Securing Devices in a UX-Centric World

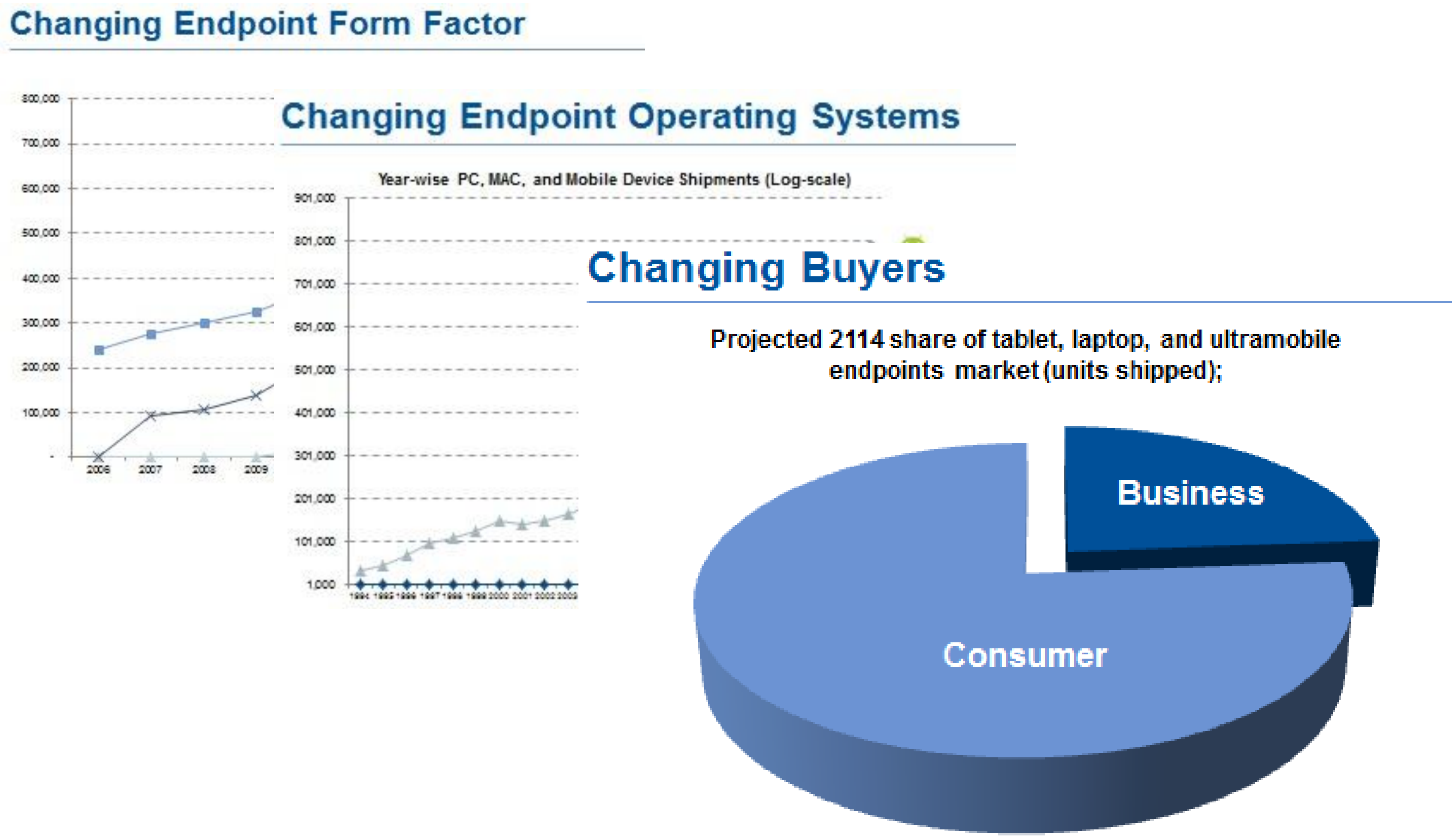
Bryan Taylor

Research Director

Tweet:#GartnerLOC

Gartner®

Change is Constant



Changing Endpoint Form Factor

Changing Endpoint Operating Systems

Year-wise PC, MAC, and Mobile Device Shipments (Log-scale)

Changing Buyers

Projected 2114 share of tablet, laptop, and ultramobile endpoints market (units shipped);

Are We Done Yet?

Nope, just getting started!

Agenda

- How is mobile security impacted by users' demands for a quality experience?
- How can organizations balance the often conflicting demands of users with the need to secure enterprise resources?

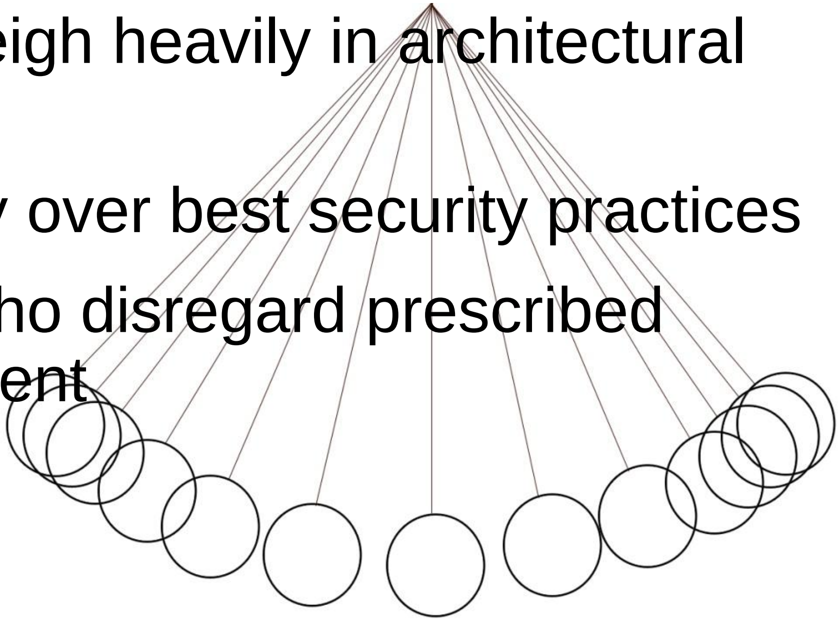
Agenda

- How is mobile security impacted by users' demands for a quality experience?
- How can organizations balance the often conflicting demands of users with the need to secure enterprise resources?

The Pendulum Swings

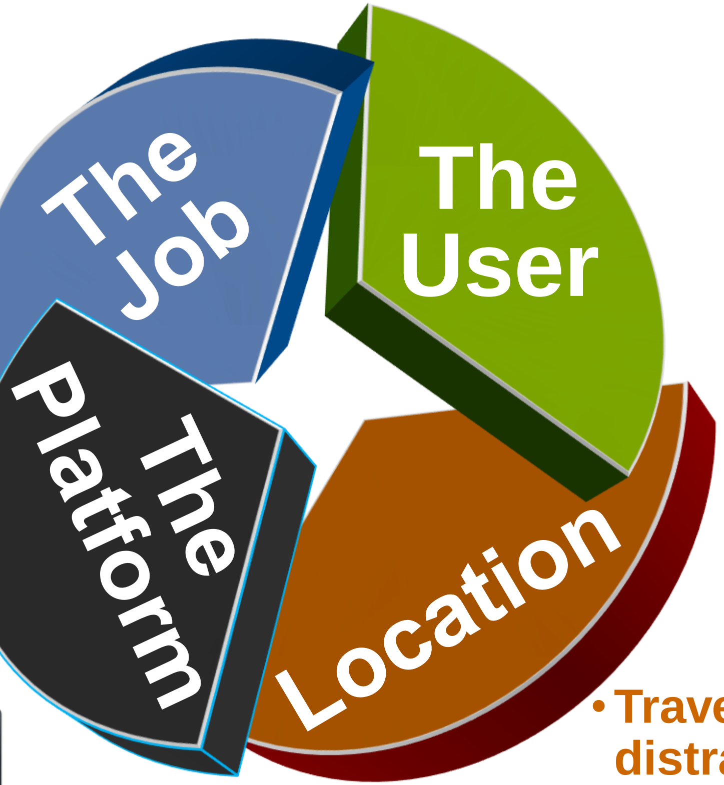
UX Trumps Security in Many Organizations

- User device preferences have driven the rise of BYOD
- Executive push-back results in altering requirements or changing toolsets
- User experience factors weigh heavily in architectural and tooling strategies
- Polices often favor usability over best security practices
- Consequences for users who disregard prescribed policies is light or non-existent



Scoping the Mobility Security Problem

- Process, data fragmentation
- Unmanaged, nonstandard apps
- Ad hoc app and data sharing



- Personal productivity focus
- Business process rebellion
- UX trumps accountability

- Fragmented app, platform security standards
- Incomplete management
- Bring your own device challenges
- Multiple devices

- Travel distractions
- Uncontrolled environments
- Exceptions and surprises

BYOD Reduces Your Policy Scope

Feasible	Debatable	Unenforceable
Passcode length, retry, timeout, lockout	Strong authentication	Camera, mic, cloud sync controls
"No jailbreak" rules	App whitelisting	App blacklisting
Secure single apps	Containerized apps	Complex containers
Expense management	Real-time location tracking	Behavior and usage monitoring
Min/max version access controls	Forced updating and patching	Full device image, backup/restore
Certificate controls	"Call-home" apps	Full device inventory

"Our BYOD policy was successfully introduced in the USA — everyone opted in. Then we tried to implement it worldwide and discovered we were breaking dozens of laws."

— *Gartner client*

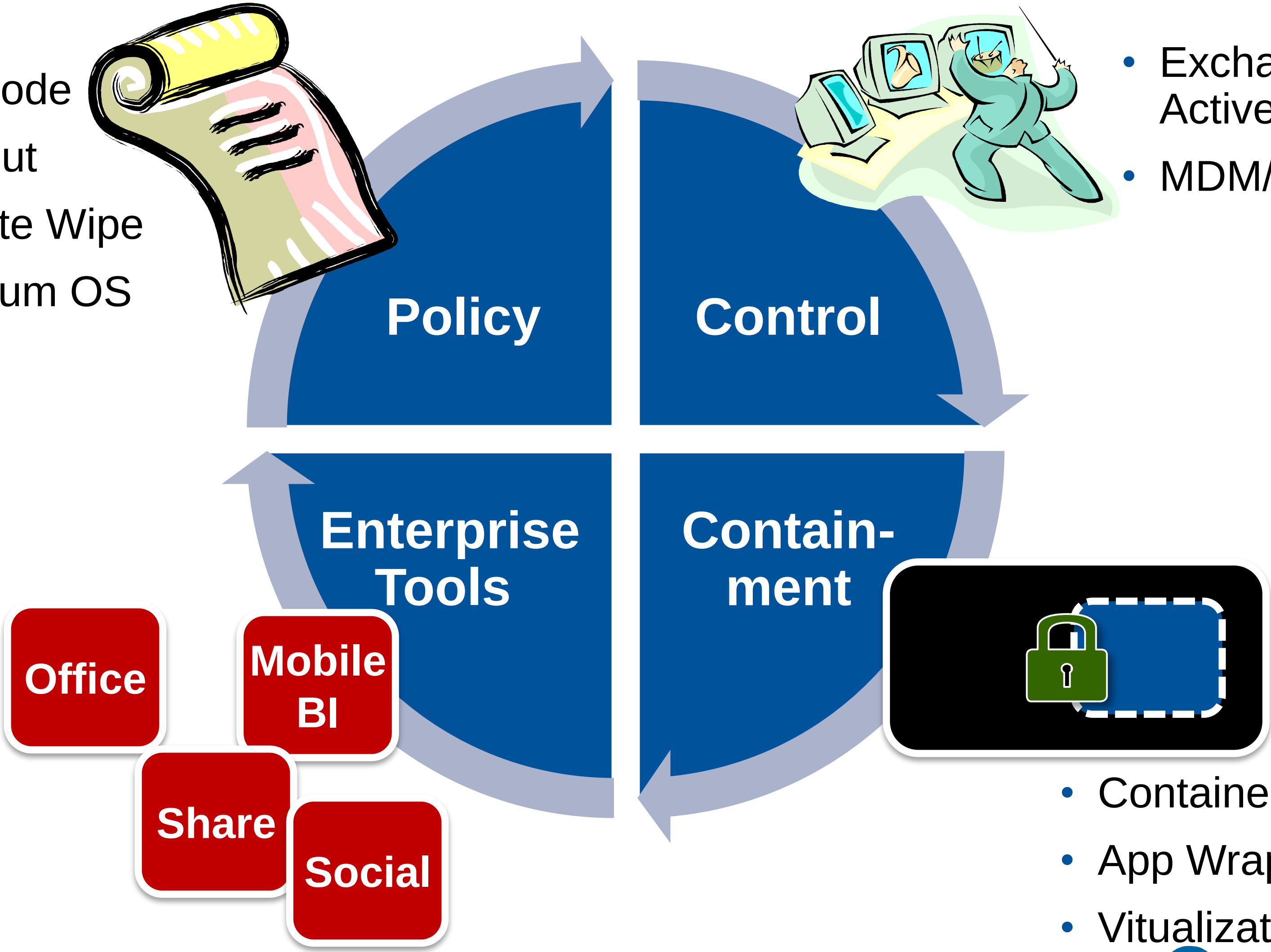
Gartner®

Agenda

- How is mobile security impacted by users' demands for a quality experience?
- How can organizations balance the often conflicting demands of users with the need to secure enterprise resources?

Balancing the Four Ingredients of the Mobile Security Mix

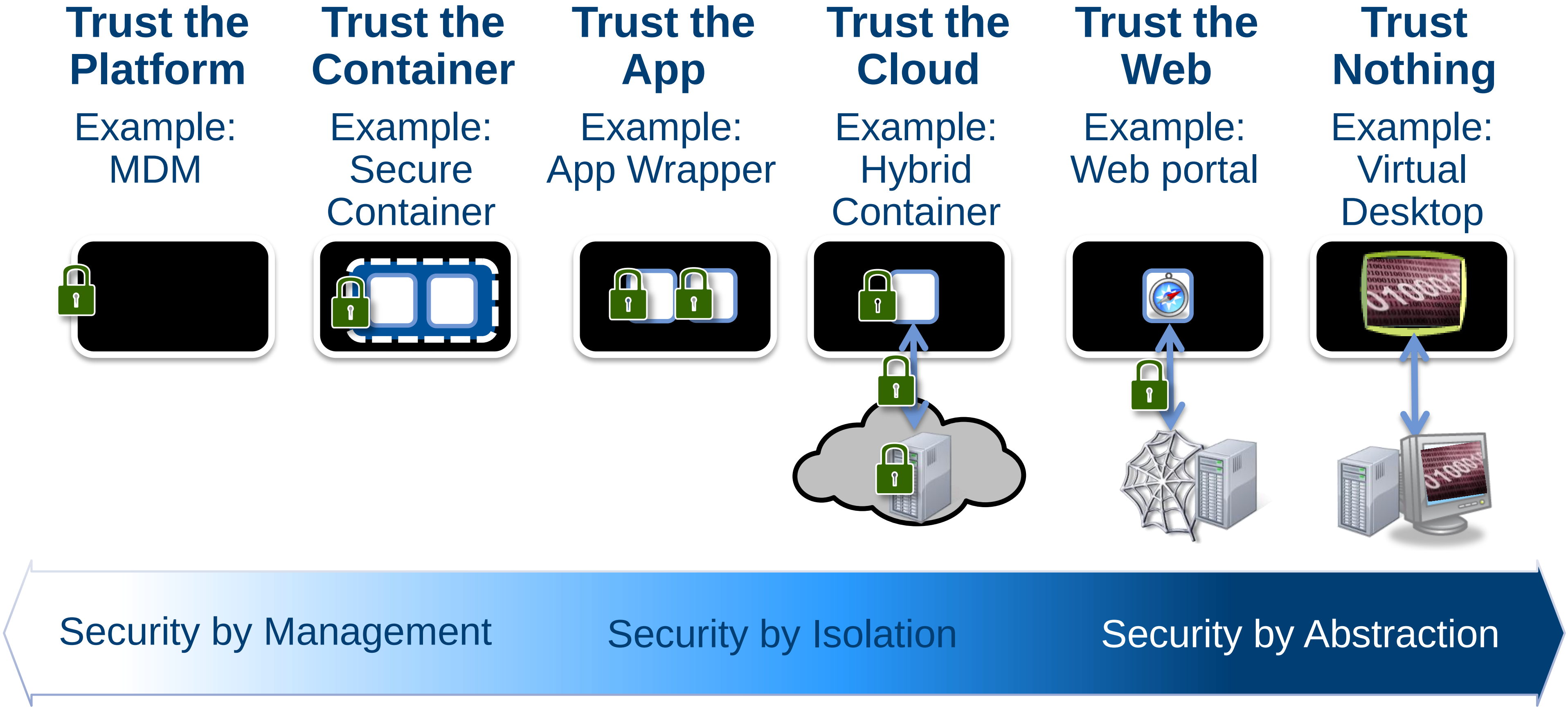
- Passcode
- Timeout
- Remote Wipe
- Minimum OS



- Exchange ActiveSync
- MDM/EMM

- Container
- App Wrapper
- Vitualization

Delivering mobile content securely – Not an Either/Or Proposition



Trust the Platform

Example: MDM

Trust the Container

Example: Secure Container

Trust the App

Example: App Wrapper

Trust the Cloud

Example: Hybrid Container

Trust the Web

Example: Web portal

Trust Nothing

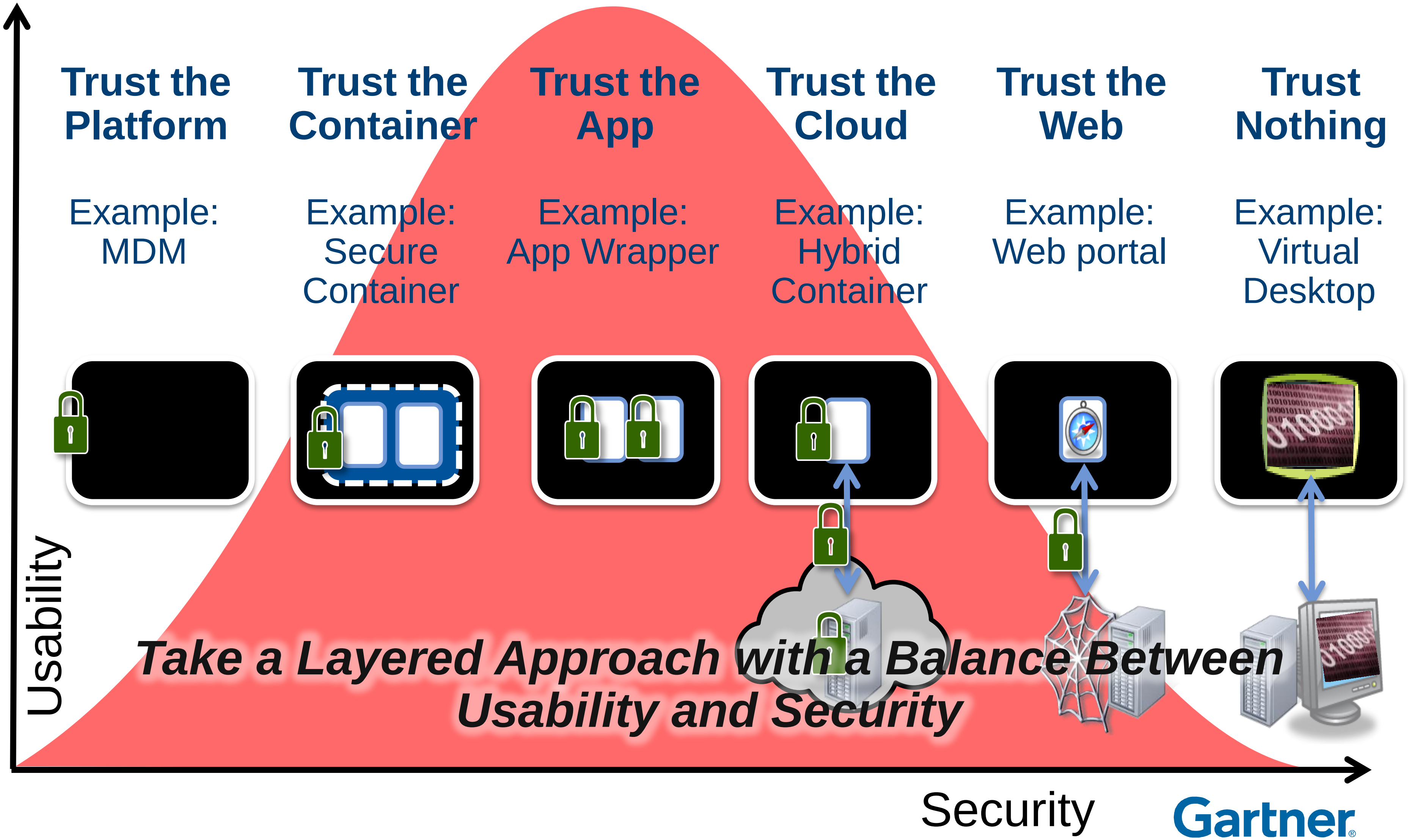
Example: Virtual Desktop

Security by Management

Security by Isolation

Security by Abstraction

Management Approaches Affect Usability



Trust the Platform

Example: MDM

Trust the Container

Example: Secure Container

Trust the App

Example: App Wrapper

Trust the Cloud

Example: Hybrid Container

Trust the Web

Example: Web portal

Trust Nothing

Example: Virtual Desktop

Take a Layered Approach with a Balance Between Usability and Security

Achieving Balance: Know the Use Case!

- What functions will the user perform?
- Will the user work offline or only online?
- What apps are needed?
- What data is needed and where does it exist?
- What platforms are needed?
- What level of sensitivity is the data?

Be Realistic About the Threat

First identify important data:

- Regulated data

- Top secret data

Next

- Identify critical transaction systems

Gartner®

Policy First, With Controls

Policy

Technology

Define policies

Educate users in policies

Policy conformance - carrots and sticks

Incentives

- Recommended devices get more / better apps
- Recommended devices get more reimbursement
- Recommended devices get better support

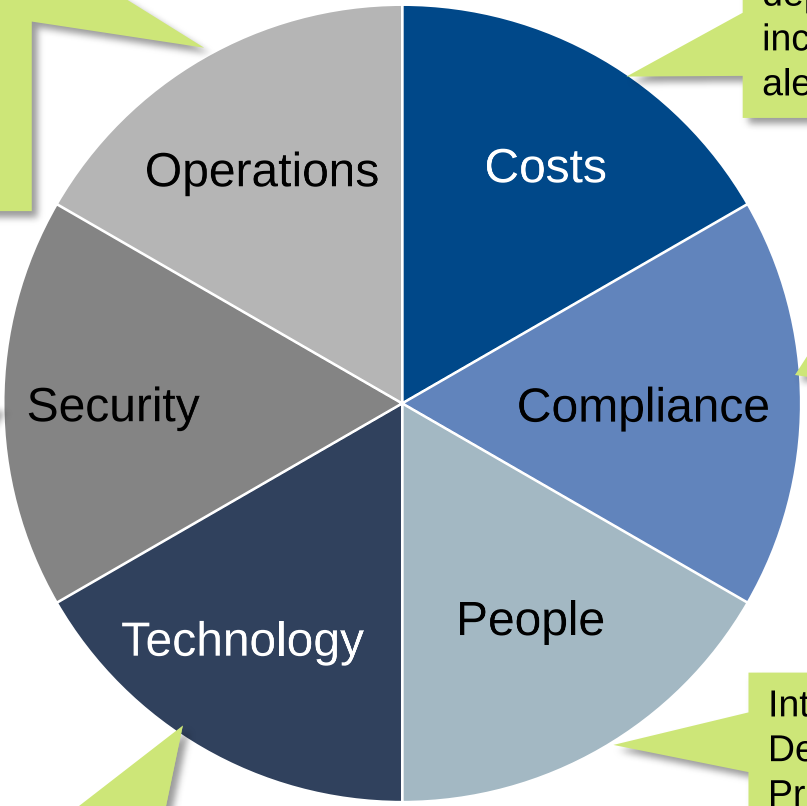
Disincentives

- Leak data and we'll dismiss you

Compliance tactics & reinforcement

- Sign and regularly refresh agreements
- Reminders - by email, voice message....

Policies to Regulate Mobility



Provisioning, De-commissioning, Auditing, Reporting, Self-Service, Patches/Upgrades, Maintenance, Levels of Support (e.g., User Portals, Trouble Shooting)

Voice/data costs, insurance, warranty, device costs, deployment costs. Policies include Inventory, reporting, alerts, policy enforcement.

Mobile Data and Corporate Server Protection (e.g., monitor and filter accesses to servers).

Application Delivery (e.g., OTA sw distribution, private app. stores).

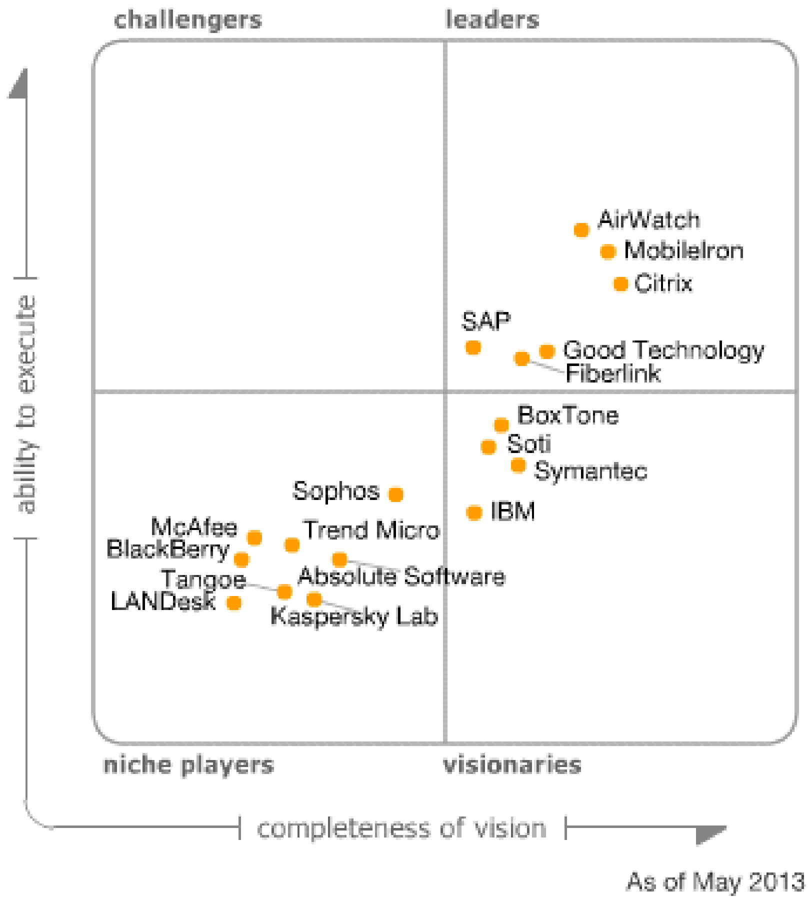
Containerization of corporate footprints on personal devices.

Liability, Contracts, Compliance, Health and Safety, Ownership, Benefits, Taxes, Accessibility.
e.g., email archiving and retrieval; local data encryption.

Supported Devices, Data Plans, Applciations, Services, Infrastructure and IT Integration.

Internal Communication, Demand Management, Privacy, Policy Sharing, Training, Work-Life Balance, Rewards

The Mobile Device Management Magic Quadrant (becomes "EMM" 2014)



Gartner Magic Quadrant for Mobile Device Management
Published May 2013

Software management

E.g. configuration, app inventory, updates, monitoring, backup....

Network service management

E.g. usage monitoring, help desk support...

Hardware management

E.g. provisioning, asset management, performance monitoring...

Security management

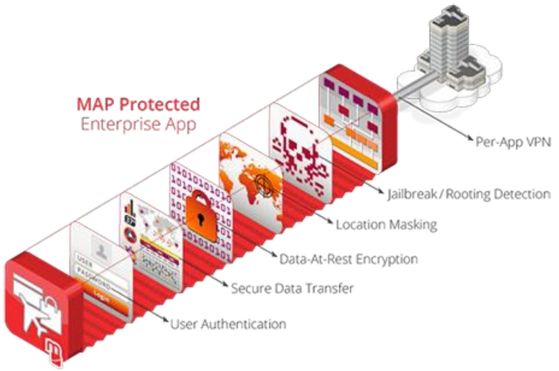
E.g. lock and wipe, policy enforcement, encryption, VPN, anti-virus, authentication....

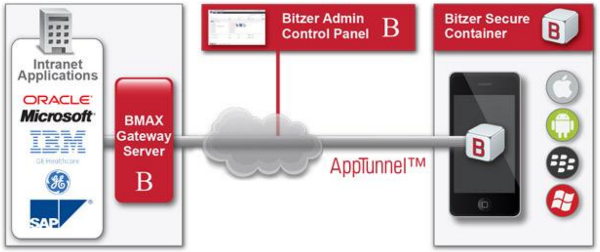
Shield or Containerize the Application

Harden the app

Add integrity to the app during development

Wrap the app





Add security post development

Develop the app in a secure container

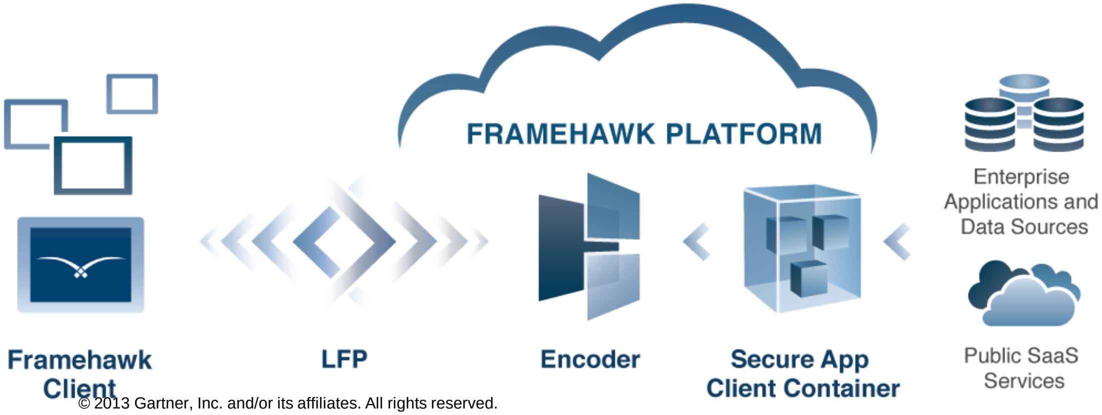
Adopt a common container for all apps

Gartner.

Virtualize the Application, Remove Data From the Device

- Don't deploy data at all to the mobile endpoint
- Specialize solutions allow for UX and application-centric secure connections
- Can greatly reduce development time

Armor5, FusionPipe (above) and Framehawk (left) allow for quick virtualization, and a good UX


FRAMEHAWK PLATFORM
Framehawk Client
LFP
Encoder
Secure App Client Container
Enterprise Applications and Data Sources
Public SaaS Services

Enterprise File Sharing and Synchronization is a Key Element of BYO

	Strong negative	Caution	Promising	Positive	Strong Positive
Accellion					🟩
Acronis				🟩	
Box					🟩
Citrix					🟩
Egnyte			🟦		
EMC				🟩	
Good Technology				🟩	
Nomadesk		🟨			
Oxygen Cloud			🟦		
WatchDox				🟩	
YouSendIt				🟩	

Gartner Marketscope for Enterprise File Synchronisation and Sharing
Published February 2013

Secure the Network

SSL VPN

- Session/Tunnel support
- Connect on demand
- x.509 certificates

Secure Web Gateway

- Two-way HTTP filter
- Cloud IPS, DLP, DRM

NAC

- Understand endpoints
- Determine ownership
- Policy-based access

Wireless LANs

- WPA2 EAP-TLS
- EAP certificates
- NAC
- Two-factor support

Legacy VPN

- Connect on demand
- IPSEC, PPTP embedded
- Third-party VPN applications

Add Context to all Access Gateways

Recommendations

- ✓ Work with the business units to understand their needs and use cases.
- ✓ Don't treat all users the same way — segment your base according to geography, platform, required business apps, data needs, security, and costs.
- ✓ Create cross-functional teams to identify issues and tradeoffs.
- ✓ Don't ignore user experience but do not allow your mobility strategy to become a prisoner to it.
- ✓ Consider policy, support, legal and other nontechnical issues.
- ✓ Tool up! Select mobile defenses using a spectrum of trust.

End-user Action Plan

Monday Morning:

- *Review* mobile device access controls with IT management.
- *Form* a team to prepare a mobile data risk assessment and gap analysis (desired protections versus reality).

Next 90 Days:

- *Educate* users on their responsibilities; put behavioral incentives, disincentives and social engineering techniques in place
- *Verify* that MDM policies are addressing your risk assessment.

Next 12 Months:

- *Develop* security specifications for procurement and internal application development as well as mobile platforms and public apps
- *Revisit* mobile device threat assessment and be realistic about risks
- *Consider* the implications of the personal cloud, data, and context-centric security, and augment your strategy.

Recommended Gartner Research

- ➔ **Solution Path: How to Create a Mobile Architecture**
  Paul DeBeasi (G00231560)
- ➔ **Decision Point for Mobile Endpoint Security**
  Eric Maiwald, Dan Blum (G00235640)
- ➔ **Decision Point for Identity and Access Management in Mobility Projects**
  Ian Glazer (G00231043)
- ➔ **Decision Point for Choosing the Right Mobility Management Option**
  Michael Disabato (G00234148)
- ➔ **Decision Point for Selecting a Mobile Application Architecture**
  Kirk Knoernschild and others (G00234823)

For more information, stop by Gartner Research Zone.

Gartner®