

INTEL® vPRO ENTERPRISE

Out-of-band Management Capabilities & Performance

We tested Intel Active Management technology to see if it surpasses the DASH standard. Here are the results.

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



An obvious need for out-of-band management

IT STAFF NEEDS FULL REMOTE ACCESS TO ENDPOINTS, REGARDLESS OF THEIR STATE

Working remotely from home isn't going anywhere anytime soon. In fact, [an AT&T study](#)¹ looking at the future of corporate work predicts that the hybrid work model will grow from 42% in 2021 to 81% in 2024. And a June 2022 [Gallup survey](#)² found that 8 in 10 remote-capable employees already work from their home office either part or full time. In fact, every employee with a laptop PC is a remote worker in some sense, and those numbers are rising. The days of employee devices staying solely within the purview of an organization's LAN will soon be a distant memory.

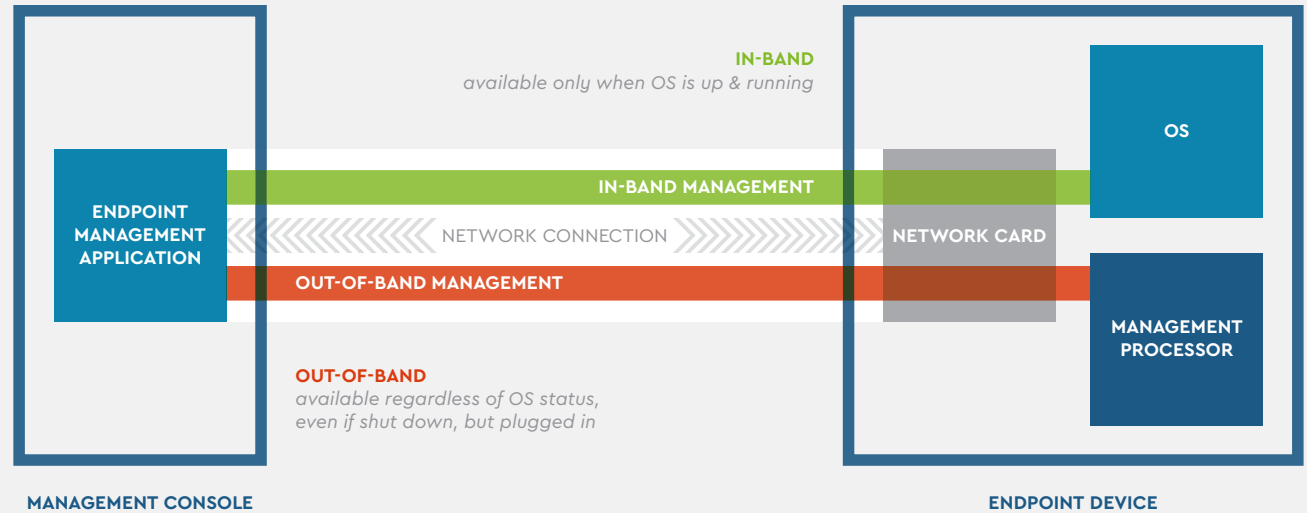
But the more freedom employees demand with their work and their devices, the more flexible their organizations' networks will have to become. Users need reliable access to the data and tools necessary to perform their responsibilities and contribute to overall productivity. Users' devices—company owned as well as BYOD—must be managed remotely to ensure security, restore uptime quickly in the event of an outage, and better allocate IT staff and resources. That's where out-of-band-management comes into play.

8 IN 10
Remote-capable employees

already work from their home office either part or full time

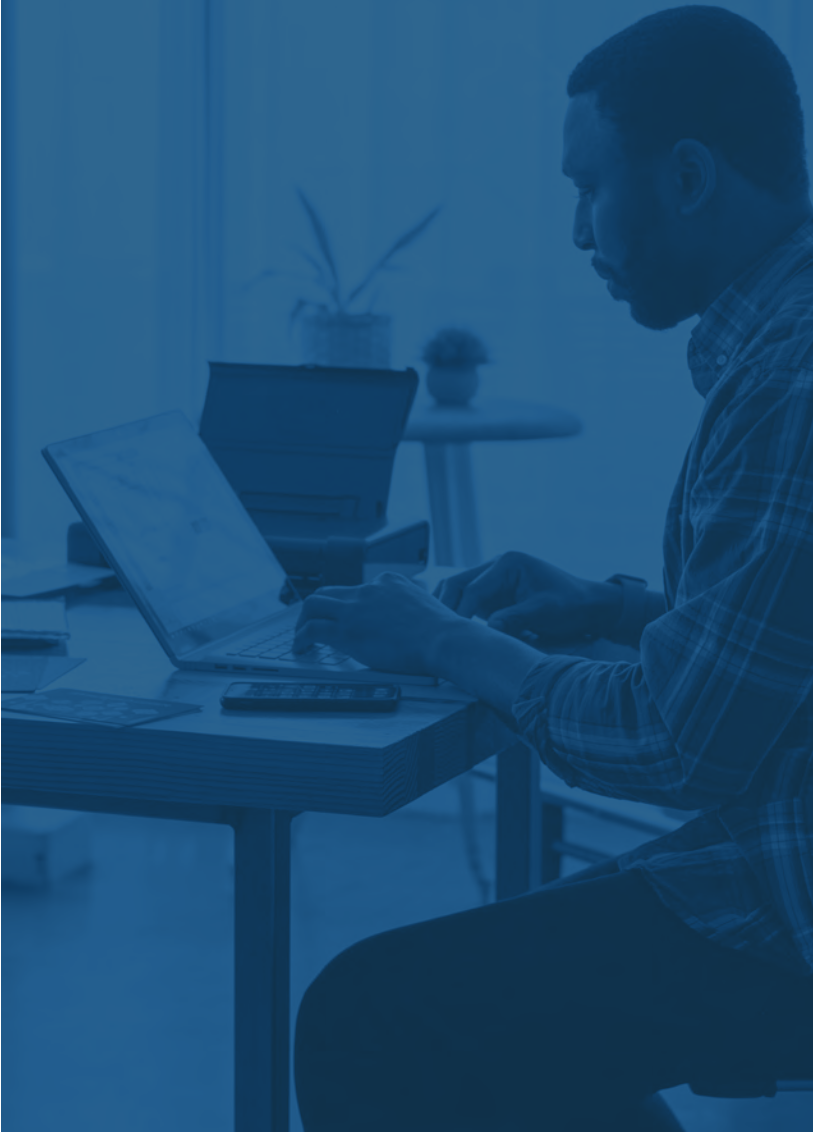
What is out-of-band management?

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



Out-of-band (OOB) management is a method of remotely controlling and managing devices using a secure protocol connection through a secondary interface that is physically separate from the primary network connection. OOB management requires specially designed hardware and firmware that enables IT staff to monitor and control devices, regardless of the OS status and often the devices' power state. More comprehensive OOB management platforms also allow IT staff to detect, monitor, and control devices regardless of connectivity type (i.e., Ethernet or Wi-Fi). In the world of remote work, OOB management is crucial.

The benefits of OOB



BUSINESS IMPACT

For an organization to realize the value of OOB management, its network endpoints, IoT devices, and network components need the software, hardware, and firmware that make OOB access possible. The organization must also configure the endpoint management solutions and endpoints correctly.

If all the prerequisites for OOB management are met, IT staff can then use it to more quickly resolve endpoint issues so that employees sidelined by an IT issue can get back to work faster and resume their focus on important tasks. It also enables more IT issues to quickly be resolved remotely, freeing up IT resources to focus on other priorities.

IT IMPACT

With OOB management, an IT staff can remotely access an endpoint that needs attention. This remote accessibility, regardless of a device's power state or OS status, translates into a more responsive IT staff that can close more tickets in a shorter span of time, respond faster to employee needs, reduced IT operations costs and create more value for the business.

IT staff can also push updates across the network and shut down security threats much more rapidly. For example, IT staff can patch a critical vulnerability on every device in their environment simultaneously, even those shut down for the night.

Today, IT staff have their pick of solutions that provide remote monitoring and management functionality. But many of these solutions only allow for remote access and control of desktops, servers, and mobile devices that are in-band (powered up with the OS running) on their organization's enterprise network. The ability to manage OOB devices requires a technology stack consisting of hardware, firmware, and software that together allow IT staff to interact with an endpoint when that endpoint's OS isn't functioning. The Intel® vPro Enterprise platform is one such technology stack.

The Intel vPro Enterprise platform



The Intel vPro Enterprise platform is a set of hardware and firmware that resides within a PC's chipset and CPU.

Specific to OOB management, Intel® Active Management Technology (Intel® AMT) is the hardware-based component of the Intel vPro **Enterprise** platform that allows IT to remotely manage employee devices even when those devices are powered off or outside the company's network. A connection between employee devices and the organization's management server is established and maintained through either Transport Layer Security (TLS) encryption or an AMT feature known as Client Initiated Remote Access (CIRA). With Intel AMT, in theory, IT could update or remediate devices no matter where they are, given they have some form of internet connection.

There are many ways for IT to take advantage of AMT, including the Intel® Endpoint Management Assistant (Intel® EMA), which is a free management console and enabling software; MeshCommander, which is a set of open-source tools; and APIs that allow seamless integration with common Remote Monitoring and Management (RMM) solutions.

But is using Intel vPro Enterprise for OOB management beneficial to organizations and IT admins?

Putting the Intel vPro Enterprise platform to the test

Intel makes several claims about the OOB management functionality and capabilities of its vPro Enterprise platform. The company asked us to put those claims to the test.

As a third-party research consultancy firm, we gather evidence, find insights, and study user experiences to help companies like Intel create intelligent and highly beneficial solutions for their clients and their clients' end-users. To test the OOB management performance of the vPro Enterprise platform, we relied on our years of consultation experience and input from industry experts to set up and conduct an experiment in an isolated test lab environment. However, before we get into the specifics of the test itself, it's necessary to discuss a topic central to all of Intel's vPro manageability claims. It's something known as the DASH standard.

What is the DASH standard?

The DASH standard defines a common framework for managing systems that aren't currently available over an organization's network. Whether a system is powered off, in a remote location, or off the network entirely, IT admins can use DASH-compliant products to manage that system below the OS. Device manufacturers can implement DASH standards without having to develop their own proprietary OOB management solutions. And because DASH is open source, it's free to use and modify. This is a major reason why so many manufacturers support it, and why it's likely to be compatible with a wide range of devices. It's also well documented, making it easy for IT admins to learn.

Where did the DASH standard originate?

The Distributed Management Task Force (DMTF), an international nonprofit organization that develops and publishes industry standards for enterprise systems management, established DASH. Intel was a founding member of the DMTF in 1992 and remains on the board to this day.

Intel® Active Management Technology (Intel® AMT)

DASH Compliance

Hardware Inventory

Robust Power State Management

Robust Endpoint Redirection

Robust Extensibility

Robust OOB KVM to BIOS or Desktop

Robust Security

Beyond Firewall Secure Cloud Connectivity

Configurable User Consent

OOB Wi-Fi Capability

DASH Standard

DMTF Defines DASH Standard

Partial



Intel claims its vPro platform builds on the DASH foundation

According to Intel, its Intel vPro Enterprise platform not only fully adheres to the DASH standard but builds on it with a more robust feature set and secure device management. For our test, we set out to confirm or invalidate the following key claims:

CLAIM #1

Intel vPro Enterprise enables OOB management over a Wi-Fi or wired connection

Intel claims that Intel AMT makes it possible to remotely access OOB devices via a management console over a Wi-Fi or wired connection.

CLAIM #2

Intel vPro Enterprise provides a secure connection between server and device

Intel also claims that AMT's CIRA feature keeps a device connected to the management server after initial configuration, eliminating the need to keep management ports open all the time. If true, this eliminates an entire avenue for cyberattacks to exploit.

CLAIM #3

IT staff can take remote keyboard, video, and mouse (KVM) control of an endpoint, even if the endpoint's OS is down

Intel's marketing claims that IT staff can use the vPro Enterprise platform to both remotely access and take KVM control of a device, regardless of whether the device is turned off and/or the OS isn't functioning.

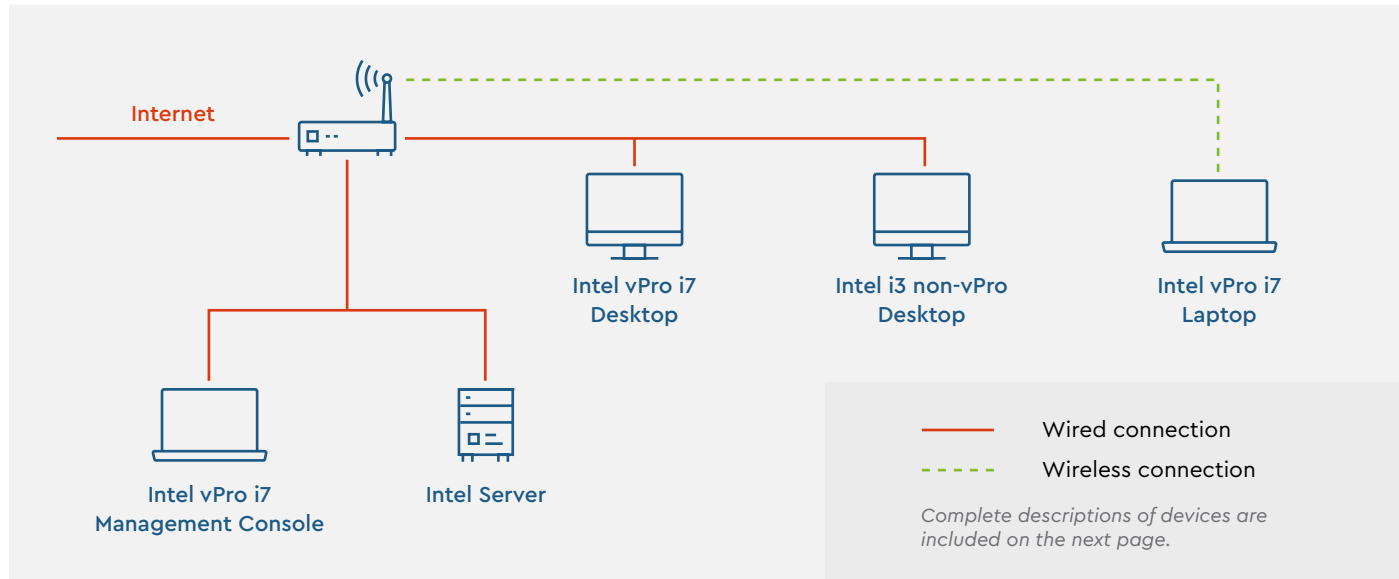
CLAIM #4

Remote PC management keeps devices secure and functioning optimally

Intel's marketing claims that OOB gives IT staff a way to ensure devices have up-to-date operating systems (OS) and antivirus and malware-scanning software. Off-hours patching helps minimize the impact of updates on productivity.

TEST ENVIRONMENT AND DESIGN

It's common for IT to conduct early tests to show a technology's viability as a product or service. We designed our test and lab environment to model how these testbeds are typically set up and conducted.



Network

We configured an isolated network that connected a management console and a server to two Intel vPro Enterprise 12th generation endpoints and one non-vPro 12th generation endpoint via a router.

Managed endpoints

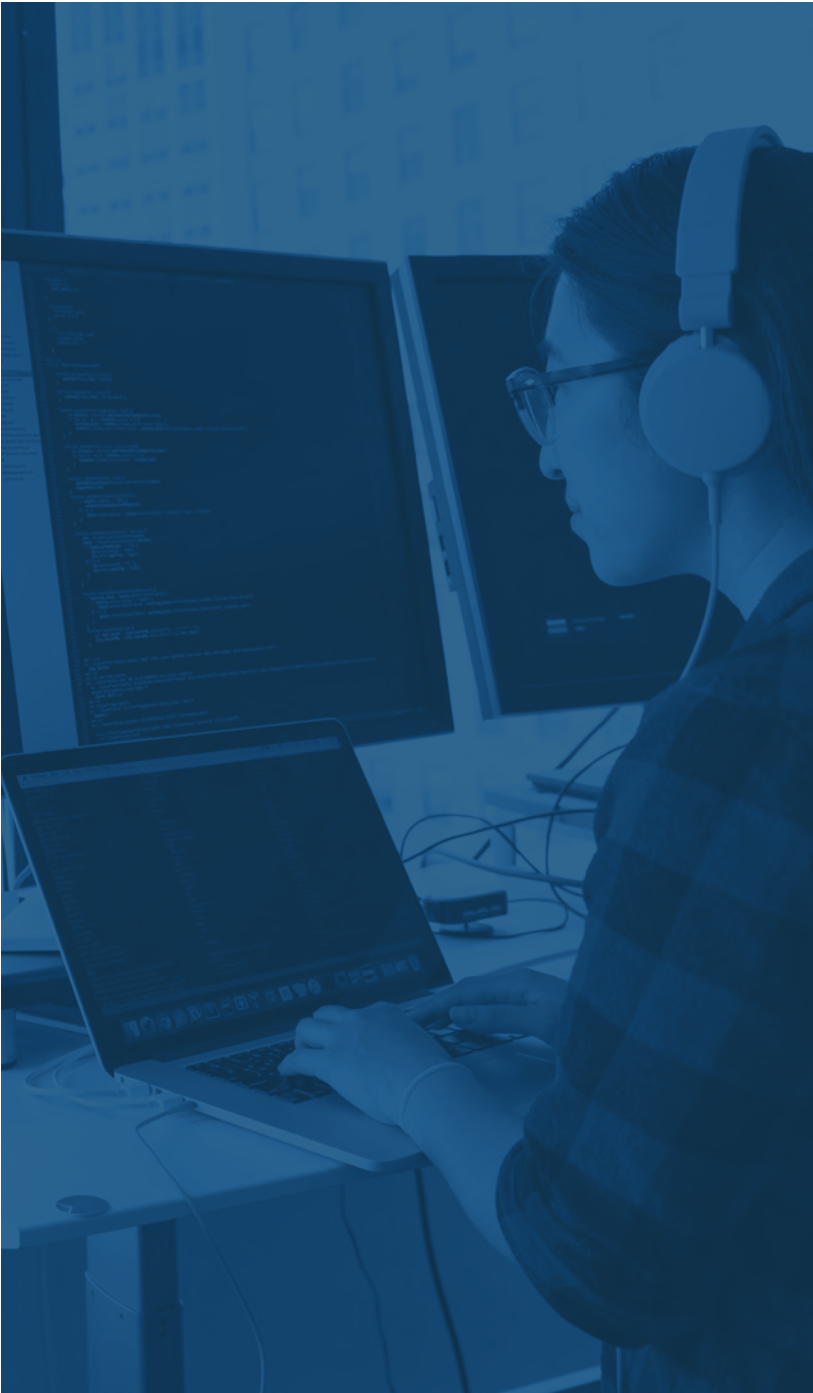
All three PCs were from the same manufacturer and were marketed as enterprise devices and fully supported OOB. They were factory reset to the most current firmware, software, and drivers. Two of the PCs were desktop models and were connected to the router via Ethernet cables. The third PC was a notebook model and had a wireless connection to the router. Additionally, one of the two desktops was a non-vPro device, meaning it lacked vPro Enterprise capabilities. This allowed us to test both CIRA and TLS deployments.

Since the PC notebook and one of the PC desktops were vPro devices, they were configured to use CIRA to communicate over the network. The non-vPro desktop used transport layer security (TLS) encryption.

All components



DEVICE	ROLE	NETWORK CONNECTION
Samsung Galaxy Book Pro 2 <ul style="list-style-type: none">Intel i7-1260P16 GB ramWindows 11 ProGoogle Chrome (for Intel EMA)	<ul style="list-style-type: none">IT management console	Ethernet
Intel 8i7HVK NUC <ul style="list-style-type: none">Intel i7-8809G8 GB ramWindows Server 2019SQL Server Express	<ul style="list-style-type: none">DNS serverIIS baselineEMA server (including bundled modules)	Ethernet/Wireless
HP Elite Mini 800 G9 Desktop <ul style="list-style-type: none">Intel Core i7-12700T16 GB ramWindows 11 ProEMA agent (CIRA)	<ul style="list-style-type: none">vPro-enabled managed endpoint	Ethernet
HP Slim Desktop 501-PF2 <ul style="list-style-type: none">Intel i3-121008 GB ramWindows 11 ProEMA agent (TLS)	<ul style="list-style-type: none">Non-vPro managed endpoint	Ethernet
HP EliteBook 830 Notebook <ul style="list-style-type: none">Intel i7-1265U16 GB ramWindows 11 ProEMA agent (CIRA)	<ul style="list-style-type: none">vPro-enabled managed endpoint	Wireless



CONDUCTING THE TEST

Two IT professionals were asked to conduct the test following a series of predetermined tasks. One is an IT technician, and the other is a managed services provider. A human factors expert was consulted on the test's design and was present during the testing session. The three professionals have over 70 years of combined IT and UX experience.

After the participants installed and configured EMA on the server and finished setting up the network, they installed the EMA on the IT management console and configured an EMA agent on the three endpoints. The experts then attempted the following tasks using the EMA management console to test AMT OOB capabilities.

TASK #	DESCRIPTION	RESULT (✓/×)
1	Confirm management console can access all three endpoints	✓
2	Power off and on wired endpoints over Ethernet	✓
3	Power off and on wireless endpoint over Wi-Fi	✓
4	Use KVM to take control of wired endpoints over Ethernet	✓
5	Use KVM to take control wireless endpoint over Wi-Fi	✓
6	Access terminal, files, processes, and WMI of all three endpoints	✓



HOW INTEL'S CLAIMS MEASURE UP TO OUR RESULTS?

CLAIM #1



Intel vPro Enterprise enables OOB management over a Wi-Fi or wired connection

The participants successfully accessed and controlled the extended capabilities available through CIRA with the vPro desktop over Ethernet and the vPro laptop over Wi-Fi. The participants were able to access and power down the non-vPro desktop using TLS over Ethernet as well, demonstrating that an IT admin can remotely manage devices and take KVM control of PCs regardless of connection type (Ethernet or Wi-Fi), power status (off or on), or vPro compatibility.

CLAIM #3



IT staff can take remote keyboard, video, and mouse (KVM) control of an endpoint, even if the endpoint's OS is down

After the participants demonstrated they could power on and off the endpoints, they successfully took KVM control of each one.

CLAIM #2



Intel vPro Enterprise provides a secure connection between server and device

CIRA endpoints maintained their own secure connection to the management server. And because the local management ports remained closed, the vPro-enabled PCs did have a more secure connection than required for DASH compliance.

CLAIM #4



Remote PC management keeps devices secure and functioning optimally

The participants demonstrated they could successfully remotely access files and processes in-band, remotely terminate or launch a process, and run Windows Management Instrumentation (WMI) actions.

Summary and takeaways

During and after testing, the experts made the following observations.

Based on lab results, all three instances either met or exceeded DASH minimums. However, the Intel vPro Enterprise platform using CIRA provided the broadest and deepest OOB management functionality.

The experts were able to control power state and gain KVM control, they successfully demonstrated in-band and out-of-band remote terminal functionality, in-band remote file browsing, in-band remote process management, and run a Windows Management Instrumentation (WMI) action.

They noted that EMA could allow for the installation of further management tools, in situations where proper onboarding was not met, and you need to be able to manage endpoints on the fly. And, while configuration of CIRA was not difficult, IT should take the time to understand exactly what kind of functionality they need prior to configuring it. Otherwise, they risk leaving out a key feature they'll need later down the road—and may only realize the feature is missing at a time when it's needed.

"The fact that EMA is database-driven means it is easy to migrate if needed or to scale to multiple sites."

—Managed Services Expert

"The documentation is both easily accessible and verbose, which results in a fast setup and fast troubleshooting."

—Human Factors Expert

"It was easy to navigate between screens and then still be able to do things effectively in Ethernet and Wi-Fi."

—Managed Services Expert

"I do like that Intel makes it known that someone is connected to the computer [with a visible KVM indicator on client]."

—IT Security Expert

Conclusion



The Intel vPro Enterprise platform does indeed go above and beyond the DASH standard to provide more OOB management capability and flexibility. While this added functionality is reflected in a higher price point than alternative solutions that do the bare minimum to meet DASH compliance, organizations implementing Intel vPro Enterprise can see a fast ROI. After all, the more functionality IT admins have in their OOB management platform, the less likely they are to travel to access a device in person. And in our increasingly hybrid world, IT staff could rack up those travel miles in no time at all.

IT staff can proactively push updates across the network and shut down security threats more rapidly. They can also become far more efficient at resolving and closing IT service tickets. So, not only are employees free from having to physically walk to an IT service counter or wait for an IT technician to arrive at their doorstep, but they can also simply put in a ticket to a more attentive IT staff. As a result, employee downtime is reduced and negative impact on productivity is minimized.

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

Intel vPro® Essentials using Intel® Standard Manageability.

NOTICES AND DISCLAIMERS: All product descriptions, dates and figures provided are preliminary, based on current expectations, and subject to change without notice.

Intel technologies may require enabled hardware, software or service activation.

Built into the hardware, Intel® Thread Director is provided only in performance hybrid architecture configurations of 12th Gen or newer Intel® Core™ processors; OS enablement is required. Available features and functionality vary by OS.

Performance hybrid architecture combines two core microarchitectures, Performance-cores (P-cores) and Efficient-cores (E-cores), on a single processor die first introduced on 12th Gen Intel Core processors. Select 12th and 13th Gen Intel Core processors do not have performance hybrid architecture, only P-cores, and have same cache size as prior generation; see ark.intel.com for sku details.

All versions of the Intel vPro® platform require an eligible Intel processor, a supported operating system, Intel LAN and/or WLAN silicon, firmware enhancements, and other hardware and software necessary to deliver the manageability use cases, security features, system performance, and stability that define the platform.

See www.intel.com/Performance-vPro for details.

No product or component can be absolutely secure. Learn more at www.intel.com/PerformanceIndex (Security & Manageability).

Your costs and results may vary.

Intel is committed to the continued development of its renewable, sustainable, and green networks, as we strive to prioritize greenhouse gas reduction. Refer to Intel Corporate Responsibility Report 2021-2022 or visit www.intel.com/2030goals for further information.

"Conflict-free" refers to products, suppliers, supply chains, smelters, and refiners that, based on our due diligence, do not contain or source tantalum, tin, tungsten or gold (referred to as "conflict minerals" by the U.S. Securities and Exchange Commission) that directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo or adjoining countries.

© Intel Corporation. Intel, the Intel logo, Intel vPro and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

Glossary

BYOD

Bring your own device

The practice of employees using personal devices to access their company's data and business applications for work purposes. BYOD policies govern what apps and data an employee can access via their personal device and enforce the necessary security measures (e.g., two-factor authentication).

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.

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.

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.

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 Assistance

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.

OOB Management

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.

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.

Footnotes (from page 2):

¹ Pereira, K. (2022, February 25). Is corporate America ready for The Future of Work?. AT&T Business.

<https://www.business.att.com/learn/research-reports/is-corporate-america-ready-for-the-future-of-work.html>

² Wigert, B., & Agrawal, S. (2022, August 31). Returning to the Office: The Current, Preferred and Future State of Remote Work.

Gallup.com. <https://www.gallup.com/workplace/397751/returning-office-current-preferred-future-state-remote-work.aspx>



The power of insight.

concreteUX.com

[LinkedIn.com/company/concreteUX](https://www.linkedin.com/company/concreteUX)

[Instagram.com/concreteUX](https://www.instagram.com/concreteUX)

© 2023 Concrete

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

WARRANTY DISCLAIMER CONCRETE, LLC ("CONCRETE") HAS EXERCISED COMMERCIALY REASONABLE EFFORTS TO ENSURE THE ACCURACY AND VALIDITY OF ITS TESTING AND THE RESULTS OF THIS PAPER; HOWEVER, CONCRETE SPECIFICALLY DISCLAIMS ANY WARRANTY, EXPRESSED OR IMPLIED, RELATING TO THE TEST RESULTS, METHODOLOGY AND ANALYSIS, INCLUDING WITHOUT LIMITATION THEIR ACCURACY, COMPLETENESS OR QUALITY AND INCLUDING ANY IMPLIED WARRANTY OF FITNESS FOR ANY PARTICULAR PURPOSE. RELIANCE ON THE RESULTS OF ANY TESTING WILL BE AT YOUR OWN RISK. YOU AGREE THAT CONCRETE, ITS AFFILIATES, AND THEIR EMPLOYEES AND SUBCONTRACTORS SHALL HAVE NO LIABILITY FROM ANY CLAIM OF LOSS OR DAMAGE ON ACCOUNT OF ANY ALLEGED ERROR OR DEFECT IN THIS PAPER, OR ANY TESTING PROCEDURE, METHODOLOGY, ANALYSIS, OR RESULT.

LIMITATION OF LIABILITY AND DAMAGES IN NO EVENT SHALL CONCRETE BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THIS PAPER, THE RESULTS OR ANALYSIS HEREIN, OR CONCRETE'S TESTING METHODOLOGY OR RESULTS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND BY READING THIS PAPER YOU HEREBY RELEASE CONCRETE FROM ANY SUCH DAMAGES RELATED THERETO.