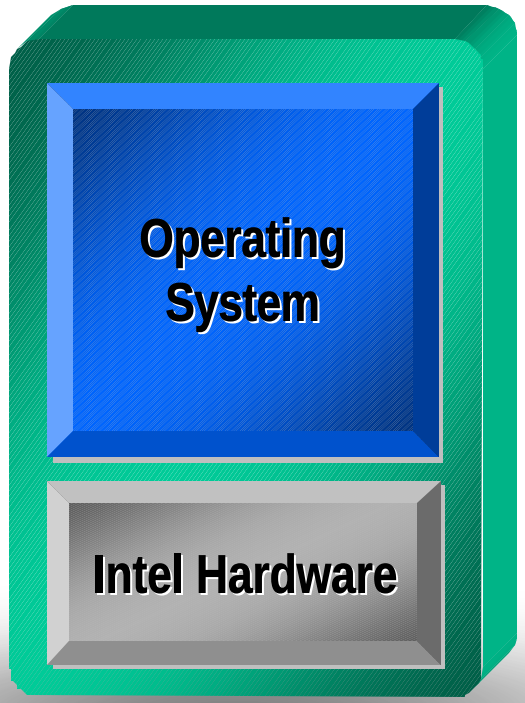
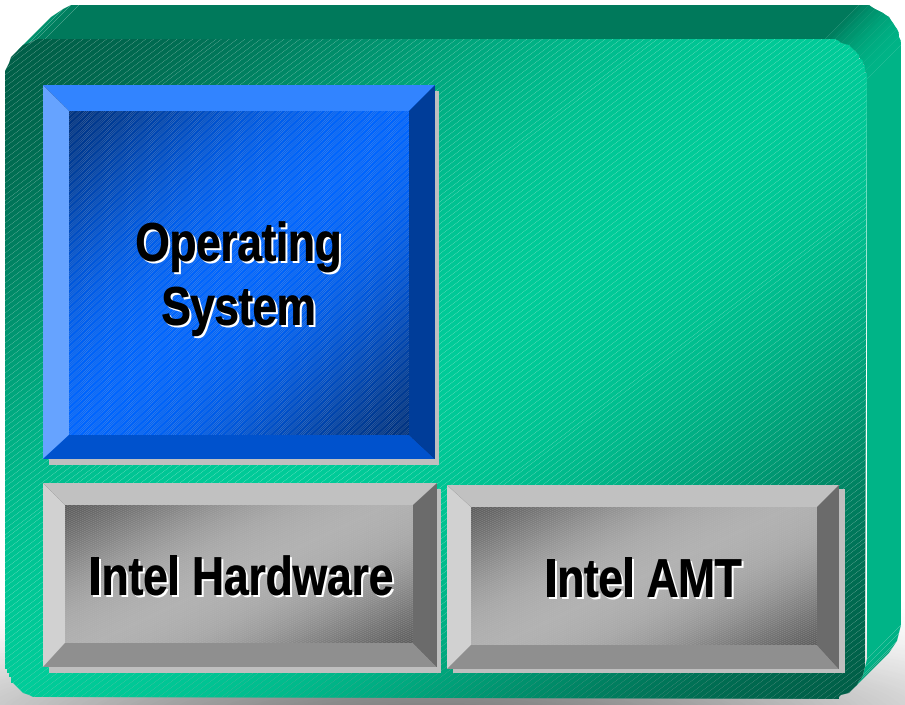
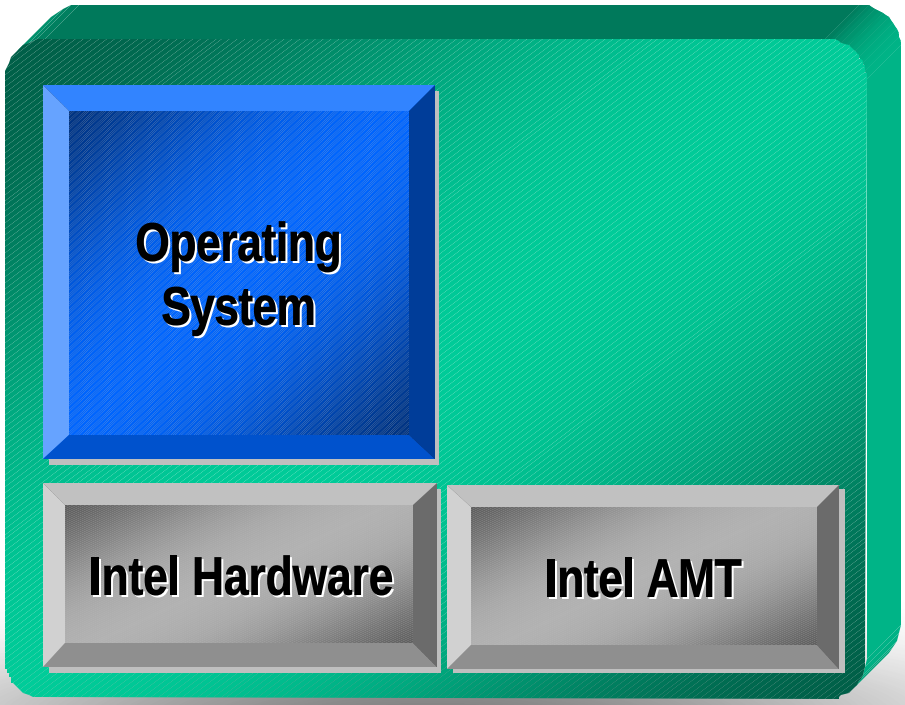
Intel Active Management Technology



Intel Active Management Technology

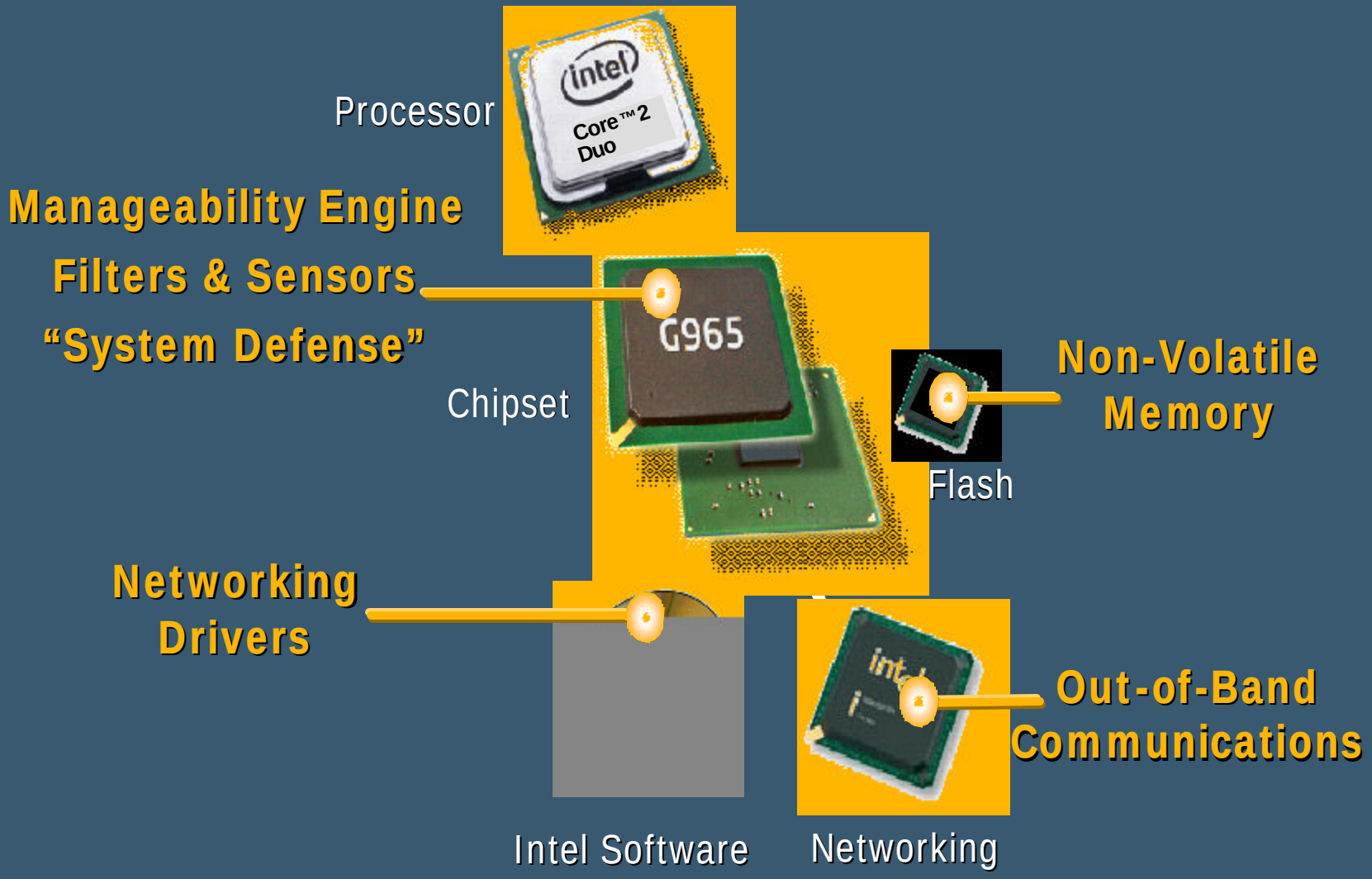


Intel Active Management Technology



Discover	Platform Audit Software Inventory Management Hardware Inventory Management
Heal	Remote Diagnosis, Remote Repair Remote Diagnosis, Local Repair
Protect	Software Version Compliance Hardware-Based Isolation and Recovery Agent Presence Checking

Intel® Active Management Technology



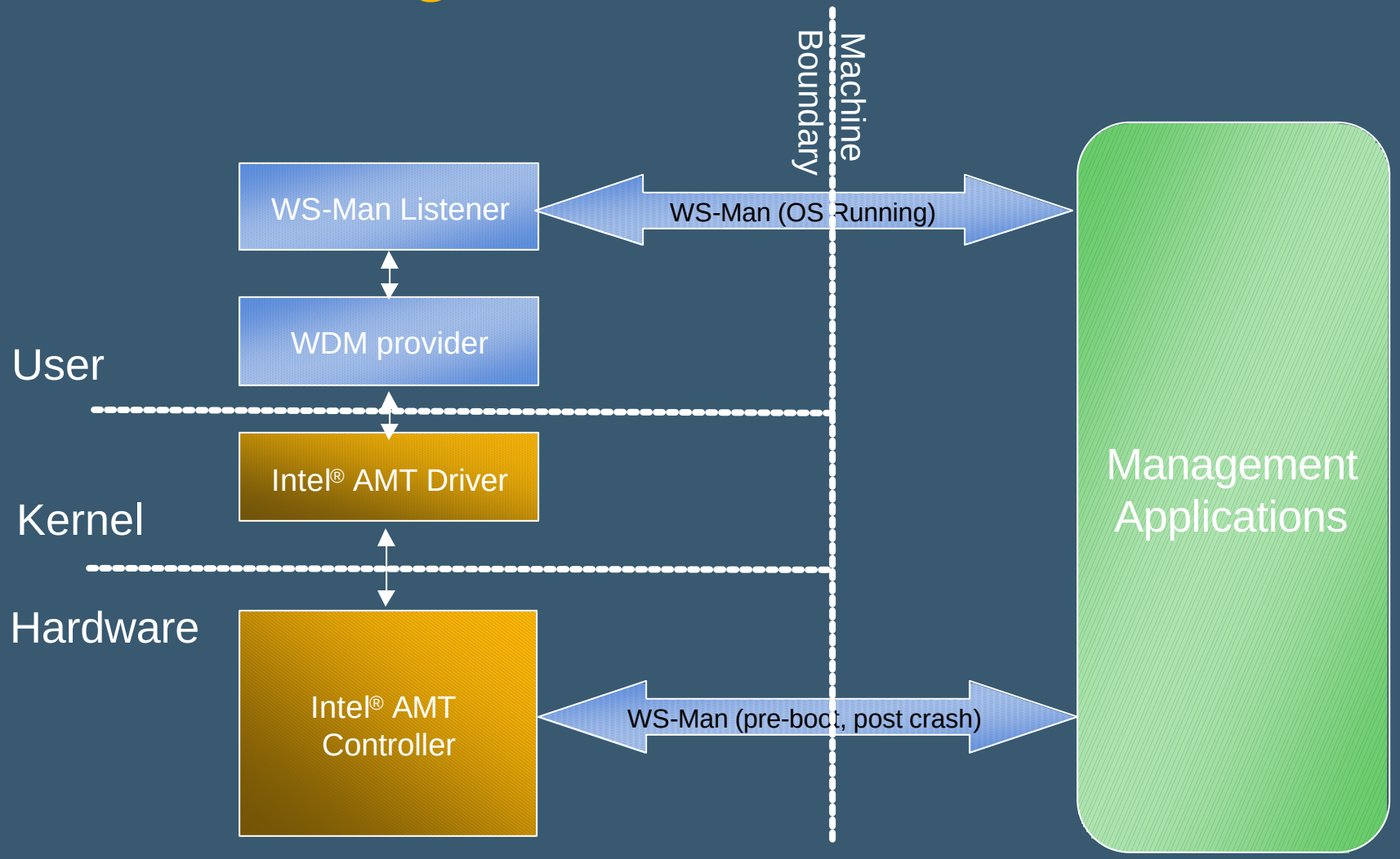
Changing the Game: Intel® Active Management Technology

- Out-of-band system management
  - Remote management regardless of power on/off state or OS state
  - Direct connection via TCP/IP firmware stack
- Tamper-resistance
  - Hardware/firmware solution
- Persistence
  - Nonvolatile storage of state
  - Survives power outages and system rebuilds

Out-of-band system management

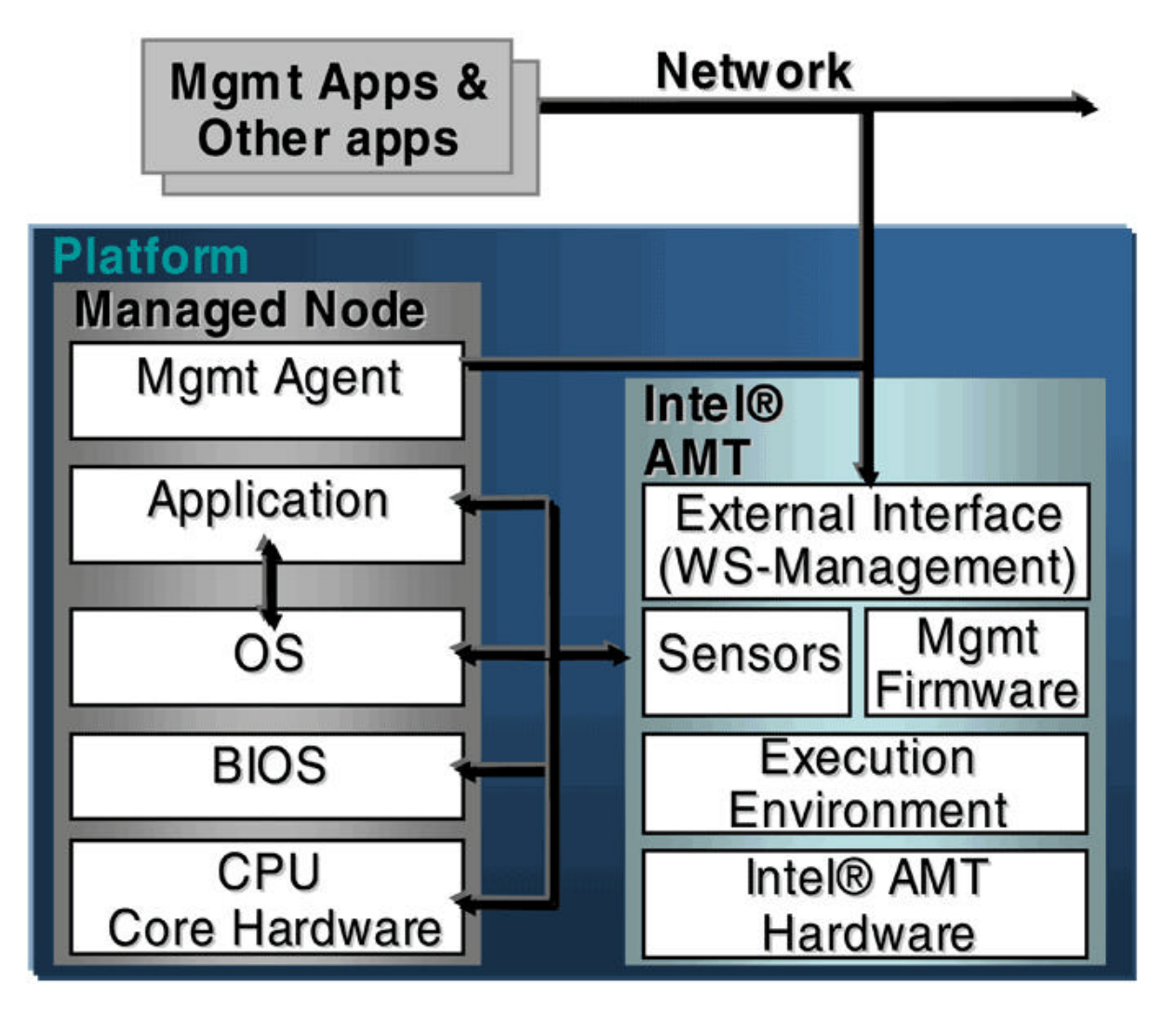
- Discover PCs and their configuration on the network independent of their operational state
  - Remote hardware/software inventories
- Securely wake & update PCs
  - Remote troubleshooting and recovery
  - Remotely repair a PC
- Prevent critical security code from being disabled
  - Process monitoring (e.g. anti-virus)
- Detect & block anomalous network behavior
  - Network packet filtering for inbound/outbound traffic
- Proactive alerting

WS-Management for In-band and Out-of-band

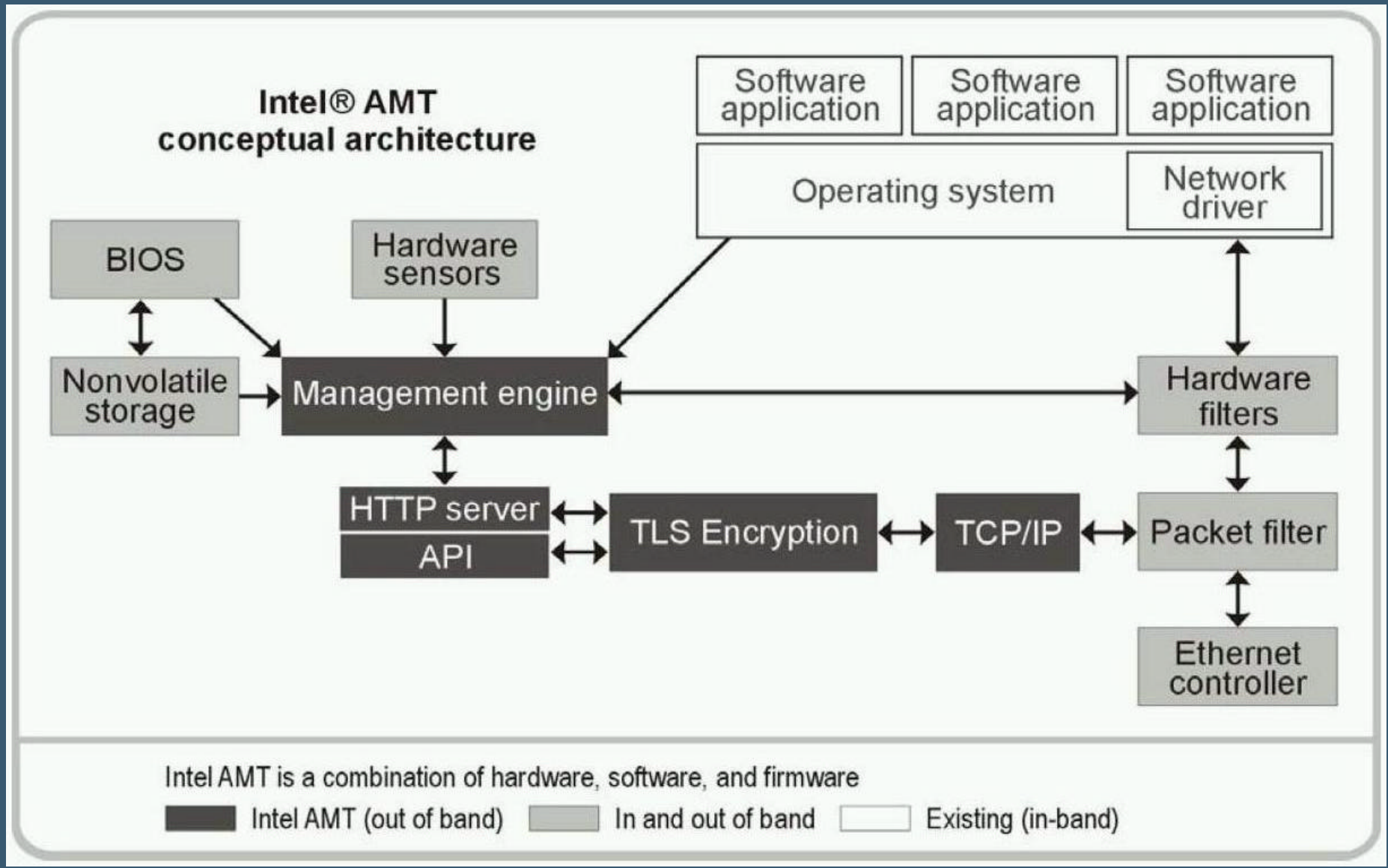


Intel, Microsoft and other industry players have announced WS-Management to help address the cost and complexity of IT management

Intel Active Management Technology

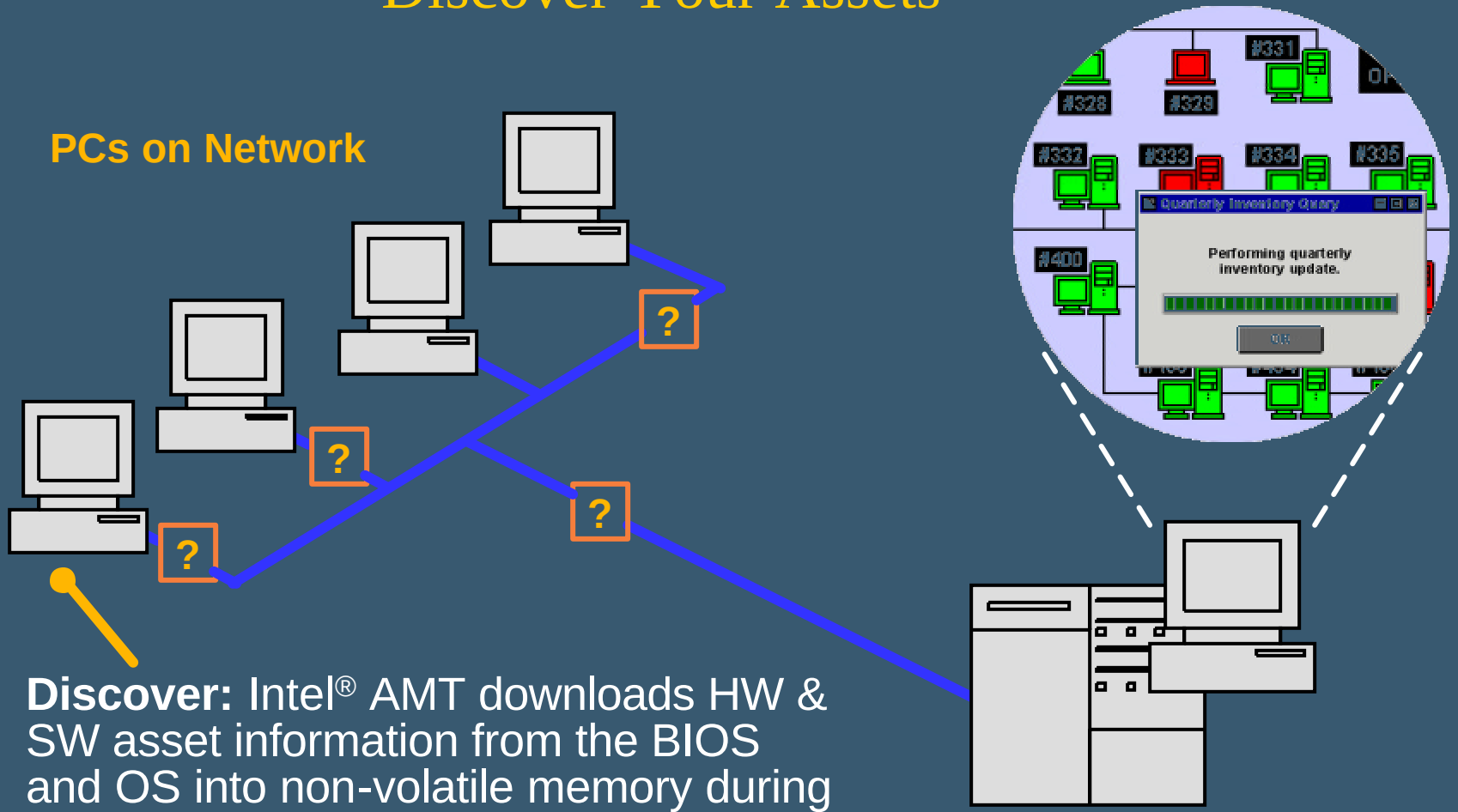


Intel AMT architecture



Intel® Active Management Technology

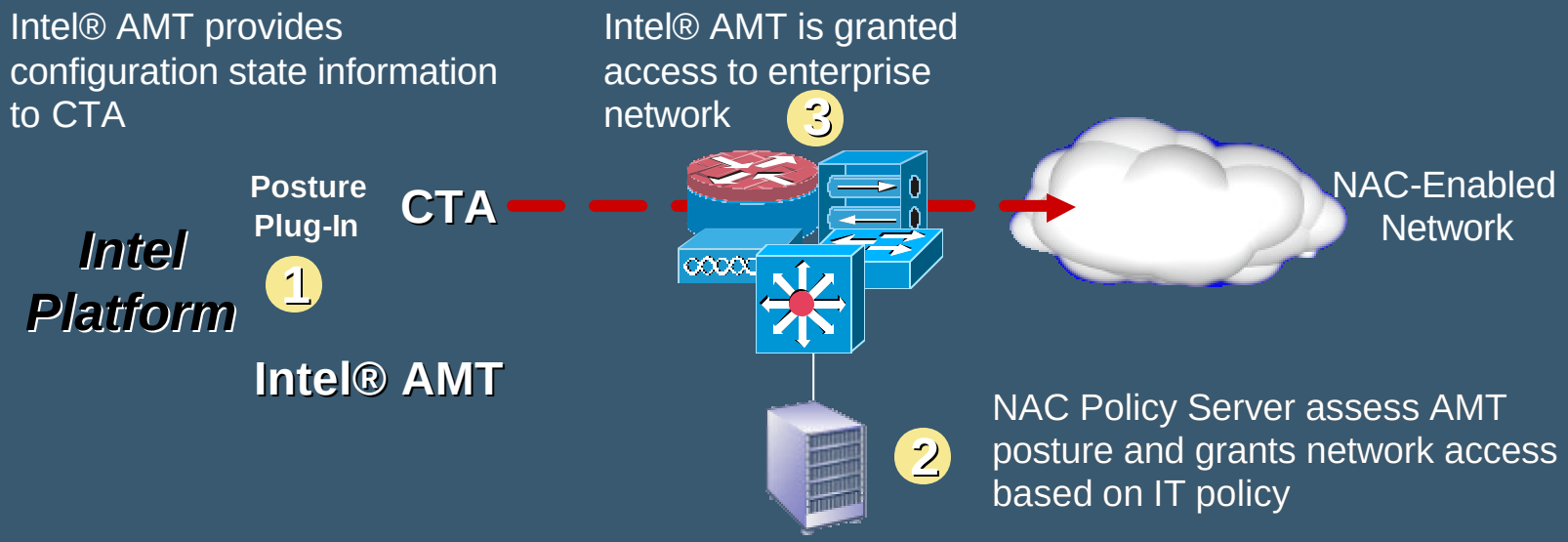
Discover Your Assets



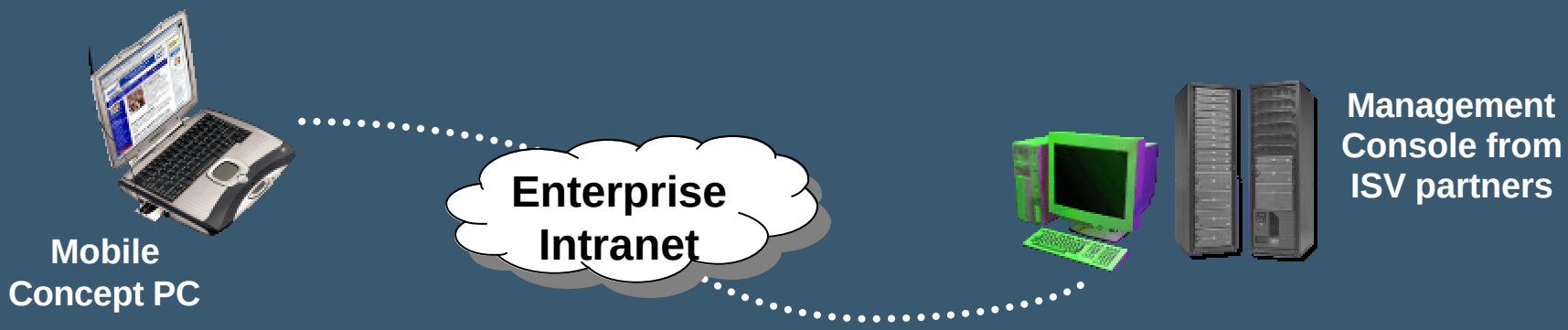
Discover: Intel® AMT downloads HW & SW asset information from the BIOS and OS into non-volatile memory during boot, which can be accessed by IT anytime because users can't remove or prevent IT access to the information.

NAC Framework Solutions: Client Security

- Example solution built with Intel
  - CTA = Cisco Trust Agent
  - NAC = Network Admission Control



Embedded IT: Proof of concept for wireless manageability and Security demo



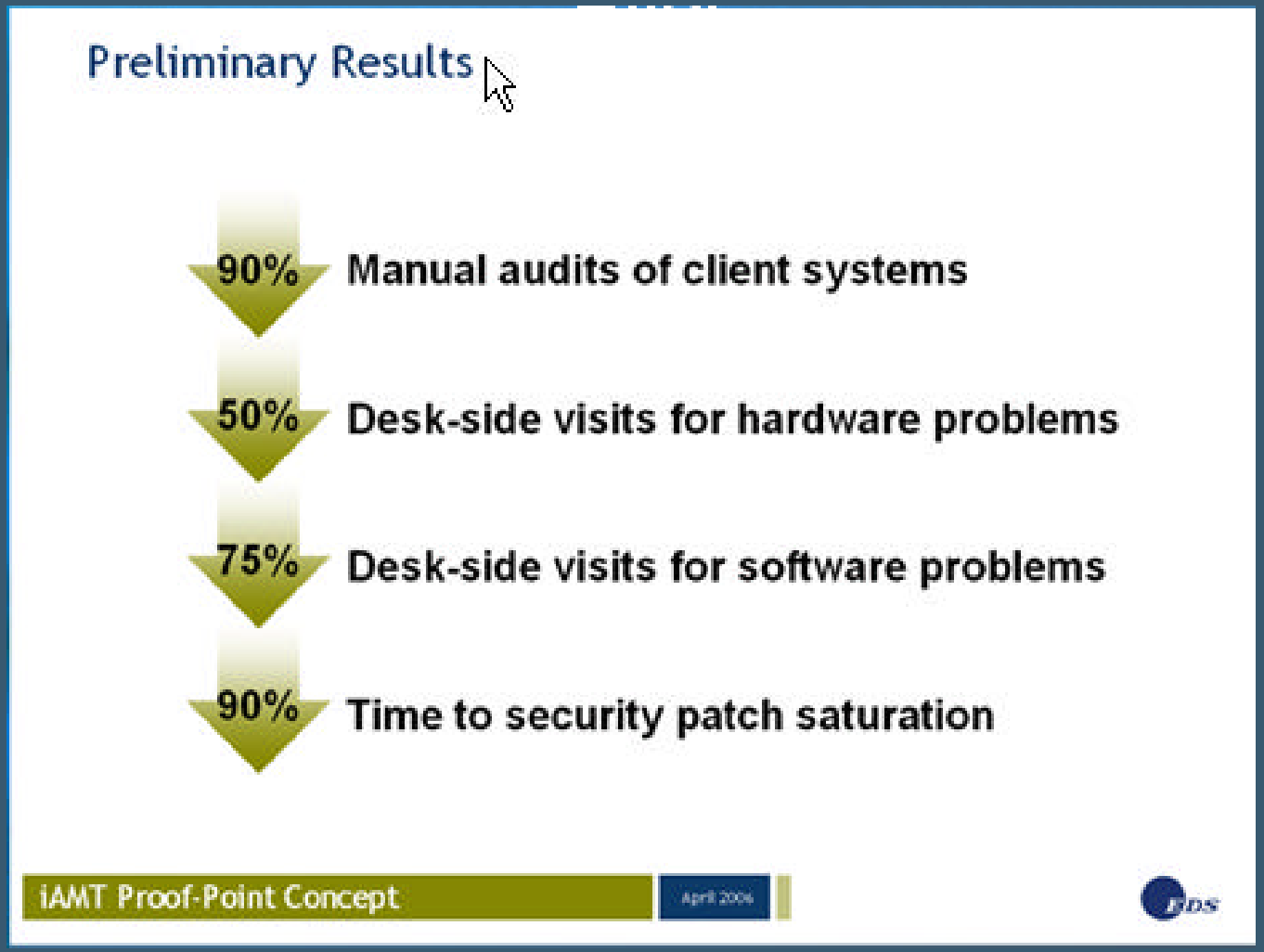
- IT embeds rule to detect a specific network based attack in NB Client's Manageability Engine
- The Manageability Engine detects specific attack and alerts IT and isolates PC from network
- IT then takes following actions via Out of Band Channel:
  - Queries PC to fix issue
  - Restores PC to network

Securing AMT

- Hardware/firmware solution
  - Only firmware images digitally signed by Intel are allowed to run
- OOB communication done via TLS with RSA keys of length 1536 bits
  - Server authentication
  - Optional client authentication
  - Maximum of 4 sessions
- HTTP Digest authentication RFC 2617 for authenticating users
- Access controlled storage of critical data to non-volatile data store in AMT hardware
- Random number generator in firmware to generate high-quality keys
- Hardware acceleration of cryptographic primitives

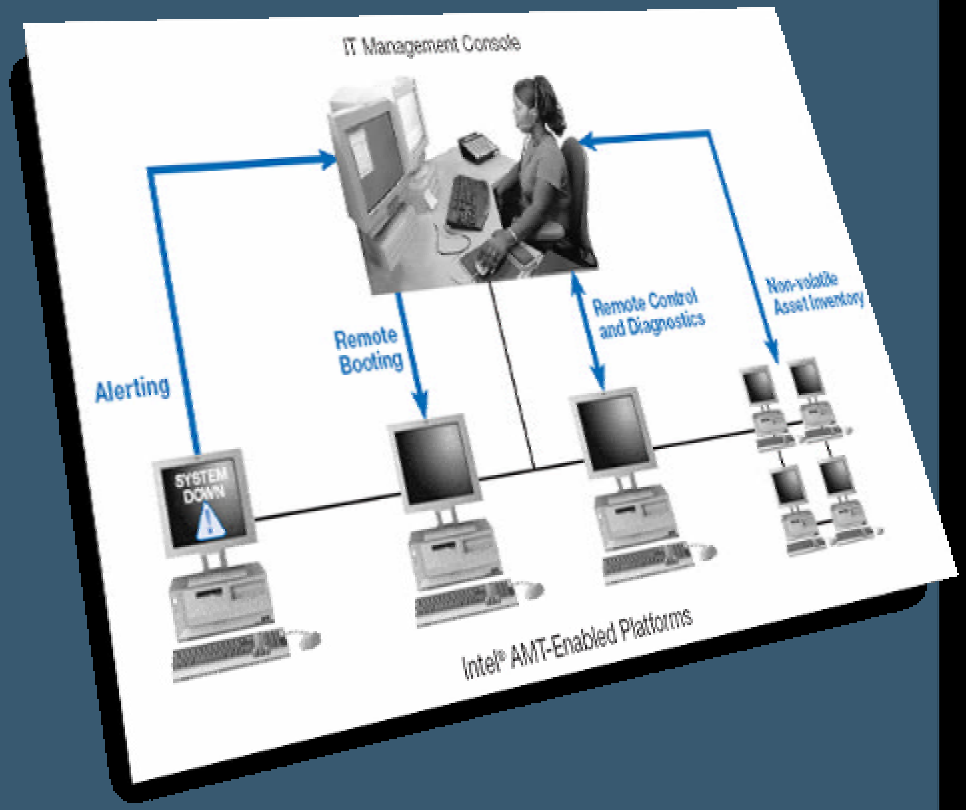
Extra slides

EDS Pilot of Intel® Active Management Technology



Hardware Enhanced Manageability

Intel® Active Management Technology with Microsoft System Management Server 2003 plug-in*



- Discover & Wake Up the PC (Even if Powered Down)
- Heal: Use Serial Over LAN (SOL) to Configure BIOS if PC is Not Responding
- Protect Against Malicious Software Attacks

Intel® Active Management Technology requires the platform to have an Intel® AMT-enabled chipset, network hardware and software. The platform must also be connected to a power source and an active LAN port.