White paper

next generation remote management

How Intel® vPro™ Technology Is Critical to Reducing Cost, Managing Choice, and Securing the Enterprise.

Your business technologists. **Powering progress**

Table of Contents

Contents

About the Authors

John J. Minnick,
Director, Global Head of Strategic Technology Partners (STeP) Team
Innovation, Portfolio, and Architecture
Atos

Vicente Bernardo,
Desktop Engineering Consultant
Atos

Greg Boitano,
Product Marketing Engineer
Intel Corporation

Executive Summary

Intel® vPro™ technology[1] delivers powerful hardware-based capabilities that improve remote management of desktop PCs. These capabilities can help information technology (IT) service providers such as Atos improve remote discovery, inventory, problem resolution, maintenance, and security when managing a fleet of desktop and laptop systems. In particular, the capabilities built into these PCs will allow Atos to perform and automate management and security tasks even if a PC is powered off, its operating system (OS) is inoperative, or management agents are missing.

Atos expects to be able to use the new capabilities to streamline many tasks, improve network security, perform more work off-hours, and automate more processes. In turn, this will help Atos offer a new level of service to customers, further reducing interruptions to business and providing even better services to enterprise clients. Through the use of vPro technology, Atos has been able to achieve a 98% rate of technician dispatch avoidance at remote offices that did not have dedicated, on-site IT staff. Thus, 98% of incoming tickets that would have otherwise required a costly and time-consuming technician dispatch were instead handled remotely by a centralized expert team.

Ultimately, Atos anticipates being able to improve the accuracy of its service estimations, reduce the number of deskside visits that are traditionally required to manage and maintain systems, and minimize business interruptions for customers. The key business value drivers of Atos' efforts are:

Increased service efficiencies

- Centralized IT support and consolidated expertise
- Reduced need to dispatch (external, part-time/temp) technicians, who may not have the experience and skills of a dedicated central resource
- Faster time to respond to unmanned, remote sites

Improved uptime for customers

- Remote sites are serviced more quickly. No need to wait for technician dispatch.

Reduced interruptions to business

- Reduced reliance on customer to perform tasks such as rebooting, BIOS changes, entering Bitlocker recovery keys, etc.

Lower management costs

Elimination/reduction of deskside visits

"Through the use of vPro technology and a centralized expert team, Atos has been able to achieve a 98% rate of technician dispatch avoidance at remote offices that did not have dedicated, onsite IT staff, thereby eliminating most of the costly and time-consuming technician dispatch costs."

John J. Minnick
Director, Global Head of Strategic Technology Partners (STeP) Team
Innovation, Portfolio, and Architecture
Atos

Introduction

In this white paper, we will take a closer look at Intel® Active Management Technology (Intel® AMT)[2]—one of the key technologies that is a part of Intel® vPro™ technology. We highlight the ideas behind this technology, demonstrate its functionality, and show how a value-added service can be implemented to enhance and leverage mobile management and security for enterprise customers.

These capabilities are designed to improve remote discovery, asset inventory, maintenance, problem resolution, and security updates for PCs. They give IT service providers such as Atos a way to remotely manage PCs regardless of the system's power state or the state of its OS.

This is a new level of manageability for service providers, and Atos intends to take full advantage of the new technology to streamline and automate more processes. For example, the company is planning to enhance its Atos Low Touch Migration* (Atos LTM*) installation process, discover PCs even before management agents are installed, and improve the accuracy of remote inventories. Atos is also planning to automate more security updates, maximize efficiencies in OS migrations, and offer new services such as remote firmware updates.

Atos' goal is to increase service efficiencies, lower management costs, improve user uptime for customers, and reduce interruptions to business. To that end, Atos has conducted several enterprise-wide customer implementations of Intel vPro that validate these points.

While this paper focuses on Intel AMT, it should be noted that Intel AMT represents a single tool within the suite of vPro capabilities. The following overview of vPro capabilities is presented to provide a more thorough understanding of this Intel® technology. Additional references are included at the end of this paper:

- Intel® Active Management Technology (Intel® AMT)[2] allows remote configuring, diagnosing, isolating, and repairing of an infected PC even if it's unresponsive, whether inside or outside the corporate firewall. It provides a secure out-of-band communication channel outside the operating system. This channel is available even when the machine is powered off or the operating system is damaged.
- Intel® Identity Protection Technology (Intel® IPT)[3] implements a processor-embedded, two-factor authentication to help prevent unauthorized access to business accounts and access points.
- Intel® Trusted Execution Technology (Intel® TXT)[4] is a hardware security solution that protects against malware by checking software launch behavior against the "known good" behavior of key components.
- Intel® AES New Instructions (Intel® AES-NI)[5] improve on the Advanced Encryption Standard (AES) algorithm and accelerate the encryption of data whenever AES is used to protect network traffic, personal data, and corporate IT infrastructures.
- Intel® Virtualization Technology (Intel® VT)[6] allows improved desktop virtualization, a key requirement in the burgeoning "bring your own device" (BYOD) movement.
- Intel® Anti-Theft Technology (Intel® AT)[7] helps IT administrators lock lost or stolen laptops, even if thieves attempt to reimage the OS, change the boot order, or install a new hard drive.

"At Atos we are committed to using vPro technology to extend the value we provide to our customers. Through our use of vPro technology we have been able to become more proactive and responsive to our customers service needs. The ability to improve service has led to greater customer productivity and satisfaction."

Andrew D. Kelemen
CTO and Head of Portfolio,
North American Managed Services
Atos

Today's IT Challenges

IT service providers face significant challenges in managing computing environments. In particular, today's PCs cannot usually be secured, maintained, updated, or repaired from a remote management console if powered off, if their operating system (OS) is not working, or management agents are missing. Instead, costly and time-consuming deskside visits are required to manage and service machines. The difficulty in providing remote service translates into customer costs in various ways:

- Users can experience significant interruptions when they must help with troubleshooting sessions, change BIOS settings, reboot or cycle PC power, or verify hardware assets.
- Manual inventories can introduce errors in reporting, and incomplete inventories can introduce liabilities in complying with government or other regulations.
- Response time to a new threat or vulnerability can be extended while service technicians hurry to the deskside to power up machines and install patches before the network becomes infected.

Especially in an enterprise environment, there is a critical need for tools that would improve remote services for managing and securing PCs. All businesses suffer from interruptions caused by hardware and software problems. In some industries, however, such interruptions may not be solely inconvenient, but also dangerous.

"vPro's power management allows remote security patch updates and computer repairs even if the unit is powered off. This avoids user interruptions, and allows inventory discovery without deskside visits and pro-active responses to new threats or vulnerabilities in a timely manner."

John J. Minnick
Director, Global Head of Strategic Technology Partners (STeP) Team
Innovation, Portfolio, and Architecture
Atos

Multitiered Approach to Intel® vPro™ Implementation

It's possible to implement Intel® Active Management Technology (Intel® AMT) using a phased approach. If resource constraints are a concern, or if a business simply wants to initially test certain capabilities, it is entirely possible to implement AMT starting with very minimal infrastructure cost.

We have categorized Intel AMT implementation in four tiers, each with a differing level of infrastructure and investment commitment along with increased functionality. Each of these tiers also shares an array of 27 baseline capabilities. These baseline and tiered capabilities are detailed in the following bullet points. The distinctions among the four tiers are illustrated below in Table 1.

Baseline Intel AMT Capabilities: Instant Back to Work, Easy Reimage, Remote Drive Mounting, Remote Drive Erase, Enhanced Remote Repair with Microsoft Windows* PE*, Enhanced Remote Repair with WinRE*, Use MSDaRT* with Intel® vPro™ Technology, EZ Help Desk Console Extender, EZ Help Desk Permissions Manager, Out-of-Box Configuration for KVM Remote Control, Enhanced Remote Repair with Drive Sharing, Enhanced Remote Repair—Virus Scan, Enhanced Remote Repair—Kernel Dump Analysis, Enhanced Remote Repair—Registry Edits, Enhanced Remote Repair—Outlook* Web Access*, Faster Booting over IDER, Remotely Trigger a Recovery OS Remote ISO Launcher (RIL), Help Desk Console for Non-TLS Environments, Update BIOS on Type 1 Hypervisor, Reimage OS with SOL/IDER and WinPE*, Outlook* Web Access* with Imaging, use FCFH to ID a Help Desk caller's PC, Small Business, local setup and configuration using a USB flash drive, Host-Based Configuration, Windows* PowerShell* module for Intel® vPro™ Technology, and use VNC Viewer Plus* with ConfigMgr.

The Intel® vPro™ Technology Reference Guide provides additional information about each of the features and can be found at: https://downloadcenter.intel.com/Detail_Desc.aspx?agr=Y&DwnldID=21362&keyword=%22vPro%22&lang=eng

Tier 1: Minimal Infrastructure

- A single Intel® Setup and Configuration Software Server (Intel® SCS) in a database-less mode as well as remote control software such as VNC Viewer Plus is required. Keep in mind that although no Active Directory integration is required in Tier 1, the use of shared device credentials may be less secure.

Tier 2: Active Directory Integration

- Intel SCS with dedicated database backend
- Active Directory integration
- SCCM integration
- Internal PKI (for TLS-secured communication)

Tier 3: Intel® Management Presence Server (Intel® MPS)

- Tier 2 infrastructure plus
- Intel MPS or equivalent third-party solution implemented to allow beyond the firewall usages such as Internet cloud accessible support.

Tier 4: Integration with Third-Party Security and Management Solutions in Lieu of SCS.

- Includes all Tier 3 requirements except MPS and SCS

Table 1. vPro™ deployment by tiers

Capabilities	Tier 1: Minimal Infrastructure	Tier 2: Ad Integration	Tier 3: MPS Server	Tier 4: Third-Party Security and Management
Baseline Intel® AMT Capabilities	•	•	•	•
Green Power Management		•	•	•
Find Intel® AMT Capable Machines		•	•	•
Automatic Remote Firmware Update		•	•	•
Automatic Remote Windows* 7 Migration		•	•	•
Automatic Overnight Patching with ConfigMgr		•	•	•
Off-Network Management Capability			•	•
Proactive Alerting				•
Hardware-Based Agent Presence Checking				•

Hardware-Based Capabilities—Always Available

PCs with Intel® vPro™ technology include powerful Intel® Active Management Technology (Intel® AMT)[2] capabilities built into system hardware and firmware. The most significant advantage of these capabilities is that they are available to authorized IT technicians, regardless of PC power state or the health of the OS:

- **Secure, remote communication which runs "under" the OS** so authorized IT administrators can communicate with the PC. The hardware-based remote-communication channel uses the TCP/IP firmware stack, not the software stack in the OS. It works even if the OS is compromised or inoperative, and even if PC power is off. As long as the PC is connected to a power source and plugged into the network, an authorized technician can use management software to communicate with PCs. The communication channel is secured through HTTP authentication and Transport Layer Security (TLS).
- **Always-available alerting** means PCs can send alerts and SNMP (simple network management protocol) traps to the management console at any time. This gives Atos visibility of fan speeds, temperatures, case intrusions, hardware failures, OS lock-ups, and other critical events as they occur.
- **Persistent event logs** so IT technicians can have access to the list of events that occurred before hardware or software problems became apparent. The event log is accessible even if the PC is powered down, or its OS is inoperative.
- **Access to persistent hardware asset information** so IT technicians can identify compatibility issues and determine the manufacturer and model of particular parts that need replacing.
- **Access to pre-boot BIOS settings** for verifying configuration information and changing settings as needed to remotely respond to service requests or help resolve PC problems.
- **Remote power-up** so IT technicians can power up, power down, or reset PCs from the management console. Security for this capability is provided through TLS, HTTP digest authentication, and enterprise-level authentication using Microsoft Active Directory*.
- **Remote boot through integrated drive electronics redirect (IDE-R)** so authorized IT technicians can redirect the boot device for a problem PC to a clean image at the help desk or an image on another remote drive. IDE-R is more secure than pre-execution boot environment (PXE) or wake-on-LAN due to required AMT authentication.
- **Console redirection and control**, through built-in serial-over-LAN (SOL) capabilities, so IT technicians can guide the PC through a troubleshooting session without user intervention and without leaving the management console.

In environments that contain a mix of new and older hardware, it is also important to understand what features of Intel AMT are enabled in the various firmware versions. For details, please refer to Appendix B of the Intel vPro Reference Guide available at: https://downloadcenter.intel.com/Detail_Desc.aspx?agr=Y&DwnldID=21362&keyword=%22vpro%22&lang=eng

Proof-of-Concept Testing for New, Hardware-Based Capabilities

To investigate the new capabilities of Intel® vPro™ processor technology, Atos conducted proof-of-concept tests at the Atos evaluation site. Because Atos is interested in how the technology would impact an actual customer, the lab provides a complex evaluation environment with multiple PC domains, as well as additional layers of data in the management-software environment. This environment replicates an existing customer environment that had significant access constraints and high security requirements.

These tests were designed to help Atos discover how to take advantage of the powerful new capabilities of Intel® vPro™ processor technology. The data, results, and extrapolations presented in this white paper are derived from Atos findings, and the Atos Proof-of-Concept Evaluation of Intel® AMT Capabilities.[8]

Atos is examing the benefits of Intel® vPro™ technology in corporate environments. Assessments are being made for incremental increases in service benefits to customers currently using Intel® vPro™ technology, and to those who have not deployed the technology. Based on test results, Atos has been working with enterprise customers to integrate the new capabilities into management tasks to improve efficiencies and automate more processes.

Results and Data Extrapolation

After examining the results of its evaluation, Atos extrapolated the data (refer to Table 2) to estimate the opportunities offered by Intel vPro processor technology for improving IT tasks for customers in any industry. Based on these results, Atos can foresee a significant improvement in device discovery, asset management, problem resolution, and patch updates. In addition, the capabilities in these PCs offer opportunities for new types of services, such as regular BIOS updates, which have not previously been practical in a large environment.

The following table quantifies the potential for service improvements attributable to the use of Intel AMT capabilities on vPro processor technology. Data is derived from Atos' direct experience with enterprise customers.

Through the Atos 'proof of concept' deployments of Intel® vPro™ technology, customers have confirmed major improvements in a wide variety of management tasks including dispatch avoidance, asset inventory, BIOS/ firmware updates, issue diagnosis and remote repair, critical patching, and image deployments.

Table 2. Atos experience based on enterprise customers

Task	Without Intel® AMT	With Intel® AMT	Atos Estimated Improvement[9]
Discover and provision new PC	▸ Discovery performed on-site ▸ Requires 1 technician on-site for every 50 systems	▸ Remote discovery ▸ Approximately 1 technician needed on-site for every 250 systems	▸ Reduce on-site presence by 80% ▸ Reduce time to discover and provision new PCs by 35%
Dispatch avoidance	▸ Smaller offices may not have dedicated IT staff on site ▸ Work such as PC builds, secure wipes, and hardware diagnostics that require a deskside visit generate a costly technician dispatch ▸ Tasks that require technician dispatches may take up to 40% longer to complete, allowing for dispatch lead time and travel	▸ Many tasks that once required booting from physical media or power cycling a machine can now be handled remotely via IDE-R and Intel AMT's KVM capability ▸ Tasks at remote sites now have the same SLAs as tasks performed at IT staffed sites	▸ Reduce costs associated with dispatching a technician to a remote site ▸ Improve quality of work by assigning to experienced central teams ▸ Reduce time to resolve issues at remote sites
Asset inventory	▸ 20% to 30% of PCs typically unavailable for remote discovery and inventory of assets	▸ Virtually all PCs respond to remote inventory processes	▸ Reduce manual inventories by 95%
BIOS/firmware update for 5000 PCs	▸ Deskside visit required to manually install the update from CD	▸ Remote, automated installation of the update	▸ Reduce manual BIOS updates by 95% ▸ Speed up update process by 85%
Diagnosing and replacing corrupt .DLL file	▸ Typically takes 90 minutes and a deskside visit	▸ Diagnostics and repair completed remotely and in less than 25 minutes	▸ Reduce deskside visits by 95% ▸ Speed up problem resolution by 75%
Diagnosing and rebuilding OS	▸ Typically takes 205 minutes and a deskside visit	▸ Diagnostics and rebuild completed remotely and in approximately 135 minutes	▸ Reduce deskside visits by 95% ▸ Speed up OS rebuilds by 35%
Hardware problem diagnostics and resolution	▸ Up to 2 deskside visits required to diagnose problem, identify the part to replace, get new part, and fix the PC	▸ Remotely identify part to replace, with remote boot, access to pre-boot BIOS, persistent event logs, and access to hardware asset information	▸ Reduce deskside visits by 50% ▸ Speed up problem resolution by 50%
Critical patch deployment for 5000 PCs	▸ Deskside visits still required to power up PCs, reinstall agents, and verify the patch. Achieve 80% saturation in 2 weeks.	▸ Remotely power up PCs, install agents, and verify the patch. Achieve 98% saturation in 3.5 hours.	▸ Reduce deskside patching by 95% ▸ Achieve 98% saturation in 3.5 hours ▸ Speed up patch deployment by 95%

Remotely Updating PCs—Even if the Power Is Off

Today, many PCs are inaccessible from the management console for remote security updates, such as critical patches and software upgrades. For example, an enterprise might maintain meeting rooms for specialized training and continuing education. PCs in such an environment are often powered down for a period of time before being powered back up—a situation that can leave them badly out of compliance. In many fields, such compliance may be mission-critical.

With Intel® AMT available in Intel® vPro™ technology, the hardware-based communication channel runs below the OS, so it remains available to authorized technicians, even when the PC is powered off or the OS is not available. Contrast this with today's environment where a technician must make a time-consuming deskside visit to power up each system from a bootable CD. The technician then makes sure each PC's security agent is not compromised, installs the updates and/or patches, and watches to make sure the updates are complete before the PC is allowed network access.

Based on the Atos experience, it takes an average of an hour per PC to perform these currently manual processes.[10] Even with multitasking between PCs, a training room with 20 systems can easily take half a day to update. In larger environments, such manual updates are not only time-consuming, they can extend the network's window of vulnerability. Clearly, the remote access provided by Intel AMT provides a significant advantage.

Remotely Installing Critical Patches

Atos plans to take full advantage of the remote power-up capability in PCs with Intel vPro processor technology to improve remote patch management (refer to Table 2). This capability will allow an Atos technician to remotely poll the PC for its power state, and then power up the PC if necessary to receive the patch. The technician can then remotely push the patch and then return the PC to its previous power state—on, off, hibernating, or sleeping—leaving the systems updated and ready for use.

In its evaluation, Atos showed that a technician could remotely power up and install a patch to 10 PCs in less than 20 minutes.[8] Extrapolating this data, Atos expects to be able to patch an environment with 5,000 PCs in approximately 3.5 hours, with a 98% patch saturation (refer to Table 2).[10] This represents a significant improvement, not just in the time required to achieve patch saturation, but in the virtual elimination of the deskside visits traditionally required to power on systems to receive a critical patch.

This could be a key capability in certain environments where IT technicians may not have immediate access to systems in order to perform updates. With a remote power-up capability, technicians can automate and perform this work off-hours, reducing the need for groups of technicians to work overtime or after hours in order to canvas a site and make sure every system is patched.

Reducing the Need for User Intervention Through Intel® vPro™ Technology's Power Management

The remote power-up capability will provide Atos with a new level of control over PCs for many tasks. For example, the capability can be used in conjunction with SCCM or other third-party security and management solutions to power down machines during emergencies caused by malicious attacks and other events.

Security and other critical updates can also be completed without requiring user intervention—a typical requirement today. Process efficiencies can increase, as can compliance with government and other regulations. Based on its experience patching or updating 5,000 PCs,[8] Atos estimates this will impact critical patch deployments by:

- Reducing deskside patching by 95%
- Achieving 98% saturation in 3.5 hours
- Speeding up deployment by 95%

Improving Discovery and Inventory Processes

An IT service provider has a critical need to know the disposition of the systems in the network given the significant financial difference between a system that is truly lost, and one that is only "missing" because it has been reallocated but not tracked.

According to Atos, as many as 20% of the systems that are reported missing still exist within the infrastructure.[10] If tracked more accurately, these PCs could be reallocated to improve reporting, revenues, and procurement. In corporations with hundreds of thousands of systems, a 20% reallocation rate can represent a substantial dollar amount. In addition, machines that cannot be found, can neither be managed nor secured—raising issues of compliance and corporate liability.

Systems with Intel® AMT can be configured to respond to scripted inquiries even when powered down. Script generation may be automated through third-party solutions, or can be developed in-house using WMI*, PowerShell*, or WinRM*. Intel supplies the necessary programming interfaces to interact with Intel AMT.

Discovering Devices—Even before Management Agents Are Installed

One of the challenges in device discovery is that it is often a manual process. If a device disappears from the network, a technician typically calls the user or office manager on-site to find out if the system is in use and residing in its expected location. If so, a field technician is dispatched to go deskside and manually install the missing software agent so the system can be inventoried and managed remotely.

Tests showed that all PCs with Intel vPro processor technology responded to the Atos polling process regardless of power state.[8] With this improved device discovery, Atos will have the ability to track these systems through their life cycle, even if they are moved, assigned to a new user, rebuilt, or reimaged. Even in environments where ongoing changes have traditionally made it extremely difficult to find and audit technology, Atos will be able to offer more consistent, effective tracking. This will not only help Atos improve life-cycle management, but also improve the accuracy of software licensing and asset reporting, critical aspects of compliance with government and other regulations (refer to Table 3).

Improving Remote Inventories to Reduce Costs

Businesses are under significant pressure to accurately track, manage, and maintain their hardware and software assets, and protect them from reasonably anticipated threats. To do this, the service provider must first know where all hardware and software assets reside.

Table 3. Atos experiences for device discovery, inventory, and provisioning

Task	Atos Estimated Improvement[9]
Discover and provision new PCs	▸ Reduce on-site presence by 80% ▸ Reduce time to discover and provision new PCs by 35%
Asset inventory	▸ Reduce manual inventories by 95%
BIOS/firmware update	▸ Eliminate manual BIOS updates ▸ Reduce time to update firmware by 85%

Atos has traditionally been able to read a PC's hardware asset information—such as component manufacturer and model, OS type, and system identification (ID)—from BIOS through the use of a management agent. However, today's software-only solutions allow Atos to acquire this information only when the system is powered on, the OS is working properly, and the asset-tracking agent is present. Since as many as 20% to 30% of systems on a typical day do not respond to asset polling processes from the management console,[10] this means Atos must perform costly manual audits. In an environment in which services are often spread over a large campus with many buildings, such manual audits can be both time-consuming and error-prone.

PCs with Intel® vPro™ processor technology, however, update their own hardware and configuration information each time the system goes through power-on self-test (POST). This information is stored in nonvolatile memory in an execution environment that works below the OS, and is available to authorized Atos technicians regardless of the presence of an OS or management agent. For customers using PCs with Intel vPro processor technology, an Atos technician will be able to capture the hardware inventory of the PC as soon as the PC is connected to a power source and plugged into the network. Atos expects this to be a valuable capability that improves the accuracy of inventory tracking and reporting.

For example, this will allow Atos to provide a new level of service in a more unobtrusive manner, helping eliminate the need to send teams of personnel into an environment to inventory hardware assets (refer to Table 3). Instead, a single console operator with a server could be sent into the environment to identify and inventory devices. This would be especially significant in environments where privacy is important, such as in clinical settings, patient records libraries, or nurses' stations.

Atos also foresees being able to use Intel vPro processor technology to selectively target which systems to power up and update. Atos anticipates that this would help improve the precision of cost calculations of PCs to be managed—an important consideration in any organization.

"With improved remote manageability, Atos expects to reduce the time it takes to troubleshoot and resolve hardware and software issues at offices without dedicated on-site IT support."

Vincente Bernardo
Desktop Engineering Consultant
Atos

Remote Power-Up for Provisioning of New PCs

Atos traditionally uses its Low Touch Migration process to bring new PCs into the managed network, migrate systems to a new OS, or rebuild PCs after a catastrophic failure. As soon as the management agent is installed and the PC is plugged into the network, the OS and application build can be performed from the remote management console. Today, Atos usually assigns one technician for every 50 systems being provisioned or rebuilt, to make sure the provisioning or migration process flows smoothly.

Because PCs with new Intel vPro processor technology can be remotely inventoried anytime, an authorized Atos technician will be able to identify the PC's configuration—including BIOS settings and firmware version information—even before management agents are installed. The technician can remotely power up the machine, push the appropriate agent to the new PC, and begin the Atos traditional LTM build—all without making a physical visit to the system.

Atos validated this process in a production environment to test potential time savings. Test results showed that a technician could discover and image a new PC with Intel vPro processor technology in only 1 hour 50 minutes[8] versus a traditional deskside visit of more than 2-1/2 hours.[10]

Atos estimates that the new capabilities in PCs with Intel vPro processor technology should improve efficiencies in provisioning new PCs by approximately 35%.[8] More importantly, Atos should be able to substantially reduce travel time associated with the number of technicians required to monitor the provisioning process by an estimated 80% (refer to Table 3).

Remotely Updating BIOS Firmware for OS Migrations

A time-consuming task in any OS migration is the BIOS firmware update. Even though this deskside task takes only about 5 minutes per PC, the cumulative time spent in a large enterprise, to update all systems can be substantial. For example, an OS migration for 8,500 PCs would require over 700 staff-hours just to update the BIOS to ready the systems for the remote rebuild. At today's rates for IT technicians, this can add up quickly in a large enterprise for basic tasks such as BIOS updates.

PCs with Intel vPro processor technology provide authorized technicians with access to pre-boot BIOS settings. This allows an Atos technician to remotely change BIOS settings and push firmware updates to the system. With remote access to the settings, Atos could automate this process as part of the Atos LTM service. Atos estimates that access to pre-boot BIOS settings could reduce the time required to perform firmware updates by a conservatively estimated 85% (refer to Table 3).

An additional benefit of remote BIOS updates is that they can now be performed as part of a regular maintenance cycle, instead of being performed on an ad-hoc basis for problem resolution. This can increase the stability of the user's system and help prevent many potential issues from becoming problems that interfere with user productivity.

Reducing Deskside Visits for Problem Resolution

Problems that prevent a system from booting typically require at least one deskside visit to boot, troubleshoot, rebuild, and restore the PC. Hardware problems often require two visits: one to diagnose the problem, and a second visit to bring back and install the replacement part. Even software issues can require a second deskside visit. For example, many SAP applications are too complex for a standard technician to support. Problems related to these applications are usually escalated to a level-3 specialist who can perform more advanced diagnostics and resolution.

Although all businesses suffer from interruptions caused by hardware and software problems, in some industries, interruptions may not be solely inconvenient, but also dangerous. In addition, users in these industries don't usually have time to help troubleshoot or rebuild a problem PC, answer system prompts as directed by a remote technician, enter settings, or otherwise help with repair. There is a critical need for tools that reduce the traditional demand for time-consuming deskside visits and speed up problem resolution.

"Computer interruptions caused by hardware or software problems can negatively affect the end-user experience and in certain use cases be dangerous and life-threatening. Where speed to resolution is most critical, vPro provides the advantage of remote management and resolution whether or not the computer is powered up or the OS is operating properly."

Simon Hardy
Global Portfolio Architect
Atos

Remote Software Problem Resolution for a PC That Won't Boot

To help improve problem resolution, PCs with Intel vPro processor technology include built-in capabilities that can significantly reduce deskside visits for both software and hardware problems. Atos validated these capabilities in the lab, including remote-boot, console-redirection, persistent event logs, and access to system configuration and asset information. These same capabilities have also been borne out in enterprise implementations at customer locations, and are especially useful in situations where access to information may be both time- and mission-critical.

For example, perhaps one of the three PCs at a nurses' station on a patient recovery floor goes down, suddenly limiting medical staff to only two PCs. Problem resolution for a PC that won't boot usually requires a time-consuming deskside visit, diagnostics, and repair—a process that typically takes over 1-1/2 hours.[10] For nurses who must record health metrics, report on patient progress, and ensure that patients receive medications on time, sharing tools is not only inconvenient, but a situation that can have serious consequences.

With the IDE-R capability of Intel vPro processor technology, an authorized Atos technician can now boot the PC from its own hard drive to reset its system state—without making a time-consuming deskside visit. If this doesn't solve the problem, the technician can quickly and remotely change the PC's boot device to an image in another location. This could be an image on a bootable CD at the help desk, a "diagnostics" server, local network storage, or another appropriate device. The technician can then use diagnostics tools at the help desk to troubleshoot the problem.

A technician could replace corrupted .DLL files, perform a virus scan, update BIOS, clean up temporary files, or other tasks as needed—all without leaving the management center. Atos' tests showed that diagnostics and repair of a PC that won't boot can now be performed in less than 25 minutes. With the new remote-management capabilities of Intel vPro processor technology, Atos estimates software problem-resolution could speed up by as much as 75% (refer to Table 4).

For a useful resource to estimate customer-specific cost savings, please refer to the Intel vPro ROI Calculator: https://msp.intel.com/assets/flash/ROICalculator.html

Remote Rebuild to Repair a Corrupt OS

Atos also validated the ability to remotely rebuild an OS. With the improved remote management capabilities of Intel vPro processor technology, even if a system requires reimaging, an Atos technician can now implement a full LTM rebuild from the service center.

The user is no longer required to help troubleshoot the system. Instead, users can work in another area or on another PC while the rebuild is performed remotely. PCs are returned to the working environment more quickly, labor costs are reduced, and user uptime is significantly improved.

The tests showed that on a PC with Intel vPro processor technology, a technician could remotely identify an OS problem and rebuild the OS in as little as 135 minutes.[8] According to Atos, this process usually requires at least one deskside visit that typically takes 205 minutes.[10] When used with third-party software, Atos foresees that the new capabilities in PCs with Intel vPro processor technology could eliminate virtually all deskside visits for OS and application problem resolution, and speed up OS rebuilds by an estimated 35% (refer to Table 4).[8]

Table 4: Atos enterprise customer experiences for problem resolution

Task	Atos Estimated Improvement[9]
Diagnosing and replacing corrupt .DLL file	▸ Reduce deskside visits by 95% ▸ Speed up problem resolution by 75%
Diagnosing and rebuilding OS	▸ Reduce deskside visits by 95% ▸ Speed up OS rebuild by 35%
Hardware problem diagnostics and resolution	▸ Reduce deskside visits by 50% ▸ Speed up problem resolution by 50%

Remote Diagnostics for Hardware Problems

In Atos' experience, diagnosing and repairing a hardware problem traditionally requires two deskside visits (one for diagnostics and one to install the new part). This process typically takes 160 minutes.[10]

Because Atos now has access to pre-boot BIOS settings, persistent event logs, and hardware-asset information, a help-desk technician can remotely identify the manufacturer and model of a failed hardware component without leaving the help desk—even if the PC is down. This will allow a field technician to arrive at the user site with the appropriate part in hand, eliminating the traditional deskside visit required for many initial diagnostics.

Atos evaluated the ability to access BIOS settings, event logs, and asset information in the simulated production environment. In the tests, a hard drive was unseated to simulate a hard-drive failure. The tests showed that a technician could correctly identify the hardware failure from the remote management center, and that the diagnostics and repair process could be completed in approximately 80 minutes.[8]

Atos expects that using the new capabilities of Intel vPro technology could eliminate an estimated 50% of the deskside visits traditionally required for hardware problem resolution.[8] Based on our experience with enterprise customers, Atos expects these capabilities to speed up hardware problem resolution by up to 50% (refer to Table 4). Especially in critical industries, this type of service improvement can have a significant impact that goes far beyond simply enhancing service-level agreements, to improving people's lives.

Remote Secure Wipe for Decommissioning PCs

One of the use cases Atos has explored with customers is the ability to use IDE-R to boot into utility and diagnostic boot images, including multi-pass DES (or better) compliant secure data wipes. What had formerly required a deskside visit is now initiated remotely with Intel vPro. Meanwhile, the technician is free to work on other tasks while waiting on the secure wipe to complete.

Summary

The ability of authorized Atos technicians to remotely access the Intel® vPro™ hardware-based communication channel below the OS—even when the PC is powered off or the OS is not available—has a profound impact in many aspects of management and security. Managing PCs with Intel vPro processor technology will allow Atos to eliminate many traditional deskside visits, shorten repair and remediation times, and improve efficiencies for many tasks. As a service provider, this will allow Atos to reduce interruptions to daily business, improve user uptime, and provide even better service to support enterprise clients while lowering customer TCO.

Atos is looking forward to integrating the capabilities of Intel vPro processor technology into current processes for customers to streamline and automate more processes, such as:

- Deskside visits
- Maintenance and provisioning of new PCs
- OS migrations
- Device discovery
- Asset management
- BIOS updates (previously impractical in a large environment)
- Patch management
- Security updates
- Hardware inventories
- Selective updates
- Problem resolution
- Remote diagnostics of hardware issues

In turn, this will help Atos offer a new level of service to customers, further reducing interruptions to business, and providing even better services to enterprise clients through remote operations performed by a centralized, expert team.

"As this paper demonstrates, by taking advantage of Intel Core vPro technology, Atos is able to improve service efficiency, lower costs, and increase user uptime, all of which benefits Atos and the customers they serve. Using Intel Core vPro technology as part of its Adaptive Workplace offering, Atos is able to deliver value-added services that enterprise customers need and want."

Yasser Rasheed
CTO and Director of Architecture
Business Client Platform Division
Intel Corporation

Endnotes

1. Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: http://www.intel.com/technology/vpro.

2. PCs with Intel® vPro™ processor technology include Intel® Active Management Technology (Intel® AMT). Intel AMT requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, and network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup, and configuration. For more information, visit http://www.intel.com/content/www/us/en/architecture-and-technology/intel-active-management-technology.html.

3. No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd gen or higher Intel® Core™ processor-enabled chipset, firmware and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems, or any resulting damages. For more information, visit http://ipt.intel.com.

4. No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules, and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit www.intel.com/technology/security.

5. Intel® AES-NI requires a computer system with an AES-NI-enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® processors. For availability, consult your reseller or system manufacturer. For more information, visit http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.

6. Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance, or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization.

7. No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware, and software, and a subscription with a capable service provider. Consult your system manufacturer and service provider for availability and functionality. Service may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit http://www.intel.com/go/anti-theft.

8. Source: The Atos Proof-of-Concept Evaluation of Intel® AMT Capabilities, which was conducted in the Atos evaluation labs. Visit http://www.na.atos.net and search "adaptive workplace."

9. Estimated improvements are based on internal Atos analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance. Contact Atos for more complete information on these improvement estimates.

10. Source: Based on Atos experiences. Visit http://www.na.atos.net and search "adaptive workplace."

Reference Links

Rick Echevarria, VP, IAG and GM of the Business Client Platforms Division, for an in-depth look at the 3rd Generation Intel® Core™ vPro™ processor family and how it's bridging the gap between what CIOs' need and what business users want.: http://www.intel.com/content/www/us/en/enterprise-security/3rd-gen-core-vpro-launch-webinar-video.html

vPro—ROI calculator: https://msp.intel.com/assets/flash/ROICalculator.html

4th Generation Intel® Core™ vPro™ Processors—Embedded security. Built-in peace of mind.: http://www.intel.com/content/www/us/en/processors/vpro/core-processors-with-vpro-technology.html?cid=sem116p15934&gclid=CIW37r6GmbcCFQUV7AodkDEAqw

4th Generation Intel® Core™ vPro™ Processor Family Overview: http://www.intel.com/content/www/us/en/high-performance-computing/high-performance-computing-4th-gen-core-vpro-overview-paper.html

Securing the Mobile Enterprise—John J Minnick, Dr. Joerg Gerschuetz, Arjun Batra: http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/anti-theft-securing-the-mobile-enterprise-white-paper.pdf

Ultrabooks for the Enterprise—John J Minnick, Daniel G. Silverman, Dave Buchholz
Delivering 3rd Generation Intel Core vPro processor family: http://na.atos.net/NR/rdonlyres/DCB12B86-6585-4AE0-ACC0-6FA4692A7EA1/0/Atos_Ultrabook_Intel.pdf

The Gordon TAFE uses Intel® vPro™ Technology to Manage Its PC Fleet: http://www.intel.com/content/www/us/en/it-management/intel-it/gordon-tafe-uses-intel-vPro-technology-to-manage-its-pc-fleet.html

Managed PKI Solution from Symantec and Intel® vPro™ Technology: http://www.intel.com/content/www/us/en/enterprise-security/vPro-symantec-testimonial-video.html

Intel® vPro™ Technology—Built-in security for greater protection: http://www.intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-technology-general.html

Intel® Active Management Technology—Query, restore, upgrade, and protect devices remotely: http://www.intel.com/content/www/us/en/architecture-and-technology/intel-active-management-technology.html

Intel® Active Management Technology Use Case #8: Agent Presence Checking (Protect): http://software.intel.com/en-us/articles/intel-active-management-technology-use-case-8-agent-presence-checking-protect
(Requires 3rd party software capable of working with Intel AMT agent presence.)

Planning to Migrate AMT-Based Computers that Are Provisioned Out of Band Management: http://technet.microsoft.com/en-us/library/gg712672.aspx#Plan_Migrate_AMT

Guidance for Microsoft SCCM 2007 and Intel SCS: http://communities.intel.com/community/vproexpert/blog/2012/08/10/now-available-guidance-for-ms-sccm-2007-intel-scs

Integrating SCCM 2012 with SCS 8.1- Blair Muller blog: http://blogs.bamits.com.au/2012/09/integrating-sccm-2012-with-scs-81.html

Measuring the Value of the Intel® Core™ vPro™ processor in the Enterprise.: https://downloadcenter.intel.com/Detail_Desc.aspx?agr=Y&DwnldID=21022

The Intel® vPro™ Technology Reference Guide: https://downloadcenter.intel.com/Detail_Desc.aspx?agr=Y&DwnldID=21362&keyword=%22vPro%22&lang=eng

About Atos

Atos SE (Societas Europaea) is an international information technology services company with annual 2012 revenue of EUR 8.8 billion and 77,000 employees in 47 countries. Serving a global client base, it delivers Hi-Tech Transactional Services, Consulting & Technology Services, Systems Integration and Managed Services. With its deep technology expertise and industry knowledge, it works with clients across the following market sectors: Manufacturing, Retail & Services; Public sector, Healthcare & Transports; Financial Services; Telecoms, Media & Technology; Energy & Utilities.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. It is the Worldwide Information Technology Partner for the Olympic and Paralympic Games and is quoted on the NYSE Euronext Paris market. Atos operates under the brands Atos, Atos Consulting & Technology Services, Worldline and Atos Worldgrid.

For more information, visit http://www.na.atos.net.

About Intel

Intel (NASDAQ: INTC) is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world's computing devices. Additional information about Intel is available at newsroom.intel.com and blogs.intel.com.

Explore Your IT Requirements

Atos solution architects build in value at each level of operations.

For more information, call us at: **(914) 881-3000**.

Visit http://www.na.atos.net and search "adaptive workplace."

atos.net