Mobile Device Management & Enterprise Applications

Solving new security risks while optimizing value

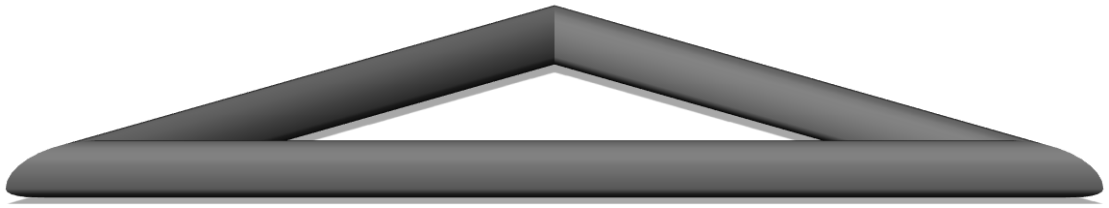
- Large public safety segment enabling dual use devices creating major security risks:
  - Data leakage from work to personal use cases
  - Malware risks from untrusted personal applications
- Containerization strategy mandatory for mitigating security risks associated with dual personal and work use devices
- Available containerization options impact key value drivers differently:
  - Public safety applications are critical drivers for productivity & field enablement
  - Containerization approaches must pass mustard with employee base for usability
- Different container options can impair secure application environment:
  - Adding complexity and increasing development costs
  - Reducing application features and impacting user experience

Mobile Device Management & Enterprise Applications

Understanding how security impacts key value drivers

Mobile Productivity
Strategic Enablement
Cost of Ownership

Public Safety Enablement



Security & Risk Management

Mission Critical Systems
Regulated Data & Compliance
Availability
Privacy

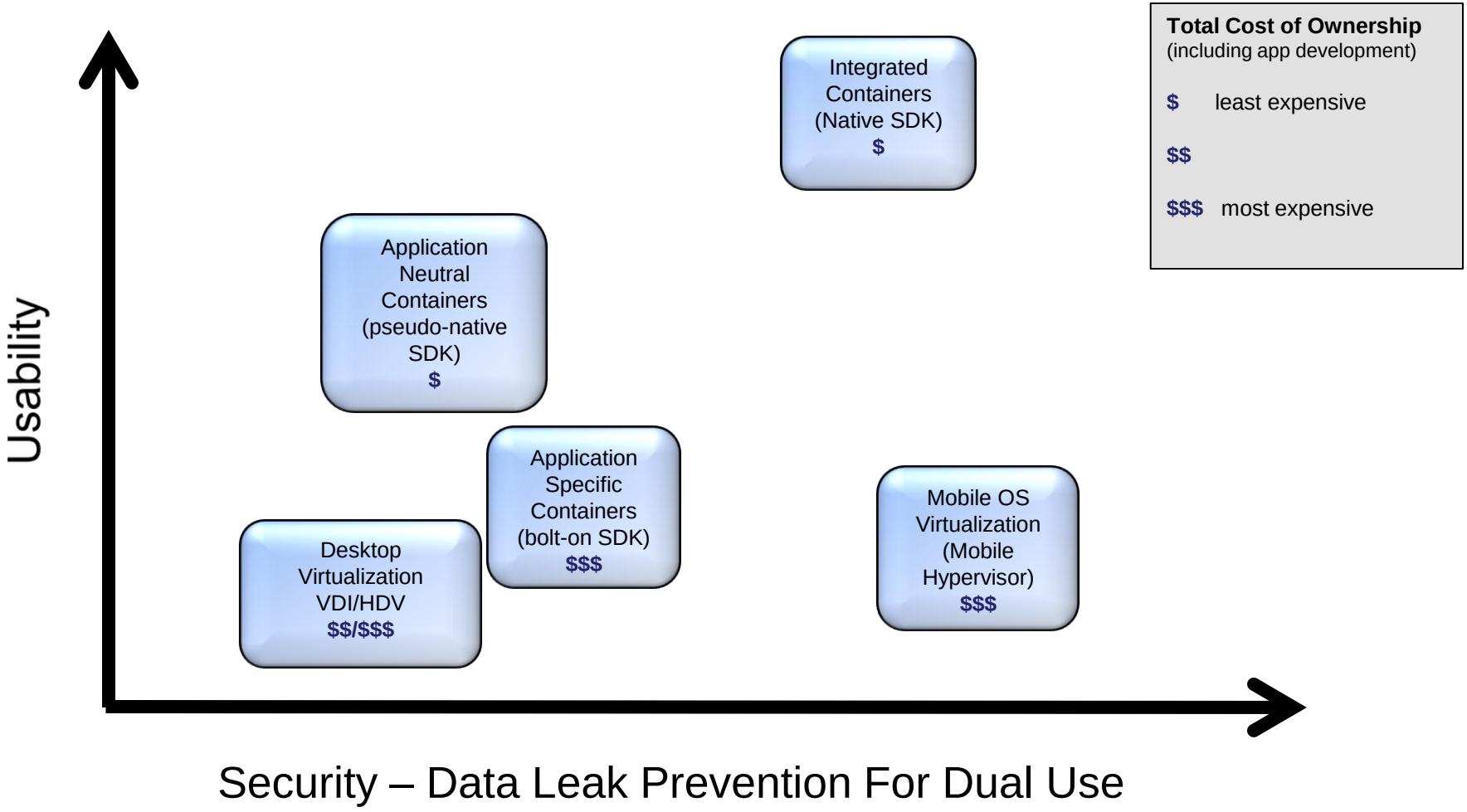
User Experience

Usability
Design / Style
Personal Preference
Personal Applications

Use this same framework for determining the best approach for mobile device containerization / DLP (Data Leak Prevention)

Mobile Device Management & Enterprise Applications

Available options for securing public safety applications



APCO International
Leaders in Public Safety Communications™

Mobile Device Management & Enterprise Applications

Mission critical, high security public safety environments

- Mission critical, high security deployments likely require complete personal use case disablement

- Mitigation for advanced threats, including denial of service attacks:
  - Hardened operating system – security only as good as OS integrity
  - Hardware root of trust: protects against sophisticated attacks on operating system
  - Supply chain security: leveraging hardware root of trust and other built-in security controls to verify integrity and authenticity of code and key components

- Strong, tamper resistant data-at-rest encryption design and implementation to protect residual application data

- Strong / two-factor authentication – look for NFC enabled smart cards on the horizon for accessing mission critical applications and back-end systems