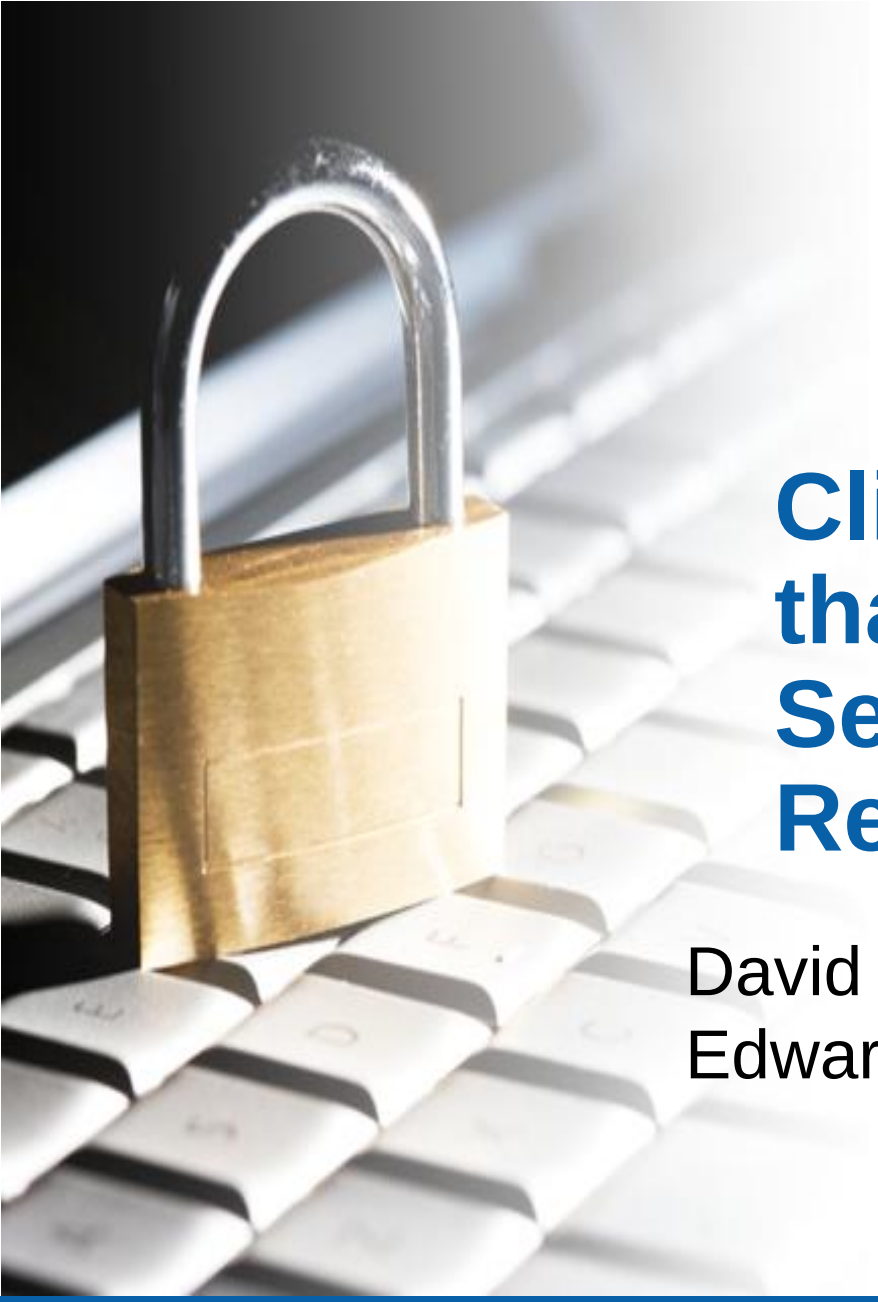


Client Technologies that Help Assist with Security and Privacy Regulation Compliance

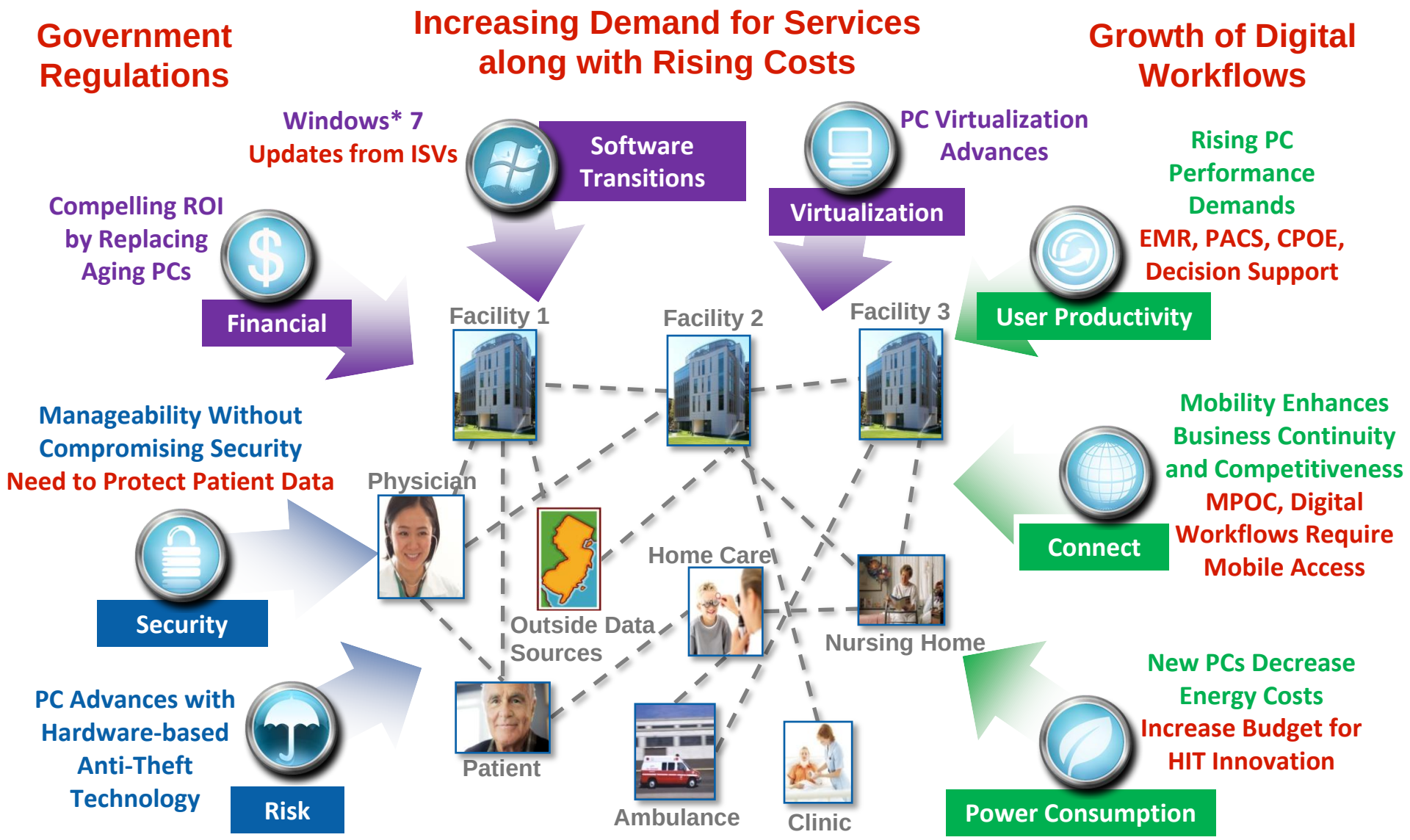
David Houlding, Intel Corporation
Edward J. Herold, Intel Corporation

Outline

- Healthcare Regulations,
  - HIPAA
  - HITECH
- Client Technologies
  - Context
  - Remote Manageability
  - Anti-Theft Technology
  - Encryption Acceleration
  - Client Virtualization

What are your client platform security & privacy needs, and does your computing solution satisfy these?

2010: Forces Shaping Healthcare Computing



Health Insurance Portability and Accountability Act - 1996

- Privacy Rule
  - provides federal protections for protected health information (PHI) held by covered entities and gives patients an array of rights with respect to that information
- Security Rule
  - specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic PHI
- Who has to worry about HIPAA? – Under review…
  - Health care providers
  - A health care claims clearinghouse
  - A health plan

Note: this is publicly available information and is not a legal summary of advice about HIPAA

HITECH Act Privacy and Security Provisions - 2009

- Ensure adequate privacy & security protections for PHI
- Calls for civil and criminal penalties to be applied equally & separately to BAs & covered entities
- Tighter restrictions on the disclosure or sale of PHI for marketing, research and similar uses
- Consumers right to obtain an electronic copy of their information from any provider with EHR
- Calls for ONCHIT to appoint a Chief Privacy Officer (CPO)
- Appropriates an additional $17 million for enforcement by CMS and OCR
- Strict breach notification requirements and penalties

Note: this is publicly available information and is not a legal summary of advice about the HITECH Act

Survey: Healthcare organizations' security not up to HITECH standards[1]

1. http://www.healthcareitnews.com/news/survey-healthcare-organizations-security-not-hitech-standards

Outline

- Healthcare Regulations,
  - HIPAA
  - HITECH
- Client Technologies
  - Context
  - Remote Manageability
  - Anti-Theft Technology
  - Encryption Acceleration
  - Client Virtualization

Client Technology Context

- Hardware based client technologies
- Dependencies to enable in an end solution
  - Correct client hardware
  - Compatible 3rd party software
  - Activation
  - 3rd party services
- Satisfying these dependencies may require some changes in your solution
- Further information
  - Remote Manageability: http://www.intel.com/technology/vpro
  - Anti-Theft Technology: http://www.intel.com/go/anti-theft
  - Encryption Acceleration (AES-NI): http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/
  - Client Virtualization: http://www.intel.com/go/virtualization

Outline

- Healthcare Regulations,
  - HIPAA
  - HITECH
- Client Technologies
  - Context
  - Remote Manageability
  - Anti-Theft Technology
  - Encryption Acceleration
  - Client Virtualization

Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. **To learn more visit: http://www.intel.com/technology/vpro**

All New 2010 Intel® Core™ vPro™ Processor Family:

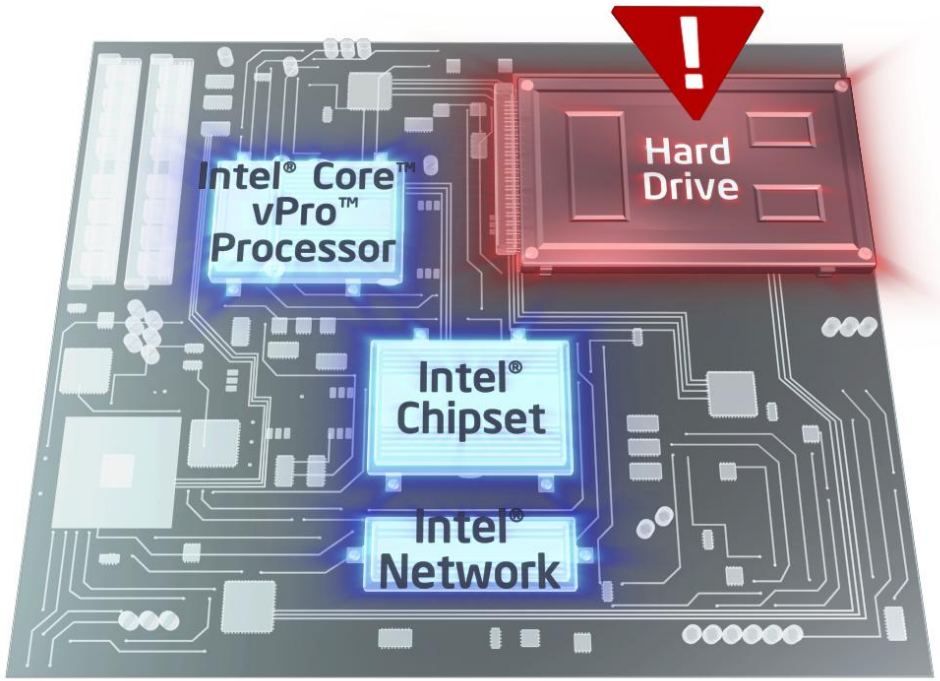
IT Computer Within the Computer

Smart Security and Cost Saving Manageability with activated features[1]

- Built into the hardware
- Regardless of OS or software agent health
- Even when powered off

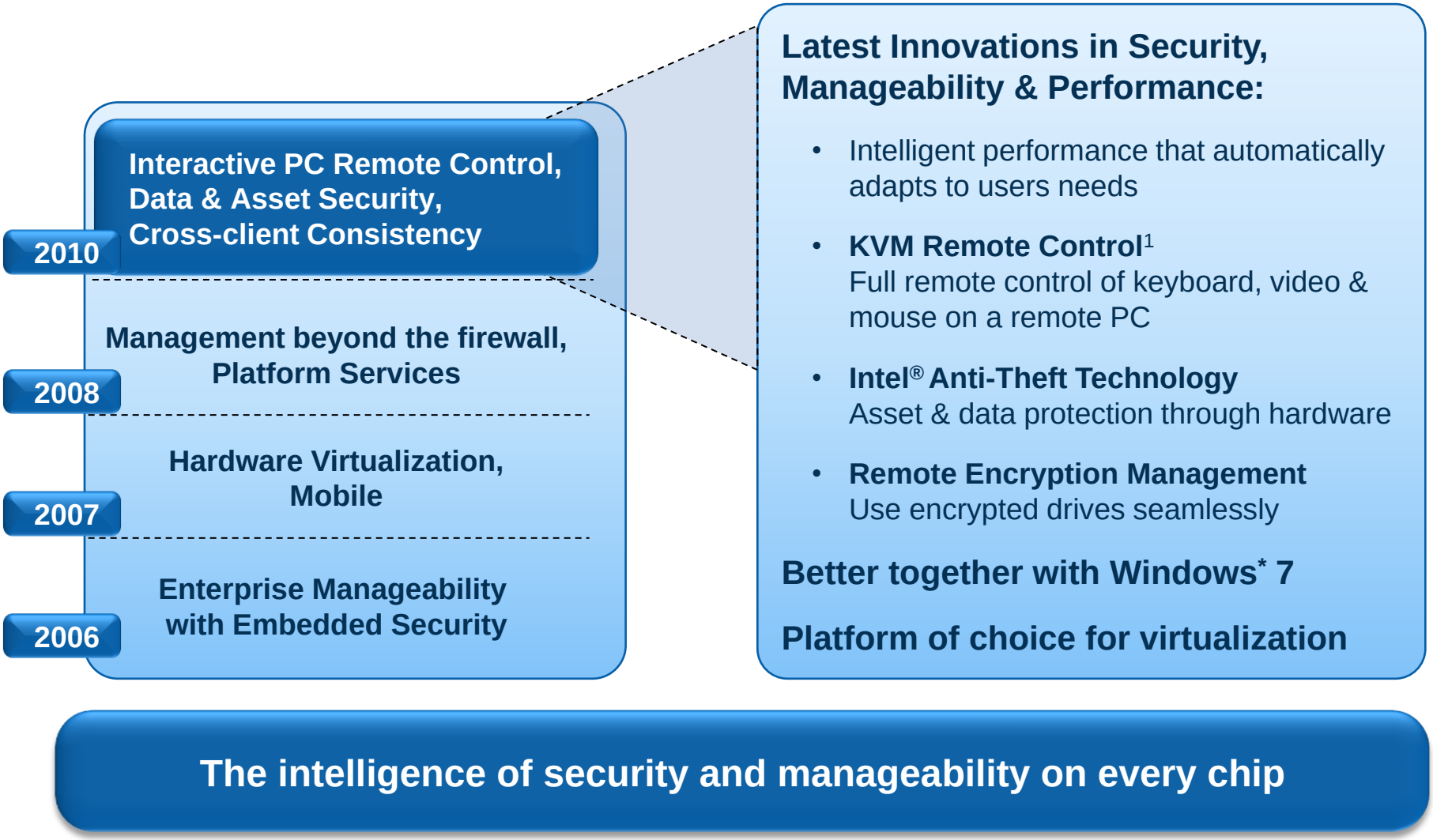
Specifically

- Secure power management
- Network isolation
- Remote remediation



1. Activated features include Intel Active Management Technology. Intel® Core™ vPro™ processor family includes Intel® Active Management Technology (Intel® AMT). Intel AMT requires the computer system to have an Intel AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection.
2. Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: http://www.intel.com/technology/vpro

All new 2010 Intel® Core™ vPro™ Processor Family: Sustained Innovation for Business PCs

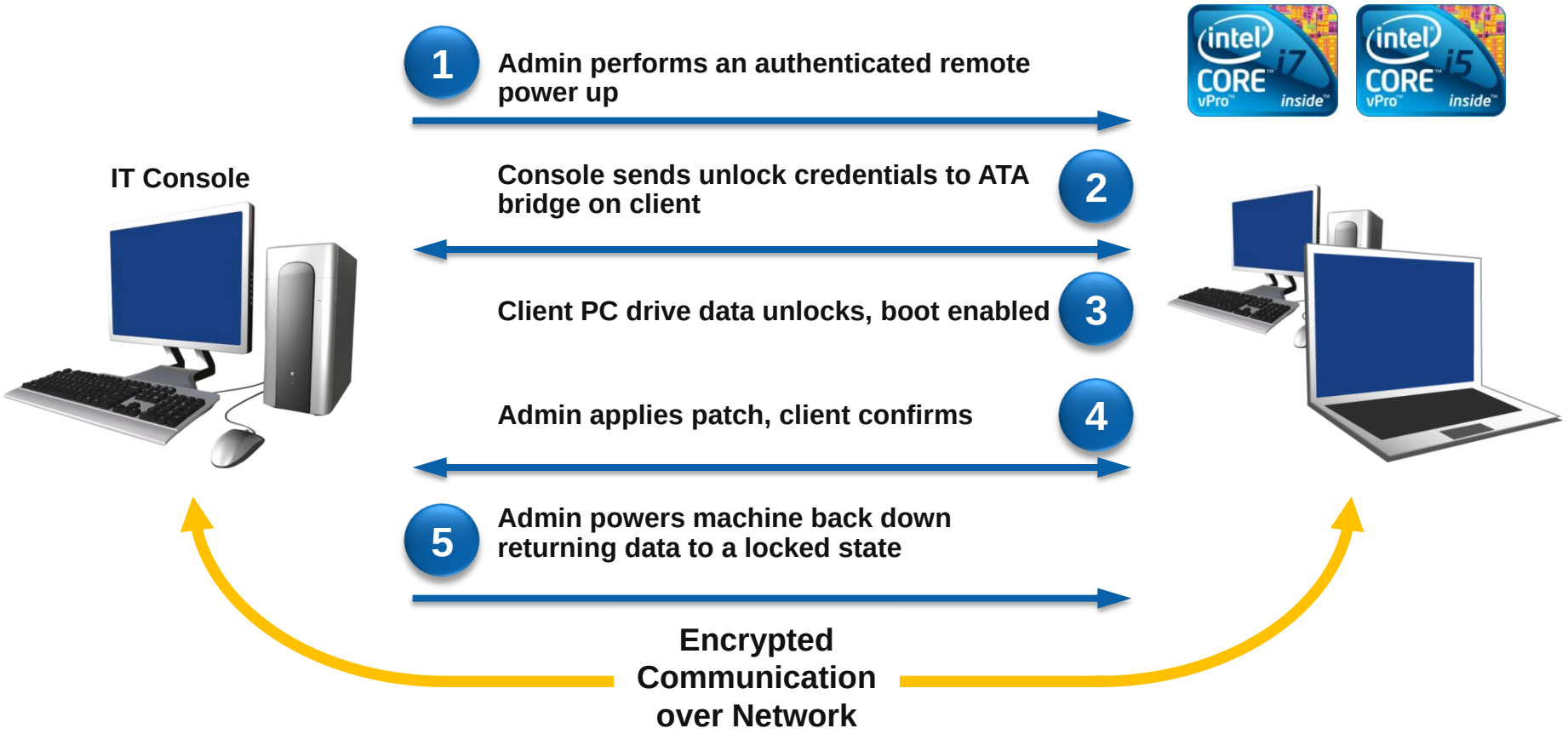


The intelligence of security and manageability on every chip

1. KVM Remote Control (Keyboard Video Mouse) is only available with dual-core Intel® Core™ i5 vPro™ processors and i7 vPro™ processors with active integrated graphics. Discrete graphics are not supported.

Data Protection and Manageability:

Extending the Reach of Your Management Console



Remotely Manage Powered Down, Unattended PCs with Encrypted HDDs

Intel® Active Management Technology requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. Intel AMT capability for notebooks may not be available or may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information see http://www.intel.com/technology/platform-technology/intel-amt

Providence Health System in Oregon

Customer Profile/Challenge

- **Reduce downtime for 11,000 PCs used by doctors and staff**
- Improve physical and electronic **asset management** to more rapidly locate PCs
- Facilitate **software patch** and **antivirus update** deployment
- Ensure **adherence with healthcare regulations**
- Assist with **software licensing compliance**
- Tighten patient information security by **keeping antivirus protection up to date** throughout the network

Solution

- The Providence IT group worked with Intel to evaluate how **Intel® vPro™ Technology can help reduce downtime, improve asset management, and tighten security**
- Intel consultants helped demonstrate the **potential benefits of Intel vPro Technology with Intel® Active Management Technology (AMT) through extensive testing and cost analysis**

Expected Results

- **50% annual savings for ensuring software compliance**
- 37% savings on desk side hardware support
- 81% savings on performing hardware inventory
- 33% savings on desk side software support
- **$510,000 USD savings over four years after costs of deploying Intel® vPro™ Technology, a 66% ROI**

"Today most of our IT budget is spent on keeping systems running. The savings we realize could help us redirect our resources toward more innovative projects."

-Michael Reagin

Chief Technology Officer, Providence Health System in Oregon

Case study available at http://www.intel.com/en_US/Assets/PDF/casestudies/ar_providience_vPro.pdf

Outline

- Healthcare Regulations,
  - HIPAA
  - HITECH
- Client Technologies
  - Context
  - Remote Manageability
  - Anti-Theft Technology
  - Encryption Acceleration
  - Client Virtualization

No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware and software and a subscription with a capable Service Provider. Consult your system manufacturer and Service Provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit http://www.intel.com/go/anti-theft

Intel® Anti-Theft Technology for PC Protection Services

Protections

- HW Based
- Works with/without NW connectivity (wired or wireless)
- Rendezvous timer
- Failed login threshold
- Poison pill
- Encryption keys in TPM

Responses

- Centrally trigger PC to display recovery message
- Disable PC (prevent boot)
- Disable access to data by either:
  - Deleting encryption keys, or
  - Deleting user credentials

Recovery

- Recovery passphrase established at PC setup time to re-enable PC
- One time token generated centrally to re-enable PC

Intel® Anti-Theft Technology—PC Protection (Intel® AT-p). Intel® Anti-Theft Technology (Intel® AT-p) requires the computer system to have an Intel® AT-enabled chipset, BIOS, firmware release, software and an Intel AT-capable Service Provider/ISV application and service subscription. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel® AT functionality has been activated and configured.

Allina Hospitals & Clinics in US

Customer Profile/Challenge

- Allina Hospitals & Clinics (Allina) is an organization of **11 hospitals**
- Allina has an extensive fleet of **3,800 mobile PCs**
- Allina has experienced a **sharp increase in laptop theft**
  - including an incident that required **public disclosure** of breached patient health information

Solution

- Allina looked to **Computrace with Intel AT for a solution** for managing the systems and protecting against data breaches

Comment from the Manager of Desktop Technology at Allina on Computrace + Intel AT

- "If a computer is lost or stolen, Computrace with Intel AT is a lifeline. If we are concerned about the information on a laptop, **we use Computrace to remotely delete the data**. Even if the machine is out of reach, we can still **'brick' the system through a local timer**. This is a **very effective tool for protecting confidential data and reducing risk**."

Information on this slide from the Intel White Paper "Built-in Protection in Laptop PCs Improves Compliance with New Healthcare Rules" at http://www.intel.com/Assets/PDF/whitepaper/health-323461.pdf

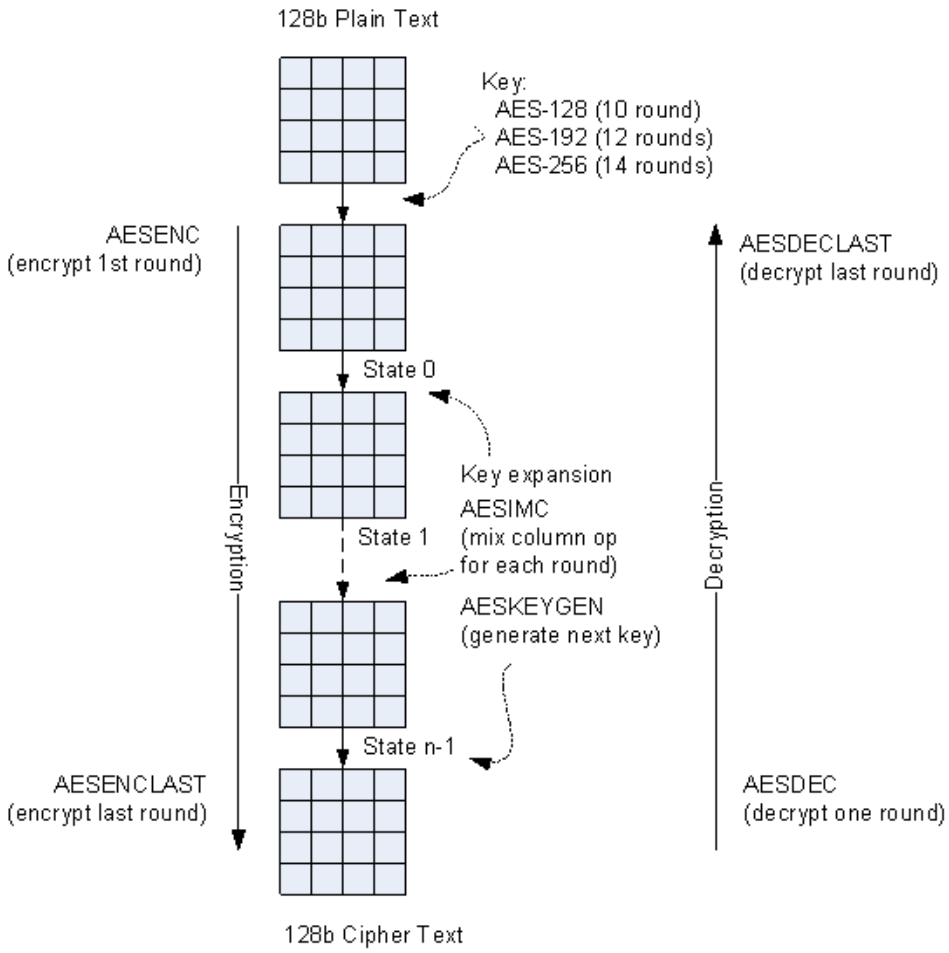
Outline

- Healthcare Regulations,
  - HIPAA
  - HITECH
- Client Technologies
  - Context
  - Remote Manageability
  - Anti-Theft Technology
  - Encryption Acceleration
  - Client Virtualization

Intel ® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/

Advanced Encryption Standard New Instructions (AES-NI)

- AES is currently the dominant block cipher, **standardized by NIST in FIPS PUB 197**
- AES-NI delivers HW accelerated encryption/decryption
  - Performance boost of 3+ times
- Mitigates the performance challenge with applying encryption
- Six new hardware instructions
- Flexible in supporting all standard usages of AES
- More robust hardware based implementation

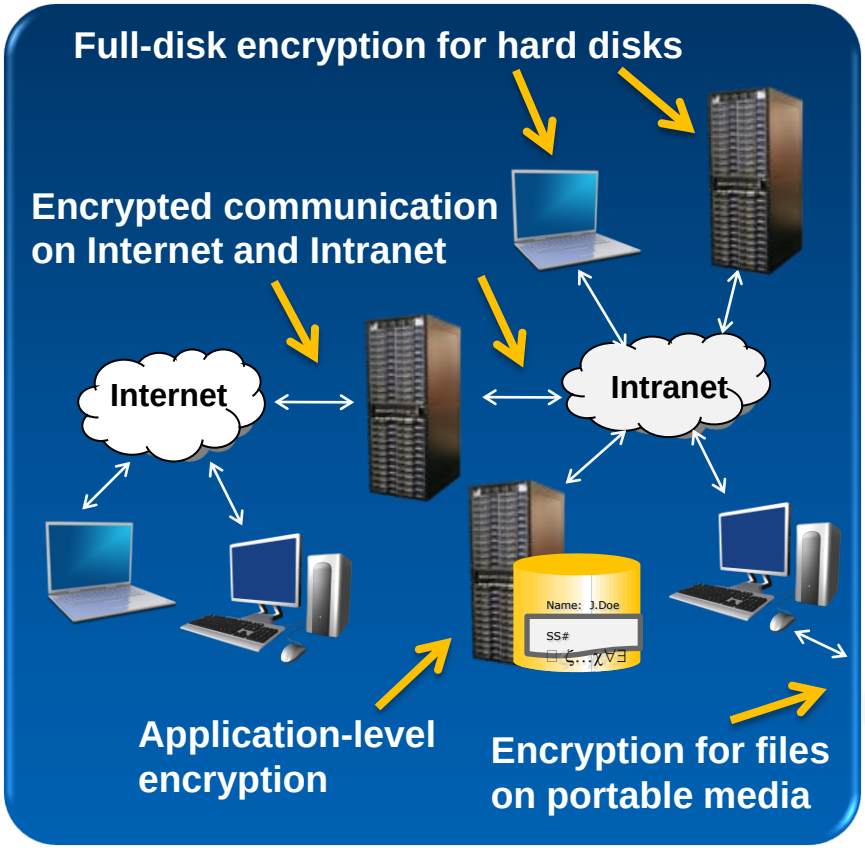


1. AES-NI is a set of instructions that consolidates mathematical operations used in the Advanced Encryption Standard (AES) algorithm. Enabling AES-NI requires a computer system with an AES-NI-enabled processor as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For further availability of AES-NI enabled processors or systems, check with your reseller or system manufacturer. For more information, see http://softwarecommunity.intel.com/isn/downloads/intelavx/AES-Instructions-Set_WP.pdf.

Example Applications of AES-NI

HIPAA Standard	HIPAA Specification Description
Access Control HIPAA Section 164.312(a)(1)	Encrypt and Decrypt EPHI
Transmission Security HIPAA Section 164.312(e)(1)	Encrypt EPHI during transmission

- AES-NI[1] can help improve the performance of
  - Secure network communication
  - Full disk encryption software
  - Applications which utilize AES



Connecticut AG sues Health Net over security breach --- Connecticut Attorney General Richard Blumenthal is seeking a court order blocking Health Net from continued violations of HIPAA by requiring **that any protected health information contained on a portable electronic device be encrypted**.[36]

1. AES-NI is a set of instructions that consolidates mathematical operations used in the Advanced Encryption Standard (AES) algorithm. Enabling AES-NI requires a computer system with an AES-NI-enabled processor as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For further availability of AES-NI enabled processors or systems, check with your reseller or system manufacturer. For more information, see http://softwarecommunity.intel.com/isn/downloads/intelavx/AES-Instructions-Set_WP.pdf.

36. healthcareitnews.com

AES-NI Ecosystem

Type	Product / Version	Availability
Secure Transactions (TLS/SSL)	Microsoft Windows Server 2008 R2	Now
	OpenSSL Patch	Now
	Red Hat Enterprise Linux 6	Beta 2 Now
	Fedora Linux 13	Now
Full Disk Encryption Software	Checkpoint Endpoint Security R73 FDE 7.4 HFA 1	Now
	McAfee Endpoint Encryption 6.0 with ePolicy Orchestrator 4.5	Now
	Microsoft BitLocker WS2008R2	Now
Enterprise Applications	Oracle Berkeley DB 11.2.5.0.26	2010
	Oracle Database 11.2.0.2	2010
Virtualization	VMware ESX 4.0 U1 (pass through support)	Now
Tools / Libraries	Intel® Compiler, V11.0	Now
	Microsoft Visual Studio 2008 SP1	Now
	GNU Compiler Collection, GCC v4.4.0	Now
	Microsoft Crypto Next Generation, CNG WS2008R2	Now
	Intel® Integrated Performance Primitives crypto library V7.0	Beta Now
	Network Security Services, NSS 3.12.3	Now

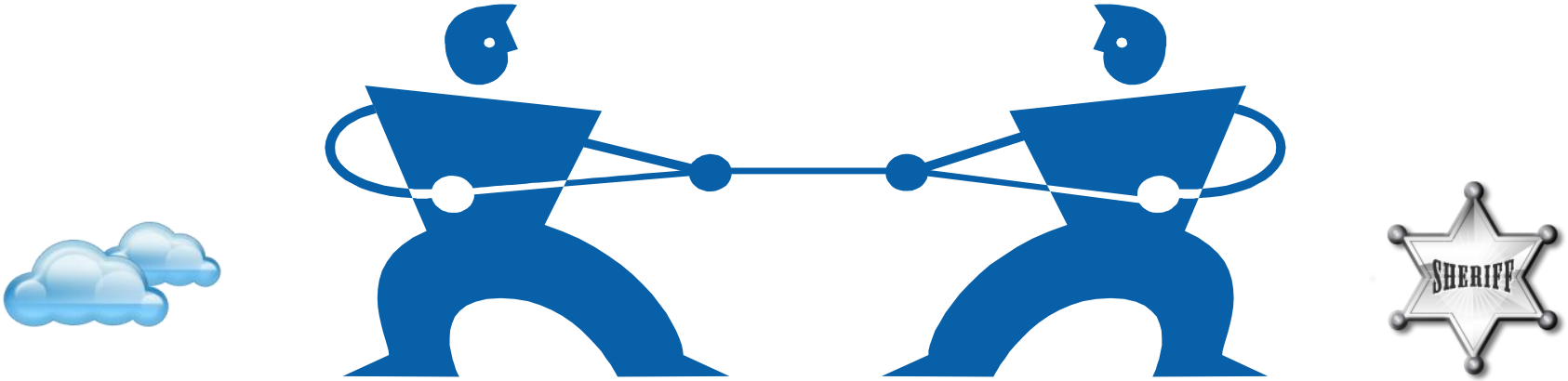
Outline

- Healthcare Regulations,
  - HIPAA
  - HITECH
- Client Technologies
  - Context
  - Remote Manageability
  - Anti-Theft Technology
  - Encryption Acceleration
  - Client Virtualization

Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization

BIG QUESTION: PHI on the Client?

As data is more portable it is more susceptible to being lost or stolen.



NO PHI on Client/Thin only

- Improved Security
- Central Manageability
- Fast Provisioning
- Network Security and Reliability
- Bandwidth Requirements

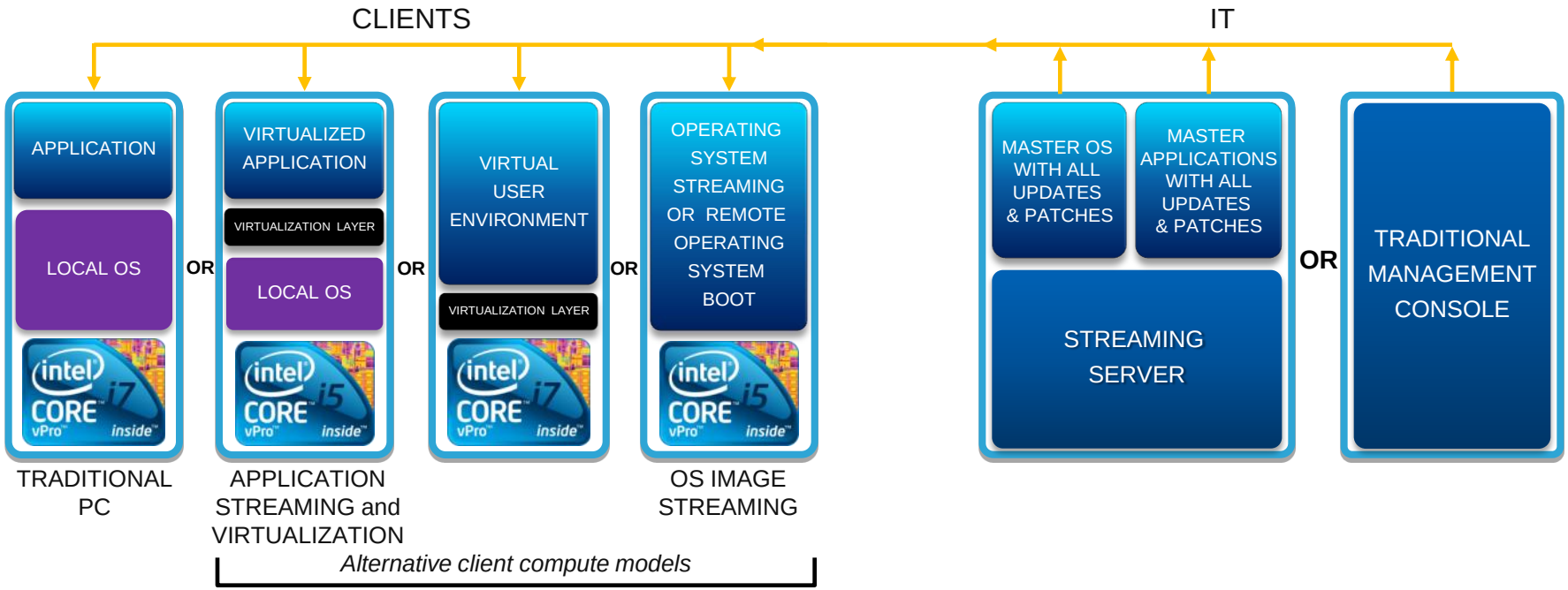
PHI on Client/Rich compute

- Flexible compute models
- Online/Offline data access
- Higher Risk, Especially Mobile
- Higher Client Platform and Manageability Costs

Choosing a client compute model requires Balancing Multiple Tensions Usage Models, Applications, Data and Regulations

Invest in a Flexible Computing Foundation With Built-In Security and Virtualization

Intel® vPro™ Technology PCs are the virtualization platform of choice



Leading ISV Support: Citrix*, Microsoft*, Symantec*, VMWare*

With the all new 2010 Intel® Core™ vPro™ processor family, be ready for today and prepared for tomorrow

Securing Virtual Client Computing

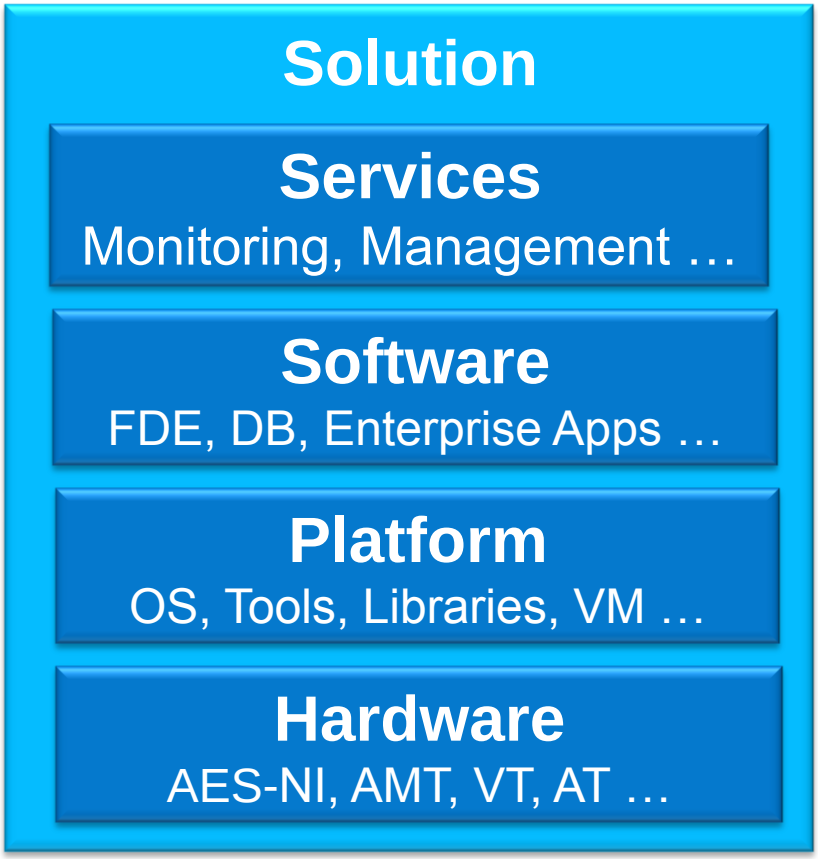
- Verified launch of VMM / hypervisor
  - Ensures integrity of the VM and underlying components
- Platform attestation for highly secure environments
- Hardware enforced separation of VM's
  - Ensures memory and process separation
- Memory scrub after VM terminates to avoid risk of residual sensitive data being compromised
- Central IT Administrator ability to disable VM's
- Separate VM's on the client for different purposes
  - Keep higher risk activities such as browsing away from most sensitive data eg PHI

Outline

- Healthcare Regulations,
  - HIPAA
  - HITECH
- Client Technologies
  - Context
  - Remote Manageability
  - Anti-Theft Technology
  - Encryption Acceleration
  - Client Virtualization
- Call to Action

Call to Action

- What are your client platform security & privacy requirements?
  - Encryption Acceleration
  - Remote Manageability
  - Client Virtualization
  - Anti-Theft Technology
- Does your solution enable you to take full advantage of these new client technologies?



Legal Disclaimers

- Intel® Anti-Theft Technology (Intel AT). No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) requires the computer system to have an Intel® AT-enabled chipset, BIOS, firmware release, software and an Intel AT-capable Service Provider/ISV application and service subscription. Intel® AT performs the encrypted data access disable by preventing access to or deleting cryptographic material (e.g. encryption keys) required to access previously encrypted data. ISV-provided Intel-AT-capable encryption software may store this cryptographic material in the PC's chipset. In order to restore access to data when the system is recovered, this cryptographic material must be escrowed/backed up in advance in a separate device or server provided by the security ISV/service provider. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel® AT functionality has been activated and configured. The activation process requires an enrollment procedure in order to obtain a license from an authorized security vendor/service provider for each PC or batch of PCs. Activation also requires setup and configuration by the purchaser or service provider and may require scripting with the console. Certain functionality may not be offered by some ISVs or service providers. Certain functionality may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof.