INTEL® VPRO™ PLATFORM
INTEL® AMT USE CASES
VALUE PROPOSITION AND CONFIGURATION

Alexander Melnikov

Field Application Engineer

Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

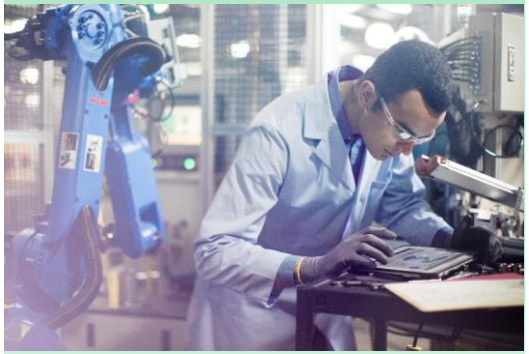
Cost reduction scenarios described are intended as examples of how a given Intel- based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. KVM (Keyboard, Video, and Mouse) Remote Control is only available with Intel® Core™ vPro™ processors with active integrated graphics. Discrete graphics are not supported. For more information, visit intel.com/AMT.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

WORKPLACE TRANSFORMATION

Manageability



Collaboration

Security

THE INTEL® vPRO™ PLATFORM

The Foundation for Business Computing

The Intel® vPro™ platform is a set of hardware, technologies and solutions utilized to build business-ready computers

BUILT FOR BUSINESS

Systems enabled with features that enable, accelerate or complement Windows* 10 Pro/Enterprise

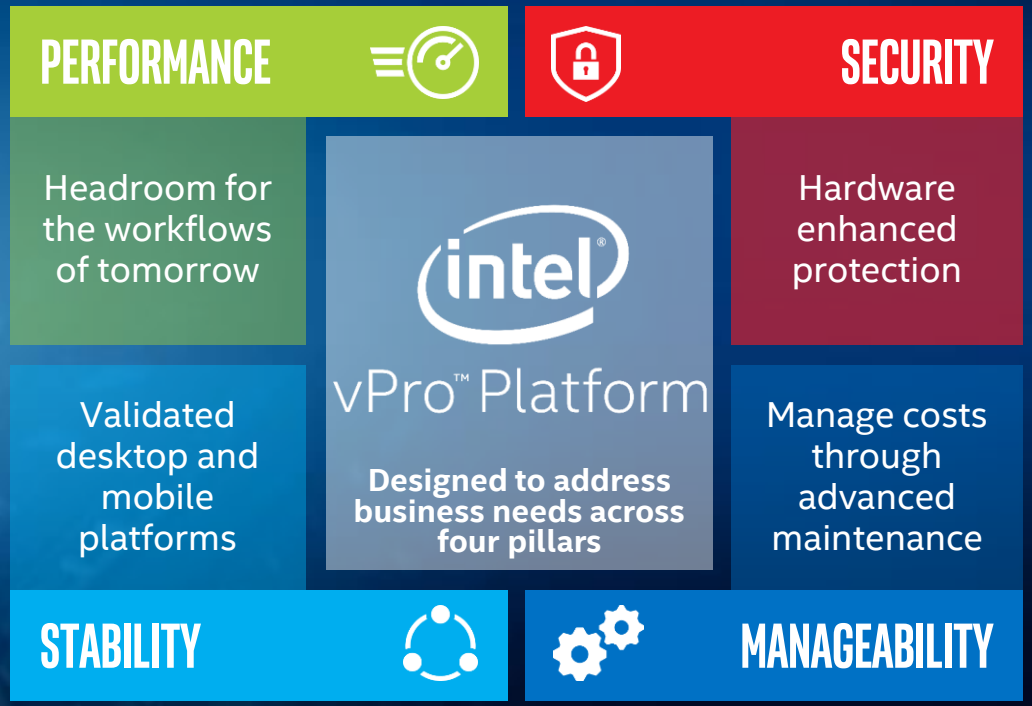
BROAD MARKET SUPPORT

Over 100 new systems every year from top manufacturers

VERIFICATION PROGRAM

Formal brand requirements and testing program to verify functionality

MORE INFO at intel.com/vpro



INTEL® VPRO™ PLATFORM HW & FW COMPONENTS

HARDWARE

Intel® Core™ vPro™ processor
Intel® Xeon® processor

+

CHIPSET (PCH) & CORPORATE ME FW

Intel® vPro™ PCH (Q370, QM370)

+

NETWORK

Intel® AMT enabled built-in LAN controller (i219-LM)
Intel® AMT enabled Wi-Fi controller

INTEL® ACTIVE MANAGEMENT TECHNOLOGY (INTEL® AMT)

INTEL® IPT PKI & DAL FOR SECURITY SOLUTIONS

INTEL® HARDWARE SHIELD

10+ YEARS OF INTEL VPRO

2006 -2009

HW Remote Management within Enterprise Network and Beyond Firewall over Wired and Wireless

Processor (VT-x) & I/O Devices Virtualization HW Support

Hardware Strengthen Security (TXT)

ME FW 2.2/ 2.6/ 3.2/ 4.2/ 5.2

2010

+HW-KVM Remote Control with Intel processor integrated GfX

Q57 / QM57
ME FW 6.2

2011

+Host Based Configuration

+KVM Resolution Enhancements (1920x1200)

+Identity Protection Technology w. OTP

Q67 / QM67
ME FW 7.1

2012

+KVM Enhancements (3 displays)

+Intel® IPT Secure Transaction Display & PKI PEAT

+Embedded Host Based Configuration[2]

Q77 / QM77
ME FW 8.1

2013

+KVM Resolution Enhancements (2560x1600)

+Graceful OS Shutdown

+Intel® Platform Trust Technology (ME FW/HW Client TPM 2.0)

Q87 / QM87
ME FW 9.1 /9.5

2014

+Secure Wireless AMT ACM setup [1]

+Microsoft* InstantGo* support with AMT not provisioned

+Remote Screen Blanking[2]

+ Intel® AMT Watchdog Automatic Reset[2]

ME FW 10.0

2016

+KVM Resolution Enhancements (4096×2160@8bpp)

+Intel® AMT supported with Microsoft* InstantGo*

+USB-R Storage Redirection

+Intel® Authenticate Technology

+Intel® SSD Pro Remote Secure Erase

QM170/Q170
ME FW 11.0 (↑ 11.8)

2017

+Intel® Manageability Commander

+WebApp Hosting in Intel® AMT FW

+Intel® AMT Extensions for docked systems

+Intel® Optane™ Memory Support

QM175/Q270
ME FW 11.8

2018

+Gigabit WiFi Speeds with Integrated Intel® Wireless-AC 9560 (Wi-Fi/BT CNVi) Support

+support for TLS 1.2 in Intel® AMT (TLS 1.0 removal)

+Intel® Threat Detection Technology[3]

QM370/Q370
ME FW 12.0


Desktops & Workstations


Laptops


2in1s


AIO


Point of Sale


Digital Signage


Servers


Vending Machines


Compute Stick & Compute Card

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

1) requires ME FW preconfiguration (USB or OEM in factory)

2) requires ME FW OEM preconfiguration in factory

3) Enabled via 3rd party independent software vendors (ISV)

INTEL® CONVERGED SECURITY AND MANAGEMENT ENGINE

HARDWARE-ENHANCED CAPABILITIES FOR INTEL PLATFORMS

The Intel® CSME is an energy efficient computing subsystem inside Intel chipsets that enables hardware-enhanced platform features

INTEL® CORE™ vPRO™ PROCESSOR

- 6th Gen CPUs and newer
- Older systems have the Intel® Management Engine (Intel® ME)

INTEL® PERIPHERAL CONTROLLER HUB

INTEL® CSME

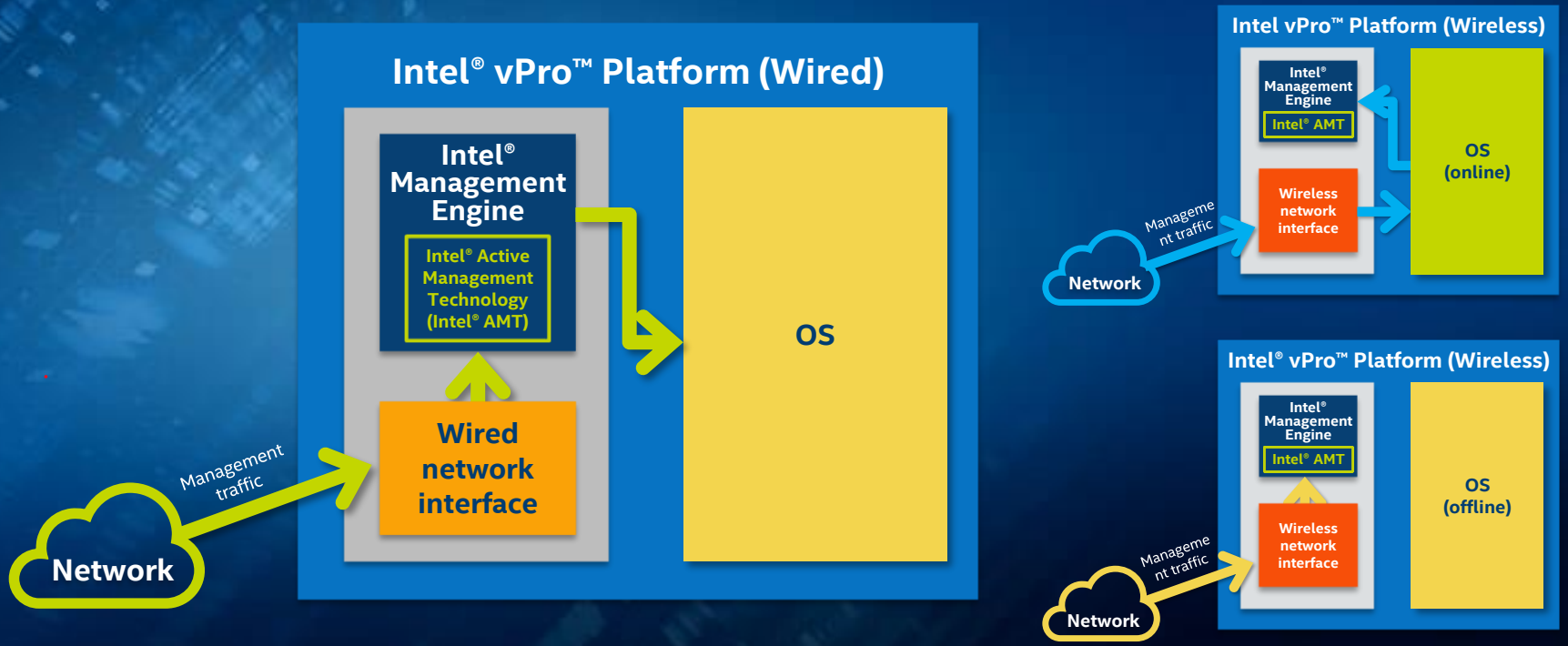
- Minute IA core
- Integrated storage
- Crypto services
- Out-of-band networking
- Firmware
- Services app loader

VALUE PROPOSITION	• Dedicated and isolated execution of low-level security and manageability algorithms and protocols (i.e. it is a **Trusted Execution Environment**)
WHAT IT DOES	• Enables **OS-independent** functions • Provides hardware **root of trust** and protection for OS, virtual machines and other software • Performs **essential** platform initialization • Security **key** generation and storage
KEY INTEL USE CASES	• Intel® Active Management Technology • Intel® DAL (Dynamic Application Loading) & Intel® Authenticate Solution • Intel® Boot Guard • Intel® IPT-PKI[1] with FIPS L1 certification • Intel® Platform Trust Technology (firmware TPM[2])
WHY IT MATTERS	• **Foundational** to the Intel® vPro™ platform • Enables **differentiation** versus consumer PCs • Future **innovations**

1. Intel® Identity Protection Technology with Public Key Infrastructure
2. Trusted Platform Module

OUT-OF-BAND MANAGEMENT WITH INTEL® ACTIVE MANAGEMENT TECHNOLOGY

Works via Intel® **wired** LAN network interface directly or Intel® **wireless** LAN routed from the host wireless driver



Intel® AMT: Take Control of Your Company's Devices

REMOTE POWER CONTROL

Manage your entire PC fleet with remote power-on

Power on a single system—or multiple systems across every work site—for remediation or patching.

HARDWARE ALARM CLOCK

Set wake-up times and schedule updates

Save energy by powering devices during business hours only. Ensure maintenance happens even when users aren't in front of devices.

HARDWARE KVM

See it remotely—even when it's down

Keyboard-video-mouse (KVM) provides visibility and control of the device, even during an OS failure, as if you were sitting in front of the system.

REMOTE ACCESS

Recover faulty systems without sending a tech

Repair devices that are far away or difficult to access, like hard-to-reach digital signage. Remotely control and reimage devices, at scale.

INTEL® AMT SAVES TIME AND SIMPLIFIES MANAGEMENT

MANAGE GROWING NUMBER OF DEVICES

Discover, repair, and help protect networked computing assets even when the system is off

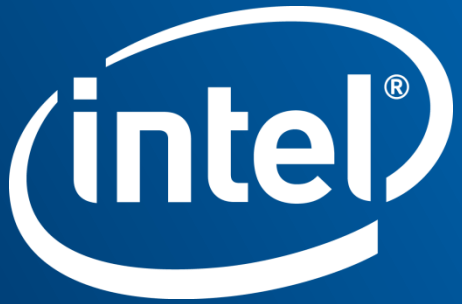
REDUCE OPERATING COSTS AND COMPLEXITY

Cut the cost of an IT service call from $187 to $60 with out-of-band remote diagnosis[1]

EASE PLATFORM LIFECYCLE MANAGEMENT

Remotely monitor installations and upgrades with out-of-band management capabilities

1. Sources: 2014 CompuCom whitepaper, Intel® vPro™ IT customer data, and 2013 Gartner benchmarking hardware support costs.


intel®