



The Endpoint Evolution – Mobility

Gunnar Kristian Kopperud

Principal Presales Consultant
Security & Endpoint Management



The Endpoint Evolution – Mobility

- *Mobilitet er på alles agenda.*
- *BYOD brukes i hytt og vær, men hva er viktig og hva er nødvendig?*
- *Vi setter fokus på hvordan du som rådgiver kan hjelpe brukere og IT med å oppnå frihet og produktivitet samtidig som sikkerhet og pålitelighet ivaretas.*

Agenda

1 Redefining Mobile Protection and solving BYOD

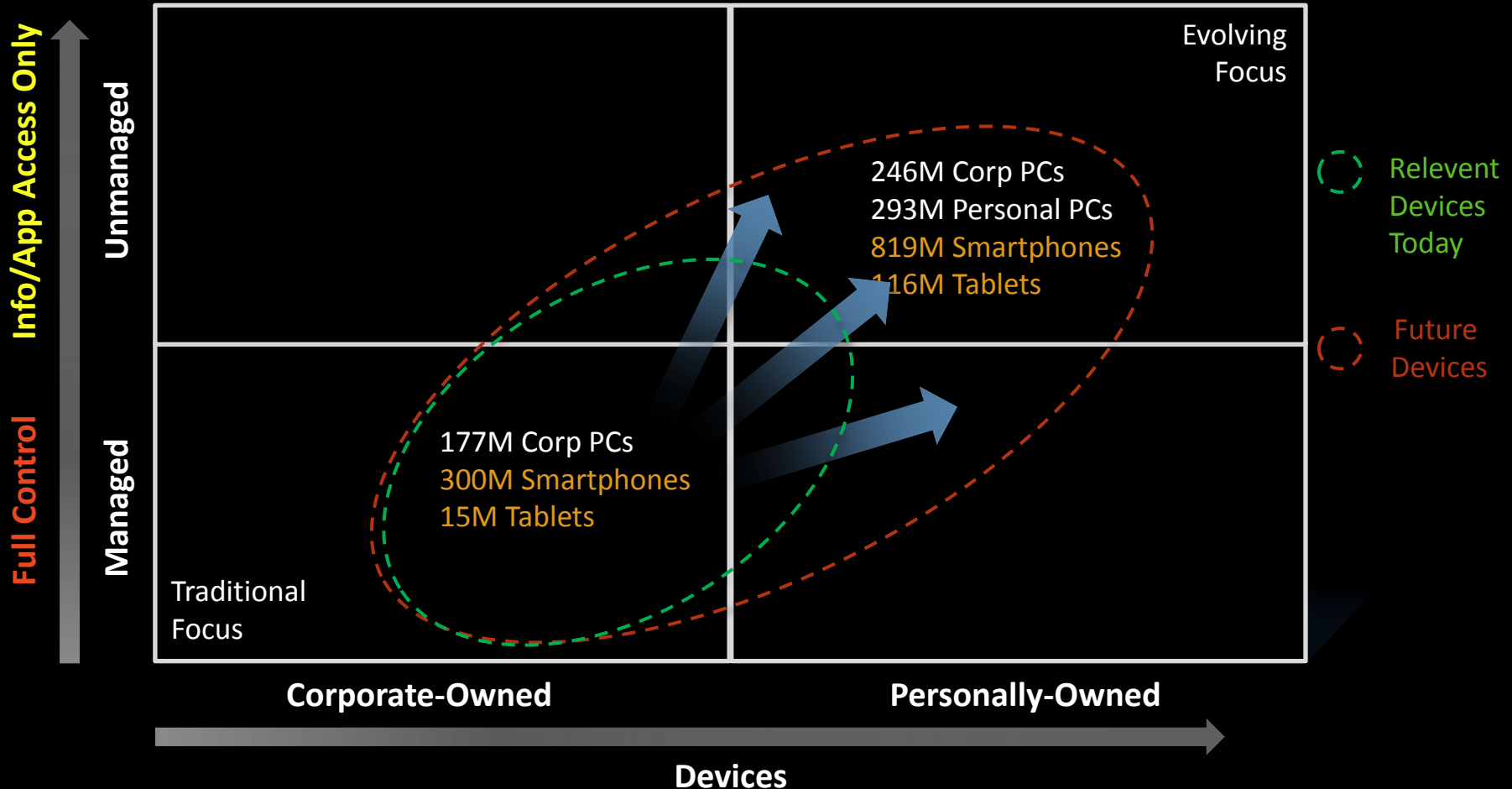
2 Mastering Control Points

3 Use Cases

4 Q&A

Consumerization is Driving disruption

Sources:
 IDC: 227941 and 227367)
 Gartner: G00212068, Apr 2011



New Frontiers and New Risks

“BYOD Adoption Is Growing Amongst EMEA Enterprise, Despite Security Concerns”



“Cisco Study: IT Saying YES to BYOD”

“...study showed a staggering 95% of respondents saying their organizations permit employee-owned devices in some way, shape or form in the workplace.”



“BYOD is Driving IT ‘Crazy’ says Gartner Analyst”



“IBM Banishes Apple’s Siri Due to Privacy Concerns”



End User Desires?



It must be fast

I want to stay flexible

I hate multiple phones..

I want to be the best I can

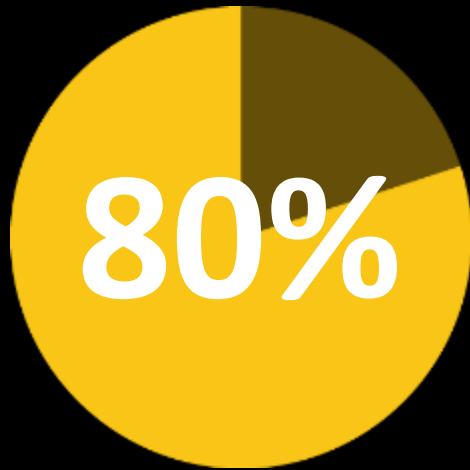
I use it when I need it..

I need access to business data

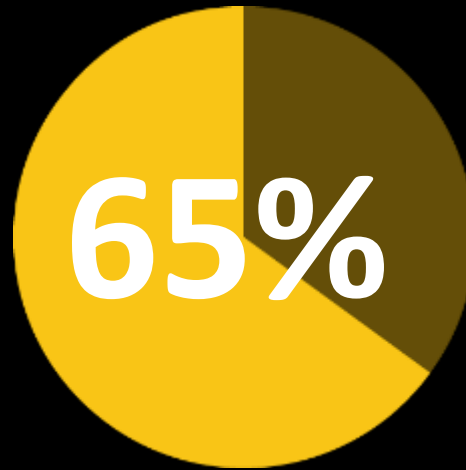
I need to share stuff..

I want a pink laptop..

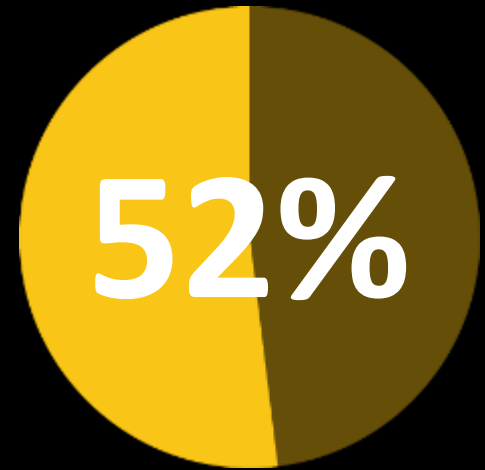
Technology at Work Is Changing



New apps deployed
in the cloud



Allow access to
their network

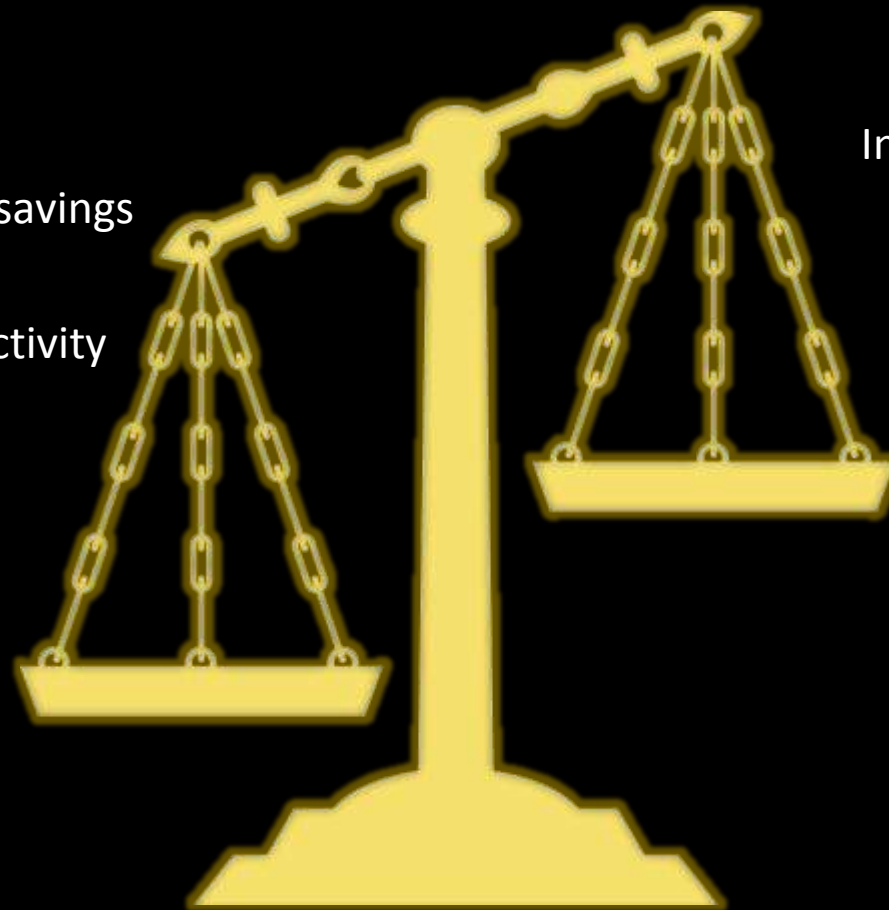


Workers use three
or more devices

Upside: BYOD Offers Tangible Business Benefits

Benefits

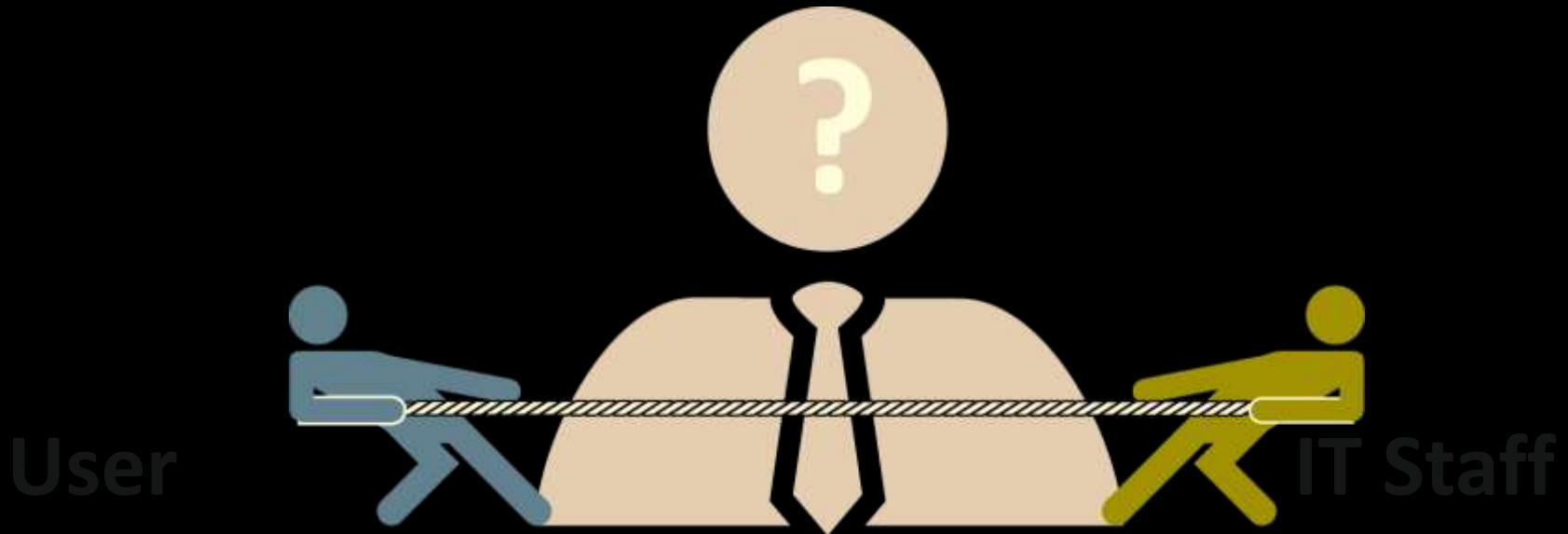
- Hardware procurement savings
- Contract plan savings
- Increased worker productivity
- Employee satisfaction
- Competitive advantage



Risks

- Information security
- Legal

The Desires of the User Versus IT Staff



Freedom, Privacy & Productivity

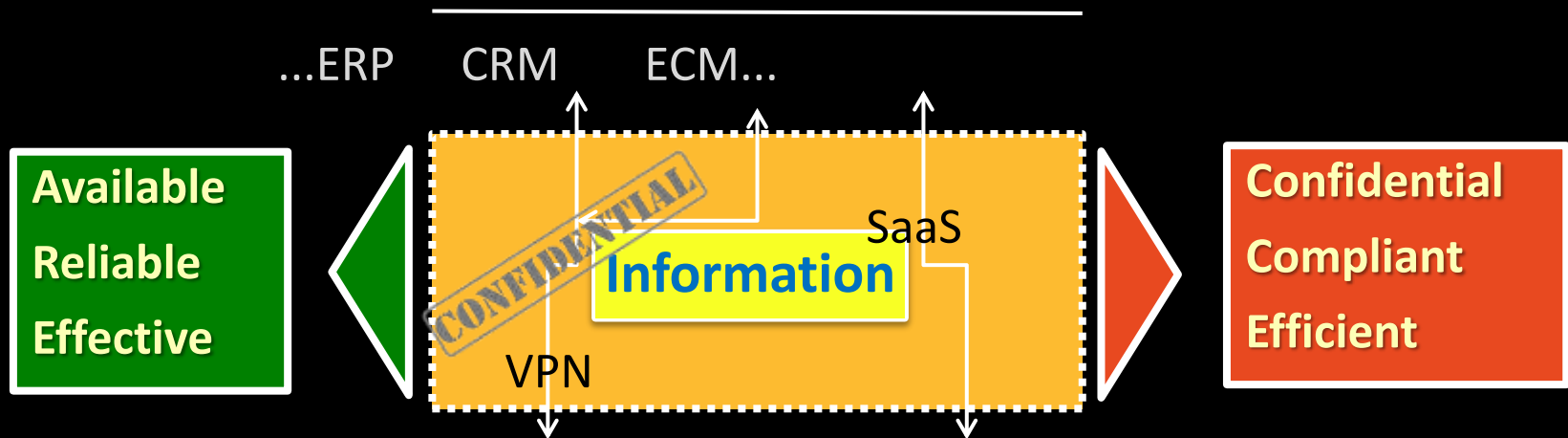
- Easy access to files, apps, email
- Use the latest technology & apps
- Personal stuff is untouched
- Do it themselves (i.e. Self-Service)

Simple, Secure & Reliable

- Protect company information
- Only let authorized users in
- Easy to work with and reliable
- Reporting, audit & monitor

Embracing Information Centricity

> Business Process <



Mastering Control Points ...

Success = Mastering Control Points



Devices



Apps



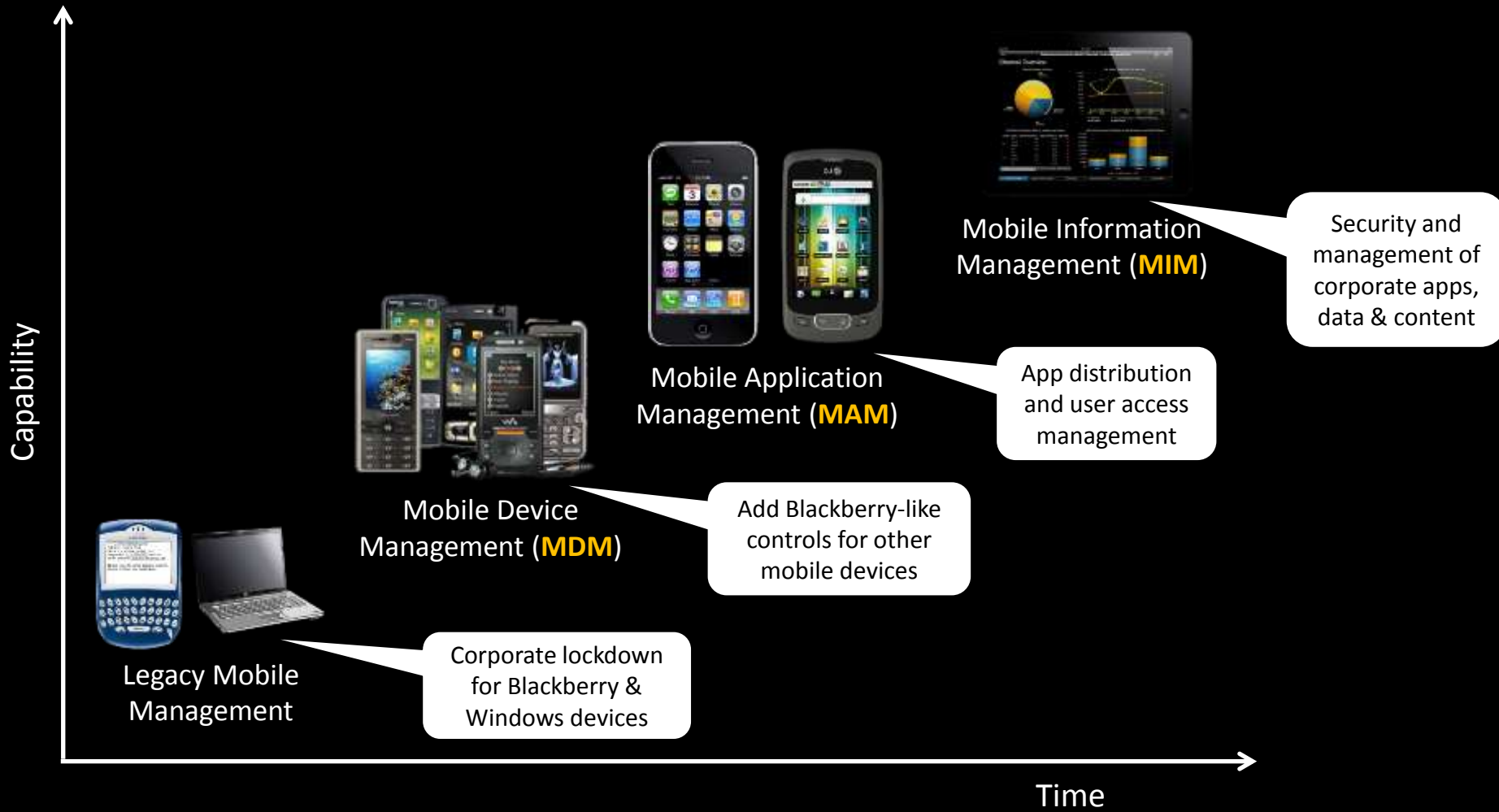
Data



Mapping Mobile Adoption



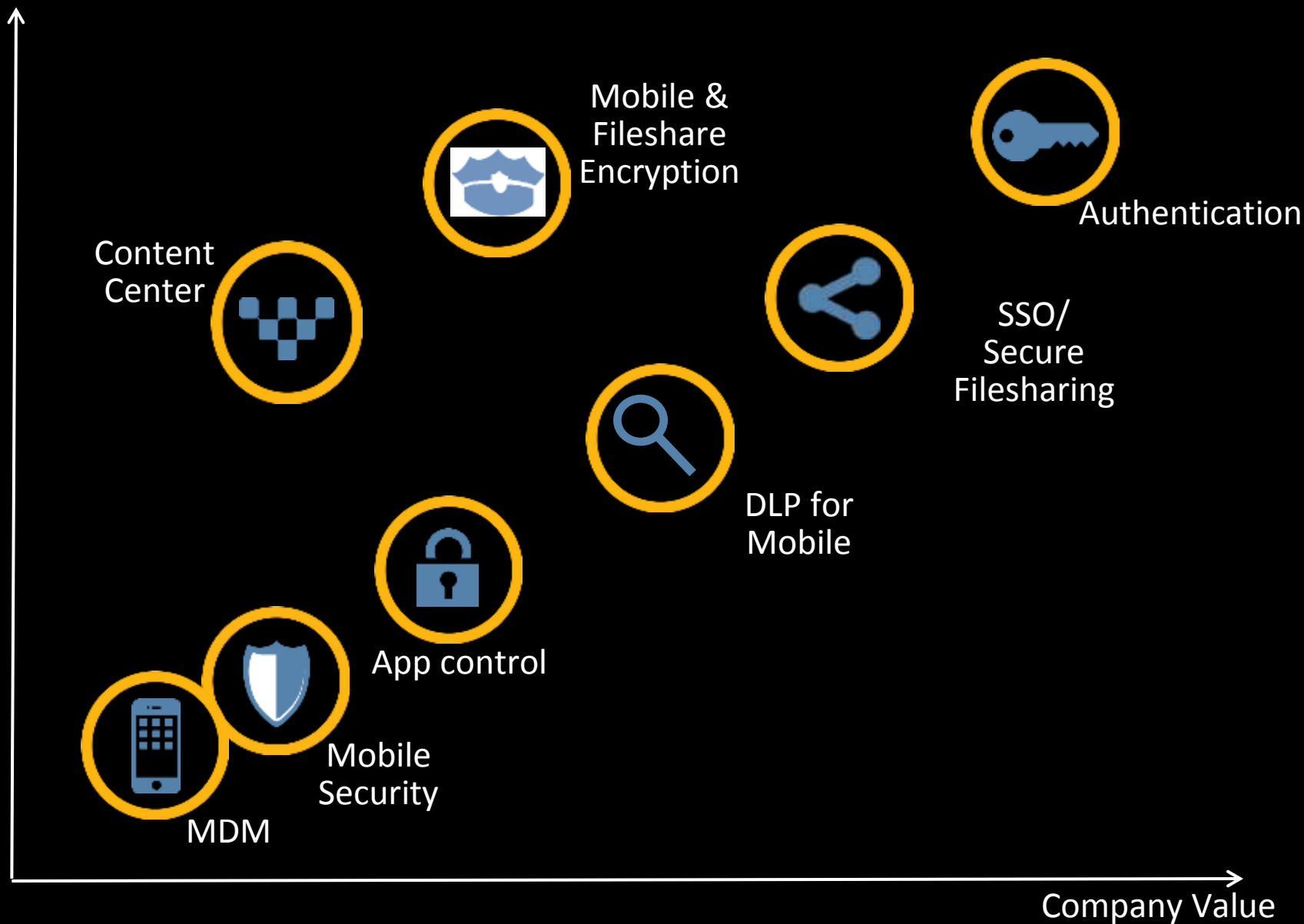
Evolution of Mobility Management



5 Pillars for Enterprise Mobility

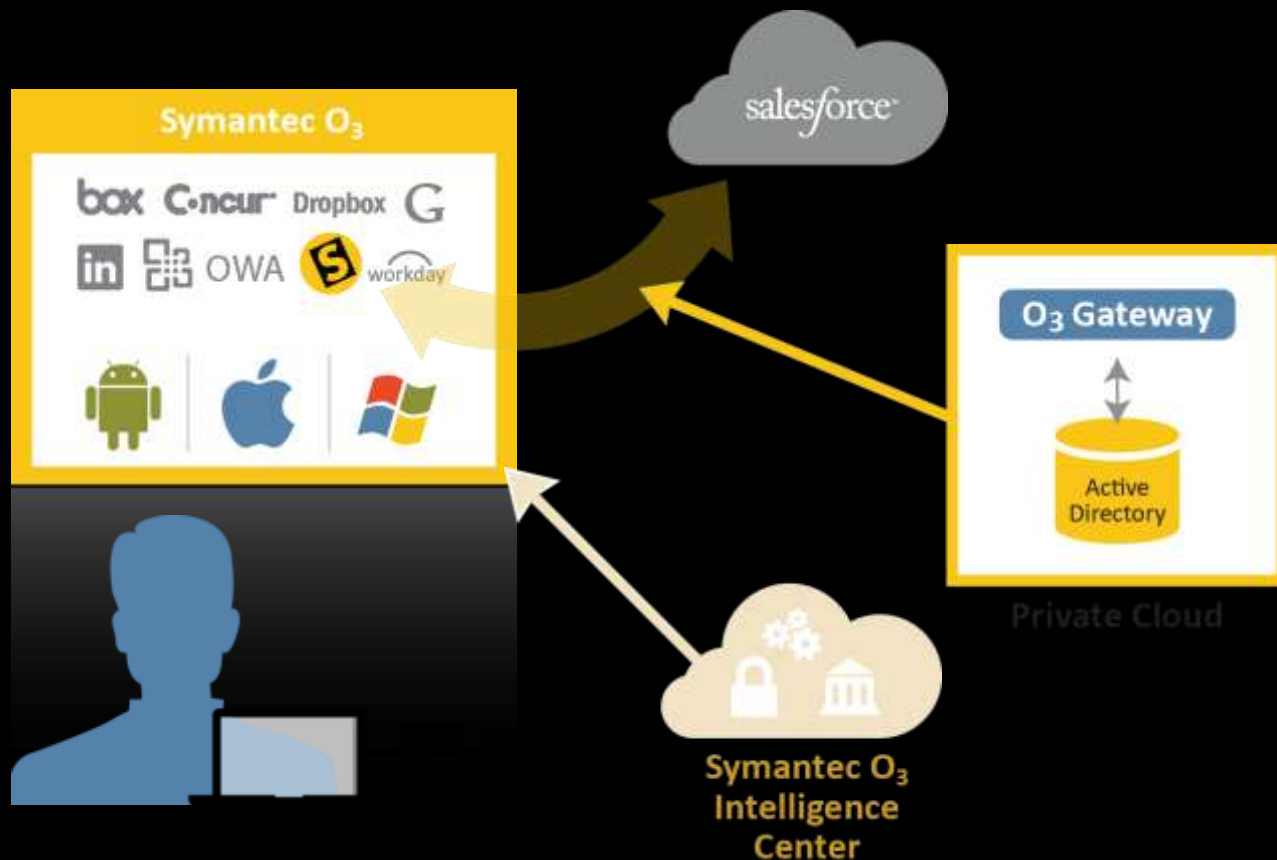


End user Value



Use cases

Use Case #1: Access SaaS Apps From Any Device



Why Symantec O₃



Proven Infrastructure

Works with federated and non-federated apps

Highly Scalable

Leverages existing infrastructure

Capture Security Events

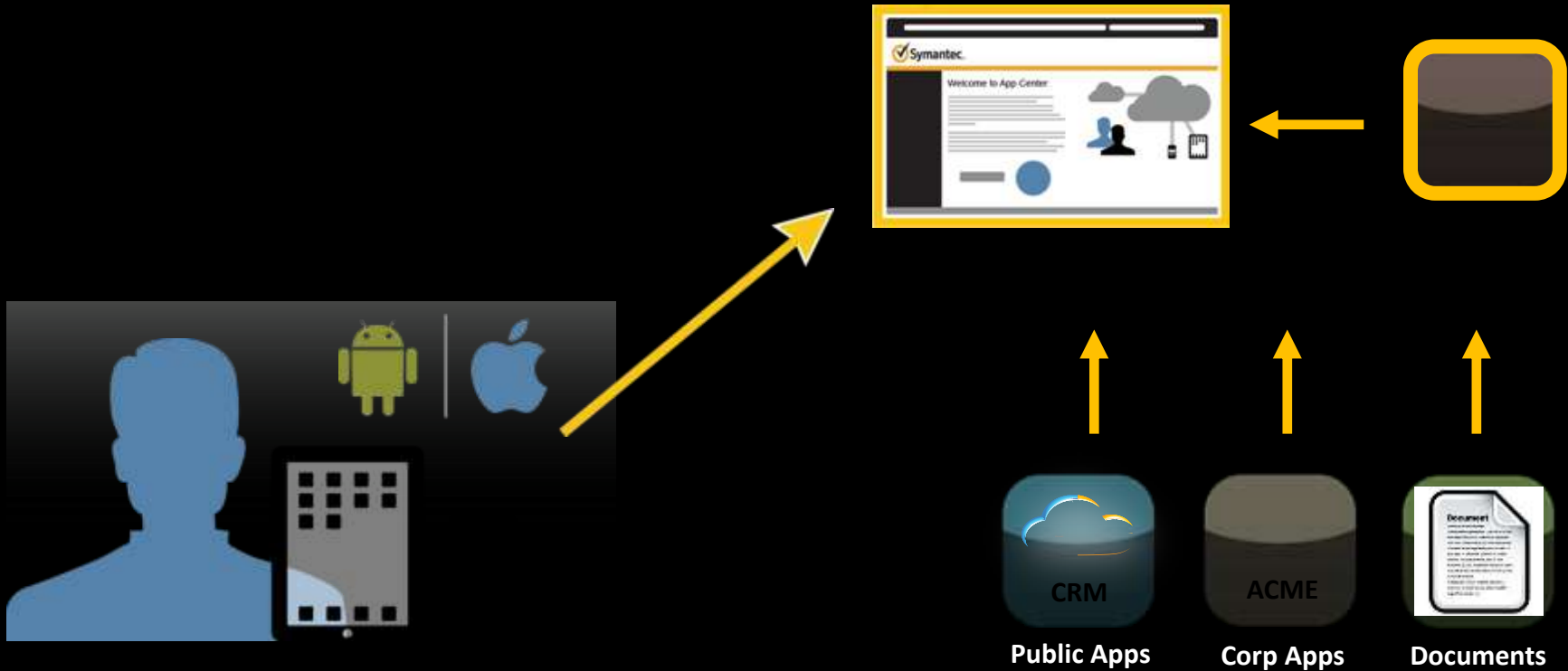
Correlation of security intelligence

O3 Single Sign On to SaaS

Demo

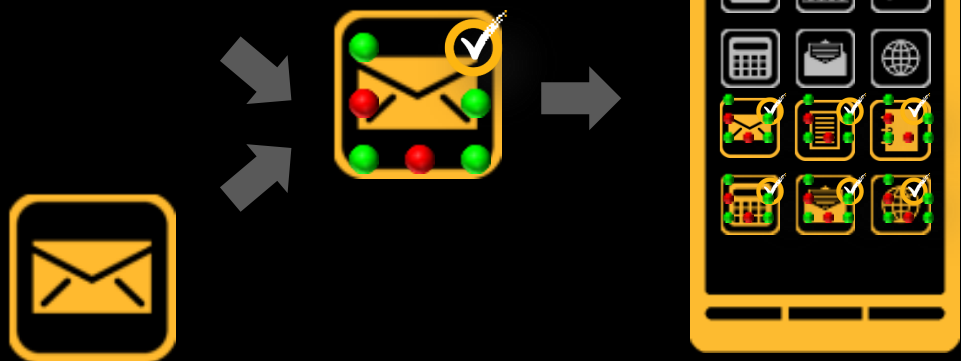
Use Case #2:

Enable BYOD – Separate Private/Corporate info



App Management & Protection

User authentication required?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Allow local storage?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Off-line access allowed?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Run on jailbroken devices?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Restrict API's (doc sharing, etc.)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Restrict network connections?	<input type="checkbox"/>	<input checked="" type="checkbox"/>



Personal Data
Corporate Data

Symantec App Center

End-to-End Process is EASY



App/Content Administrator



Upload app to console

Select policy settings for app

Select target group and apply



End user



Login to App Center

Get the Apps

App Center

Demo

Comprehensive Mobile App Management

Deploy Apps

Enterprise app store for internal apps
Recommendations from public appstore
Group based targeting



Deploy Content

Enterprise content store for docs, videos
Containerize data with per object policies
Group based targeting



Manage Lifecycle

Revoke and update apps selectively
Centralized visibility & control
MDM features for policy management



Protect Data

Security and Management layer around data
Passwords, encryption, offline access, rooting
Separate corporate and personal data



Symantec App Center Enables Productivity

Mobilize Apps & Content

In-house Store

- Distribute/Update/Revoke specific apps/content
- Web, Native, HTML5 – in-house, external apps
- PDF's, Videos, ePub documents, Forms

User and IT Friendly

- Consumer-style portal, reviews, screenshots
- Corporate Branding
- Versioning and expiration options



Symantec App Center Secures Corp Data

Mobilize Apps & Content

Enterprise Security Policies

- Authentication: LDAP/SAML – online, offline access
- Encryption: FIPS 140-2, AES 256 – for all selected data
- Data Loss Prevention: Copy-paste, Sharing restrictions

Advanced Protection: Targeted Data

- Corporate Apps and data are containerized
- Applies to in-house, custom or third party apps
- No source code changes required

Note: Creating an app policy will automatically modify the admin password policy for maximum protection.


Name

Authentication User authentication required

- Re-authentication required after minutes of idle.
- Offline authentication permitted (not supported by Android 2.2)
- Destroy data and disable app upon password lockout.

On-Device Storage Allowed


- Encryption required
- Clear data on app close

 The following On-Device Storage options are effective for Android only


- Permit SDcard storage

Usage Restrictions Block inter-app document sharing

- Block clipboard copy operations. (Not supported for Android Secure Web Apps)
- Destroy data and disable app on jailbroken (iOS) or rooted (Android) devices.

 The following Usage Restrictions are effective for iOS only

- Block iTunes file sharing. (This setting is not updated dynamically)
- Block iCloud file sharing

 The following Usage Restrictions are effective for Android only

If the client is removed or MDM is disabled:

- Allow data and app access.
- Block app from running.
- Destroy data and disable app.

Poll Server Automatically connect to the server to check for updates.

Check for updates every hours

- Fail-Safe Revocation Timer

Symantec App Center Truly Solves BYOD

Clear Separation of Corporate & Personal Data

Allow Personal Devices

- Access to corporate information, securely
- Auto-configuration of settings like Wi-Fi, VPN
- Lock and wipe specific corporate data only

Privacy - Addressed

- No device level controls
- No monitoring of device apps or data
- Focus on corp. data and apps vs. entire device



Personal Data / Apps

Corporate Data / Apps

- Per-app policies
- Pinpoint revocation

Extends Containerization to Third-Party Public Apps

- Delivery through vendor app stores
- Apps with built-in Symantec security technology
- 150+ commercial apps



Moxier Mail

Enterprise Email with direct push



Polaris Office

Mobile Office to edit MS Office docs



Good Reader

PDF reader with annotation features



Barcode Essentials

Instant access to asset management workflows



iKonic Mail

Secure access to enterprise email



Xavy

Connects to MS Lync & Office Communicator



iAnnotate

Read, Annotate and Share PDF documents



Picstel Smart Office

View, Create, Edit and Share Office documents

<http://www.symantec.com/app-center-ready>

Why Symantec for Mobile Apps



Quick & Easy

Expedite deployment of apps with an easy-to-use SaaS app store

Scalable & Seamless

Enable any number of apps with no source code changes

Independent of MDM

Address mobile application needs without managing the complete device

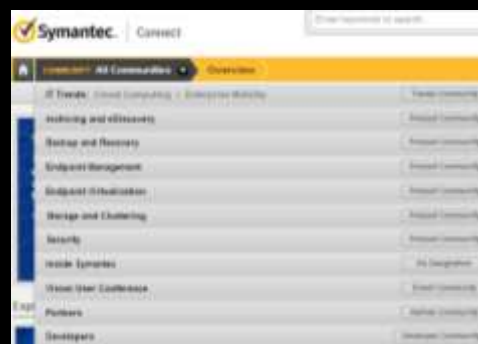
Bringing It All Together



Devices. Apps. Data.

Kontakt oss på:

- Symantec Brukerforum
 - <http://www.symantec.com/connect>
- Symantec Norge på Facebook
 - <http://www.facebook.com/SymantecNorge>
- Norton Norge på Facebook
 - <http://www.facebook.com/norton norge>
- Symantec Norge på Twitter
 - <http://twitter.com/SymantecNorge>
- Lisenser og Support
 - Tips: rapporter på web - ring etterpå
 - <http://my.symantec.com/>





Thank you!

Gunnar Kristian Kopperud

gkopperud@symantec.com

+47 480 18 908

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

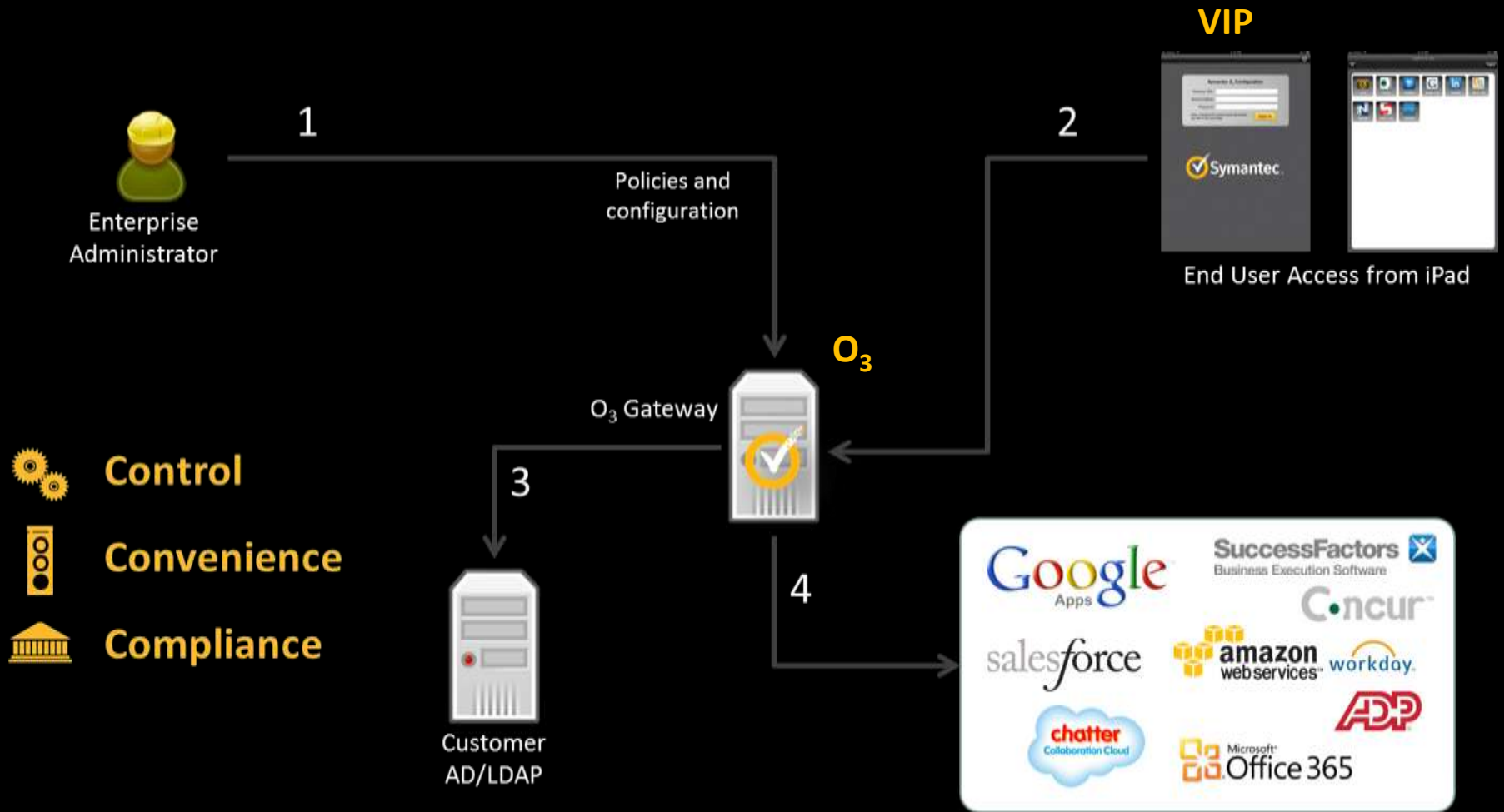
Other Use Cases

User & App Access



+ Symantec **O₃**
Symantec Validation and ID Protection Service (**VIP**)

User & App Access



App Driven Use Case

Distribution, Data Separation & DLP



✓ MAM w/ App Wrapping

Single Sign-on & Cloud Gateway



✓ O3

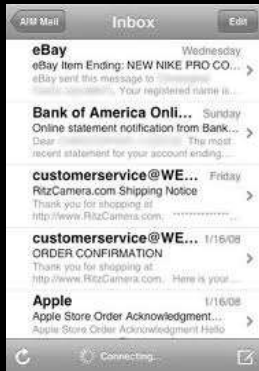
Built-in Strong Authentication



✓ VIP

Email Driven Use Case, Continued

Provision, Policy Control,
Selective Wipe



✓ MDM w/ Native Email Client

Data Loss Prevention, Encryption,
Data Separation



✓ MAM w/ Third Party Email Client

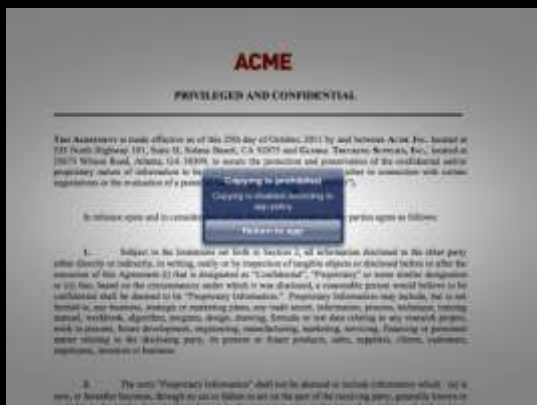
Integration with Enterprise
Encryption Email System



✓ PGP Viewer w/ Native Email

Data Security Driven Use Case

DLP on Device



MAM / App Wrapping

DLP Integrated with Network



for Mobile

App/Data Encryption



FIPS 140-2 Protection

Authentication Driven Use Case

Two-Factor Authentication



✓ MPKI & VIP

2FA for Applications



✓ VIP SDK

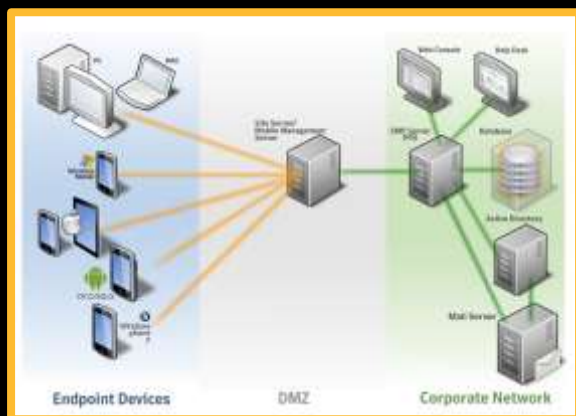
Single Sign-on for SaaS



✓ O3

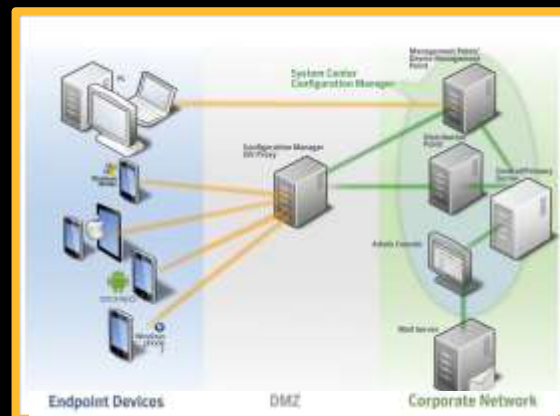
Management Driven Use Case

Altiris



Mobile Management w/ Altiris

Microsoft SCCM



Mobile Management for SCCM