Intel Leap ahead™

Intel Israel Design Center

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 assent

Information can be lost by:

- Technical problem (HW failure).
- Device lost or stolen
- Malware attack
- Small form factor devices theft or lost.

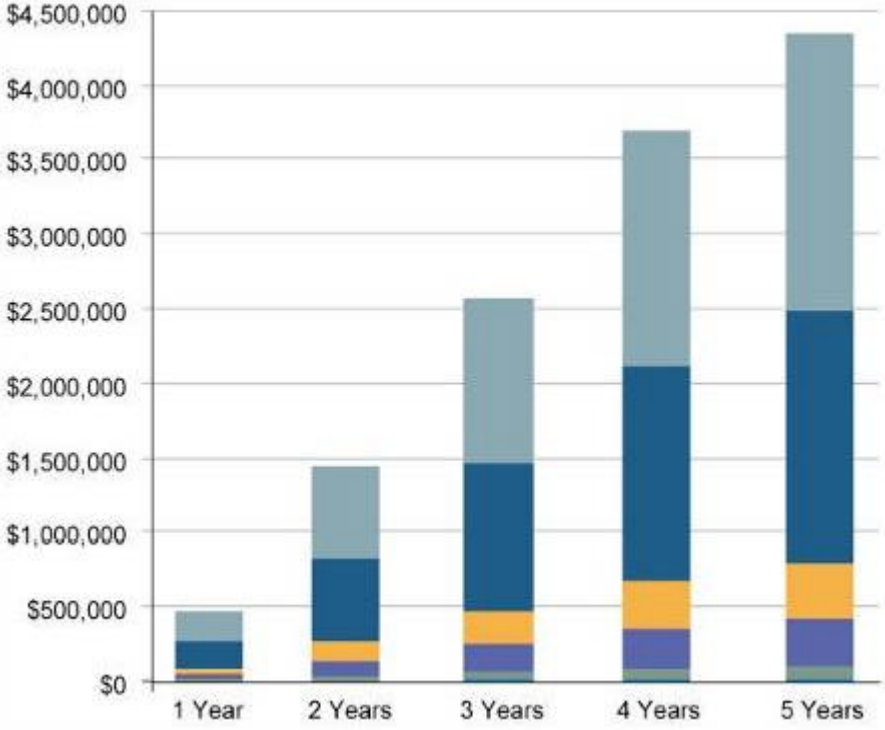
How important are those issues?

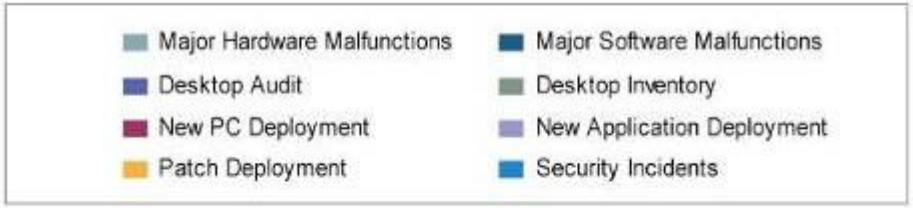
- Laptop technical problems are consider as the biggest issue for laptops and laptops theft are in the second place.
- 1 of 8 laptop will be theft this year, and 95% won't be recovered.
  - 33% of Intel's laptop theft was from an employees' cars and 27% at employees' home.
- Small form factor devices 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





	1 Year	2 Years	3 Years	4 Years	5 Years
New Application Deployment	$35	$107	$190	$274	$323
New PC Deployment	$703	$2,132	$3,792	$5,467	$6,444
Security Incidents	$1,299	$3,934	$7,000	$10,090	$11,895
Desktop Inventory	$9,235	$27,981	$49,784	$71,761	$84,594
Desktop Audit	$34,698	$105,135	$187,053	$269,628	$317,847
Patch Deployment	$39,932	$120,993	$215,267	$310,298	$365,789
Major Software Malfunctions	$185,604	$562,381	$1,000,574	$1,442,280	$1,700,208
Major Hardware Malfunctions	$203,453	$616,461	$1,096,793	$1,580,975	$1,863,706
TOTAL	$474,959	$1,439,124	$2,560,454	$3,690,773	$4,350,806

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

	ADWARE	TROJANS	SYSTEM MONITORS	TRACKING COOKIES
Global Infection Rates	48%	7%	5%	77%
North America	66.72%	9.75%	6.96%	89.39%
UK	46.35%	6.77%	4.84%	74.48%
Germany	43.27%	6.32%	4.52%	69.53%
France	38.69%	5.65%	4.04%	62.17%
Japan	43.37%	6.34%	4.53%	69.69%
China	55.32%	8.08%	5.77%	88.9%
Australia/New Zealand	39.88%	5.83%	4.16%	64.09%
Other	49.73%	7.26%	5.19%	79.91%


intel
Leap ahead™
Introducing Intel® vPro™ Technology
A leap forward in business PCs.
intel
vPro™

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

Intel vPro Technology.
A Leap Forward in Business PCs.

> MANAGEABILITY

> SECURITY

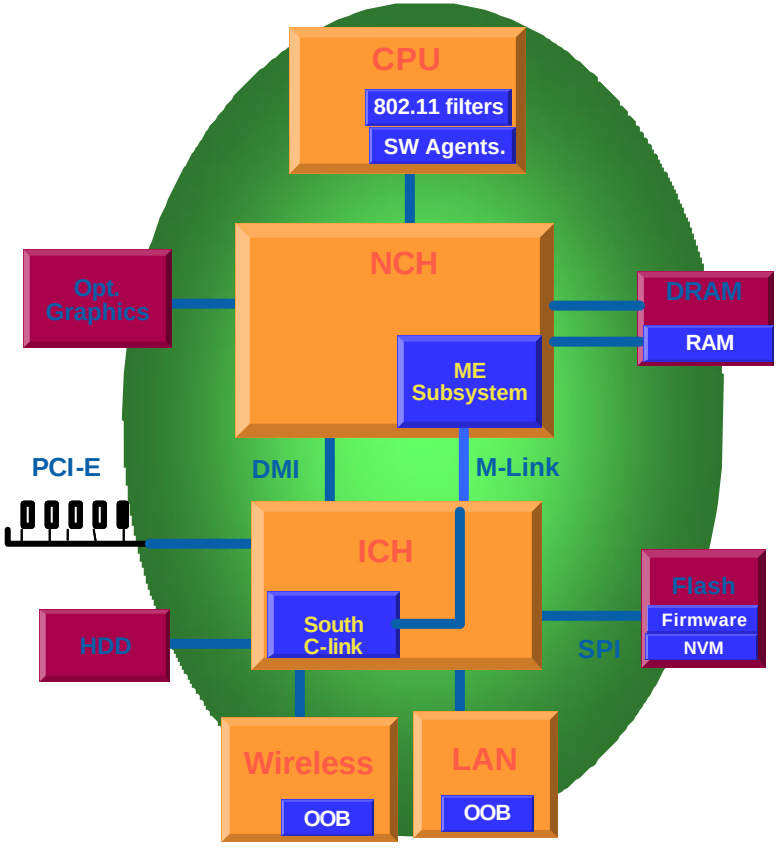
> ENERGY-EFFICIENT PERFORMANCE

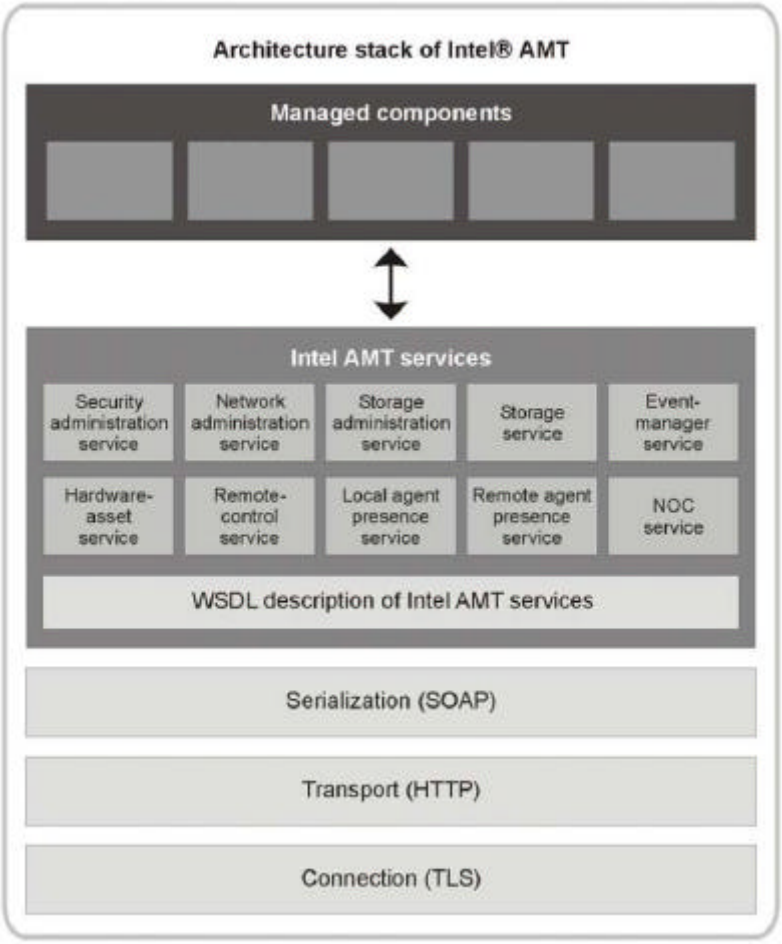
intel vPro™

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 deskside 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

** Requires power supply and an active network connection

Intel® vPro™ Architecture





intel

Handling Technical Problems

Networked systems

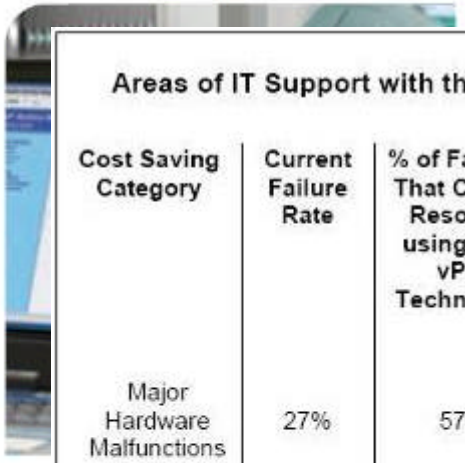
Numbers refer to process steps.

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



Areas of IT Support with the Most Cost Savings Potential

Cost Saving Category	Current Failure Rate	% of Failures That Can be Resolved using Intel vPro Technology	Current Cost of Resolving Failures	Projected Cost of Resolving Failures with Intel vPro Technology
Major Hardware Malfunctions	27%	57%	$2,034,526	$406,905
Major Software Malfunctions	26%	56%	$1,856,042	$371,208
Patch Management Failures	22%	43%	$399,316	$79,863
Audit Failures	10%	54%	$346,980	$69,396

Malware Protection

Networked systems

Numbers refer to process steps.

1 System Defense capability scans incoming traffic for known viruses and worms.

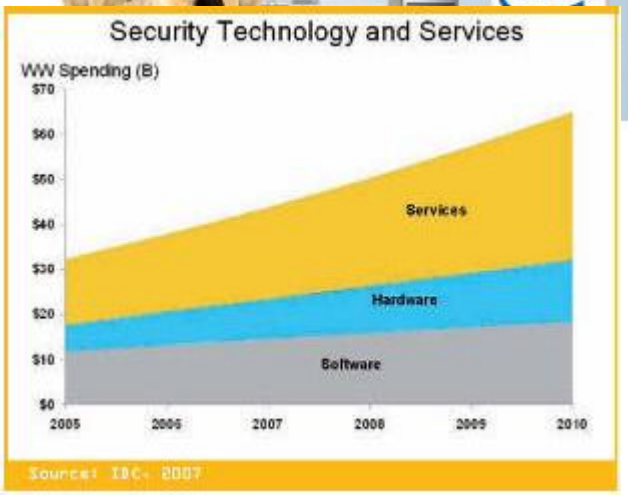
2 Based upon IT policy, System Defense capability alerts, then isolates infected PCs from the network or simply limits their transmission rate until the problem can be investigated.

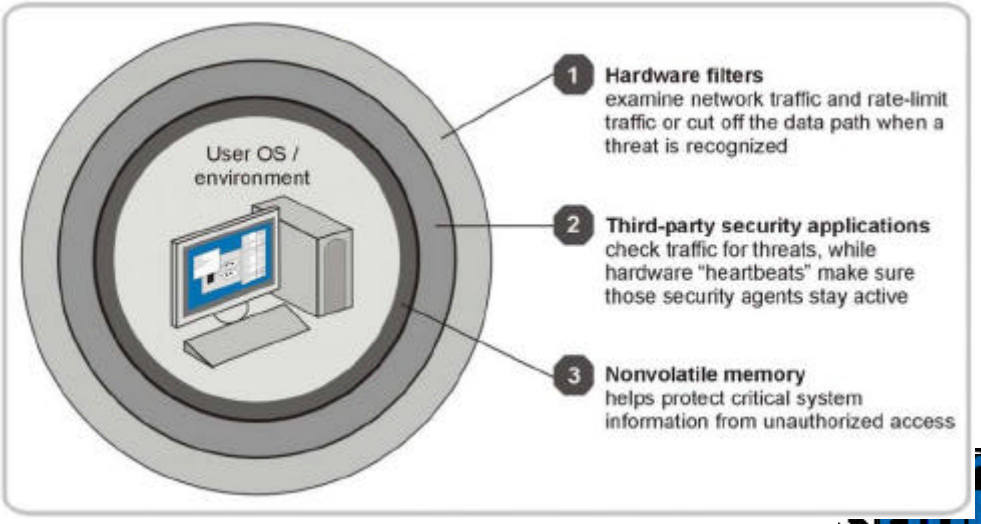
3 Using watchdog timers, Intel AMT quickly recognizes when critical management and security agents are disabled—either intentionally or accidentally—and immediately alerts IT staff.

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.





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.

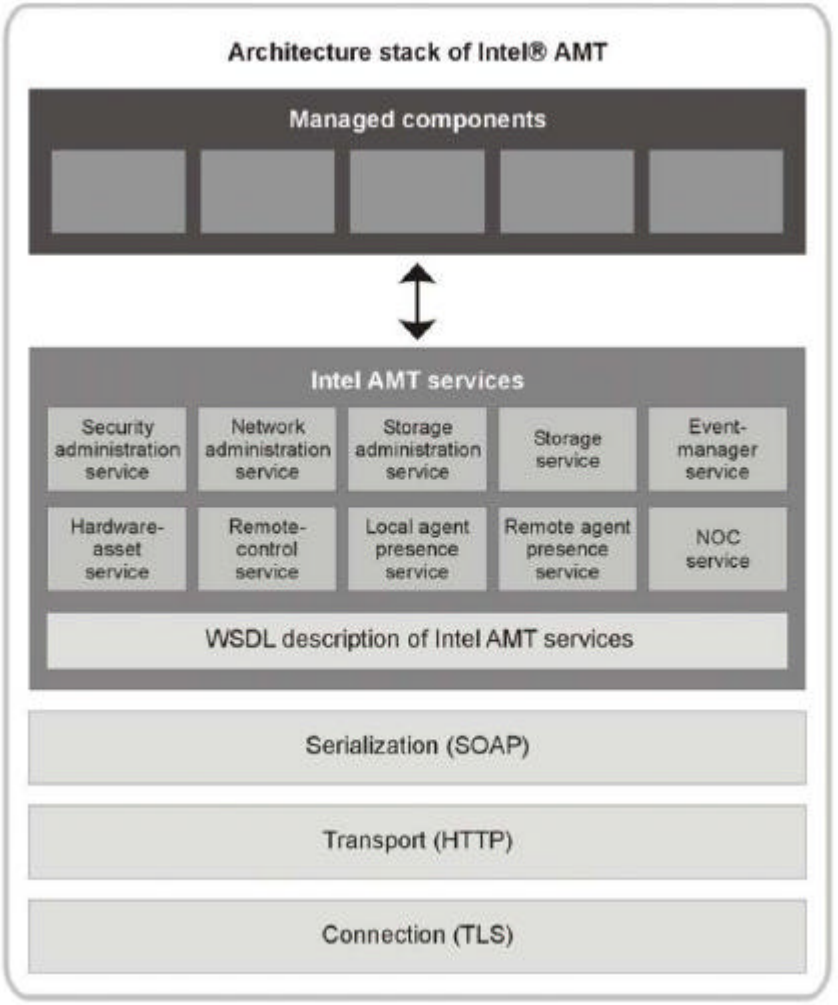
Track of the stolen system.

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.



intel

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.

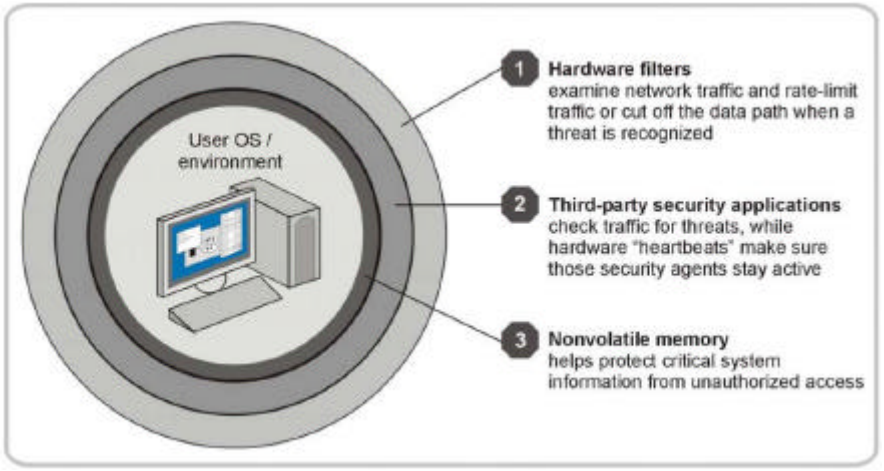
How can I protect the information on those small factor devices?

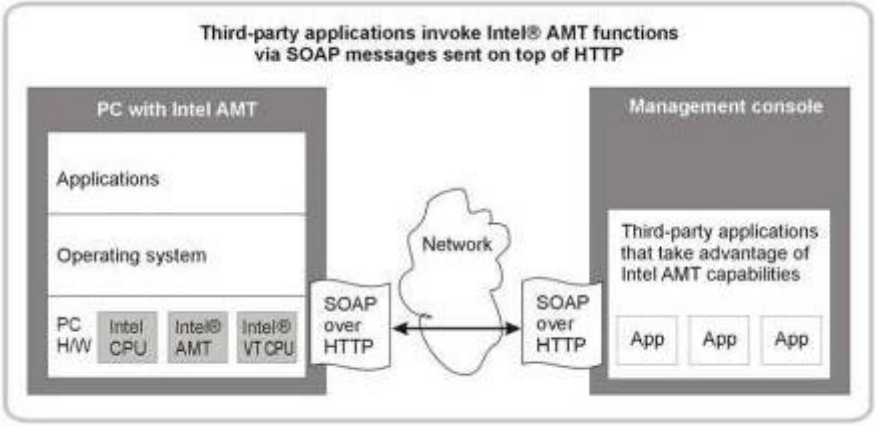
Technology:

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

Itai.Yarom@Intel.com

intel