Intel® vPro™
and Information Security

Itai Yarom
Senior Technical Lead
LAN Access Division
Intel Israel
The Power of Two:

*It’s all about You*

The Intel brand delivers a promise to you and your customers, that when we partner, we deliver the “power of two”

- Together we deliver:
  - A more powerful promise
  - Unmatched products and experience
  - Powerful combination of brands
  - New excitement in the industry
  - More business opportunities for all of us
Information

Companies most valuable asset

Information can be lost by:
• Technical problem (HW failure).
• Device lost or stolen
• Malware attack
• Small form factor devices theft or lost.

How important are those issues?
• Laptop technical problems are consider as the biggest issue for laptops and laptops theft are in the second place.
• 1 of 8 laptop will be theft this year, and 95% won’t be recovered.
  – 33% of Intel’s laptop theft was from an employees’ cars and 27% at employees’ home.
• Small form factor devices are in higher risk for being stolen or lost over laptops.
Technical Problems

Most of IT spending is related to Hardware and software malfunction

Estimated desktop management-related cost savings associated with Intel vPro technology-enabled PC
Malware

Malware costs:
- Malware costs over $150 per PC user per year – not to mention the billions of dollars at stake if confidential information is leaked or lost due to malware infections. IronPort Systems
- Spy ware software exists on nearly 90% of all computers. This year alone more than 500,000 Americans will be robbed of their identities...with more than $4 billion stolen in their names. Every 79 seconds, a thief steals someone's identity, opens accounts in the victim's name and goes on a buying spree. CBSnews.com

Types of Malware:
• adware
• rootkits
• tracking cookies
• Trojan horses
• browser hijackers
• worms
• Internet dialers
• viruses
• keyloggers
Introducing Intel® vPro™ Technology
A leap forward in business PCs.
Intel® vPro™

**Manageability**
- Asset Inventory: Finding systems remotely
- Remote management for problem resolution

**Security**
- Three layers of defense
- Filtering threats and isolating PCs
- Push updates and patches down the wire regardless of PC power state

**Energy efficient performance**
- Intel® Core™ microarchitecture
- Cutting-edge transistor technologies
- Energy-efficient technologies

---

**Feature** | **Benefit**
---|---
Out-of-band (OOB) system access | Allows remote management of PCs regardless of system power** or OS state
Remote troubleshooting and recovery | Significantly reduces on-site visits to increase the efficiency of IT technical staff
Proactive alerting | Accelerates problem detection and decreases end-user downtime
Remote HW and SW asset tracking | Increases speed and accuracy over manual inventory tracking, reducing asset accounting costs
Third-party nonvolatile storage | Eliminates reliance on local software agents to store and retrieve data to help prevent accidental data loss
Proactive blocking and reactive containment of network threats | Helps prevent certain viruses and worms from infecting end-user PCs and spreading, increasing network uptime

**Note:**
** indicates power supply is active or network connection.
Handling Technical Problems

Networked systems
Numbers refer to process steps.

1. Problem occurs and system sends proactive alert to IT management console.
2. IT management console performs remote reboot of system.
3. IT heals system with remote control and diagnostics.

IT Management Console

<table>
<thead>
<tr>
<th>Areas of IT Support with the Most Cost Savings Potential</th>
<th>Cost Saving Category</th>
<th>Current Failure Rate</th>
<th>% of Failures That Can be Resolved using Intel vPro Technology</th>
<th>Current Cost of Resolving Failures</th>
<th>Projected Cost of Resolving Failures with Intel vPro Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major Hardware Malfunctions</td>
<td>27%</td>
<td>57%</td>
<td>$2,034,526</td>
<td>$406,905</td>
<td></td>
</tr>
<tr>
<td>Major Software Malfunctions</td>
<td>26%</td>
<td>56%</td>
<td>$1,863,042</td>
<td>$371,209</td>
<td></td>
</tr>
<tr>
<td>Patch Management Failures</td>
<td>22%</td>
<td>43%</td>
<td>$398,316</td>
<td>$79,863</td>
<td></td>
</tr>
<tr>
<td>Audit Failures</td>
<td>10%</td>
<td>54%</td>
<td>$346,980</td>
<td>$69,396</td>
<td></td>
</tr>
</tbody>
</table>
Malware Protection

**Networked systems**
Numbers refer to process steps.


2. Based upon IT policy, System Defense capability alerts, then isolates infected PCs from the network or simply limits their transmission rate until the problem can be investigated.

3. Using watchdog timers, Intel AMT quickly recognizes when critical management and security agents are disabled—either intentionally or accidentally—and immediately alerts IT staff.

4. Intel AMT uses OOB communications to automatically query systems for software versions and make appropriate updates and patches—even if systems are powered down.

**IT Management Console**

Keeping software and virus protection current.

---

**Security Technology and Services**

- **Services**
- **Hardware**
- **Software**

*Source: IDC - 2007*

---

**User OS / environment**

1. Hardware filters examine network traffic and rate-limit traffic or cut off the data path when a threat is recognized.

2. Third-party security applications check traffic for threats, while hardware "heartbeats" make sure those security agents stay active.

3. Nonvolatile memory helps protect critical system information from unauthorized access.
Theft protection

1 of 8 laptop will be theft this year, and 95% won’t be recovered.
- 33% of Intel’s laptop theft was from an employees’ cars and 27% at employees’ home.

Goals:
Secure sensitive information.
Restore information from the stolen system.
Track of the stolen system.

Technology:
Using the Intel® AMT™ secure memory to store encryption keys.
Use networking resources to send ‘beacon’ signal.
Lock system in case of theft scenario.
Protection Information on Small Factor Devices

Intel® Cross Platform Manageability Program

Small form factor devices are in higher risk for being stolen or lost over laptops.

How can I protect the information on those small factor devices?

Technology:

Use Intel® AMT™ secure memory to store encryption keys.

Connected devices can use Intel® AMT™ services from a connected client.

Other suggestions?
Summary

- Intel® AMT™ is one of the main component of the Intel® vPro™ Platform.
  - It was invented and developed in Intel Israel Design Center (IDC).
- Intel® AMT™ provides benefits to the corporate and hold promise for the consumer market.
  - Intel® AMT™ frame work can be extended to new usage model.
Resources for Technology at Intel

• Subscribe to Technology@Intel magazine and the Intel Technology Journal

• Attend Intel Developer Forums - www.intel.com/IDF

• Cooperate through the Intel Software Network - softwarecommunity.intel.com

• Watch for Intel research and development related topics in the news
  – Technology and product announcements
  – Profiles of leading research professionals and initiatives

www.intel.com/technology