

White Paper  
Atos\* Workplace Solutions  
Intel® vPro™ Technology



# Improving IT Services and Increasing User Uptime with Intel® vPro™ Technology

Atos Origin conducted an investigation of the new remote management and security capabilities built into PCs with Intel® vPro™ technology. Atos Origin concluded that these capabilities create new possibilities for remotely managing and repairing PCs. When combined with their workplace management services, Atos Origin expects the new capabilities of Intel vPro technology to improve the speed and effectiveness of maintenance, problem resolution, and automated update processes. As Intel vPro technology is deployed into enterprises, Atos Origin expects to be able to significantly reduce desktide visits and increase user productivity with improved remote management and security for PCs.



## TABLE OF CONTENTS

|   |           |
|---|-----------|
| <b>Executive Summary</b>  | <b>2</b>  |
| <b>Atos* Workplace Solutions using PCs with Intel® vPro™ Technology</b> | <b>3</b>  |
| <b>Challenges in providing IT services today</b>                        | <b>3</b>  |
| <b>Atos Workplace Solutions and PCs with Intel® vPro™ technology</b>    | <b>3</b>  |
| Hardware-based capabilities—always available                            | 3         |
| <b>Testing and validating Intel® AMT capabilities</b>                   | <b>4</b>  |
| <b>Improving problem resolution</b>                                     | <b>5</b>  |
| Locked-down and open-build PCs  | 5         |
| Remote problem resolution for custom, open-build PCs                    | 5         |
| Faster servicing for standardized, open-build PCs                       | 7         |
| Expanding service offerings for locked-down PCs                         | 7         |
| Reducing desktside visits for hardware problems                         | 7         |
| <b>Increasing user uptime by improving security</b>                     | <b>8</b>  |
| Remotely detecting and removing a virus                                 | 8         |
| Emergency mass shutdown—even for problematic PCs                        | 8         |
| <b>Improving PC performance</b>   | <b>9</b>  |
| <b>Results and extrapolating the data</b>                               | <b>10</b> |
| <b>Looking into the future</b>  | <b>10</b> |
| <b>Summary</b>  | <b>11</b> |
| <b>For more information</b>   | <b>12</b> |

### Company:

Atos Origin is an international information technology services company, whose business is turning client vision into results through the application of consulting, systems integration, and managed operations.

# Executive Summary

As a world leader in integrated information technology (IT) outsourcing, Atos Origin provides their customers with best-of-breed services for PCs. Atos Origin expects to further improve those offerings through the use of new, remote-management capabilities that are built into the hardware of PCs with Intel® vPro™ technology.

Atos Origin can now remotely communicate with PCs with Intel vPro technology, even if PC power is off, the operating system (OS) is inoperative, or software agents are missing. This will help Atos Origin perform more effective and efficient management processes.

Atos Origin expects all enterprise PC environments to benefit from Intel vPro technology. The hardware-based capabilities of PCs with Intel vPro technology improve remote troubleshooting, so problem diagnosis is faster. Since most software problems can be resolved within the first call to the help desk, many costly desktside visits can be eliminated. Many desktside visits for hardware-based problems can also be eliminated, since technicians can now diagnose hardware failures using remote-boot and console-redirection capabilities directly from the management console.

Because Intel vPro technology enables new repair and remediation paths, Atos Origin expects to be able to minimize replace-and-restore processes for problematic PCs. With improved remote security capabilities, Atos Origin also expects to achieve faster, more complete saturation of a PC environment with critical updates. This will help Atos Origin provide customers with greater network stability and less user downtime.

Atos\* Workplace Solutions (AWS)<sup>1</sup> can now offer customers remote management and security services that have been unavailable in less-capable PCs or in software-only solutions. Systems can be serviced and repaired faster, and businesses can minimize losses since user uptime can be significantly improved.

# Atos\* Workplace Solutions using PCs with Intel® vPro™ Technology

## Challenges in providing IT services today

Advances in remote-management software allow IT organizations to automate and remotely handle many management and update tasks for PCs. However, today's software-only management solutions are usually ineffective when a PC is powered off or its operating system (OS) is not functioning.

In an effort to simplify management tasks and improve user uptime, the PCs in many business environments are "locked down." This can be effective for task workers who are constantly connected to the corporate network, and who do not require the ability to install applications or store data locally. Although a locked-down build makes it easier for IT technicians to manage and secure PCs, it greatly reduces user flexibility. In the typical business environment, 10% to 50% of users require standardized or custom "open" builds.<sup>2</sup> However, it is more difficult to inventory, maintain, repair, and remediate PCs with an open build.

In an ideal computing environment, IT technicians would have the ease of management inherent in locked-down configurations, while users enjoy the flexibility of an open-build. Achieving a better balance between manageability and flexibility requires new tools that improve remote maintenance, problem resolution, and patch management for both open-build and locked-down PCs.

## Atos Workplace Solutions and PCs with Intel® vPro™ technology

Intel vPro technology gives IT service providers, such as Atos Origin, a way to manage and secure both open-build and locked-down PCs from a remote, centralized location. The new, hardware-based manageability capabilities in PCs with Intel vPro technology include a remote communication channel, remote boot, remote power-up, console redirection, persistent event logs, and access to preboot BIOS settings and hardware asset information.

Replace-and-restore processes can now be minimized for locked-down PCs that become problematic. Atos Origin should also be able to significantly reduce deskside visits for both standardized and custom open-build PCs, even if an OS is inoperative. Maintenance and update tasks should be easier because IT technicians can now remotely manage PCs with Intel vPro technology, even if those systems are powered off at the start of the maintenance or update cycle.

The capabilities in PCs with Intel vPro technology allow Atos Origin to quickly manage systems that have traditionally been inaccessible from the management console. In turn, this opens up more management and remediation paths for PCs.

## Hardware-based capabilities—always available

PCs with Intel vPro technology include Intel® Active Management Technology (Intel® AMT) capabilities built into system hardware and "firmware."<sup>3</sup> The most significant advantage of these capabilities is that they are always available to authorized IT technicians, regardless of PC power state or the health of the OS, as long as the PC is connected to a power source and plugged into the network.

- **Remote communication**, which runs "under" the OS (refer to Figure 1), so authorized IT can communicate with the PC. The remote communication channel is based in hardware and firmware, not on the software stack in the OS, so it works even if the OS is compromised or inoperative, and even if PC power is off. The channel is secured through HTTP authentication and Transport Layer Security (TLS).
- **Always-available alerting**, so the PC can send alerts and SNMP (simple network management protocol) traps to the management console anytime. This gives an IT technician policy-based 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 a hardware or software problem became apparent. The event log is accessible even if the PC is powered down or its OS becomes inoperative.
- **Access to hardware asset information**, so IT technicians can identify compatibility issues and determine the manufacturer and model of a part that needs replacing.
- **Access to preboot BIOS settings**, for verifying configuration information and changing settings as needed to help resolve 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 authentication, and enterprise-level authentication using Microsoft\* Active Directory.

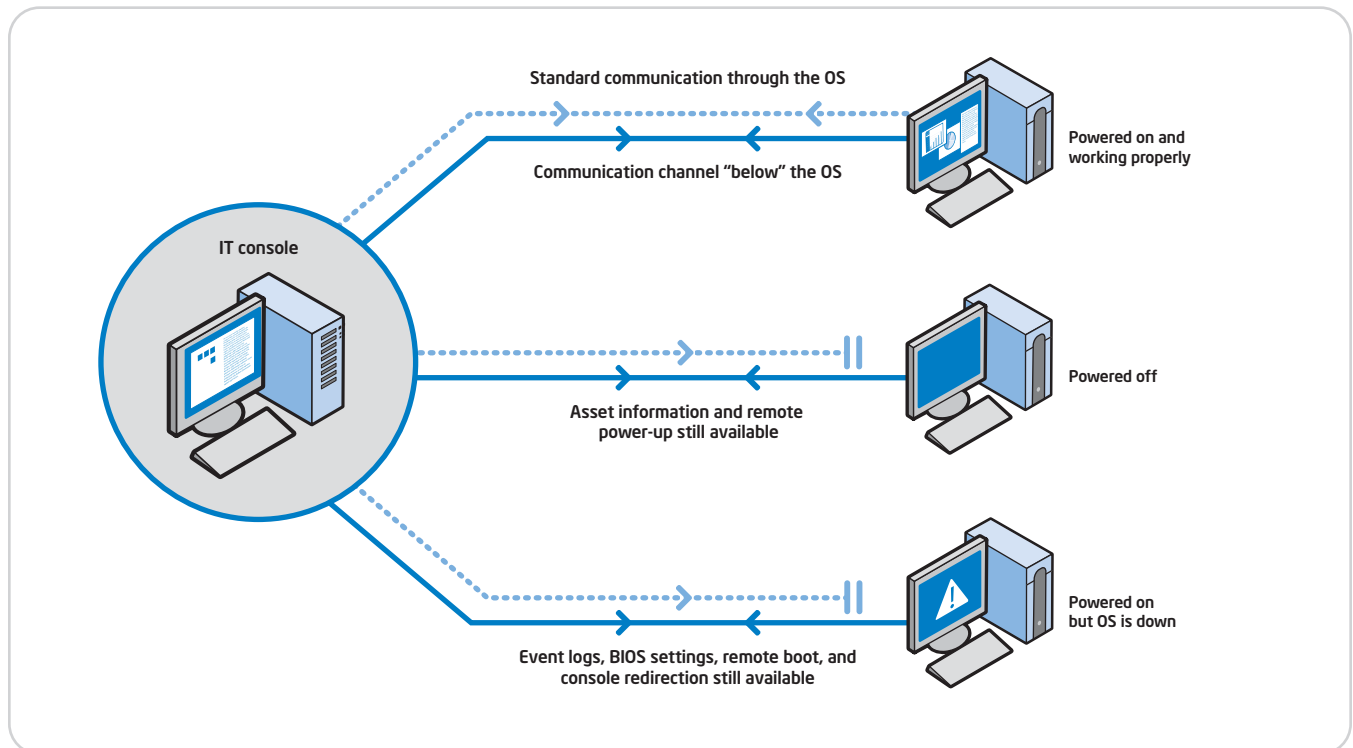
- **Remote boot**, through integrated drive electronics redirect (IDE-R), so authorized IT technicians can redirect the boot device for a problem PC to a clean image at the help desk or to an image on another remote drive. IDE-R is more secure than pre-execution boot environment (PXE) or wake-on-LAN (WOL).
- **Console redirection**, through built-in serial-over-LAN (SOL) capabilities, so IT technicians can walk the PC through a troubleshooting session without user intervention, and without leaving the management console.

### Testing and validating Intel® AMT capabilities

Atos Origin has been using a lab environment (refer to sidebar) to investigate the Intel AMT capabilities for use in production environ-

ments. The data, results, and extrapolations presented in this white paper are from the Atos Origin knowledge base and the 2006 Atos Origin Study of Intel AMT Capabilities.<sup>2</sup>

Conducting this early testing of Intel AMT will help Atos Origin implement these advanced remote management and security capabilities effectively, as soon as PCs with Intel vPro technology begin to enter corporate networks. By investigating Intel AMT now in preparation for upcoming PC deployments, Atos Origin will be in a leading position to offer customers the benefits of this technology. And, being able to demonstrate through measurements an improvement in user uptime, Atos Origin expects to be able to increase its service offerings and establish a more competitive position in the IT marketplace.



**Figure 1: Remote communication channel.** The hardware-based communication channel runs outside the OS, so it remains available even when the PC is powered off, its OS is not available, or software agents are disabled or not yet installed.

**Atos Origin test environment**

Atos Origin tested the capabilities of Intel AMT in a lab that was configured with the same infrastructure that Atos Origin deploys to their customer base. The Atos Origin test environment consists of the full Atos Workspace Solutions (AWS) 2.0, and includes the following standardized services running on a virtual server environment:

- Basic services: Microsoft Windows\* Server 2003 Enterprise Edition (login, directory, print and file service)
- Unified communication services: Microsoft\* Exchange server, Microsoft\* SharePoint, and Microsoft\* Life Communication server.
- Deployment services: Microsoft\* Systems Management Server 2003 (SMS), with the Intel® Active Management Technology (Intel® AMT) Add-on for Microsoft SMS 2003. The add-on provides integrated Intel AMT capabilities to the SMS Management Console Software.
- Management services: Microsoft\* Operation server (MoM), with interfaces to the Atos Origin standard service management environment.

**PC configurations in the test environment**

Atos Origin tested and verified the Intel AMT capabilities on five Lenovo\* desktop systems and ten unbranded desktop systems. All PCs were based on Intel AMT-enabled hardware.

Lenovo PCs were ThinkCentre\* M52 8212 systems, which include an Intel® Pentium® 4 processor. Unbranded PCs were configured with an Intel® Desktop Board D945GTP and an Intel® Pentium® D processor. Minimum processor speeds were 3.0 GHz, with a range of 512 MB to 2 GB of RAM.

**Multiple PC states tested**

Intel AMT capabilities were tested on open-build PCs in multiple "states:" PCs with a management agent installed, PCs without an agent installed, and PCs whose OS state was unknown. Capabilities were also tested on open-build PCs in various power states: powered on and in use, powered on but hibernating (sleep state), powered off, and unknown.

**Improving problem resolution**

PC boot failures can trigger time-consuming, reactive maintenance processes for both locked-down and open systems. Intel vPro technology now helps reduce the time it takes to diagnose and repair both software and hardware problems remotely, from the management console. This gives Atos Origin more options for repair paths and more efficient processes for dealing with problem PCs.

**Locked-down and open-build PCs**

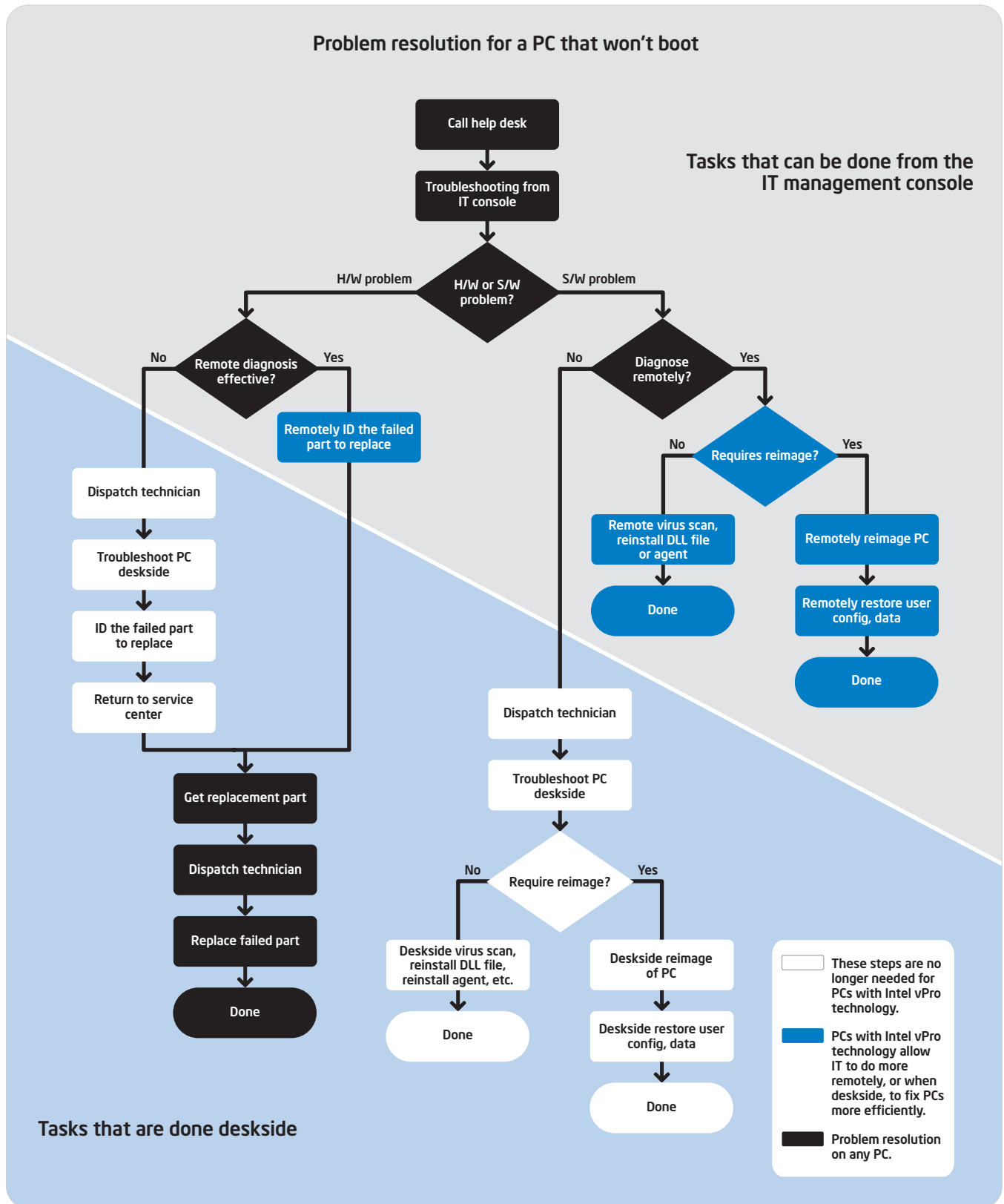
For IT service providers, there is a significant difference in resource requirements and management processes for troubleshooting and repairing PCs that are locked down versus PCs with open builds.

- **Locked-down PCs** have a common hardware and software base. Users on these systems do not have access to install or modify user applications or store data on the PC. Instead, data is accessed and stored on a remote server. Repair is usually a replace-and-restore process, which typically takes about 1 hour.
- **Standardized, open-build PCs** are for users with common needs, such as a group of users in accounting, or a group of users in an administrative area. The PCs in a particular build group have the same hardware (motherboard, processor, memory, graphics card, etc.), and the same OS and user applications. Repair options include desktside troubleshooting and repair, but also reimaging. Reimaging can be acceptable because standardized PCs can be fairly easily restored from an image of the common build. User data and preferences are then manually restored. This process can take up to 2 hours 30 minutes.
- **Custom, open-build PCs** are for users who need specialized applications, variations in OSs, virtualized systems, or other more individualized configurations. Users who might typically need custom, open builds include product developers, researchers, product support technicians, CAD (computer-aided design) designers, and handicapped users. Repair options for these PCs do not usually include replacing or reimaging because of the complexity and time involved to rebuild these systems with the user-specific OS, applications, and data. These systems usually require costly desktside visits and time-consuming troubleshooting and desktside repair.

**Remote problem resolution for custom, open-build PCs**

Atos Origin expects the most significant benefit of using Intel vPro technology will be in problem resolution for custom, open-build PCs. For these builds, replacing a system means backing up user data (if possible), replacing unique hardware, rebuilding an OS, installing a unique application configuration, then restoring the last known good data for the user. The process can take 2 hours 30 minutes plus one working day to install and verify user-specific applications. It is the last choice for both IT organizations and users.

On PCs with Intel vPro technology, Atos Origin can now perform diagnostics and repair for a custom-build system, directly from the help desk, even if the OS is not working (refer to Figure 2). For example, a software-related boot problem might be caused by a corrupted DLL (dynamic link library) file. Instead of making a desktside visit to boot the system from a CD, troubleshoot and diagnose the problem desktside, and restore the missing file on-site, the IT technician can now do this entire process from the management console.



**Figure 2. Minimizing deskside visits for an open-build, standardized PC.** Remote management capabilities help Atos Origin diagnose and resolve more problems from the management console for open-build PCs. This helps Atos Origin minimize costly deskside visits for both software- and hardware-based problems.

The technician first uses the built-in IDE-R capability in the user's PC to remotely change the system's boot device to a diagnostics image on an IT server or help-desk CD. When the system boots, the technician uses the built-in console-redirection capability of the PC to remotely walk the system through a troubleshooting session, using diagnostics tools at the help desk. When the corrupt file is identified, the technician pushes a new DLL file to the PC, overwriting the corrupt file. In scenarios like this one, there may be no need for a costly deskside visit.

According to the Atos Origin study of Intel AMT capabilities, remote diagnosis and repair for this type of software problem could take as little as 10 minutes. User uptime can be significantly improved, and IT labor and travel costs reduced.

### **Faster servicing for standardized, open-build PCs**

Atos Origin also expects to use the capabilities built into PCs with Intel vPro technology to improve problem resolution for standardized, open-build systems.

When a standardized PC is inoperative, if a technician can't resolve the problem within 5 to 15 minutes, the technician makes a deskside visit to resolve the problem. PCs with Intel vPro technology now allow IT technicians to use remote boot, console redirection, and persistent event logs to remotely diagnose problems for these systems more quickly. This can be done even if the OS is inoperative, PC power is off, or management agents are disabled. Especially for typical boot-related problems that do not require reimaging, such as corrupted files, password problems, and driver compatibility issues, remote problem resolution can save a significant amount of time.

If a system does require reimaging, that process can also be performed remotely. The traditional deskside visit can be eliminated, saving both time and labor costs, while the user is back up and working more quickly.

### **Expanding service offerings for locked-down PCs**

In an environment managed by Atos Origin, when a locked-down system is unresponsive, the IT technician usually tries to troubleshoot and fix the system within 5 to 10 minutes. If the problem can't be diagnosed and fixed in that time, the technician instructs the user to swap out the PC.

PCs with Intel vPro technology give Atos Origin the option to remotely repair a locked-down system from the help desk instead of swapping it out. This can offer businesses a significant savings in time. For example, with remote-management capabilities built into the PC's hardware, many software-related problems can be resolved in 10 to 20 minutes.

For IT, there is an additional benefit of minimizing replace-and-restore processes. This also minimizes the number of PCs that must later be diagnosed, reimaged, repaired, or remediated in a service depot. By fixing more systems remotely and more quickly, Atos Origin may be able to save significant costs in service-center labor.

#### **Lab test for remotely resolving a software-related boot failure**

To test the ability to diagnose and fix an OS problem remotely, Atos Origin removed a critical DLL file from an open-build system. This corrupted the OS and prevented the system from booting. The technician then attempted to remotely boot the PC and restore the missing file without leaving the help desk. The technician:

|       |   |
|-------|---|
| 1 min | Asked the user questions to identify the problem.   |
| 3 min | Used IDE-R to change the boot device for the PC to a boot image at the help desk. The boot image was a DOS/network bootable CD with NTFS-write capabilities and common DLL files stored on the image. |
| 2 min | Pushed the corrupted or missing DLL file to the problem PC.   |
| 4 min | Remotely rebooted the PC and watched the boot process to make sure it was successful.   |

The problem was resolved from the management console during the first phone call, and within 10 minutes.

In contrast, the same problem on a less-capable PC would have required a time-consuming deskside visit. According to the Atos Origin body of knowledge, travel time to the desk, troubleshooting, and deskside problem resolution could have taken approximately 100 minutes.

On PCs with Intel vPro technology, most OS problems can now be resolved remotely.

### **Reducing deskside visits for hardware problems**

Atos Origin expects to use Intel vPro technology to improve resolution of hardware problems, not just software problems. For example, if a PC won't boot because of a failed component or BIOS configuration issue, a technician can now remotely boot the system from an image that resides at the help desk. The technician can then use console redirection to watch the BIOS load, check and correct BIOS settings, and/or determine which hardware component is not responding.

With hardware-asset information stored in the PC's nonvolatile memory, the technician can then acquire the specific manufacturer and model information for the component, such as a failed hard drive. A replacement part can be immediately ordered. Instead

of making one deskside visit to diagnose the problem, and a second visit to replace the failed component, the technician can now make only one visit to the PC to install the new hard drive. User down-time can be minimized and IT can save significant resources on deskside visits.

### Increasing user uptime by improving security

IT organizations have a critical need to provide their customers with security services that quickly detect vulnerabilities, update security software, and remediate machines faster when a threat is identified. In particular, IT organizations need to be able to reach the “last 10%” of PCs more quickly and effectively. These are the systems traditionally out of reach of the management console because power is off, the OS is not working, or security or management agents have been disabled.

#### Remotely detecting and removing a virus

If a help-desk technician suspects that a PC's problems are related to a virus, the technician usually tells the user to disconnect the PC from the network. A technician is then dispatched deskside to reboot the PC, run a secure version of a virus scan on the system, clean the virus from the system, update the agent and apply a patch. In today's business environment, this process typically takes 1 to 2 hours.

When managing PCs with Intel vPro technology, this entire process can be completed remotely, from the management console. With Intel vPro technology, Atos Origin has access to the PC even if the OS is down and standard network communication through the OS software stack is unavailable.

For example, an IT technician might suspect (such as by a malfunction of the anti-virus software) that a PC has been compromised by a virus. In this case, the technician can remote-boot the PC to a remediation drive where the PC is not allowed network access. Or, the technician could remote-boot the PC to a bootable CD image that contains a stand-alone virus-scan application. The technician can then begin remote remediation using tools from the management console.

In this case, no deskside visits are required, and IT labor costs can be reduced. A customer's corporate policies can be enforced more completely, PCs can be returned more quickly to the user network, and productivity losses can be minimized. This is a significant improvement over traditional patch management.

#### Emergency mass shutdown—even for problematic PCs

In cases of an imminent or actual threat of a virus or vulnerability exploitation, IT administrators need to be able to shut down an

#### Lab test for remotely remediating a machine after a malicious attack

To test the ability to detect and remove a virus, Atos Origin infected an open-build PC with a virus (W32sasser.worm). The Atos Origin technician then used Intel AMT capabilities to manage and remediate the PC remotely. The Atos Origin technician:

|        |  |
|--------|--|
| 1 min  | Asked the user questions to identify the problem.  |
| 3 min  | Used IDE-R to change the boot device for the PC to a boot image at the help desk. The boot image was a DOS/network bootable CD with NTFS-write capabilities, common DLL files, and an antivirus utility stored on the image. |
| 3 min  | Ran McAfee* Virus Scan Command Line Scanner (through console redirection) to detect the virus.   |
| 30 sec | Remotely removed infected files from the user's system.  |
| 4 min  | Remotely rebooted the PC from the user's hard drive and returned keyboard control to the user.   |

Although the PC was not responsive to typical management software, the Atos Origin technician was able to resolve the problem from the management console. No deskside visits were required.

In the test lab, remediation took less than 15 minutes. In a real-world environment, Atos Origin expects to reduce the time required to resolve this type of problem by approximately 35 minutes, or 25% to 50%.

Another benefit of remote security and remediation to Atos Origin is that the technician can start scanning and patching processes, then help another user while the remediation occurs across the network.

entire population of PCs. This helps prevent a threat from spreading, and limits the consequences of infection.

Atos Origin is currently able to remotely power down working systems. However, a percentage of PCs with both locked-down and open builds have traditionally been out of reach of the management console during patch deployments. Some of these PCs are powered off. In some cases, users with open-build PCs refuse an update because it would be inconvenient. Sometimes PCs are already compromised and can't be remotely shut down or updated until they have been remediated. In today's business environments, IT organizations achieve, on average, a patch deployment of only 85%—after 5 days.

Atos Origin can now shut down PCs with Intel vPro technology from the management console, even if the OS is not responding. This allows an IT technician to reach almost all of these PCs, even those which would traditionally not be included in an emergency mass shutdown or remediation. To do this, the technician first uses management software to poll machines for their power state. The

technician then uses the built-in remote power-down capability to shut down problematic or compromised machines. PCs that are problematic can be rebooted remotely to a remediation drive, where they can be restricted from network access until repaired and brought back into compliance.

No desktside visits may be required, threats can be more quickly contained, and losses from malicious attacks can be minimized. With remote power management, Atos Origin can help reduce a customer's window of vulnerability from days to approximately hours (refer to Figure 3).

**Lab test for remotely installing a critical patch**

To test the ability to remotely install a patch on PCs off-hours, Atos Origin powered down 15 open-build machines to simulate an office environment in which users had left for the night. The process consisted of the following steps:

- |        |  |
|--------|--|
| 15 min | The technician created a notification (or "advertisement") using a patch-of-vulnerability package in SMS, by: <ul style="list-style-type: none"> <li>▪ Selecting the target audience for the package. In this case, the audience was the entire population (15 machines).</li> <li>▪ Scheduling the update as a mandatory assignment, using SMS.</li> <li>▪ Selecting "assign immediately after this event" in SMS.</li> <li>▪ Including the power-up and power-down commands for PCs with Intel vPro technology.</li> <li>▪ Launching the advertisement.</li> </ul> |
|--------|--|

|        |   |
|--------|---|
| 45 sec | The patch notification began powering up all Intel AMT-enabled machines. All 15 Intel AMT-enabled PCs in the lab were powered up as directed. |
|--------|---|

|        |  |
|--------|--|
| 10 min | SMS deployed the patch to all powered-up machines. |
|--------|--|

|       |  |
|-------|--|
| 5 min | SMS shut down the PCs in an orderly manner when the update finished. |
|-------|--|

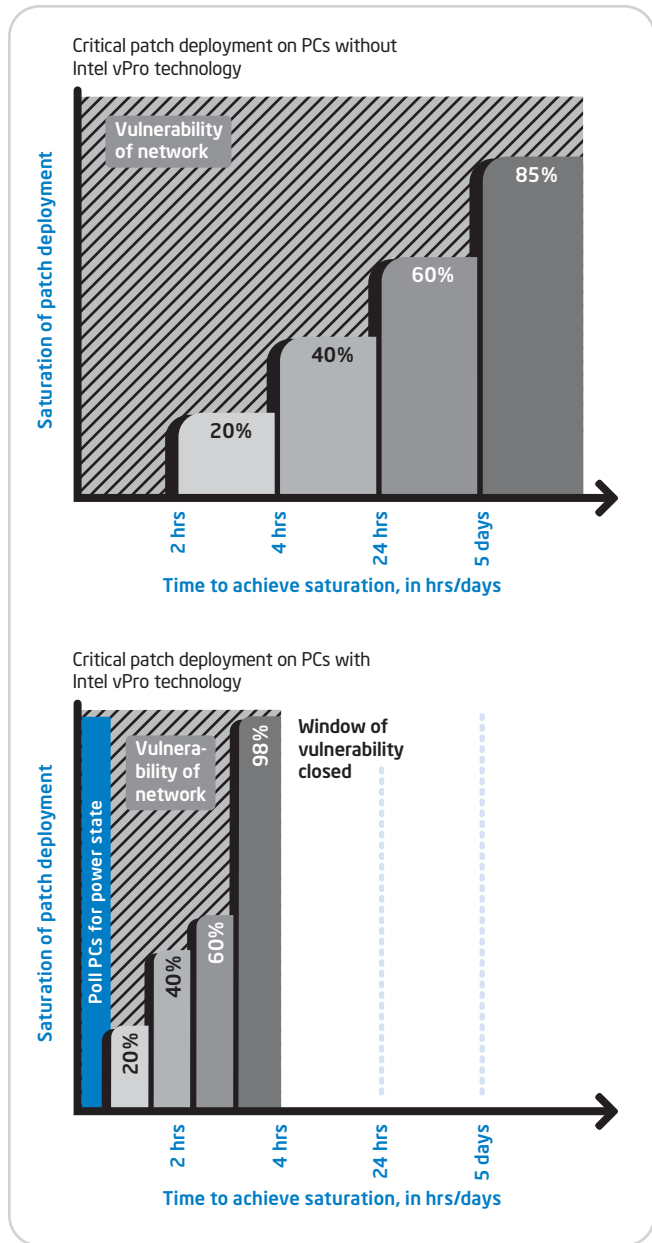
The patch was deployed with 100% saturation within 31 minutes. Atos Origin has extrapolated this data to an environment of 8,500 open-build machines across multiple campuses (refer to Figure 3).

**Improving PC performance**

A small percentage of performance issues in open-build PCs are not the result of a specific software or hardware problem. Instead, these issues are related to memory leaks, application compatibility issues, an overabundance of background processes, and so on.

Today when these problems are reported, a desktside visit is required for extensive troubleshooting and diagnostics, with all the asso-

ciated downtime for the user. Although the number of performance calls is relatively tiny, they are a serious issue for user productivity. For example, in an environment with 8,500 PCs, Atos Origin received 10,000 help-desk calls in two months, of which only 30 calls were related to PC performance.<sup>4</sup> However, to ensure problem resolution, Atos Origin assigned 10 technicians to address these 30 calls along with their other tasks.



**Figure 3: Saturation of patch deployment.** Atos Origin has extrapolated the test data, and expects to be able to deliver a 98% saturation in approximately 4 hours for patch deployment on up to 8,500 PCs with Intel vPro technology. Patch deployment on less-capable PCs achieved only 40% saturation after 4 hours of deployment, and 85% saturation after 5 days.

When managing PCs with Intel vPro technology, Atos Origin can now use the remote power-up capability to power problem PCs on and perform diagnostics off-hours. This allows Atos Origin to create a baseline for the performance of an open-build system. Atos Origin can then reboot the machine to a clean image on a CD and run diagnostics again to create comparison data. This helps Atos Origin rule out suspected issues and identify actual problems which can then be addressed.

The remote power-up capability also allows Atos Origin to do random testing on a regular basis to survey open-build PCs on different subnets. By using statistical analysis, Atos Origin expects to be able to identify more issues for these PCs before they escalate into service center calls. Being able to power up the machines remotely also means Atos Origin can perform other compute-intensive tasks off-hours, such as maintenance, back-ups, and upgrades.

Atos Origin can now consider extending its AWS services catalog, by offering a regular PC performance-enhancement service aimed at open-build PC environments. An enhancement service could include hard-disk defragmentation, integrity checks, and performance testing and reporting. Intel vPro technology makes it easier for Atos Origin to establish such a service, even for custom, open-build machines.

## Results and extrapolating the data

After examining the results, Atos Origin extrapolated the data to understand the benefits of using this technology to improve service for nonstandard PCs in a real-world environment. Table 1 shows the extrapolated data and expected results of deploying PCs with Intel vPro technology across a division of a large corporation, with 8,500 open-build machines at multiple locations.<sup>4</sup> Table 2 shows the estimated average time saved for the various steps in the IT processes.

## Looking into the future

In the future, Atos Origin expects to offer customers the advantages of additional capabilities that will be built into PCs with Intel vPro technology:

- **Automatic presence checking for software agents.** Built-in, hardware-based “heartbeats” and programmable “watchdog” timers help make sure software management and security agents remain present. If an agent misses its predetermined check-in, the system immediately logs the event in nonvolatile memory and sends an alert to the management console, based on AWS policy. The PC itself now helps make sure that critical security and other agents remain active.
- **Hardware-based filtering of network traffic.** Programmable hardware filters check inbound and outbound network communication for known threats to help identify potential problems faster. IT administrators can now define the packet behavior conditions that will trip a hardware filter and trigger an alert and/or event. Because filters are hardware-based, they are active even if an OS is down or an agent disabled. They can also be used to help automate containment and remediation processes. For example, automated responses could include sending an alert to the management console, applying isolation policies, launching a virus scan, or running an executable that takes a particular remediation action.
- **Containing threats quickly.** An embedded, hardware-based switch (or “circuit breaker”) for rapid threat containment can be triggered off the built-in hardware filters. When a filter is tripped, the switch can disconnect the network data path at the OS software stack—even if the OS is compromised or down. Network traffic is halted before it is passed to the OS. The PC can now isolate itself from the network. Or, the system could set a policy-based rate-limit for its own inbound and outbound network traffic, to give IT administrators more time to investigate a threat.

These and other capabilities will help Atos Origin remotely manage all PCs in a network, not just those whose power is on or whose OS is working properly.

| Process   | With / without Intel® AMT | Initial call to help desk | Extended services from IT console <sup>2</sup> | Travel to / from desk <sup>3</sup> | Deskside diagnosis and repair | Total time to resolve | % of savings in time |
|---|---------------------------|---------------------------|--|------------------------------------|-------------------------------|-----------------------|----------------------|
| Diagnose and repair PC that has corrupted DLL file                                | W/o Intel AMT             | 15 min                    | 0  | 30 min                             | 15 min                        | 60 min                | 83%                  |
|   | W/ Intel AMT              | 10 min                    | 0  | 0                                  | 0                             | 10 min                |                      |
| Diagnose and repair hardware problem  | W/o Intel AMT             | 15 min                    | 0  | 60 min                             | 25 min                        | 100 min               | 55%                  |
|   | W/ Intel AMT              | 10 min                    | 0  | 30 min                             | 5 min                         | 45 min                |                      |
| Off-hours maintenance to update a PC that is off at the start of the update cycle | W/o Intel AMT             | NA <sup>1</sup>           | NC <sup>4</sup>                                | 30 min                             | 5 min                         | 35 min                | 86%                  |
|   | W/ Intel AMT              | NA                        | 5 min  | 0                                  | 0                             | 5 min                 |                      |
| Patch a virtual machine: boot machine into specific OS, push files or patch       | W/o Intel AMT             | 15 min                    | 0  | 30 min                             | 60 min                        | 105 min               | 76%                  |
|   | W/ Intel AMT              | 10 min                    | 15 min   | 0                                  | 0                             | 25 min                |                      |

<sup>1</sup> NA = not applicable.  
<sup>2</sup> Extended services include remote power-up, pushing a patch, and reimaging a machine.  
<sup>3</sup> Assumes a 30 minute total travel time to and from the user desk.  
<sup>4</sup> Without Intel AMT, management software cannot usually communicate with machines that are powered down, so these machines are often missed in the maintenance cycle. With Intel AMT, Atos Origin can remotely power up these machines and perform the maintenance.

**Table 1: Estimated times for IT tasks on a PC with an open build.**

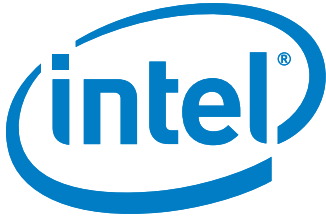
| Estimated average savings in time                      | % savings |
|--|-----------|
| Average savings in time required for first-level calls | 33%       |
| Average savings in travel time                         | 80%       |
| Average savings in on-site support time                | 95%       |
| Average savings in labor time                          | 40%       |
| Average total savings in time                          | 70%       |

**Table 2: Estimated average savings in time for a PC with an open build.**

### Summary

PCs with Intel vPro technology deliver new hardware-based capabilities that can help Atos Origin improve management and security for both locked-down and open-build PCs. In particular, Atos Origin expects to be able to significantly reduce the number of deskside visits required to manage open-build systems. At the same time, replace-and-restore processes can be minimized for locked-down PCs. With the remote power-up capability in these PCs, Atos Origin also expects to reduce a customer's window of vulnerability from malicious attacks and other security threats.

For Atos Origin, Intel vPro technology creates opportunities for new and more efficient processes to manage and secure PCs that have traditionally been inaccessible from the management console. When using PCs with Intel vPro technology, Atos Origin expects to be able to deliver new services, improve service level agreements, and innovate their offerings more quickly in a competitive market.



### **For more information**

PCs with Intel vPro technology give authorized IT administrators critical, hardware-based security and manageability capabilities not available in software-only solutions. When provisioned with third-party software, these PCs can be managed directly from the management console, regardless of their power state or the health of their OS.<sup>3</sup>

### **For more information about Intel vPro technology, visit**

[www.intel.com/vpro](http://www.intel.com/vpro)

### **For more information about Atos Workplace Solutions, visit**

[www.atosorigin.com](http://www.atosorigin.com)



<sup>1</sup> All content regarding Atos\* Workplace Solutions was provided by Atos Origin.

<sup>2</sup> Source: Atos Origin knowledge base, and/or the 2006 Atos Origin Study of Intel AMT Capabilities. The 2006 Atos Origin Study of Intel AMT Capabilities was conducted in February and March, 2006, at the Atos Origin test site. Other IT service providers may see different results, depending on their service environments.

<sup>3</sup> PCs with Intel vPro technology include Intel® Active Management Technology (Intel® AMT). Intel AMT requires the computer to have an Intel AMT-enabled chipset, network hardware and software, connection with a power source, and a network connection.

<sup>4</sup> Based on Atos Origin internal data for services provided to a division within a typical, large corporation. Other IT service providers may see different results, depending on their service environments.

Copyright ©2006 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel vPro, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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