Motegrity

“End-to-End Trust”

“The Security of a Closed Platform on Open Platforms”

April ’08

Vision

Solve key trust and security problems in mobile internet Endpoints

Improve functionality & lower the cost of Endpoints through trusted virtualization

Enable delivery of trusted Value Added Services

How?

By delivering a solution that:

a) Provides end-to-end security for the mobile internet Endpoint

b) Provides an Endpoint functional virtualization architecture

c) Provides a trust framework for services delivery

Motegrity History

- Tallwood Mobility Initiative (MI)
  - Kicked off early ’06
  - Key questions:
    - What are key issues facing delivery of web services to mobile internet Endpoints?
    - What are key challenges to realizing “thin/stateless” mobile internet Endpoints?
- Motegrity (Mobile Integrity) incubation
  - Kicked off early ‘07
  - Team assembled (7 people - 3 full time)
  - Proof of Concept demo system developed
  - First customer engagements

Current Team

- Reyaz Ahmed
  - Firmware, Linux drivers
  - Phoenix, JNI, AMCC (Principal Engineer)
- Ken Baylor (CISO)
  - McAfee, Symantec, VP and CISO, Global Head of Security
- Jithendra Bethur (FT – Dir Endpoint SW) [Since April '07]
  - Firmware, client device software
  - Phoenix, Sr. Eng Manager/Product Manager for Firmware Security Group
- Rao Cherukuri (VP Biz Dev)
  - Phoenix, Founder/CTO Ramp Networks, Founder/CEO/CTO Euclid
- Pete Foley (CEO)
  - Tallwood Exec-in-Residence
  - Predicant, nBand, Benchmark EIR, Chromatic, SuperMac, Apple
- Rajesh Gupta (CTA)
  - Research, System architecture
  - UCSD Qualcomm endowed chair
- Brent Haines (FT - VP Eng) [Since late July '07]
  - Server side architecture and software
  - Tumbleweed Comm, Chief Software Architect

Software team "in waiting"
India (Bangalore) resources

FT = Full Time

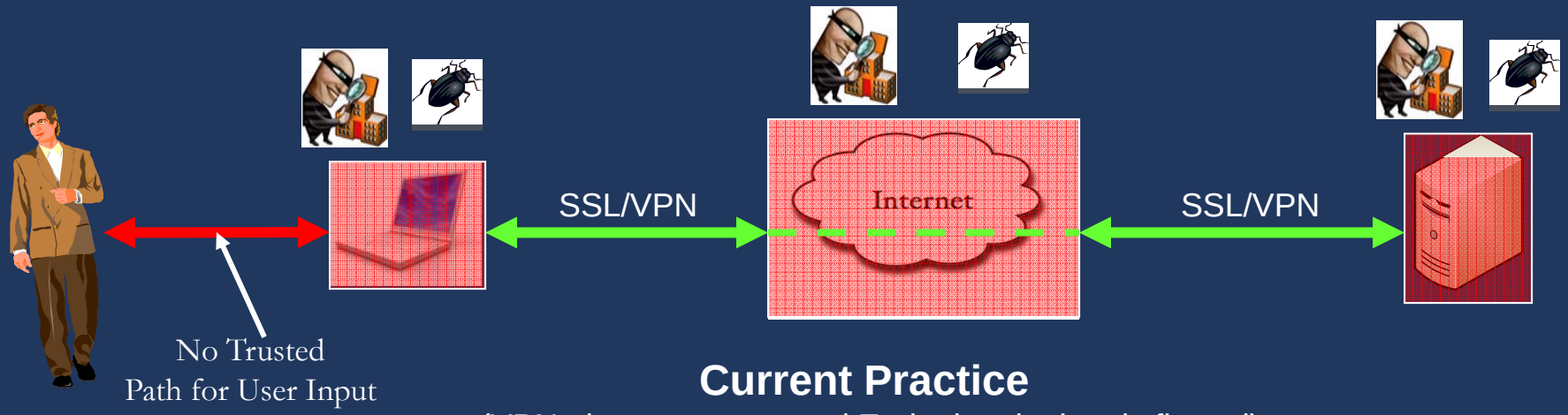
Target Markets

- Initial Market: Financial Services
- Adjacent Markets: Security conscious enterprise
  - Health care, government, retail
- Long Term: Consumer Endpoints
  - Platform security, secure mobile services
  - Facilitating “thin client”/virtualized devices

Financial Svcs Mkt Pain Points

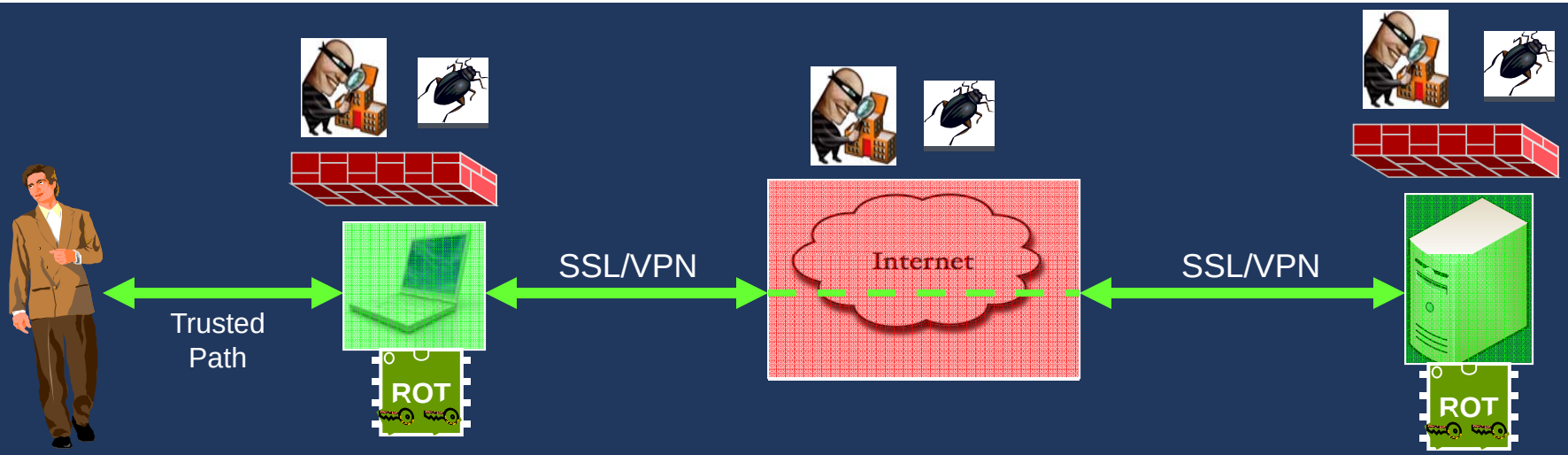
- Security and Compliance
  - OCC (Outbound Content Control)
    - Data Leakage Protection (DLP)
    - Lost Data Destruction (LDD)
  - Secure “container” needs on Endpoints to host:
    - Corporate access environment
    - Virtual desktop clients
  - Hostility assumption: IT must regard all Endpoints – even within corporate perimeter – as hostile
  - Regulatory requirements make above pain-points more immediate
    - FFIEC, Sarbanes-Oxley, HIPAA
    - Drive demand for improved auditing (audit trails, non-repudiation), authentication (trusted paths), and Endpoint provisioning.
- Corporate Mandates & Work Culture
  - Mobilize and virtualize the workforce
  - Integrate employee purchased Endpoints
    - Need to support “multiple personalities” on Endpoints

What is missing (from a security perspective)?



Current Practice

(VPN alone, on untrusted Endpoint, is deeply flawed)



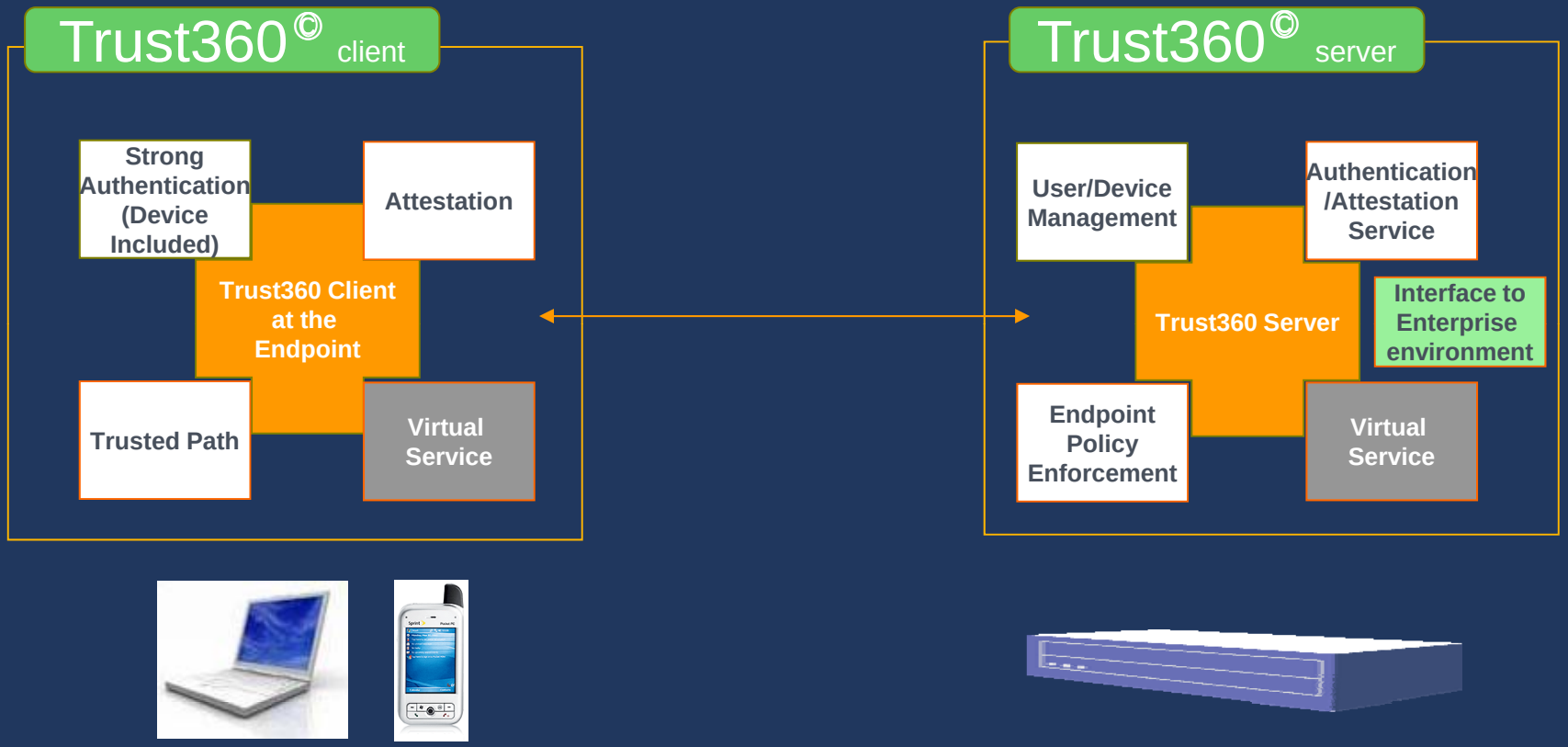
Motegrity Model – End to End Security Guarantees

(Based on hardware Root-of-Trust, Secure Boot, Virtualization)

Motegrity's Solution

- "End-to-end" security and virtualization based on hardware trust anchors, efficient lightweight VMMs, and paravirtualized OS
  - Standards based – TCG/TPM/Xen – to accelerate adoption
  - Key capabilities:
    - Trusted boot
    - Per VM and Session-specific capabilities:
      - Dynamic (mutual) Attestation
        - Realtime on demand proof of integrity
      - Resource Provisioning
    - Server and/or Endpoint based initiation of trusted Agents/Services

Product Offering



- Deployment
  - Virgin Enterprise Install
  - Over the Air (OTA)

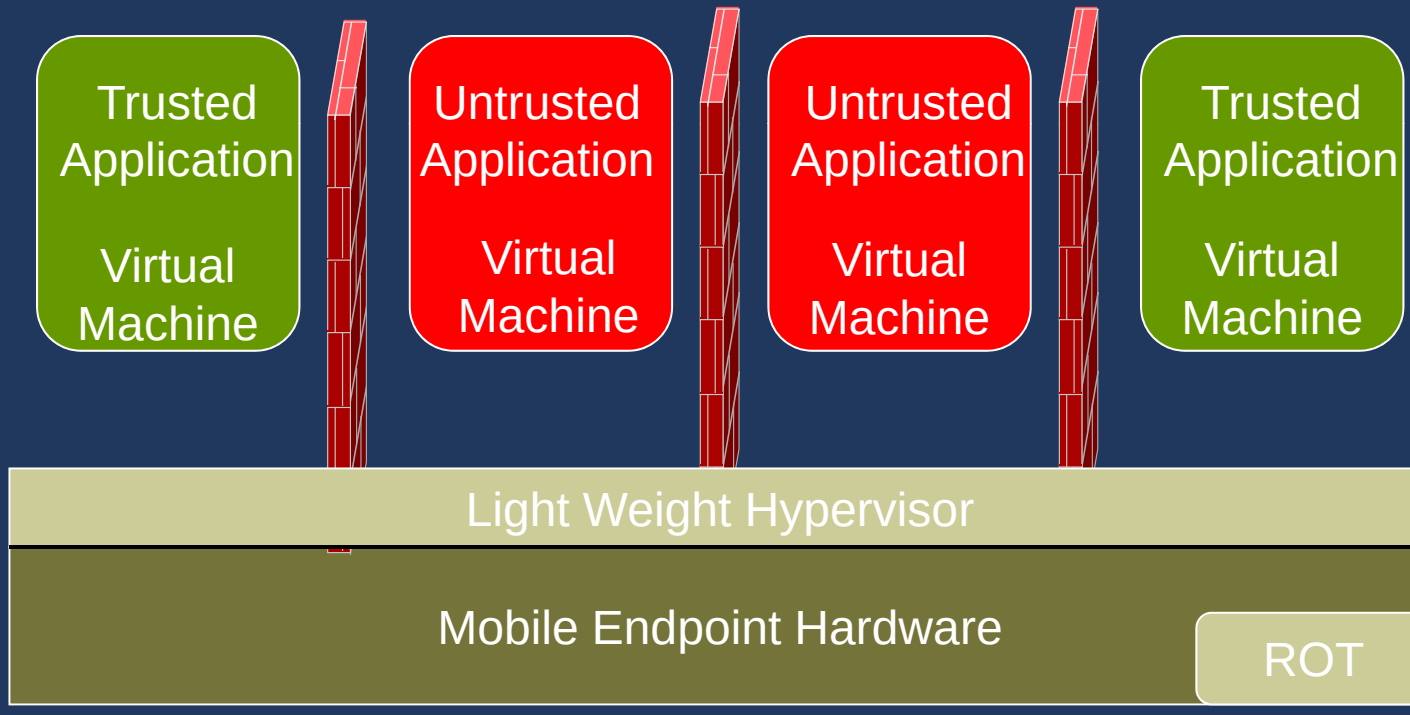
- Deployment
  - 1U Rack
  - VM Hosted

Trust360© Product Components

- Trust framework
  - Both server and Endpoint side software
- Server side web services interfaces
  - Hosting framework (Agents & virtual services)
- Third Party Development Tools
  - API/SDK
- Provisioning & Management Tools
  - User installation & provisioning
  - Server installation & provisioning
  - IT Endpoint provisioning tool
- Initial Applications
  - Secure Enterprise virtual desktop hosting, authentication services, push data environment

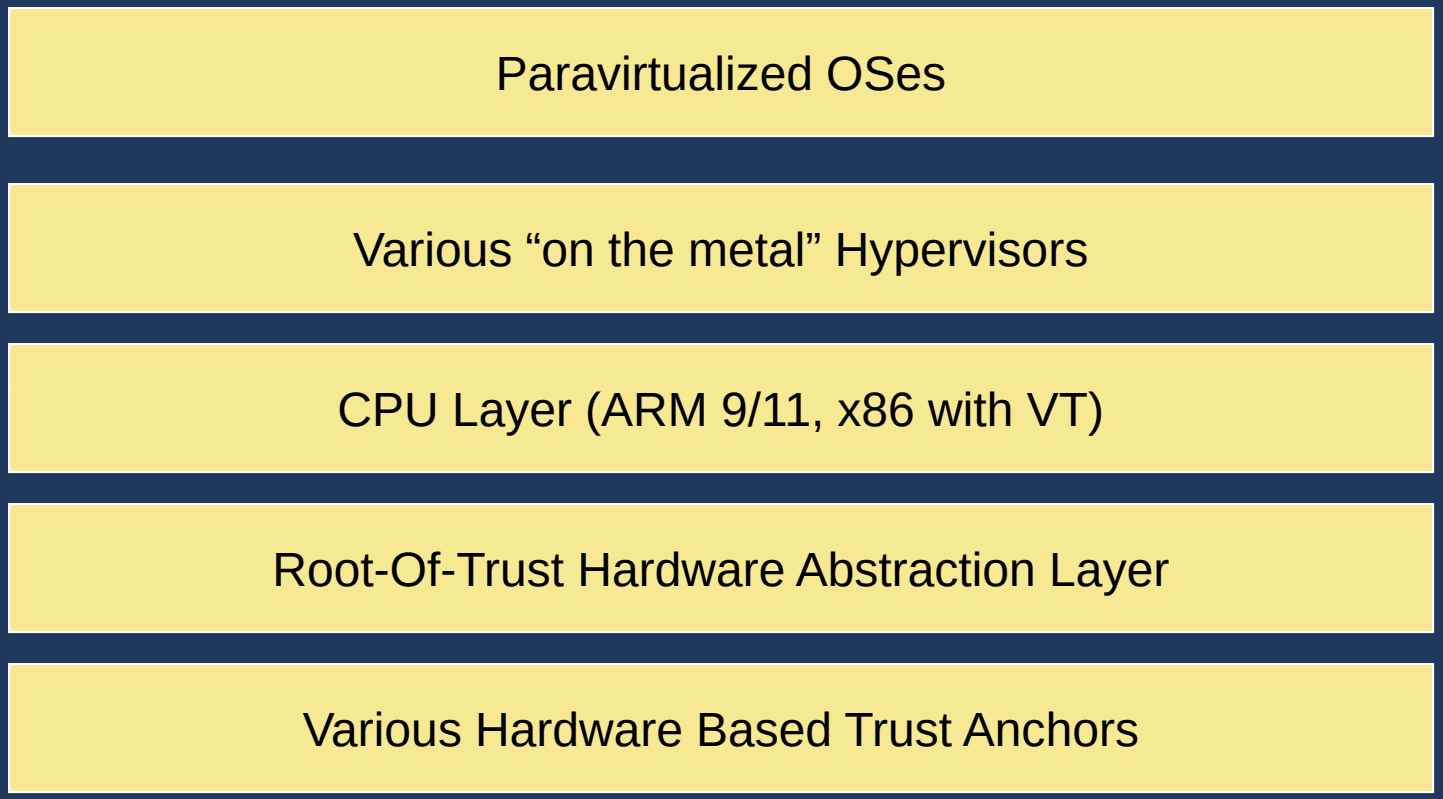
How We Do It

- Through *Virtualization* – built on a hardware based Root-of-Trust (ROT)



The Secure Open Endpoint

Trust360 Architecture



- The Motegrity Trust360 is Trust Anchor and Hypervisor agnostic
  - Example Trust Anchors include:
    - TPM - shipping in 90% of all Laptops/PCs in ’09 (IDC)
    - Texas Instruments M-Shield in OMAP-2/3
    - HSM (Hardware Security Module) - common in server space

Customer Feedback

- Credit Suisse
  - "If you really care about security – you guys are going about it exactly the right way" – Chris Swan, Head of Security R&D
- Sprint
  - "You are preaching to the choir – I have been advocating this kind of approach for several years" – Team lead Security Research
- India: Carriers - Spice & Airtel; Mobile payment aggregators – mCheck & TechProcess
  - All interested in follow up
  - mCheck thought Motegrity could potentially offering a "platinum" security level for financial transactions

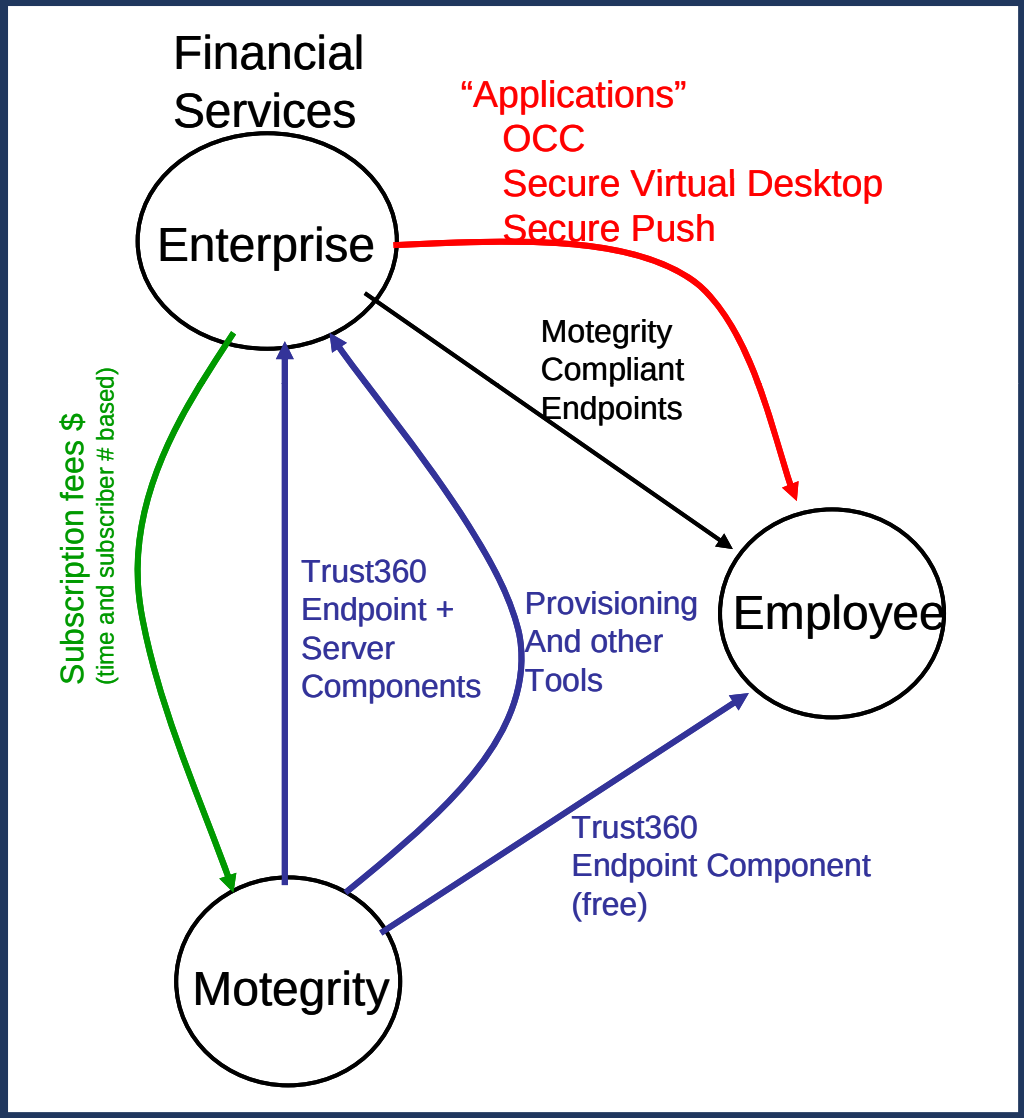
Market Size

Security Software	2009 ($B)	2004-2009 CAGR (%)
OCC – Outbound Content Compliance Data Leakage Protection (DLP) Lost Data Destruction (LDD)	$1.9	49
Identity and Access Management (IAM) - Includes SSO ($1.6B)	$3.9	11.3
Secure Content Management (SCM) – anti-malware, etc	$9.7	16.1

Source: IDC

- Total VAS market will reach $190B in 2009 (Telenity)

Enterprise Biz Model (laptop Endpoint)



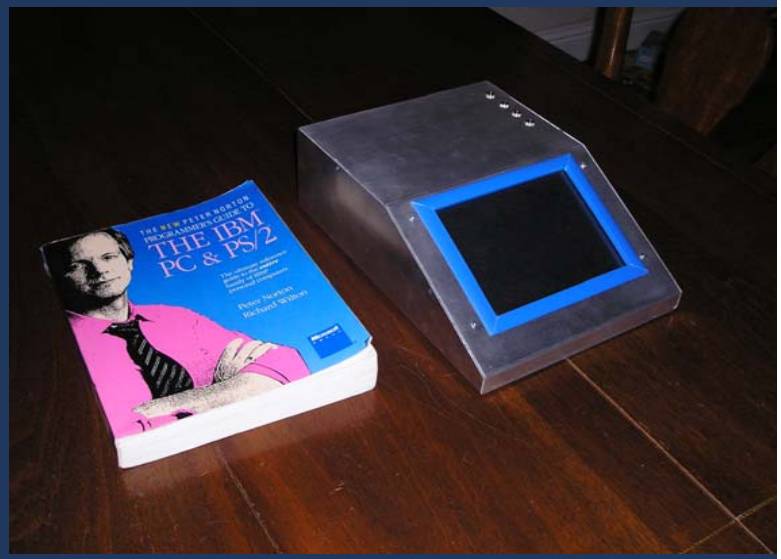
- Monetization
  - Base server offering
  - Endpoint subscriptn
    - Perpetual & annual
    - 30% annual maint
  - Major release fees

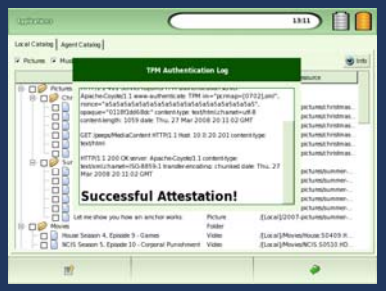
Product Roadmap

Server Deployment	1U Chassis Linux 2.6 Server '08	VM Hosted	MSP: Subscriber Service
Endpoint Deployment	Laptop/PC Vista/XP	Smartphone Android	Smartphone WinMobile & Symbian
Endpoint Applications	1) Citrix Virtual Desktop 2) LDD	Data Push	TBD
Server Applications	1) Endpoint Provisioning 2) Authentication Tools	1) OTA Endpoint Deployment 2) Data Push	Back-end Integration with .NET
3rd Party Tools	API/SDK V1	API/SDK V2	API/SDK V3
	15 mo	21 mo	27 mo

Development to Date

- Demonstrated in Completed POC
  - TPM ROT, VMM, ARM9 (PXA-270) as host CPU, Linux 2.6 OS, P2P Video Proxy as Agent/Service demo
  - Endpoint trust framework
    - Trusted boot process
    - Linux port, ROT virtualization
    - Initial Trust UI (Qtopia based)
    - Attestation
  - Server Services Framework
    - Agent hosting/initiation





IP

- Provisional Patent filed Oct ’06 (system and method patent)
  - “A Distributed Trusted Virtualization Platform”
    - Extensions in process.

TAB

- Dr. Rajesh Gupta (UCSD) – Chairman
  - Qualcomm endowed chair in embedded microsystems
  - Tallwood “Professor in Residence” and Motegrity CTA (Chief Technical Advisor)
- Dr. Andreas Schmidt (Fraunhofer Institute)
  - Trusted Computing and Mobile Security Expert
- Chris Swan (Credit Suisse) Head of Security R&D

Competition

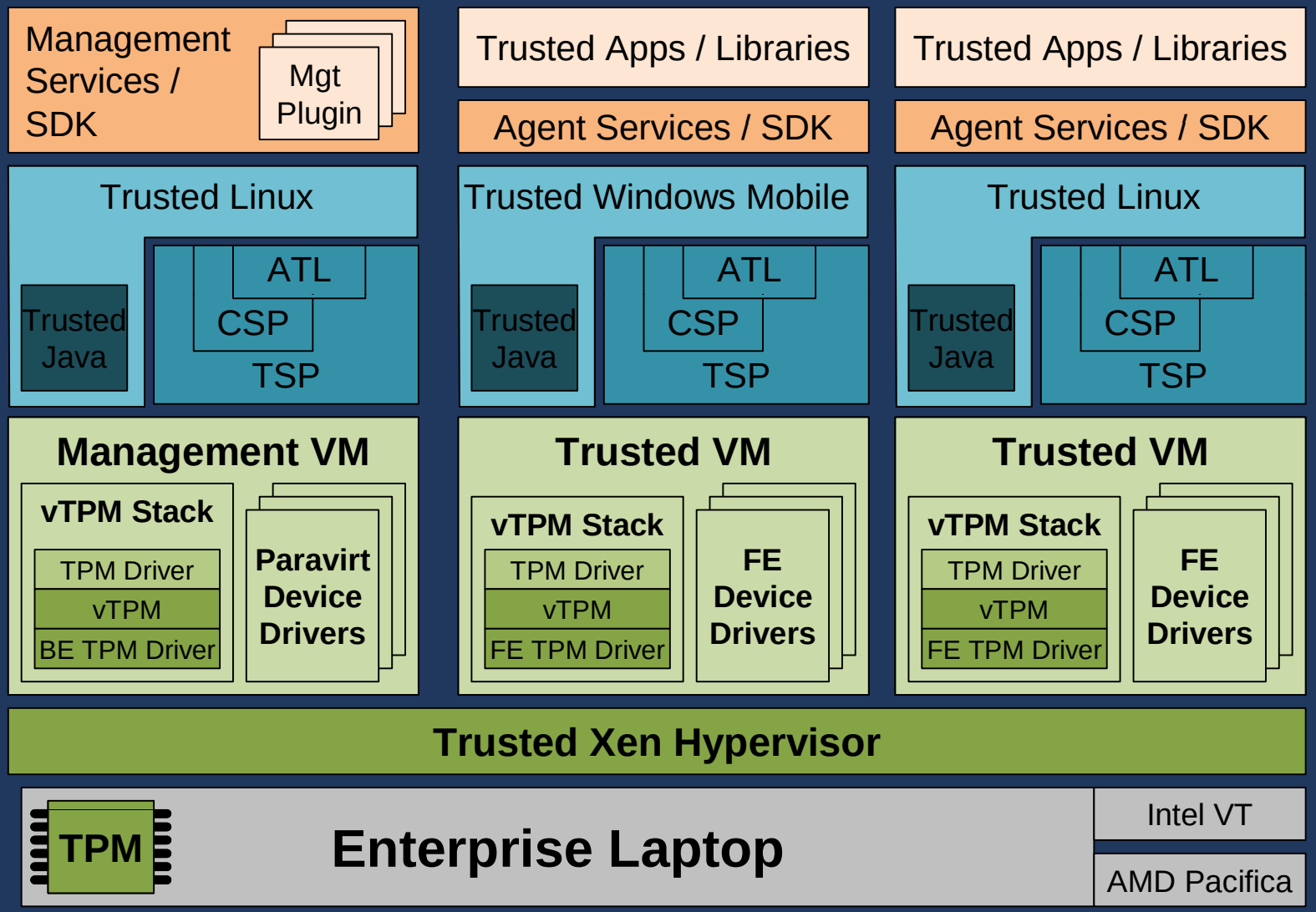
- Citrix
  - Xen acquisition provides strong Hypervisor technology base
  - But focused on enterprise server virtualization and virtual desktop markets
- Virtuallogix
  - “Real time virtualization for connected devices”
  - Security model is inadequate
- Avenda Systems
  - “End-to-end trust and identity policy solutions for Enterprise”
  - Focused on interoperating with Cisco NAC/NAP infrastructure
  - Lacks core security model – trusted boot, attestation, & trusted paths

Capital

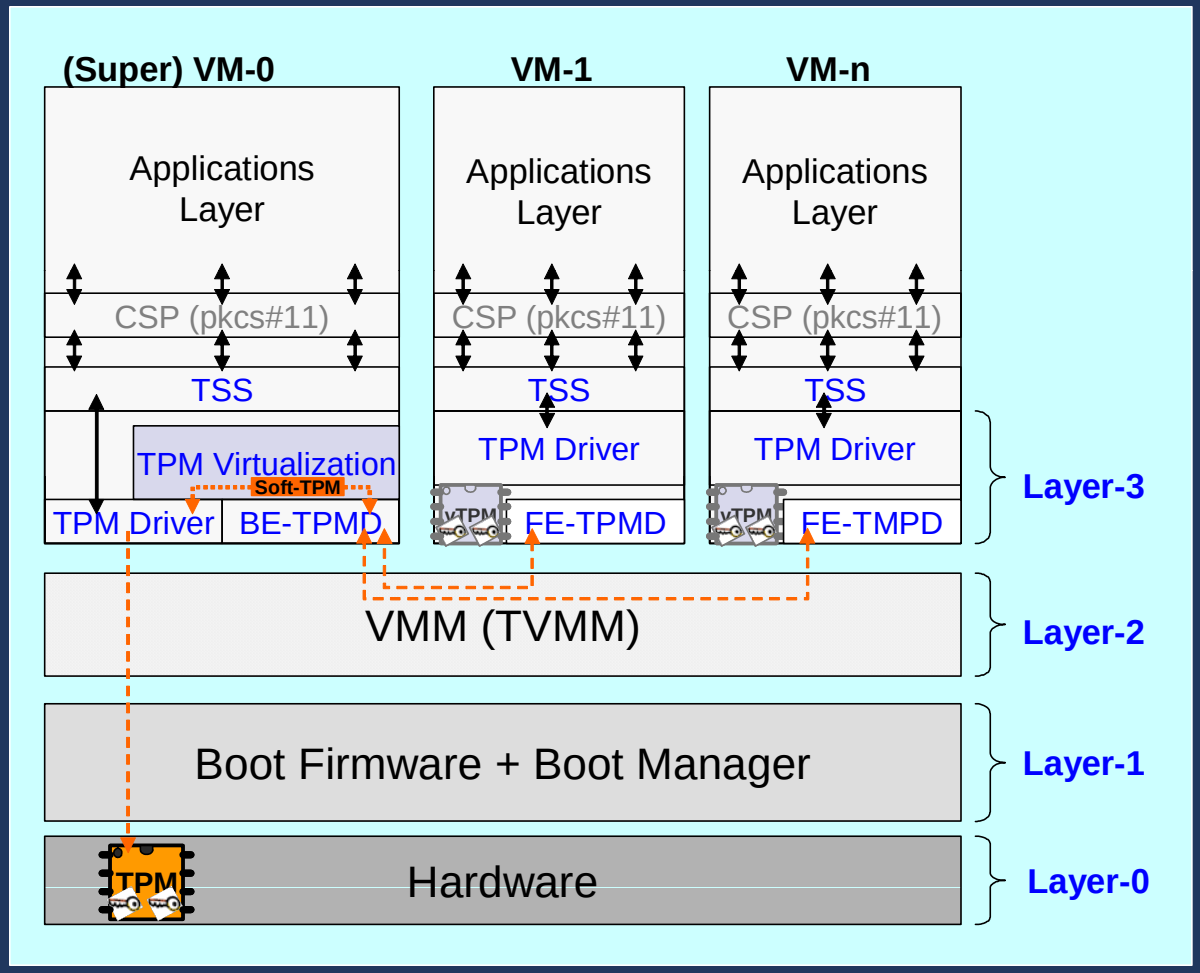
- $8M Series A
  - Provides 18 mo runway
  - Headcount grows to ~35 towards end of ’09
  - ~30% outsourced to India
  - Gives us 3 mo headroom after product launch

BACKUP SLIDES

Server Software Stack



Endpoint Software Stack



Example Scenario: Secure Corporate Access

- Single trusted instance/browser established to interface to corporate network via cellular link
- POLICY enforced at client disabling all other infection I/O routes for that VM
- This VM cannot be compromised by other instances on the client
- Email, anti-SPAM, and anti-virus scan on all IP streams performed by Agent on the server