Wireless Networks: Can Security Catch Up With Business?

John Pescatore
VP, Internet Security
Gartner, Inc.

Wireless Security NewsFlash

- General Francissimo Franco is still dead
  - and so are WEP and WAP
- A cellphone virus has been sighted!
  - But it was just a wrong number…
- Airport security screenings are much more thorough
  - And many more laptops and PDAs are being left at the security checkpoints
- WLAN Security Standards are here
  - Sorta
  - Lots of them, too

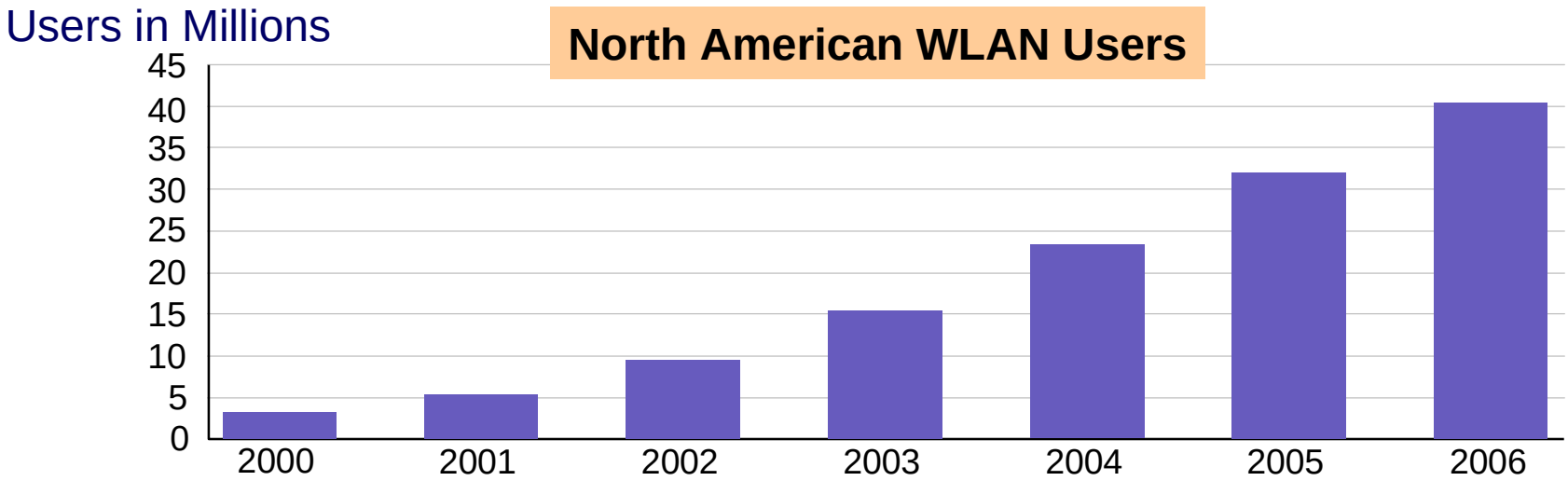
What do enterprises need?

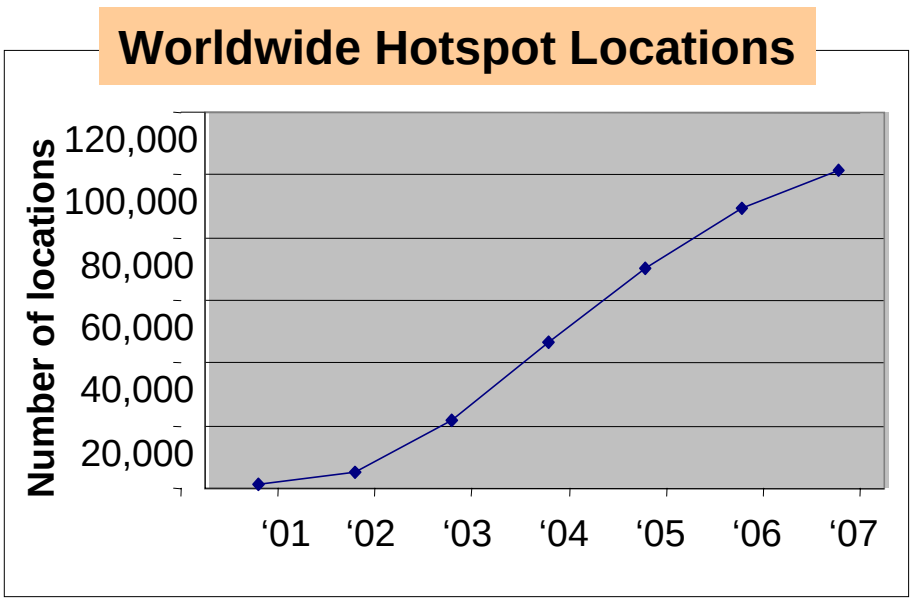
- Secure out of the box defaults
- Multi-vendor interoperability
- Security that lasts longer than the products
- Hotspot private connections
- WLAN Intrusion Detection from the wired side
- Basically, they need

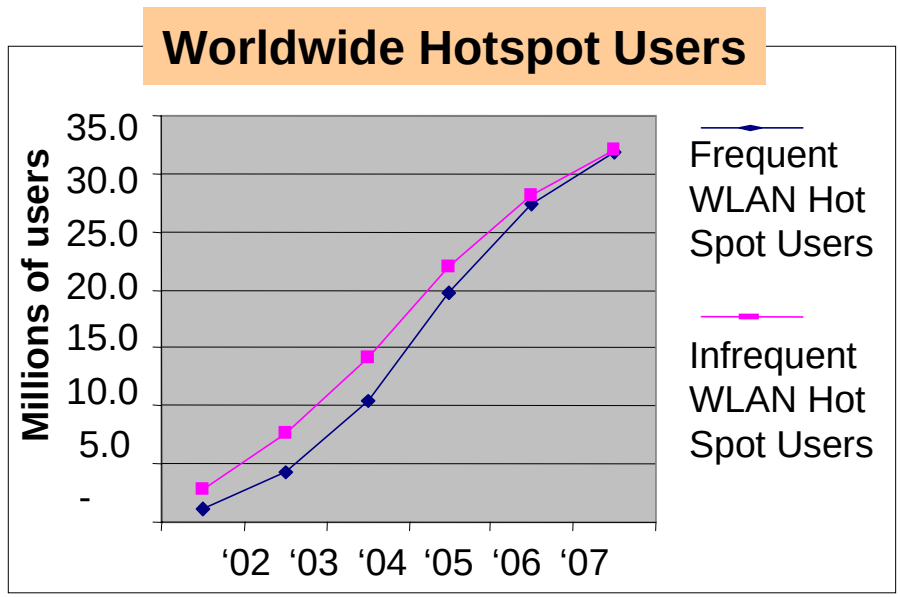
WIRED EQUIVALENT SECURITY

- Then bring on roaming, voice, etc.

WLAN: Fastest Growing Wireless Technology





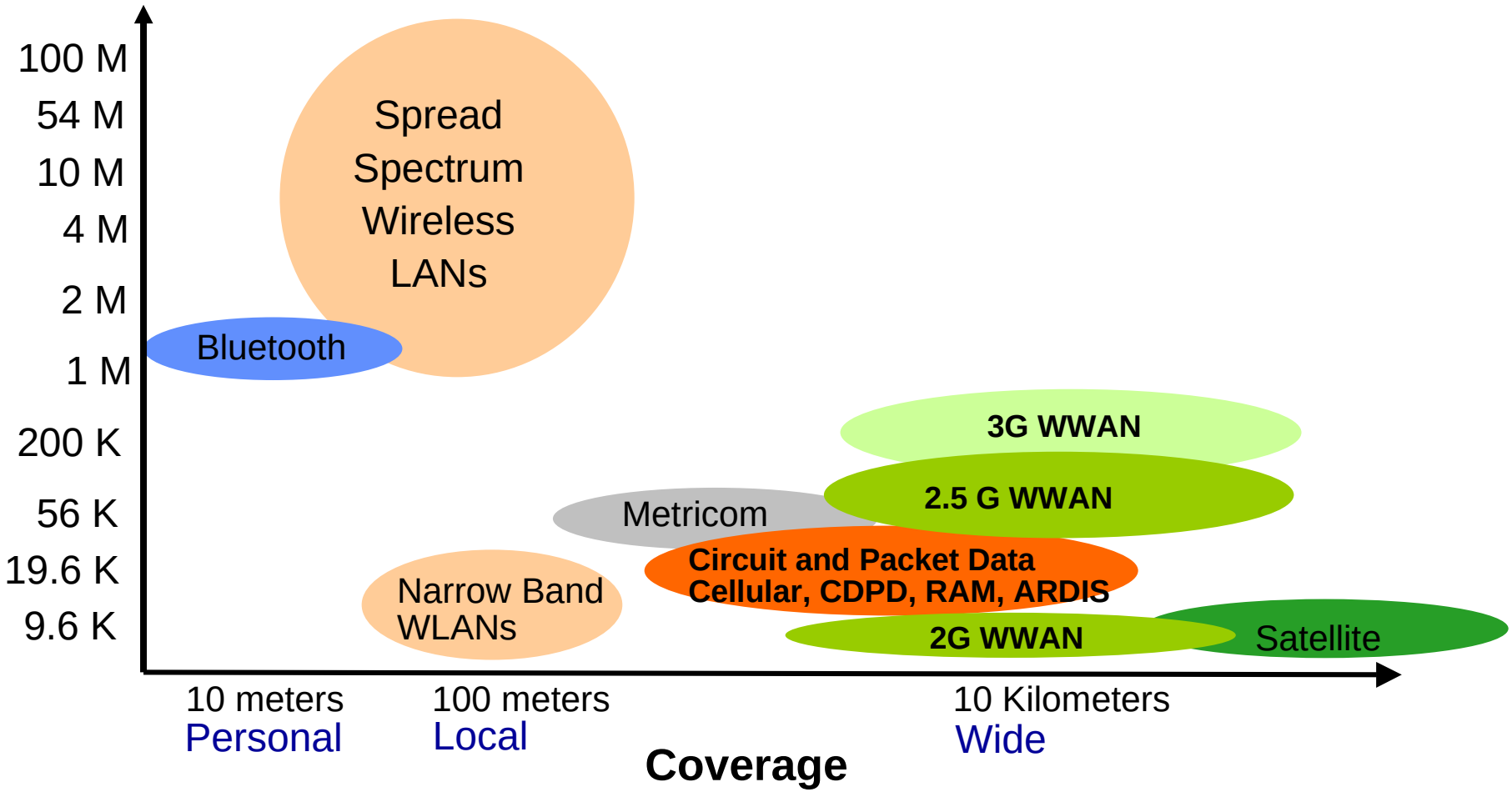


Gartner

Where Does WLAN Fit?

Gartner

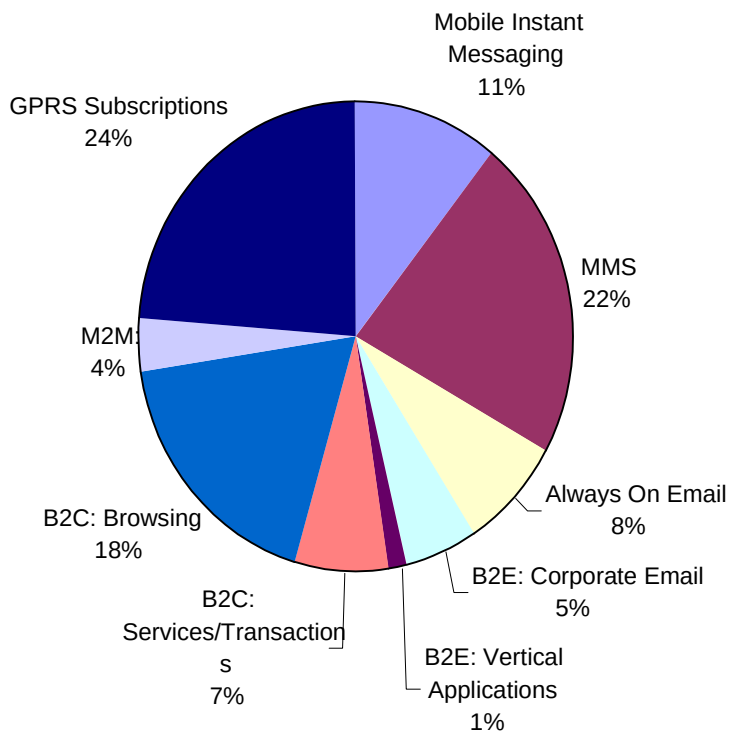
Where Does WLAN Fit?



Gartner

Mobile Packet Data Applications

Percentage of GPRS Revenue, 2006



WWAN Data Drivers

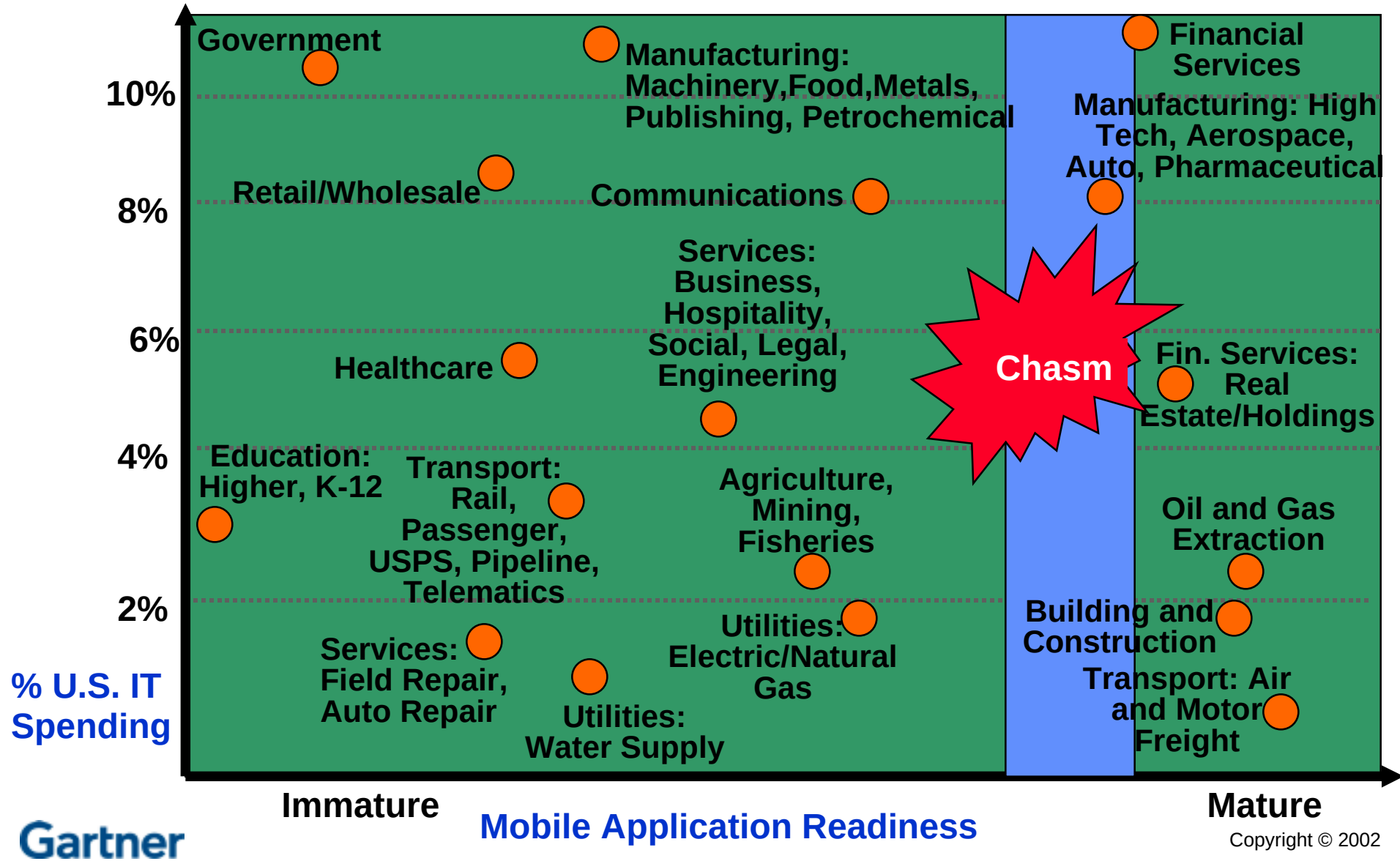
- Complementary to WLAN Explosion
- Introduction of 1xRTT and GPRS technology
- Maturing WAG offerings
- Improved device form and functionality

WWAN Data Inhibitors

- Monthly cost
- Support issues for wide array of SW Platforms
- Billing and Roaming issues
- Lack of standard e-mail clients/servers
- Confusing device landscape

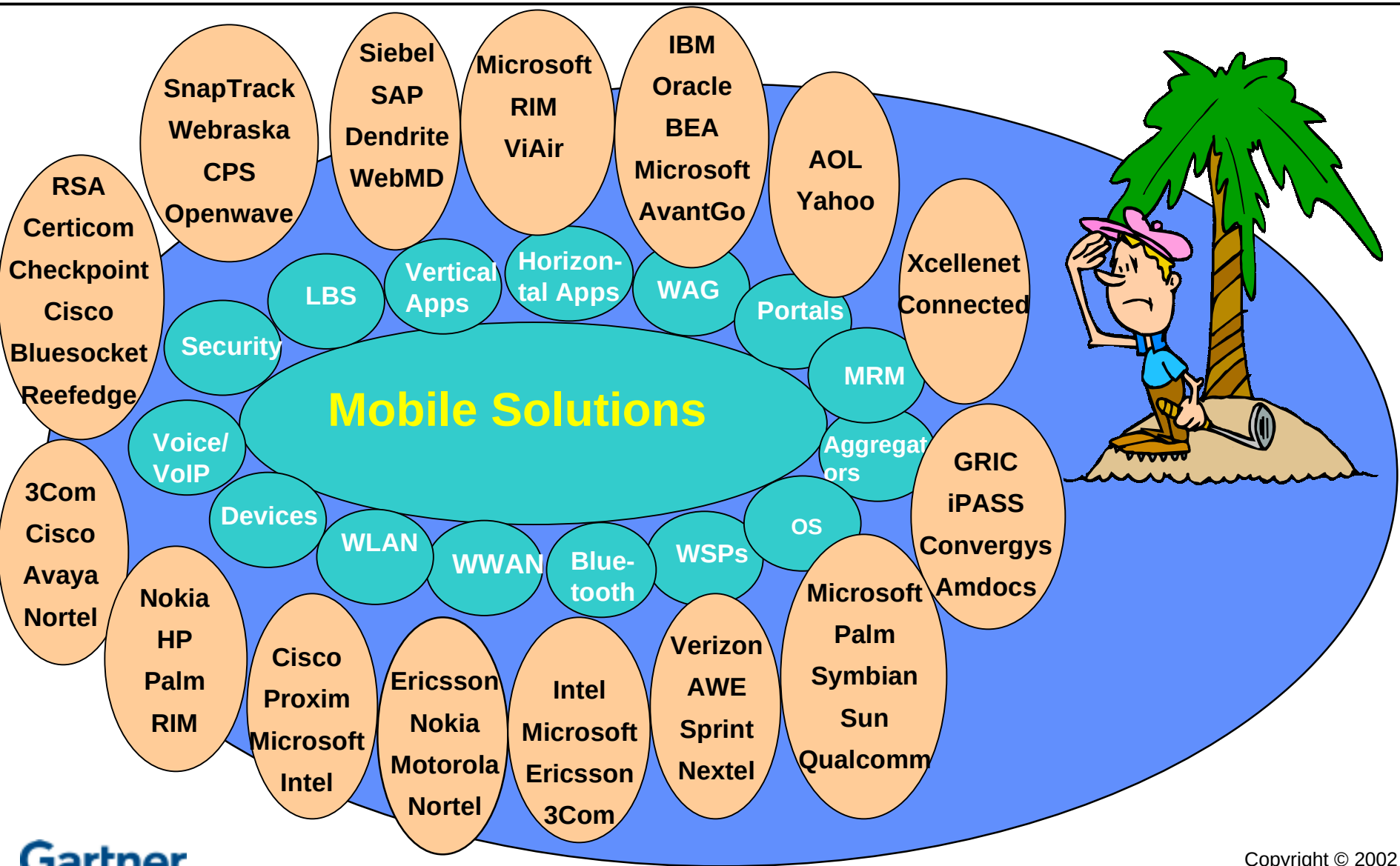
Gartner

Industry Segments: Vertical Mobile Application Trends



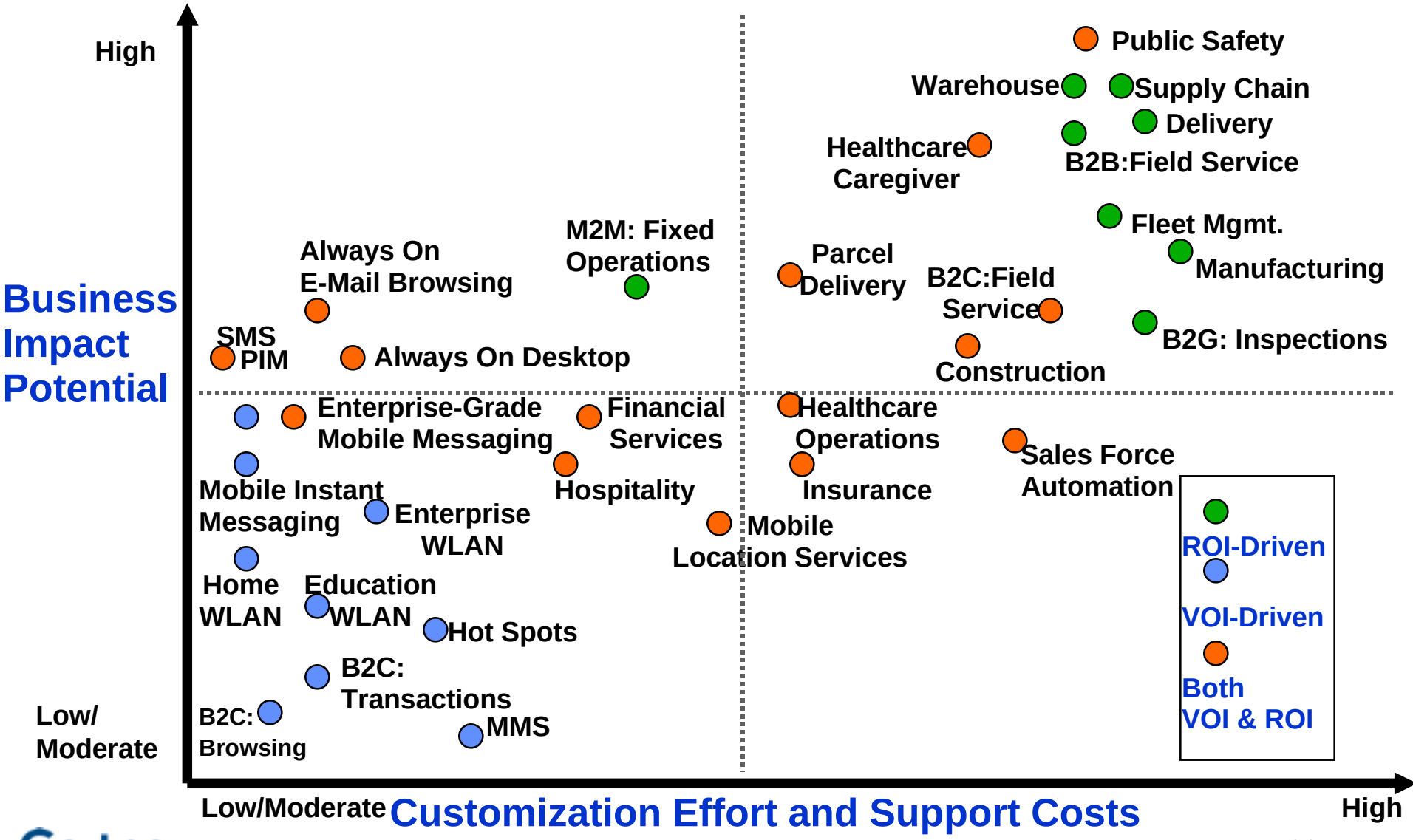
Gartner

Competing Mobile Ecosystems



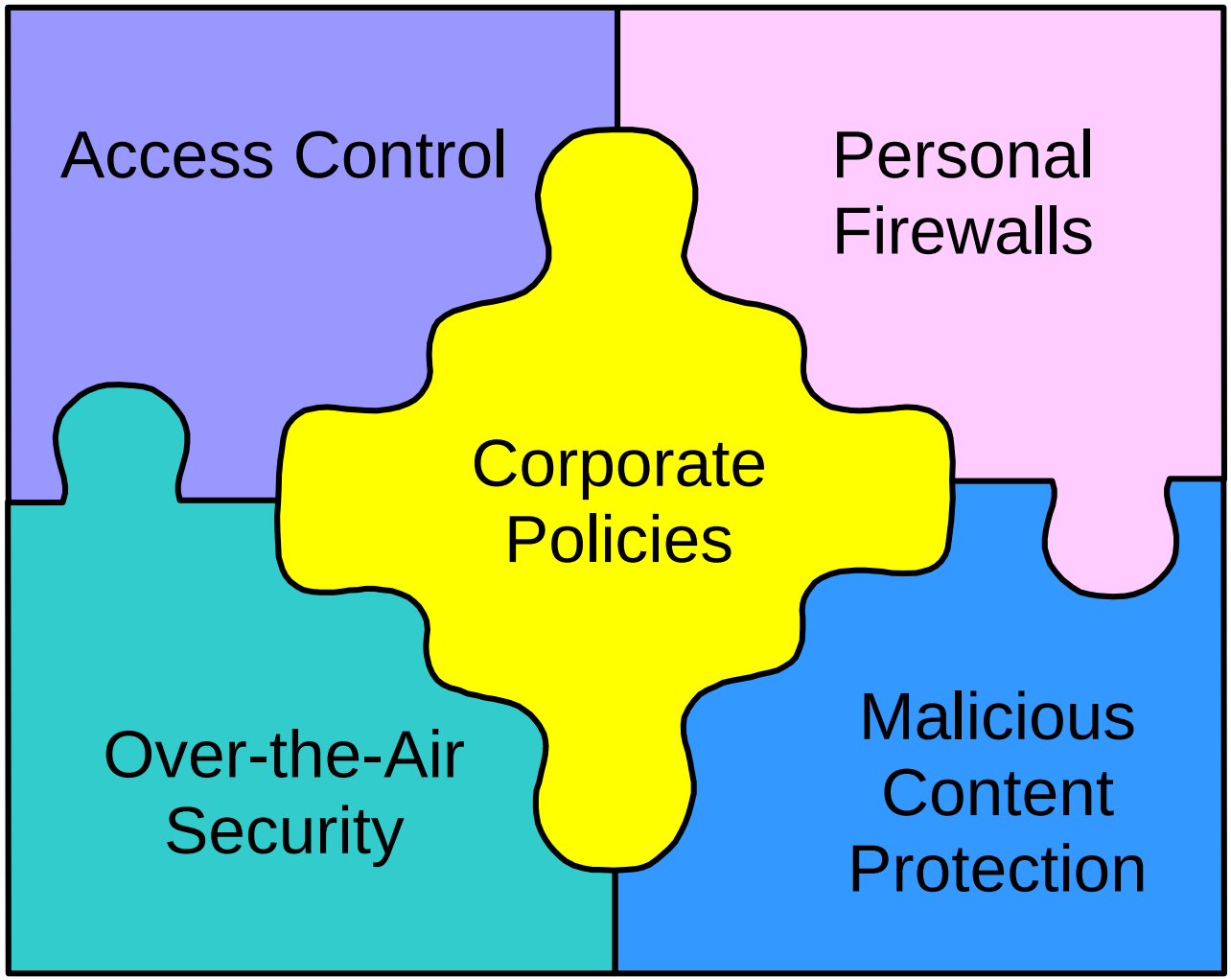
Gartner

Impact of Mobile Applications



Gartner

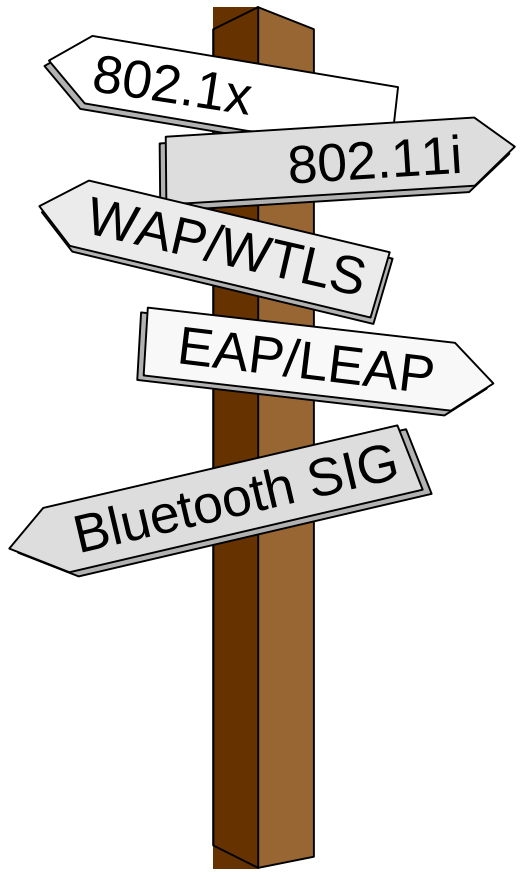
Mobile Access Security



Gartner

The Complexity of Standards

- Most standards bodies have become competitive battlegrounds vs. cooperative coalitions
- Since wireless has been seen as “the next big thing,” the battles have been long and hard-fought
- Assume single vendor lock-in until Phase V:
  - Standards body formed
  - First vendor press release
  - Standard ratified
  - Rampant vendor press releases
  - Second trade show after Phase III
- Assume security flaws will be found until 18 months after Phase V



Cell Phone Wireless Threat Time Frame