace

Data sharing example



Secure Email, Calendar & Contacts

What employees and IT require

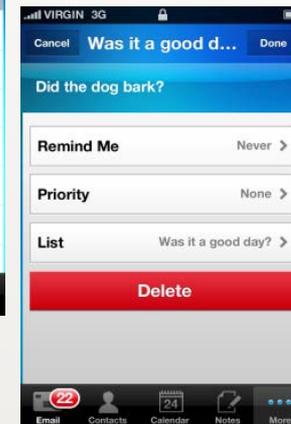
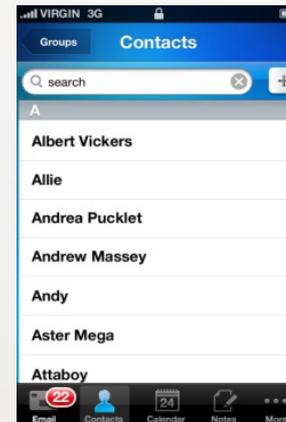
Integrated enterprise email, calendar, contacts, notes

Employees

- User experience
- Access to email, calendar and contacts

IT

- Exchange ActiveSync synchronization
- Push configurations for remote setup
- Global address list integration
- Secure storage and networking
- Manageable by IT



Managed Browser

Optimize your VPN investment

Secure connectivity for corporate-only use

Important Features

- Integrated blacklists and whitelists without reliance on proxies
- Enterprise proxy configuration
- Push configurations



Enterprise App Store

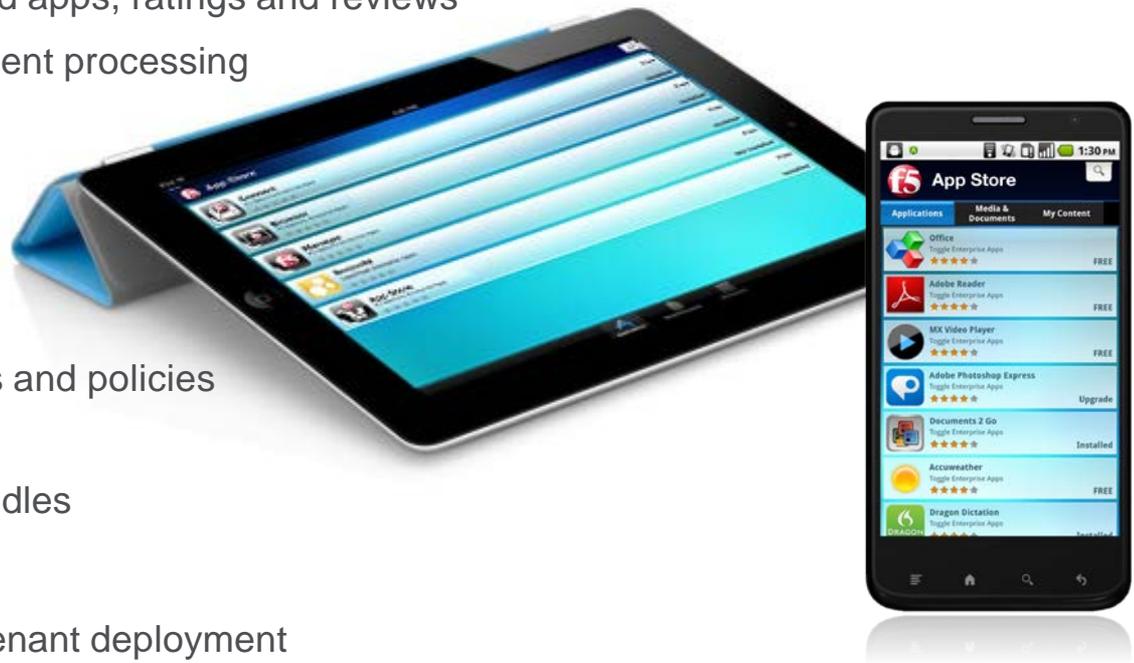
Enabling the mobile work-force with self-service

Enterprise content and application store

- Full-featured catalog including screen shots, descriptions, recent change history, featured apps, ratings and reviews
- Supports PCI-compliant payment processing
- Multiple app licensing models
- Restrict content based on role

App management

- Organize apps, content, users and policies into bundles
- Role-based distribution of bundles
- Push and pull apps
- Large-scale, multi-tier, multi-tenant deployment



Mobile App Management

Key features

Device management

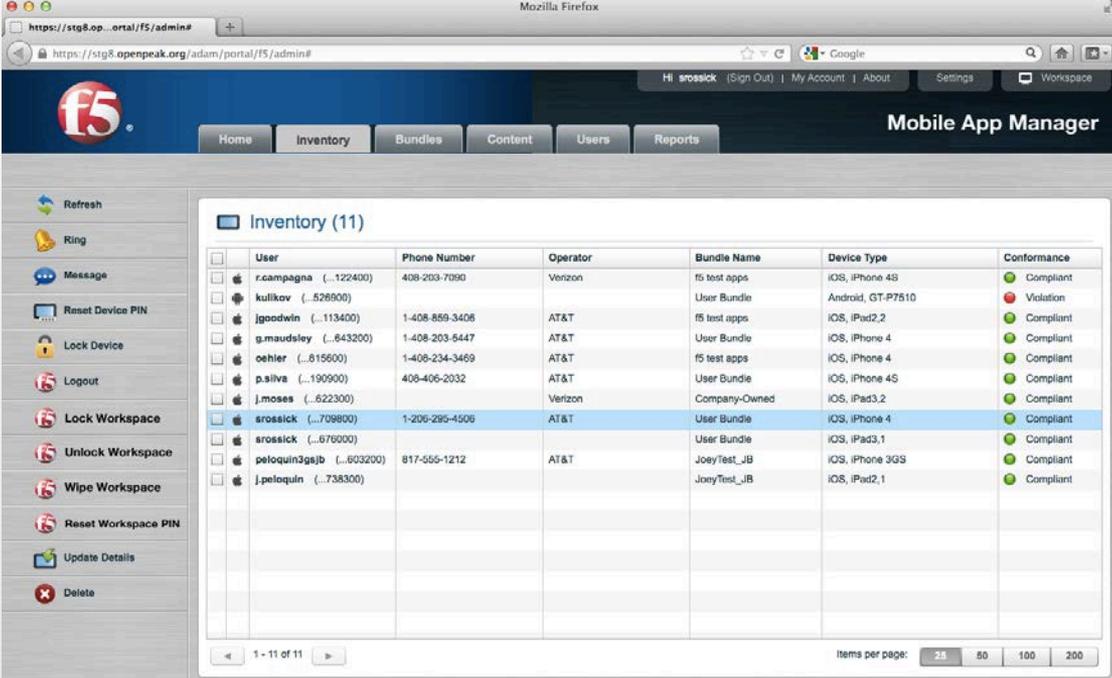
- Asset management: lock/wipe/reset
- Location tracking, status logging
- Device settings, network configuration

Policy-based management

- Criteria-based control (location, SSID, etc.)
- Password policies

User management

- LDAP/Active Directory integration



The screenshot shows the Mobile App Manager web interface in a Mozilla Firefox browser. The page title is "Mobile App Manager" and the user is logged in as "Hi srossick". The main navigation menu includes Home, Inventory, Bundles, Content, Users, and Reports. The "Inventory" section is active, displaying a table with 11 items. The table has columns for User, Phone Number, Operator, Bundle Name, Device Type, and Conformance. The user "srossick" is highlighted in blue.

User	Phone Number	Operator	Bundle Name	Device Type	Conformance
r.campagna (...122400)	408-203-7090	Verizon	f5 test apps	iOS, iPhone 4S	Compliant
kulkov (...528900)			User Bundle	Android, GT-P7510	Violation
jgoodwin (...113400)	1-408-859-3406	AT&T	f5 test apps	iOS, iPad2,2	Compliant
g.maudsley (...643200)	1-408-203-6447	AT&T	User Bundle	iOS, iPhone 4	Compliant
oehler (...815600)	1-408-234-3469	AT&T	f5 test apps	iOS, iPhone 4	Compliant
p.silva (...190900)	408-406-2032	AT&T	User Bundle	iOS, iPhone 4S	Compliant
j.moses (...622300)		Verizon	Company-Owned	iOS, iPad3,2	Compliant
srossick (...709800)	1-206-295-4506	AT&T	User Bundle	iOS, iPhone 4	Compliant
srossick (...676000)			User Bundle	iOS, iPad3,1	Compliant
pelouquin3gsjb (...603200)	817-555-1212	AT&T	JoeyTest_JB	iOS, iPhone 3GS	Compliant
j.pelouquin (...738300)			JoeyTest_JB	iOS, iPad2,1	Compliant

Mobile App Reporting

Key features

Advanced business intelligence

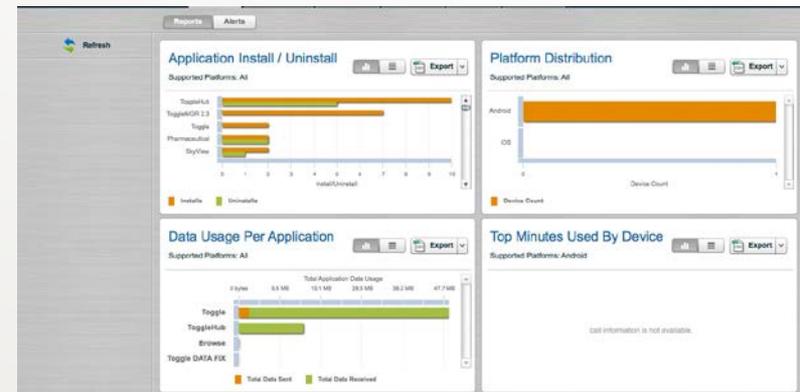
- Policy-driven reporting engine
- User logs
- Phone activity
- App activity

Device status reporting

- System settings
- Changes to settings
- Device and network usage statistics
- Location tracking

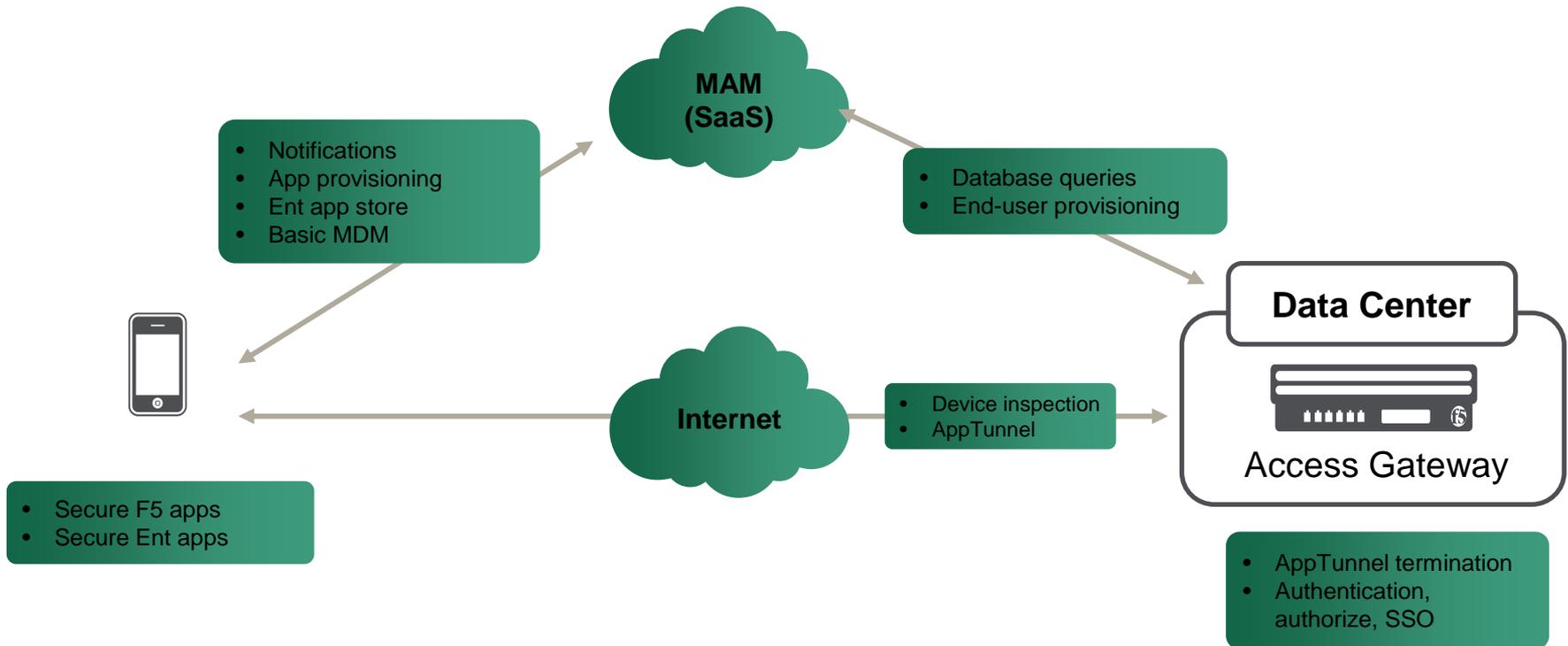
Application reports

- Downloads
- Revenue
- App usage



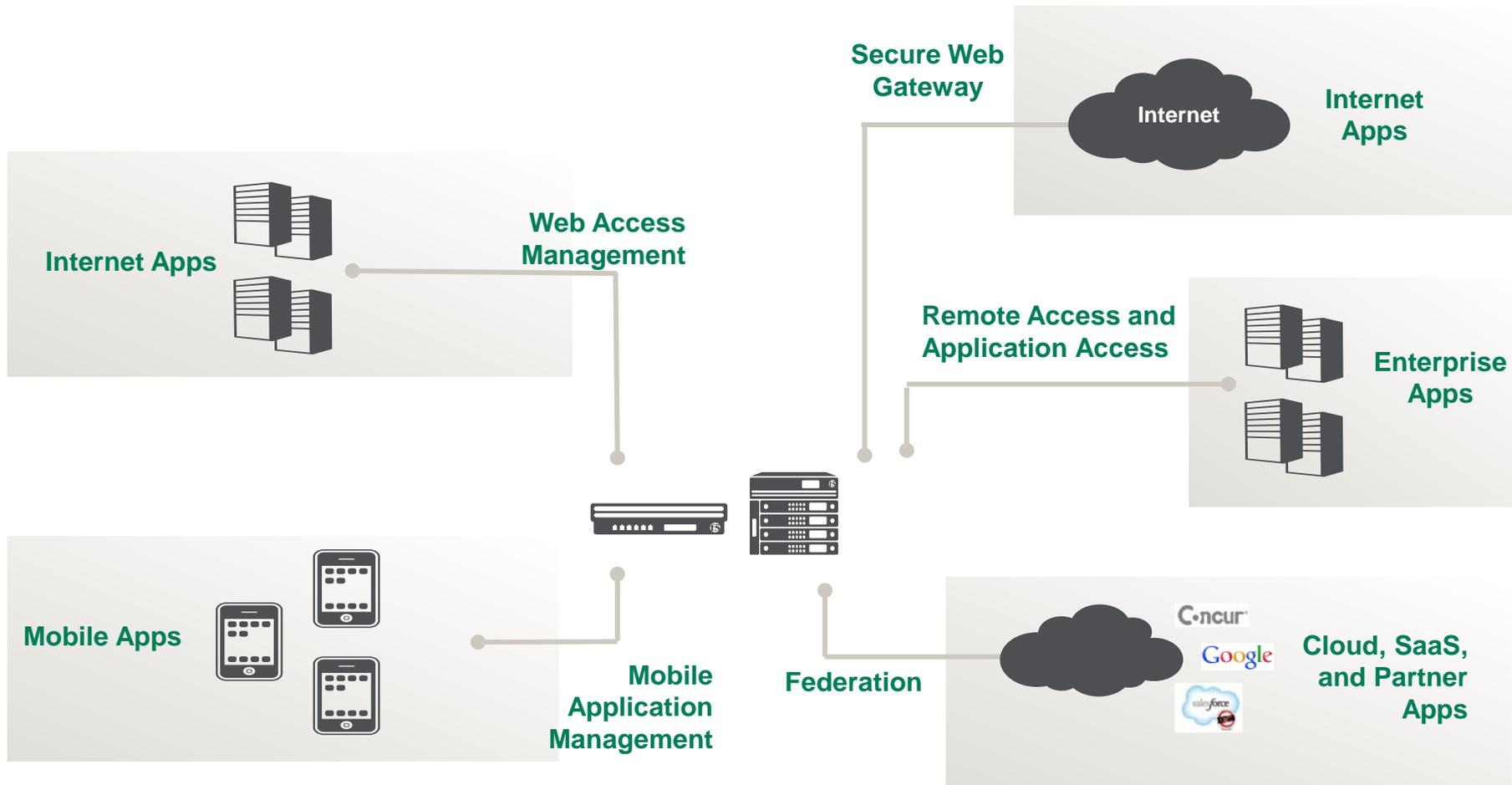
BYOD Architecture

App Mgmt + Network Access



Unified Access Solution

BYOD should be part of a larger solution



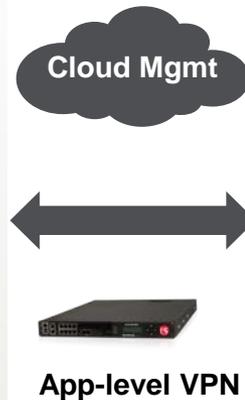
Summary

Streamlined Admin Experience



Reporting

App
management



Intuitive End-user Experience



Secure PIM

App Store

Secure
Browser

COMPLIANCE • SECURITY • MANAGEMENT



devcentral.f5.com

facebook.com/f5networksinc

linkedin.com/companies/f5-networks

twitter.com/f5networks

youtube.com/f5networksinc