INTEL vPro® vs. AMD® PRO* OUT-OF-BAND MANAGEMENT

WHITE PAPER
MARCH 2020

Deborah Mrazek *Senior UX Strategist*
Colin Bay *Chief Research Officer*

concreteUX.com

concrete

DASH COMPETITIVE ASSESSMENT

THIRD-PARTY TESTING FINDS AMD® PRO MANAGEABILITY LAGS BEHIND INTEL VPRO® PLATFORM

IT administrators and decision-makers seek the best solution for managing their networked endpoints for both wired and Wi-Fi connected devices when powered off or the OS isn't running (i.e., out-of-band management).

Hired by Intel as a third party, we put management of the Intel vPro® platform to the test in the hands of some pretty savvy IT administrators, then asked them to compare its capabilities with AMD PRO—you'll want to hear what they had to say. They had some compelling ideas about which of these two platforms most capably and robustly meets the growing need for remote, in-band, and out-of-band endpoint management.

This white paper investigates and compares manageability aspects of the AMD PRO and Intel vPro platforms, with a focus on functionality, usability, and standards adherence. AMD suggests that AMD PRO is more robust and more compatible than Intel vPro technology. We found stark differences. We'll show you why. We'll present user experience test findings, expert reviews, and analyses that spotlight the Intel vPro platform's advantages, particularly in critical areas like security, features, and out-of-band management over Wi-Fi—one of the biggest advantages of the Intel vPro platform.

We'll also address knowledge gaps in customer understanding. Our testing showed that often, the IT admins considering these two platforms had a limited understanding of their differences and of DASH, the protocol both platforms were built on. Our test results also showed that even savvy IT admins lack clarity about in-band vs. out-of-band management and its benefits. We'll explain out-of-band remote management and the DASH standard. Then we'll share the evidence from our testing showing that Intel vPro technology is significantly more powerful than AMD PRO. You'll see that when our participants peeked under the hood, **AMD PRO with DASH vs. the Intel vPro platform** turned out to be **AMD PRO with *only* DASH vs. Intel vPro platform with DASH plus important additional capabilities**.

WHO ARE WE? WE ARE CONCRETE

concrete

The power of insight.

Manufacturers naturally tout the virtues of their products. Every parent thinks their baby's a genius. Some manufacturers even conduct their own consumer testing, but with their inherent biases, such studies may not provide the big picture objectively. **That's where a third-party group like ours comes in.**

We're **Concrete**, a research consultancy that brings evidence, insights, and the voice of the user to help disruptive innovators define intelligent, interface-based products. Concrete fundamentally reimagines how customers interact with the technology and information they encounter every day, by employing approaches like insight mining, experience modeling, and impact measurement. We gather directive data from an array of practices that include ethnographic studies, contextual inquiry, longitudinal studies, user experience, and competitive assessment, as well as futurecasting and ideation, to name a few.

Commissioned by Intel, Concrete conducted a study to test AMD's DASH technology and Intel vPro technology to see how their manageability experience compares—because that's what we're good at.

For our independent testing of these two platforms, we brought years of experience and expertise to the table to create and conduct a fact-based study in the supporting infrastructure of a lab environment. Here, typical IT admins and expert reviewers carried out the hands-on experience of configuring and using the **AMD PRO and Intel vPro** platforms. This allowed us to uncover the strengths and weaknesses of both platforms through the real-life experience of IT professionals. By observing end users' interactions, struggles, and successes using these products, we collected useful intelligence for both customers and manufacturers.

MYTH AND FACT

LET'S BREAK DOWN THE PRIMARY DIFFERENCES BETWEEN THE AMD PRO AND INTEL VPRO PLATFORMS

1. In their marketing materials, AMD firmly asserts that AMD PRO is compliant with the DASH standard while Intel® Active Management Technology (Intel® AMT) is proprietary.[1] Actually, dozens of products with Intel vPro technology are in the DASH standards body's registry of certified devices. And it turns out that Intel vPro technology actually offers a superset of DASH's defined capabilities.

2. AMD's marketing mentions the Distributed Management Task Force (DMTF), the open industry standards consortium that created the DASH standard, as if it is unique to AMD. We learned that Intel was a founding DMTF member and today sits on the DMTF board.

3. AMD describes their platform as an "open standard" and the Intel vPro platform as "proprietary." In fact, we found that they're both built on the DASH standard. We also looked at third-party consoles to see how well-supported the two platforms are. Leading endpoint management applications actively support the Intel vPro platform's functionality via public APIs and SDKs for Intel AMT (the management technology in the Intel vPro platform). Those include consoles from Symantec, SolarWinds, LANDesk, and Kaseya, for example. We struggled to find third-party consoles advertising AMD DASH support, beyond a Microsoft SCCM (System Center Configuration Manager) plugin written by AMD.

4. So, what's the difference in functionality? At first glance, the AMD PRO and Intel vPro platforms seem to offer similar capabilities, since they both support out-of-band management. Looking further, we learned that Intel vPro technology not only includes DASH functionality but goes beyond the minimum standards to bring real-world benefits like TLS security, Active Directory authentication, in-band management, and out-of-band device control over Wi-Fi. This came as a surprise to IT admins, given that most laptops always run on Wi-Fi.

5. At first blush, AMD's open standard might look like the obvious choice for saving money, because we saw differences of about $25. Other research showed that while companies may save a few dollars in up-front hardware costs, AMD's more limited functionality could result in higher costs due to deskside visits for the same issues that Intel vPro technology can manage without dispatching a tech.

[1] Originally found in videos at www.amd.com/en/technologies/security-manageability, accessed 2020-01-15. As of 2020-03-23 available at www.youtube.com/watch?v=6m6_2K45Y7k and www.youtube.com/watch?v=39XAMP73MiQ .

WHAT YOU NEED TO KNOW...

OUT-OF-BAND MANAGEMENT OVER WI-FI... WHY YOU NEED TO CARE ABOUT IT

70%

OF EMPLOYEES

are working at least one day a week somewhere other than the office[1]

91%

OF BUSINESS PEOPLE

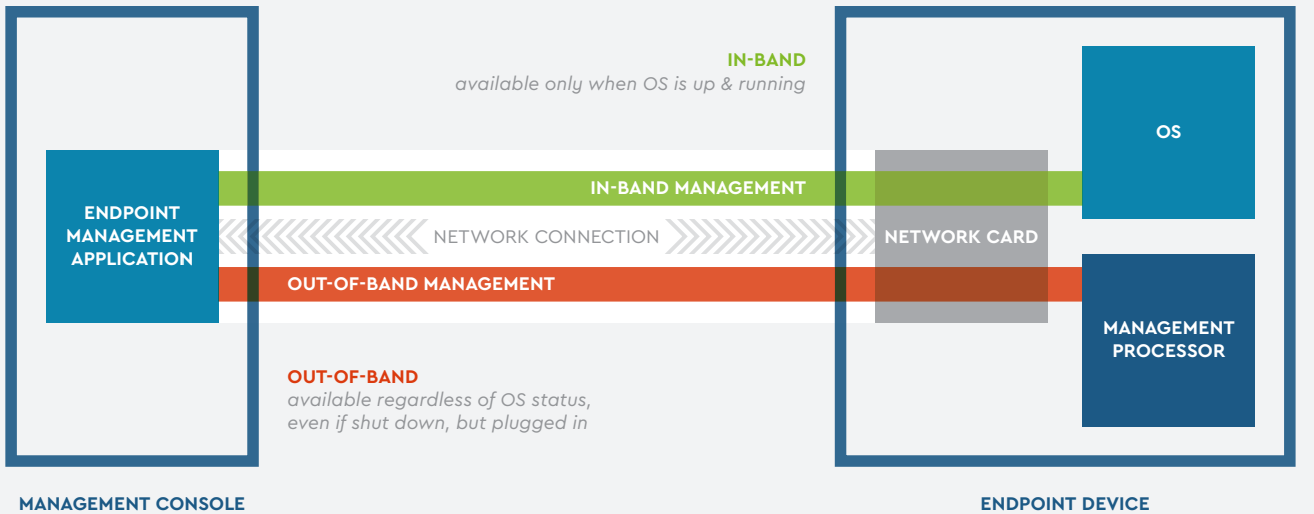
say flexible workspaces enable mobile employees to be more productive[2]

94%

OF MILLENNIALS

say that collaboration is "critically important" to their work[3]

OUT-OF-BAND MANAGEMENT... HOW IT WORKS



[1] "70% of people globally work remotely at least once a week, study says," 2018-05-30, www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html. From worldwide study by Swiss company IWG.

[2] "The Workspace Revolution: Reaching the Tipping Point," 2018-05, www.contact.regus.com/GBS18_Report_Download_Request.

[3] "Meeting the Demands of a Mobile Workforce," 2017-07-17, www.cio.com/article/3206277/meeting-the-demands-of-a-mobile-workforce.html.

OUT-OF-BAND MANAGEMENT

WHAT IS IT?

Out-of-band management (OOBM) combines specially designed hardware and firmware with a management console for troubleshooting and checking the status of computers and other devices on a corporate network. A robust manageability platform with OOBM permits IT admins to detect and monitor the status of the endpoints on a network, *independent* of their power state, operating system status, or connectivity type. By contrast, a weak platform will not cover all the bases. DASH protocols are a starting point for platforms and hardware to communicate, but they aren't all-inclusive.

"Robust" means the OOBM platform can monitor a client device even when its operating system is showing the "blue screen of death," or power it on when it's been powered off. Just imagine the cost benefits realized when a company's admins can perform tasks on your networked endpoints without having to send technicians out to an employee's desk or a distant kiosk. With the right platform, configured properly, a hardware failure is about the only thing they'll need to dispatch a tech for.

And that's not all. With some forms of out-of-band management, IT admins can do more than just monitor and diagnose. They can power on and take KVM control of a remote client, whether it's a laptop, a tablet, point-of-sale machine, IoT device, or a kiosk, connected by wire or wirelessly from anywhere, regardless of the state of its OS. What if the OS isn't installed yet or isn't working properly? Even then an IT admin can reach it remotely to troubleshoot and solve problems. It's really useful technology.

A well-chosen remote management platform can turn a company's IT admins from commuters shuttling between faraway devices into maestros who can perform all kinds of maintenance and prevention tasks from their own desks.

WITHOUT LEAVING THEIR DESK, IN JUST A FEW KEYSTROKES AN IT ADMIN CAN DO THINGS SUCH AS:

- **Reboot, shut down, power on**
- **Run device health checks: monitor hardware sensors such as fan speed, power voltages, chassis intrusion, etc.**
- **See a client's in-band and out-of-band video output**
- **Control an endpoint during its boot cycle to adjust BIOS settings before the operating system has loaded, troubleshoot OS boot issues, or perform diagnostics**
- **Boot from a USB drive or disk image for bare-metal provisioning**
- **Install, not just update, the entire operating system remotely**
- **Perform virus patching, driver, and security updates**
- **Conduct asset inventory**

OUT-OF-BAND MANAGEMENT

HOW IT'S ACCOMPLISHED

Historically, enabling remote management on computers and servers required adding a remote management card. Easily enough accomplished but without a standard, such cards could support only a limited list of motherboards. To expand the availability of OOBM capabilities, the industry needed a way for manufacturers and developers to create hardware and software standards that could work together. This need drove the creation of DASH.

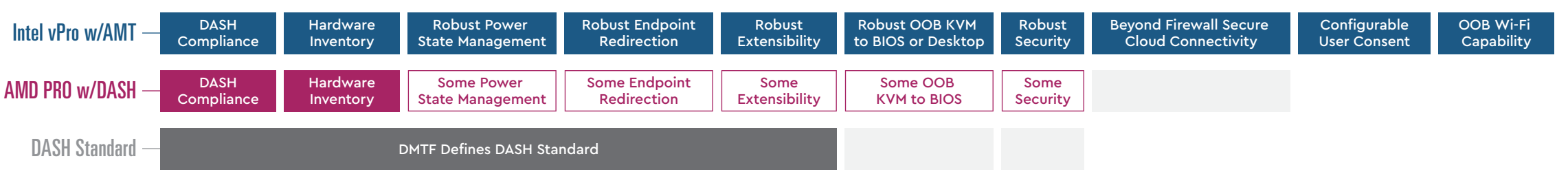
WHAT'S DASH?

DASH is the set of industry standards for the web services management of desktop and mobile client systems followed by the original equipment manufacturers (OEMs) of chipsets, like AMD and Intel. DASH is *the* standard for the secure in-band and out-of-band and remote management of all desktop and mobile devices.

DASH was created by the Distributed Management Task Force (DMTF), an international, not-for-profit, standards body founded in 1992. The organization's purpose is to simplify network-accessible technologies through the open collaboration of leading technology companies like Broadcom, Cisco, Dell, Emerson, HP, Intel, Lenovo, NetApp, and Oracle, to name a few, who are all committed to increasing interoperability across all brands. Notably, Intel was one of the founding members of the DMTF and today maintains a seat on its board of directors.

Although DASH standard is the *foundation* of both the AMD and Intel platforms, **DASH only defines a minimal set of capabilities** for client PC systems. When a system has DASH-defined functionality and no more, it's like a refrigerator that only nominally meets the standards for a refrigerator, at least by today's expectations. It's electric, it keeps food cool, and it has shelves—but it doesn't have an icemaker, a water dispenser, a vegetable drawer, or automatic defrosting. You get the idea. DASH is that bare-bones refrigerator. IT admins need more.

There's no dispute that a well-executed remote management platform has the potential to bring a multitude of benefits to a company, from cost and time savings to preventive security advantages. But which of these two, the AMD PRO or Intel vPro platform, provides the greatest scope of everything you need with the fewest limitations? This is exactly what our testing sought to find out. Let's examine both platforms more closely.



A TALE OF TWO PLATFORMS

AMD PRO PLATFORM

According to AMD's marketing, "Our powerful management tools also offer remote diagnostics and troubleshooting, asset management, automated system startup and shut down. Solutions based on DASH can also help avoid the pitfalls of proprietary systems, by providing vendor neutral, platform-independent, and economical approaches to out-of-band client management."[1]

[1] "Technology That Won't Lock You In," accessed 2020-03-11, www.amd.com/en/technologies/security-manageability.

INTEL VPRO® PLATFORM WITH INTEL AMT® AND INTEL® EMA

Intel describes Intel AMT as "Hardware and firmware for the remote out-of-band management of business computers running the Intel Management Engine." Intel AMT's purpose is "to assist with the monitoring, maintaining, updating, upgrading, and repairing of computers remotely." Intel® Endpoint Management Assistant (Intel® EMA) is Intel's management console that leverages Intel AMT. Other consoles and custom IT applications can use Intel AMT features, via an SDK and API.

The Intel vPro platform with Intel AMT is designed to use a manageability processor located on the chipset. It uses TLS-secured communication and strong encryption to provide additional security. Intel AMT is built into every PC branded with Intel vPro technology. Intel AMT release 5.1 and later generations actively support DASH version 1.0 and 1.1 standards for out-of-band management, *contradicting* AMD's implication that only their platform supports DASH.

Another unique Intel AMT feature gives it an enormous security advantage: Client Initiated Remote Access (CIRA). When CIRA is first provisioned on a device, it makes a secure connection to the management server and keeps itself connected. When the console has a request, it doesn't have to scan the network for your laptop because it's already connected to the server—and thus the client doesn't have to leave management ports open all the time, frustrating any hackers.

Here's what performing remote management without CIRA is like. Imagine a spacecraft with a phone number every spammer can call to give the astronauts commands, even though those should come only from Mission Control. But if it's the spacecraft that makes the initial call to Mission Control and keeps the phone call active, communication is much safer. That's how CIRA works to keep endpoints secure, even if an intruder gets through your firewall. That's a powerful feature, and we didn't see anything comparable with AMD PRO.

WHAT'S THE DIFFERENCE BETWEEN INTEL VPRO TECHNOLOGY AND INTEL AMT?

Intel AMT is a critical feature of the Intel vPro platform. The Intel vPro brand goes on systems that meet a strict set of technology requirements, including manageability with Intel AMT. Intel AMT uses the silicon-based Intel Management Engine for out-of-band capabilities. The Intel management features described in this report all pertain to Intel AMT. So, when we say "Intel vPro technology" in this report, we're generally talking about this specific ingredient—Intel AMT.

CONCRETE TESTING

To evaluate these two platforms from a real-world perspective, Concrete sourced a collection of platform-agnostic IT admins and assigned them a series of tasks in a test environment. Then we collected their candid thoughts and experiences about using and configuring the in-band and out-of-band remote features with each. The results provide a relevant, realistic assessment of the pros and cons of each platform.

TEST SETUP

Console: We designated an HP EliteDesk 800 DASH-enabled computer running Windows 10 Pro, as a management console. The AMD Management Console and Intel Endpoint Management Assistant (Intel EMA) were set up on this PC.

Endpoints: We set up 5 endpoints, each running Windows 10 Pro, with DASH enabled in the BIOS and running an Intel EMA agent. The endpoints consisted of:

+ **1 AMD PRO laptop[1]**
+ **1 AMD PRO desktop[2]**
+ **1 Intel vPro laptop with Client Initiated Remote Access (CIRA)[3]**
+ **1 Intel vPro desktop with TLS (Transport Layer Security)[4]**
+ **1 Intel non-vPro desktop with TLS[5] (to experience consoles managing non-DASH-enabled devices)**

We connected locally through an Ethernet switch and a local wireless router, with static IP addresses to minimize variation. We turned off firewalls. We ran Intel EMA in the Chrome browser. Participants used AMD Management Console software (which in this paper we'll call "the AMD console") as a Windows desktop application, which was set up and configured in advance. Both the AMD console and Intel EMA quick start and user guides were made available within their respective consoles.

TEST ENVIRONMENT CONFIGURATION

	AMD PRO Laptop	AMD PRO Desktop	Intel vPro Laptop	Intel vPro Desktop	Intel non-vPro Desktop	Management Console
Connectivity	Isolated (in-room only) Ethernet or wireless—static IP					
DASH enabled (BIOS)	✓	✓	✓	✓	✓	✓
Intel EMA Agent	✓	✓	✓ CIRA	✓ TLS	✓ TLS	
Win 10 Pro	✓	✓	✓	✓	✓	✓
Firewalls	OFF	OFF	OFF	OFF	OFF	OFF

[1] HP EliteBook 735 G5 AMD, model 4HZ55UT, CPU AMD Ryzen* 3 PRO 2300U, 4C/4T, 3.4GHz, Radeon Vega 6 graphics, 8GB x 1 memory, 256 GB SSD m.2. Serial no. 5CG917093J.

[2] HP EliteDesk 705 G4 AMD, model 4HX42UT, CPU AMD Ryzen* 5 PRO 2400GE, 4C/8T, 3.8GHz, Radeon Vega 11 graphics, 8GB x 1 memory, 256GB SSD m.2. Serial no. MXL92062P6.

[3] HP EliteBook 840 G4, model 1GE42UT, CPU Intel® Core i5-7300U, Product 1GE42UT, 2C/4T, 3.5GHz, HD620 graphics, 8GB x 1 memory, 256GB SSD. Serial no. 5CG7040RCB.

[4] HP EliteDesk 800, model 4CD93UT, CPU Intel Core i5-8500T, 6C/6T, 3.5GHz, UHD630 graphics, 8GB x 1 memory, SATA 1TB HDD. Serial no. 8CC8281GTM.

[5] HP ProDesk 600 G4DM, model 4HG95UT, CPU Intel Core i3-8100T, 4C/4T, 3.10GHz, UHD630 graphics, 4GB x 1 memory. Serial no. MXL93444ZR. See www.ivanti.com.

Measurements based on: SYSmark2018* Overall Score. Performance results are based on testing from October 29, 2019 to November 5, 2019 and may not reflect all publicly available security updates. See configuration disclosure for details. No product can be absolutely secure. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to www.intel.com/benchmarks.

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

CONCRETE TESTING

TASKS

1. **Familiarize yourself with the capabilities of both systems**
2. **Set up, configure, and provision each console to manage all five endpoints**
3. **Power each endpoint off and on and control KVM OOB, from each console over Ethernet**
4. **Power each endpoint off and control KVM OOB, from each console over wireless**
5. **Explore both systems for security implications**
6. **Review DMTF, AMD, Intel, and third-party documents for capabilities, limitations, strengths, and weaknesses (over 60 documents reviewed)**

METHODOLOGY NOTES

Tasks 1–6 were all performed by the expert review team. Tasks 1, 3, and 4 were performed by all participants. Test participants performed their tasks from different perspectives than the expert review team. To use an automotive analogy, our test participants were asked to take the platforms for a test drive, while our experts were asked to push the limits to determine cornering, handling, and braking.

PARTICIPANTS

Twelve participants engaged in a qualitative blind study and were unaware of who it was commissioned by. All the data collected is based on the testers' individual experiences and thinking. In general, none of the participants understood the significance of DASH, and most were unfamiliar with the terms "in-band" and "out-of-band." Once they knew more about OOBM capabilities, each felt the capabilities provided a potential business benefit.

+ Participants spent 2 hours each: 80–90 minutes interacting with the systems and 30–40 minutes answering questions.
+ Participants' industry experience varied from 5 to 40 years and represented a range of roles including system admins, desktop support, IT support, developers, and network support staff.
+ Some were partially self-taught or had on-the-job training, some were certified (e.g., Microsoft Certified, Citrix Certified, IBM Certified) and some had formal college training or were college graduates.
+ Each had at least some remote desktop or endpoint management experience and none had used Intel EMA or the AMD console before, although many had experience with Microsoft System Center Configuration Manager (SCCM) or other Microsoft tools, as well as Citrix, Puppet, Dell, or other third-party endpoint management solutions.
+ Included in the group were individuals who supervised teams managing up to 1000 endpoints seated both locally and remotely. Endpoints managed included Intel and AMD devices running Windows, Mac, Linux, and Unix on tablets, phones, imaging equipment, and other devices through a combination of Ethernet, Wi-Fi, and VPN.
+ In addition, we included a subset of experts to review both solutions from a technical perspective. Unique expertise for this group included:
    - **A network expert** with over 15 years of IT systems and application management experience with expertise in software development, applications solution delivery, and operations experience at the 100,000-employee scale, who spent significant time reviewing documentation and experimenting with the systems.
    - **A security expert,** a full-stack operations professional, highly skilled at solving large-scale, complex problems on distributed systems.
    - **A human factors engineer** with over 30 years of human factors experience with expertise in usability, UI design, design strategy, experience design, and experience research.

THE FINDINGS

GENERAL IMPRESSIONS 1

These are the overall impressions collected objectively from test participants of both platforms and analyzed by our expert review team. Based on that broad set of observations, we found the Intel vPro platform had the most mature, feature-rich, and secure technology for manageability.

AMD PRO PLATFORM WITH THE AMD CONSOLE

STRENGTHS

+ Participants noted that the AMD console featured a good running log on the main screen.
+ They liked the simple interface but noted its limited functionality.
+ The managed node list was on the home screen rather than one click away.

WEAKNESSES

+ Provisioning DASH required physically visiting the AMD PRO machine making initial setup labor-intensive and thus expensive.
+ The AMD console power state status often lagged or was inaccurate.
+ Participants found the color-coding scheme of the interface unclear.
+ They observed that the AMD console was usually unable to interact with Intel machines.
+ Over Wi-Fi, neither in-band nor out-of-band manageability and endpoint acquisition worked for our participants on AMD PRO.
+ Many of the AMD console's error messages were unclear.
+ Available documentation was sparse and hard to find. Any useful information tended to be third-party support articles on the web, to participants' disappointment. With Microsoft SCCM, some key configuration required for setting up a client's network hardware was unavailable.
+ Participants were unable to act on groups of endpoints using the AMD console, which implied each had to be individually managed.
+ The AMD console named endpoints by IP address, not by host name. This was a curious choice since with DHCP, heavily used in corporate networks, the IP address can change.
+ The AMD console Windows application requires no login. Participants were concerned that an unauthorized user with access to the console PC could reach managed endpoint files, a serious security vulnerability.

THE FINDINGS

GENERAL IMPRESSIONS 2

The overall impressions collected objectively from test participants of both platforms.

INTEL VPRO WITH INTEL AMT AND INTEL EMA

STRENGTHS

+ Participants experienced that Intel EMA offered greater capability for managing both Intel and AMD machines.
+ Intel AMT technology (found in Intel vPro devices) allowed successful managing of both in-band and out-of-band KVM over Wi-Fi. (Both platforms were manageable over Ethernet.)
+ Participants found Intel EMA could create and run scripts on one or many endpoints, allowing control, customization, automation, and flexibility.
+ Participants felt the availability of endpoint agents offered a more robust and more secure solution.
+ Intel EMA could batch-manage devices and send messages to endpoints.
+ With the Intel vPro platform, CIRA endpoints maintain their own secure connection to the management server, offering better security.
+ Intel EMA can reliably access unattended devices remotely, regardless of their location or state—including via the cloud for kiosks and IoT devices outside of the firewall.
+ Intel AMT provides an API for integration with third-party consoles, large or small, and custom scripts.
+ Documentation within Intel EMA was easy to find and follow.
+ Participants commented that Intel EMA was more polished and more responsive.

WEAKNESSES

+ Participants sometimes needed to access documentation for definitions of values in the Intel AMT tab in Intel EMA because the contextual help, tooltips, and keys in the embedded help were limited.
+ At times the Intel AMT plugin tab in Intel EMA did not load consistently, and participants had to manually refresh.

THE FINDINGS

GENERAL IMPRESSIONS 3

The overall impressions collected objectively from test participants of both platforms.

OPEN STANDARD vs. PROPRIETARY

AMD marketing videos say that AMD PRO is DASH-compliant and imply that Intel is not. However, other manufacturers also follow DASH standards widely and produce compliant chipsets using open standards that work with DASH. So we looked into how the Intel vPro platform compared with AMD PRO in this aspect.

+ AMD crafts a strong message about openness by virtue of building on DASH, describing the purchase of Intel vPro platforms as being "locked in." We learned that Intel vPro technology was actually designed to meet DASH standards. We also found in the DASH specification that it allows for extensions—which Intel has used to add extra functionality.

+ Besides DASH-compatible extensions, Intel further opens up Intel AMT by providing a full SDK for third-party consoles or custom IT apps. We reviewed the SDK documentation and could see that it allows any in-house or third-party developers to use Intel AMT functionality in their software or scripts. The narrow compatibility implied by "locked in" is inaccurate, based on our analysis.

+ Our testers found a significant area where AMD limiting itself to a more minimal DASH implementation also limited IT admins in unfortunate ways: Wi-Fi support. Intel vPro technology gives control over configuration, security, and compatibility with wireless out-of-band connectivity. For a corporate network with large numbers of laptop users, who typically connect only with Wi-Fi, this is an enormous practical advantage for IT admins. The number of laptops is going ever upward—even desktop PCs that use Wi-Fi are expanding.

+ In our testing, both AMD and Intel devices could be managed with Intel EMA. But on the AMD console side, participants could not get the software to display status info other than power state, and the AMD console uses Windows RDP rather than out-of-band management to enable remote desktop capabilities. That limits its availability in troubleshooting situations. The AMD console could do very little with non-AMD devices.

+ Although DASH is a valuable standard and has been around for more than a decade, our IT admins had scarcely even heard of it. By and large they were looking for specific endpoint management capabilities—not adherence to a standard. For that reason, the importance of DASH seems overstated in some of AMD's marketing materials.

AMD PRO WITH DASH vs. INTEL VPRO WITH INTEL AMT AND DASH

	AMD PRO		Intel vPro with Intel AMT	
	Wired	Wireless	Wired	Wireless
Hardware Inventory	✓		✓	✓
User Account Management	✓	✓	✓	✓
Boot Control	✓		✓	✓
Power State Management	✓		✓	✓
Endpoint Redirection	✓		✓	✓
Agent Presence			✓	✓
Remote Configuration			✓	✓
OOB BIOS & Desktop KVM Remote Control	BIOS Only		✓	✓
KVM User Consent (configurable)			✓	✓
Beyond Firewall Secure Cloud Connectivity			✓	✓
Extensibility	Developer Tools & Command Line Only		SDK, Command Line, Multiple Free Tools, Open Source Tools, & Utilities	

DISPELLING THE MYTH

THAT PROPRIETARY SYSTEMS ARE CLOSED AND MORE DIFFICULT TO USE

USER COMMENTS

IN-BAND AND OOB POWER MANAGEMENT

"Obviously, if I had a mixed shop, I would use Intel because I can do WMI [Windows Management Instrumentation] from EMA to both Intel and AMD machines." —IT admin participant

The test findings related to power management showed significant gaps in the capability of the AMD platform. When users viewed power information with the AMD console they could see power status, but it was not always the correct status, unless they drilled into each device or waited a minute or more for system refreshes. Additionally, with the AMD console, participants could see when an endpoint was on or off and could power down (which is an in-band function), but could not power on (an out-of-band function). This suggests potential weaknesses that could increase management costs due to unreachable endpoints.

IN-BAND AND OOB ENDPOINT SYSTEM STATUS

"I prefer this interface [the AMD console], but I would like it to work."

"Intel worked for both; AMD worked for AMD." —IT admin participant

+ Intel EMA performed as expected for in-band and out-of-band management
+ The AMD console could only report power state and power off over Wi-Fi for AMD devices
+ The AMD console could show very little information about connected Intel devices
+ The AMD console could not power on either Intel or AMD devices over Wi-Fi
+ Because participants experienced issues with connectivity, participants had system stability concerns about switching from a wired to a wireless network connection
+ The AMD console labeled endpoints by IP address, not by host name, even though DHCP often changes endpoint IP addresses—making it harder for an IT admin to know which endpoint they were managing at any given time

Participants found that relying on DASH alone as a minimum standard often translated into not being able to do everything required for effective endpoint administration. Our expert review team wondered, "Why not choose a fuller-featured platform that not only offers its own suite of solutions but plays nicely with third-party endpoint management consoles, too?" AMD PRO adhered to DASH standards but didn't offer much beyond that. It's far from the deluxe refrigerator with in-door water, ice and temperature display that it sounded like in promotional materials—after testing, it was just an icebox.

USER COMMENTS

IN-BAND AND OOB KVM

"This is pretty cool." —IT admin participant

"My first thoughts were... I liked AMD's [console] better for its appearance, but EMA with its fast navigation between screens won me over. I don't want to be waiting for more than a few seconds trying to do what I need." —IT admin participant

In this area, Intel EMA performed as described in the documentation. The AMD console performed *mostly* as described in the documentation, except that it had to rely on RDP and other Microsoft capabilities for in-band KVM. The non-Microsoft and out-of-band KVM route was generally displayed as disabled in AMD's software—which unfortunately removes one of the most important labor-saving features of DASH.

IN-BAND AND OOB SECURITY IMPLICATIONS

"AMD needs better security—anyone who has access to the console can open the app and do whatever they want." —IT admin participant

Testing showed that Intel's manageability solution is significantly more secure than AMD's on several points: the Intel vPro architecture uses a combination of endpoint agents, digital certificates, tighter integration between the processor and network controller, optional end-user authentications, and port management to create the most secure solution available. During discovery and provisioning tasks, by its design, AMD left endpoint management ports open and vulnerable to attacks.

To the point, the AMD console requires **no authentication password** to run, allowing anyone with access to a PC running an instance of the AMD console free access to the managed devices and everything on them. Launching the app didn't appear to require two-factor authentication, or even a login.

Intel EMA's endpoint agents provide a more secure solution for these reasons: **1)** When using CIRA on an endpoint, the local management ports remain closed. **2)** The endpoint does not take any action on AMT. It only sends the requests directly from the management server. **3)** All transactions are encrypted.

Concerns also arose during testing regarding the AMD console's ability to securely discover once-known endpoints after they were moved off of the known network (e.g., to access a stolen laptop remotely to wipe the disk, but with AMD that was unlikely to be possible given the requirement the connection be wired).

+ Based on the AMD documentation, it's unclear how HTTP security hardening takes place and in what situations.
+ There are security concerns related to AMD leaving ports vulnerable to hacking during endpoint discovery to provision via DASH.

USER COMMENTS

USABILITY

"I was surprised that the AMD console couldn't even show the power status of their own devices over Wi-Fi." —IT admin participant

Test participants repeatedly found that AMD's manageability solution was unable to support either in-band or out-of-band management over Wi-Fi. This came as a big surprise to IT admins. Modern corporations are heavily reliant on laptops, tablets, and other portable devices that are nearly *always* connected by Wi-Fi—not wired Ethernet dock. AMD requires a laptop be docked with a wired Ethernet connection to be eligible for out-of-band management. We question the assumption that most of a company's laptops would spend most of their time connected to Ethernet. Our test participants confirmed that in their organizations, laptop end users do indeed connect primarily with Wi-Fi.

+ AMD's wireless solution is very limited—it doesn't support wireless, which is a big part of managing today's enterprise networks.
+ By comparison, Intel AMT performed reliably with both in-band and OOBM over Wi-Fi.

WHAT OUR PARTICIPANTS SAID

"I do like that Intel makes it known that someone is connected to the computer [visible KVM indicator on client]. If [AMD] doesn't, that's scary." —IT admin participant

"The [AMD console] GUI, the graphical interface, looks pretty out of date. It looks like this was made in the early 2000s...When I look at this, it looks like it's a legacy product." —IT admin participant

"[With Intel] It was easy to navigate between screens and then still be able to do things effectively in Ethernet and Wi-Fi." —IT admin participant

OOBM COST EQUATION

$25 FOR INTEL VPRO CHIPSET[1]
+ INTEL AMT
+ INTEL EMA
+ KVM OUT-OF-BAND CONTROL OVER WI-FI
– DESKSIDE VISITS

= PRICELESS!

The total cost of ownership of any computer is estimated to be five times the initial cost of the device, calculated in minutes of reactive incident response added to downtime. IT executives tasked with choosing a platform for remote management must consider the needs and characteristics of their networks today, what they'll look like tomorrow, and next year. Most IT admins are already managing networks where 70% of their users are working somewhere remotely at least once a week,[1] 94% are collaborating routinely with others who are not necessarily on the LAN,[2] and 91% of workers believe that the ability to work in flexible locations makes them more productive.[3] Choose an incomplete remote management platform and you risk sending an IT technician out in-person more frequently—and that eats into the bottom line.

The cost of Intel vPro technology per machine is small considering the cost of *not* having more secure manageability and Wi-Fi out-of-band support. At the end of the day, users want the platform with the most capability for their dollars. AMD PRO might appear less expensive up front, but hardware prices do not include the cost of extra deskside visits by IT techs.

RANKED OOB OFFERINGS BASIC CONCEPTS

All either meet or exceed DASH minimums (CIRA does it in a proprietary way).

BEST
Intel vPro/Intel AMT solution using CIRA (Client Initiated Remote Access) is the fullest-feature OOB offering available.

BETTER
Intel vPro/Intel AMT using Admin Control Mode (www.software.intel.com/en-us/amt-developer-guide-basic-concepts).

GOOD
Non-Intel vPro using Intel® Standard Manageablilty.

[1] Personal interview, Dell sales representative, 2019–11–17. Context was volume sales of PCs: "To remove it [Intel vPro] from a quote is a savings of only $25 per system."

[2] "70% of people globally work remotely at least once a week, study says," 2018–05–30, www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html.

[3] "Meeting the Demands of a Mobile Workforce," 2017–07–17, www.cio.com/article/3206277/meeting-the-demands-of-a-mobile-workforce.html.

[4] "The Workspace Revolution: Reaching the Tipping Point," 2018–05, www.contact.regus.com/GBS18_Report_Download_Request.

IN CONCLUSION

MISCONCEPTIONS ABOUT THE DIFFERENCES BETWEEN AMD PRO AND INTEL VPRO PLATFORMS COULD HARM IT DEPARTMENTS LOOKING FOR HIGH SECURITY, HIGH FLEXIBILITY, AND LOW OVERALL COSTS WHEN MANAGING THEIR ENDPOINTS.

The IT professionals that worked with us in this study told us they want a platform with robust remote manageability and reliable, easy-to-configure hardware and firmware. That platform should offer its own console application for convenience but also play nice with third-party solutions. These professionals did not consider DASH conformance important. Full management over Wi-Fi they considered an obvious advantage. IT executives everywhere are facing a critical need for solutions that can help them keep their fleets updated, secure, and running, no matter whether they connect by LAN or Wi-Fi, whether local, or a continent away. That's what IT pros said they want.

The solution our test participants declared more consistent, with better overall performance, and with much broader capability was Intel vPro.

Reviewing the data from our study, here's what we learned, in a nutshell:

+ AMD implies that the Intel vPro platform doesn't have DASH capabilities, but it didn't take much testing for our participants to conclude that the Intel vPro platform does indeed have those capabilities.
+ Modern companies have huge numbers of laptops that use Wi-Fi. With the AMD solution, they'd get no out-of-band support unless connected to Ethernet. How many of your company's laptops are typically connected to Ethernet? Wi-Fi out-of-band support isn't a DASH requirement, but the Intel vPro platform has done the work of enabling it.
+ AMD's description of the Intel vPro platform as "proprietary" neglects an uncomfortable truth. Any improvement a company provides beyond a public standard is proprietary, in a sense. The purpose of a standard is to offer a *minimum* baseline, not to stifle innovation and improvement. We found that Intel vPro technology starts with lowest-common-denominator DASH capabilities, fills in missing basics (like out-of-band management over Wi-Fi and better security), and then provides extras that allow IT admins to solve problems better.
+ The Intel vPro platform offers an API and SDK so developers of management consoles and in-house tools can access the features of Intel AMT. As a result, we found many more management consoles that use Intel AMT's out-of-band features than AMD's out-of-band features.
+ The small premium it costs per device to get Intel vPro technology is more than made up for by savings in IT technician hours because they don't have to make so many deskside visits. And if going with the Intel vPro platform's more robust security architecture saves even one information breach, that savings becomes exponentially greater.

Our investigation found that the Intel vPro platform and functionality not only met the bar for DASH standards but went beyond it in practical features, openness via API, security, and savings in total cost of ownership. The conclusion we came to at the end of all our research was a simple summary: **when it comes to out-of-band management, more is more.**

GLOSSARY OF TERMS

CIRA
Client Initiated Remote Access
Feature of Intel AMT that makes the managed device responsible for staying connected to the management server after initial configuration. This removes a significant security vulnerability by making it unnecessary for the client to leave management ports open all the time.

DASH
Desktop and Mobile Architecture for System Hardware
Standard that defines a set of interoperability industry protocols for managing, monitoring, and controlling PCs regardless of system power state (on, off, standby) or operating system capability. DASH uses standards-based management technologies for management and monitoring of desktop and notebook systems.

DHCP
Dynamic Host Configuration Protocol
Common protocol for a router to assign an IP address dynamically (typically on startup) to an endpoint on the network.

DMTF
Distributed Management Task Force
Former name of the DMTF standards organization (now a four-letter name, not an acronym) that develops open standards for managing various types of IT infrastructure. The DMTF created the DASH standard, for example.

Intel® AMT
Intel® Active Management Technology
Technology built into the chipset of Intel vPro devices, allowing secure out-of-band management of those devices independent of the state of the operating system, allowing such uses as KVM control during the boot process and startup of a powered-off endpoint over Wi-Fi.

Intel® EMA
Intel® Endpoint Management Assistant
Cloud-based device management application that performs in-band (via an agent program) and out-of-band operations (via Intel AMT) on endpoints in a corporate network.

In-Band Management
Commands for management operations such as disk access, powering off, KVM, and system status that can only happen through the operating system, i.e., not when the system is shut down or the OS won't start up.

ISM
Intel® Standard Manageability
Manageability solution for Intel PCs without Intel vPro technology. It enables some out-of-band features but doesn't support other useful functions such as KVM.

OEM
Original Equipment Manufacturer
A company that makes devices from component parts bought from other suppliers, and in our context, refers to a computer maker like HP, Lenovo, Dell, etc.

OOBM
Out-of-Band Management
In the world of endpoints (it has a slightly different meaning for networking equipment), commands for operations such as disk access, powering on or off, KVM, and system status without reliance on the operating system. This requires hardware support in the chipset and compatible communication protocols.

SDK
Software Development Kit
Set of tools, libraries, APIs (application programming interfaces), and documentation to enable a developer to access software capabilities that would otherwise have to be written from scratch.

TLS
Transport Layer Security
Encrypted protocol used by client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.

WMI
Windows Management Instrumentation
The infrastructure for management data and operations on Windows-based operating systems. You can write WMI scripts or applications to automate administrative tasks on remote computers, but WMI also supplies management data to other parts of the operating system and products.

The power of insight.

concreteUX.com

LinkedIn.com/company/concreteUX
Instagram.com/concreteUX

2189 NW Wilson Street Portland, OR 97210

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