



**Secure Hardware-Based PC  
Management**  
*for*  
***Enterprise Business DT & NB***

Ed Herold  
Enterprise Technology Specialist  
Intel Federal

September 2008

# Legal Disclaimers

All dates and products specified are for planning purposes only and are subject to change without notice.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit <http://www.intel.com/performance/resources/limits.htm> or call (U.S.) 1-800-628-8686 or 1-916-356-3104.

Relative performance is calculated by assigning a baseline value of 1.0 to one benchmark result, and then dividing the actual benchmark result for the baseline platform into each of the specific benchmark results of each of the other platforms, and assigning them a relative performance number that correlates with the performance improvements reported.

SPEC, SPECint2000, SPECfp2000, SPECint2006, SPECfp2006, SPECjbb, SPECWeb are trademarks of the Standard Performance Evaluation Corporation. See <http://www.spec.org> for more information.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor series, not across different processor sequences. See [http://www.intel.com/products/processor\\_number](http://www.intel.com/products/processor_number) for details.

Intel products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

•Intel, Intel Xeon, Intel Core microarchitecture, Intel Pentium-D, Intel. Leap ahead. logo, Xeon Inside logo and the Itanium 2 Inside logo and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

\* Other names and brands may be claimed as the property of others.

Copyright © 2007-2008 Intel Corporation.



# Agenda

- Management & Security Capabilities
- Federal Usage – Energy Efficiency & Policy Enforcement

# With Active Management Technology (AMT)



**PC assets that are turned off can be electronically located, inventoried and/or patched.**

**PCs with an inoperable OS can be fixed down the wire.**



**You can remotely boot a PC into BIOS and then edit the BIOS.**



**ISV "console" communicates with vPro PC clients even if they are turned off**

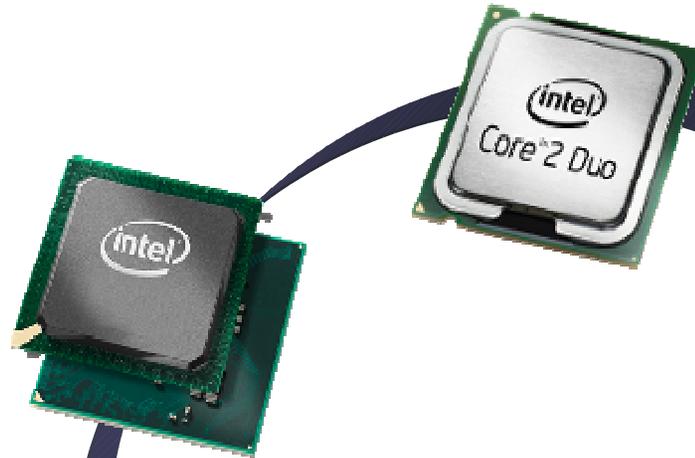
**Protection from virus outbreak or denial of service attack can be provided via a hardware filter on the Intel vPro chipset.**



# Ingredients

Intel® Core™2 Duo Processor

Intel® Chipset



Intel® 82566DM  
Gigabit Network  
Connection



Intel Platform  
Software &  
Ecosystem Solutions



Intel® Active  
Management  
Technology

Intel vPro Platform  
Technologies

Intel®  
Virtualization  
Technology

Intel®  
Trusted  
Execution  
Technology

Future (2009):

- HDD Encryption
- TPM v1.2
- Anti-Theft

# Agenda

- Management & Security Capabilities
- Federal Usage – Energy Efficiency & Policy Enforcement

# Energy Efficiency & Policy Enforcement

## Discover

- Remotely power on/off reliably
- Out-of-band asset inventory
- Discovery of connected systems

## Heal

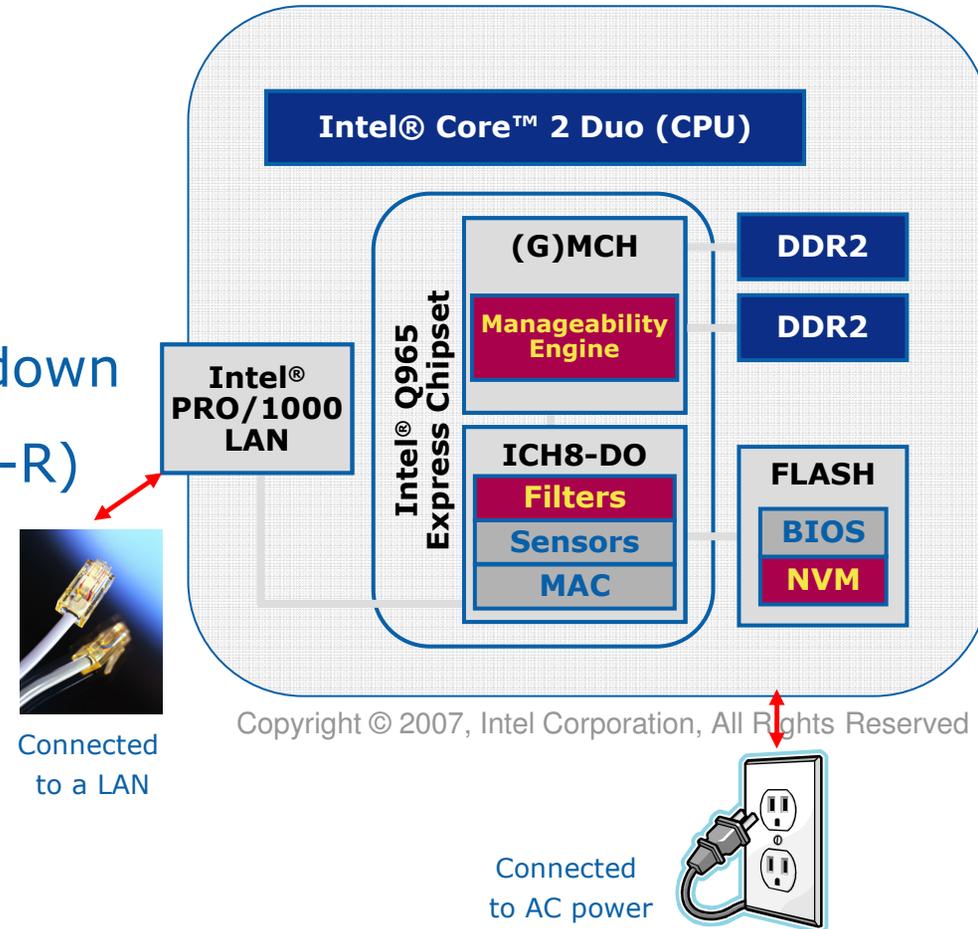
- Boot powered off PC, patch, shut down
- Redirect (Serial-over-LAN and IDE-R)

## Protect

- System Defense\*
- Agent Presence\*
- (Future) AT-d & AT-p \*

\* Implemented by  
3<sup>rd</sup> party software

## vPro Enabled PC



# ROI Estimator

ROI Estimator  
Security and manageability on the chip

Welcome to the business PC ROI Estimator. Simply enter your IT data into the ROI Estimator and instantly see the estimated IT support costs and savings possible with notebooks with Intel® Centrino® Pro processor technology and desktop PCs with Intel® vPro™ processor technology.

[Launch Estimator](#)

[View Sample Scenarios](#)

Copyright © 2007 Intel Corporation

Data and modeling based on 41 businesses with 1000 PCs or more from N. America and Europe

Adjustable inputs

Savings and Cost Difference output via table and graph

Select a Chart Option:  
 Costs  Savings  Details

Select a Currency:  
 U.S. Dollars

Estimate Annual Costs with and without Intel® vPro™ Technology and Intel® Centrino® Pro Processor Technology

Year	Estimated Yearly Cost without Intel® Centrino® Pro Processor Technology	Estimated Yearly Cost without Intel® vPro™ Processor Technology	Estimated Yearly Cost with Intel® Centrino® Pro Processor Technology	Estimated Yearly Cost with Intel® vPro™ Processor Technology
Year 1	\$4.1M	\$3.5M	\$2.9M	\$2.2M
Year 2	\$4.1M	\$3.5M	\$2.9M	\$2.2M
Year 3	\$4.1M	\$3.5M	\$2.9M	\$2.2M
Year 4	\$4.1M	\$3.5M	\$2.9M	\$2.2M

Cost Variables

Cost Variable	Enter Data
Number of Desktop PCs in the Enterprise	32,000
Number of Notebook PCs in the Enterprise	5,000
Number of Desktop Models Deployed Per Year	8
Number of Notebook Models Deployed Per Year	3
Number of Desktop PCs in the Intel® Stable Image Platform Program (Intel® SIPP) today	10%
Number of Notebook PCs in the Intel® Stable Image Platform Program (Intel® SIPP) today	5%

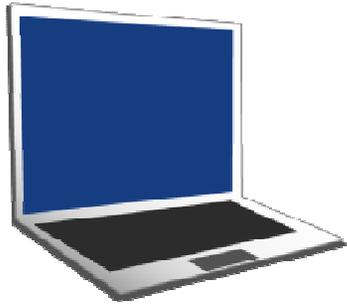
Copyright © 2007 Intel Corporation

# Activation, Deployment and Management

- AMT Community – on the internet  
<http://www.intel.com/go/vproexpert>
- Select the “Activation” Link

# Anti-Theft Technology Roadmap

## Montevina



**AT-p  
Notebook only**

**AT-d & AT-p  
converge on both  
Notebook &  
Desktop**



## McCreary



**AT-d  
Desktop only**

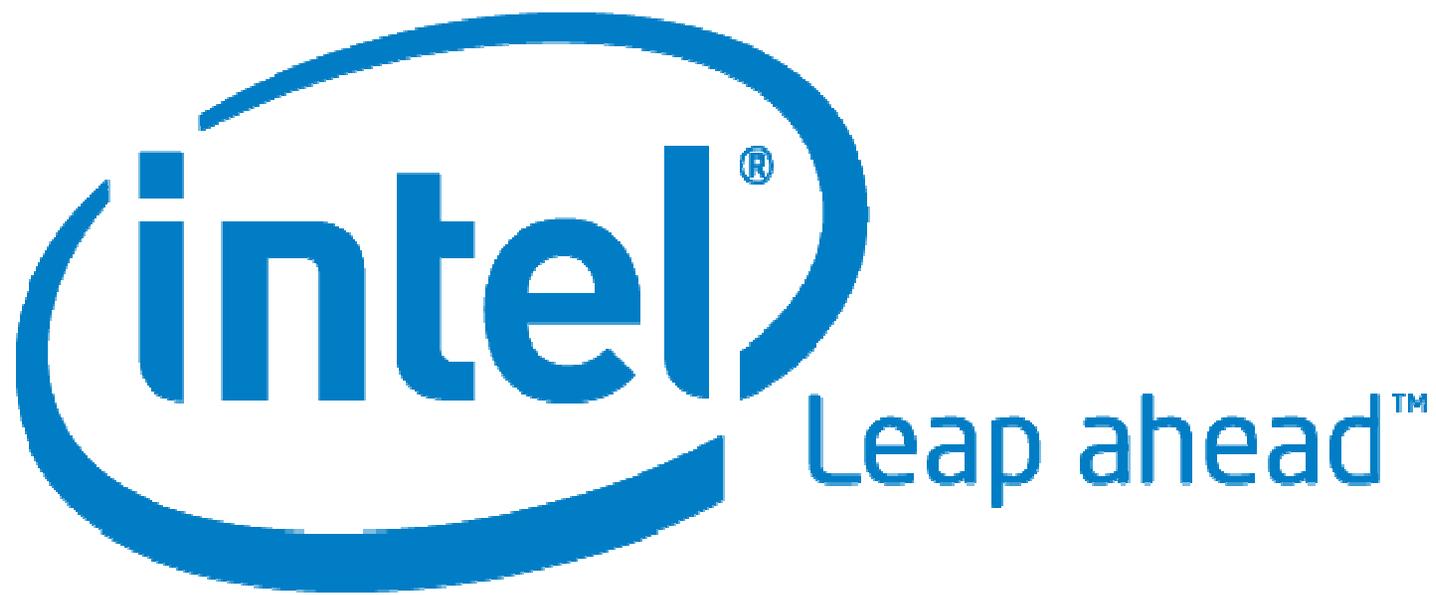
## Calpella/Piketon

Q4 2008

Q4 2009

**Cross client alignment with Calpella/Piketon**





# vPro Enterprise Provisioning

## Intel AMT Configuration States

### 1. Factory State

- AMT disabled
- No network configuration
- No security credentials

### 2. Setup State

- AMT enabled
- Basic network configured
- Admin credentials loaded

### 3. Configured State

- AMT fully configured (e.g power policies)
- Security credentials fully loaded
- Ready for remote management

