Support Hybrid Work from the Cloud with Remote Manageability and Endpoint Security

Manage your business desktop and laptop devices from the cloud with Intel vPro® technology.

intel®

Glossary of terms

DASH: Desktop and mobile Architecture for System Hardware (DASH) standards set by the Distributed Management Task Force (DMTF) standards organization.

Intel® Active Management Technology (Intel® AMT): Hardware and firmware that allows remote management and persistent out-of-band connectivity that operates below the operating system (OS).

Intel® Endpoint Management Assistant (Intel® EMA): Software that modernizes Intel AMT with cloud-based functionality. Enables both in-band and out-of-band connectivity to PCs.

Intel® Remote Secure Erase (Intel® RSE): A feature that allows IT admins to wipe the drive of a client device from the Intel EMA management console.

KVM: Keyboard/video/mouse.

Out-of-band management (OOB): Refers to management technology that interacts with an endpoint directly on the hardware layer, below the OS. Such technology can power on or otherwise interact with endpoints, even when the OS on those endpoints is not functioning.

Table of Contents

Introduction

Nearly every industry today is considering how to transition to a hybrid workplace. The hybrid workplace is one in which some employees work in-office, some work from home or co-working spaces, some visit customer sites, and some mix any of these scenarios throughout the day or week. Hybrid work is only going to increase: by 2025, an estimated 70 percent of the workforce will be working remotely at least five days per month.[1]

Technology plays a prominent role in the success of hybrid work. It allows employees to stay at a high level of productivity while giving them the flexibility to work anywhere, increasing job satisfaction and employee retention. Remote-management solutions are available, but some provide more capabilities than others to address the challenges of the new workplace paradigm.

For IT, the new workplace paradigm presents many challenges:

- **Incredibly dispersed infrastructures**. In large enterprises, IT might manage thousands of client devices worldwide.
- **Broadened attack surfaces**. The Federal Bureau of Investigation (FBI) reported that in April 2020, when many employees were working from home, it received between 3,000 and 4,000 cybersecurity complaints each day, a major jump from 1,000 per day pre-pandemic.[2]
- **Stretched IT resources.** As more employees work outside the corporate firewall or access applications via the cloud, IT must work remotely to manage troubleshooting, device lifecycle management, and security requirements.

IT administrators need cloud-based management capabilities to address real-world scenarios for today's hybrid work, such as:

- Connecting to malfunctioning devices outside the firewall to see what remote workers are experiencing
- Updating the operating systems on devices or power cycling a system when it is no longer responding
- Installing software, upgrading security, releasing patches, and troubleshooting problems over a wired or Wi-Fi connection

Table of Contents

Intel vPro platform: Enabling IT for modern manageability

The Intel vPro platform provides the cloud-based manageability and security capabilities needed for client devices in a diverse range of locations. IT can remotely manage these clients, help secure data, and enhance productivity to enable the hybrid workplace. And the good news is that many businesses are already using devices with Intel vPro technology, and they can take advantage of the other technologies inside.

This e-book examines how modern endpoint management from the Intel vPro platform lets IT manage devices everywhere, both in-band and out-of-band from the cloud.

An out-of-band endpoint-management technology stack

The Intel vPro platform, which spans Intel® Core™ vPro® processors and Intel® Xeon® Scalable processors (on workstation functionality), includes Intel® Active Management Technology (Intel AMT) and Intel Endpoint Management Assistant (Intel EMA).

- Intel AMT is a set of hardware and firmware technologies that can be configured on Intel vPro platform–based devices to allow "out-of-band" management. This means remote management regardless of power state or whether an operating system (OS) is functioning.
- Intel EMA is a downloadable software application that modernizes Intel AMT with cloud-based functionality. IT administrators interested in managing devices remotely from a cloud-based environment can do so within the Intel EMA portal. Intel EMA enables an easy process to configure Intel AMT on remote devices.

Intel AMT is the only solution with remote remediation to return your PCs to a known good state, no matter where your employees are working—even when the OS is down.[3,4]

Table of Contents

Transition to hybrid work with Intel vPro technology

With Intel vPro technology, IT can be both proactive and reactive at the same time to save time and costs in the hybrid workplace. Through Intel AMT and Intel EMA, IT can manage devices from the cloud throughout device lifecycles by updating software and security patches while also troubleshooting problems and making repairs.

Common hybrid work use cases for Intel vPro technology include:

- Service desk function
- Incident management
- Hardware upgrade/software release and deployment management
- Lifecycle management
- User-less device management (for example, kiosks and digital signage)

The next sections discuss how Intel AMT and Intel EMA help IT accomplish proactive and reactive tasks in the hybrid workplace.

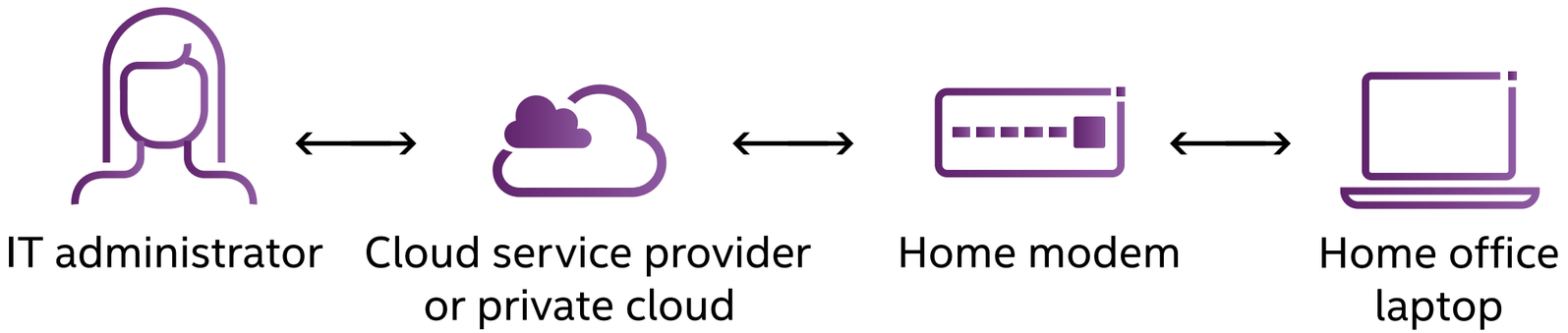

Figure 1. IT can manage a remote device from the cloud with Intel vPro technology; here is a typical workflow when managing a device used by an employee working from home

Table of Contents

Proactive management from the cloud

With Intel AMT and Intel EMA, IT can reach out to devices and install software or patch the devices remotely, erase disks, reimage disks, and reboot remote devices—everything they could do as if they were physically there, next to the device, all from the cloud. Managed devices can reside in the public or private cloud, and the console can reside in a public or private cloud or at the edge.

Installing software

IT can install third-party software applications on remote devices using Intel EMA and their preferred software-distribution method.

Organizations no longer need someone onsite to manually turn on a device. With power-on capabilities, IT can install software quickly, and it can then put the system back to sleep or power it off, reducing or eliminating employee downtime.

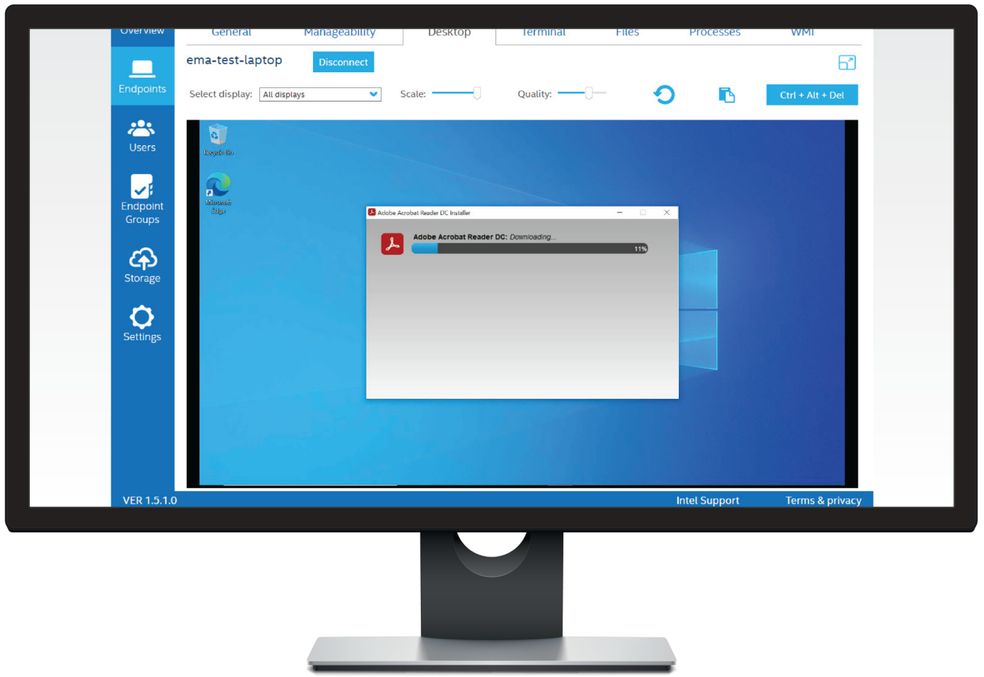

Figure 2. IT can install an application remotely using Intel EMA when logged in as a local administrator

Table of Contents

Routine software patches

IT can schedule endpoints to power up during off hours, allowing existing tools to deploy patches and updates so that business continuity and employee productivity are not affected. IT can power systems up for diagnostics and overnight patch deployment, and it can then power down when not in use to help improve security and help reduce energy spend. This helps IT quickly update security software for all endpoints at one time, before users even realize there's a problem, which can help keep data safe and the business running smoothly. Security updates can be made even with clients outside the firewall, helping to stop threats in their tracks before breaches can occur.

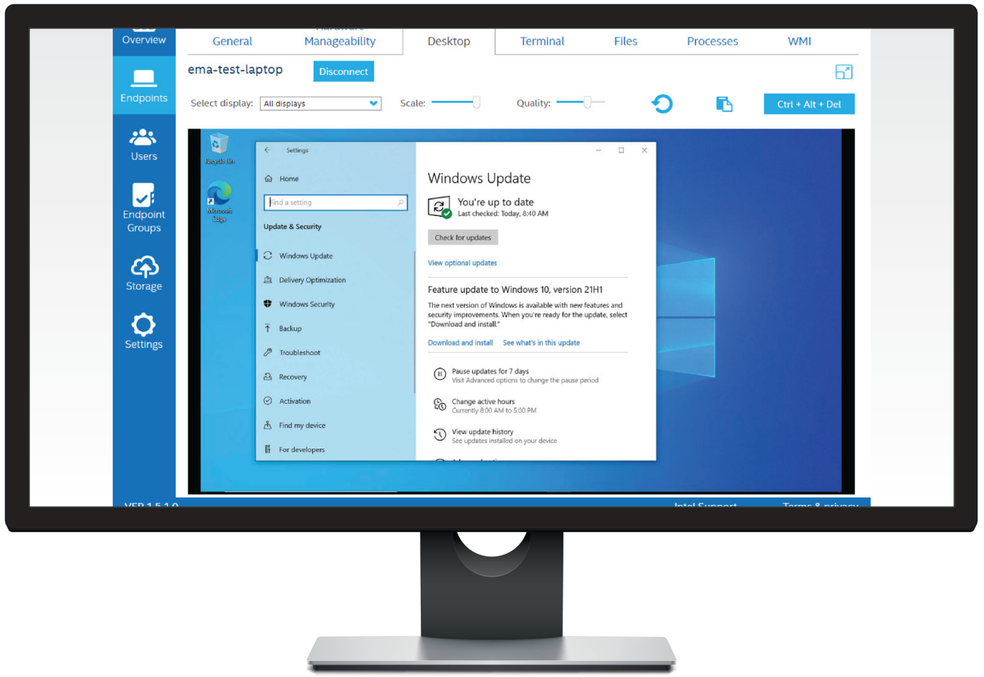

Figure 3. IT can use Intel EMA with software patching tools to help ensure that security updates are current on devices outside the corporate firewall

Table of Contents

Intel Remote Secure Erase

When a PC is retired, repurposed, returned for repair, or lost, information security policies often require data to be “wiped” from the drive. Wiping can be difficult and time-consuming when working onsite, but nearly impossible when remote. The Intel Remote Secure Erase (Intel RSE) option, supported only by Intel solid state drives (SSDs), offers a convenient solution and is available through Intel AMT.[5]

How **Intel RSE** works

Two-step administrative process:	
1	Select target system(s).
2	Send **remote secure erase** command.

What happens behind the scenes:	
•	Intel EMA locates target systems over the Internet/intranet.
•	A WS-Management command is sent to initiate Intel RSE on the next boot.
•	The command is received by Intel AMT on an Intel vPro platform–based system.
•	Secure erase is initiated on the SSDs. Data is erased, and the encryption key is deleted.
•	Intel EMA polls for updates throughout the process.
•	The BIOS reports back to Intel AMT, which clears the Intel RSE trigger and reports the results to the Intel AMT audit log.
•	Intel AMT reports completion to the remote console.
•	The console can initiate a remote shutdown.

Figure 4. Intel RSE allows IT to remotely erase disks with a streamlined, automated process

Table of Contents

Remote reboot

Remote reboot lets IT administrators restart a machine with a non-working OS, much like hard-resetting via the device power button.

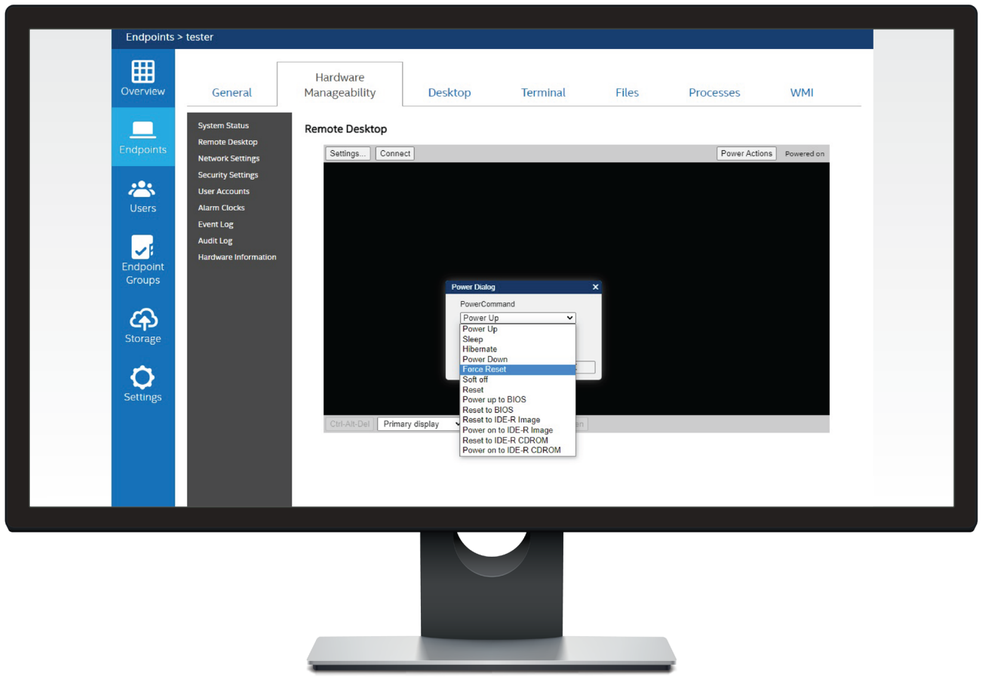

Figure 5. If a device is not turning on due to a non-working OS, IT can remotely restart it

Table of Contents

Reactive management from the cloud

With Intel AMT and Intel EMA, IT can see exactly what's happening on a device when unpredictable problems arise. A key part of this capability is the powerful hardware-level remote control feature on Intel AMT. Using keyboard, video, and mouse (KVM), IT can connect to a remote device and view what's happening on the client desktop as if physically there, even when the device is on the worker's home Wi-Fi or on a known Wi-Fi network.

Troubleshooting

The ability to view what's happening in real time is possible independent of whether the OS is operating, and the KVM session can be maintained even during reboots and when working inside the BIOS.

Because Intel AMT and Intel EMA work together to operate independently of the OS, repairs can be made on a wider range of issues, including:

- Corrupted drivers
- Application software
- Non-responsive systems that won't boot

Boot redirection

As mentioned earlier, KVM sessions are persistent. IT can view computer reboots as they are happening, or it can boot into another OS with virtual disks mounted onto the system remotely. Boot redirection puts an otherwise inoperable PC into a temporary work environment. This is useful, for example, in the case of a failed hard drive. While waiting for a new hard drive to be delivered, an employee can continue to work and access web-based e-mail and Internet services.

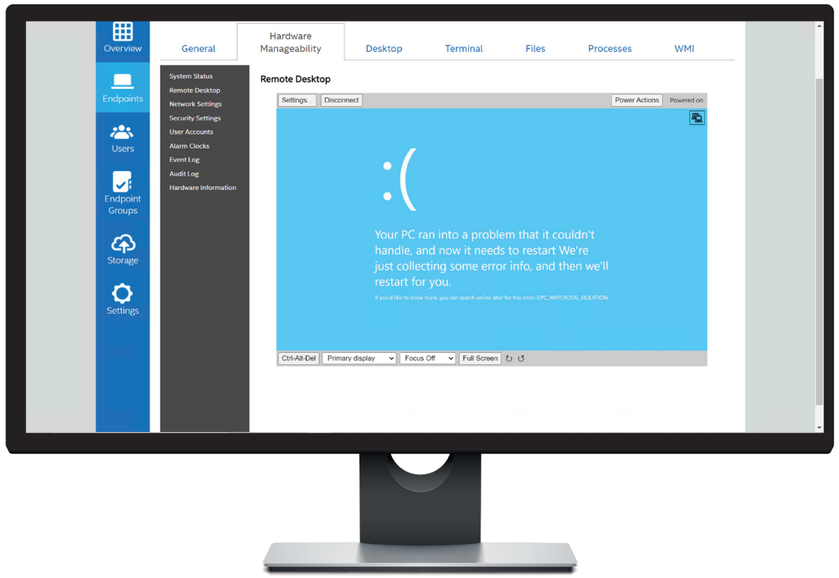

Figure 6. With out-of-band KVM, IT can see what's happening on a device, even if the OS is non-functioning

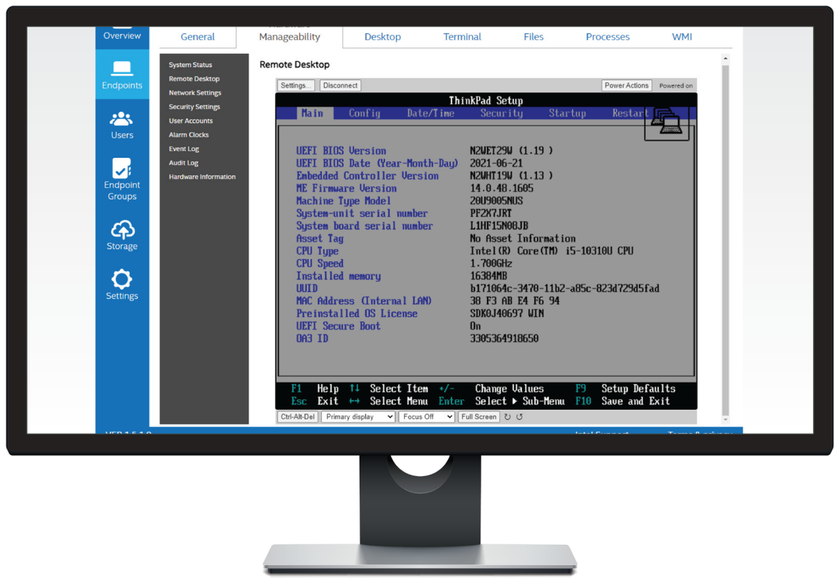

Figure 7. The KVM feature allows access to a remote system's BIOS

Table of Contents

Remote reimaging

Remote reimaging is similar to remote reboot. For instance, an IT administrator in the United States can reimage a laptop in South Korea so that it can be used by a new employee.

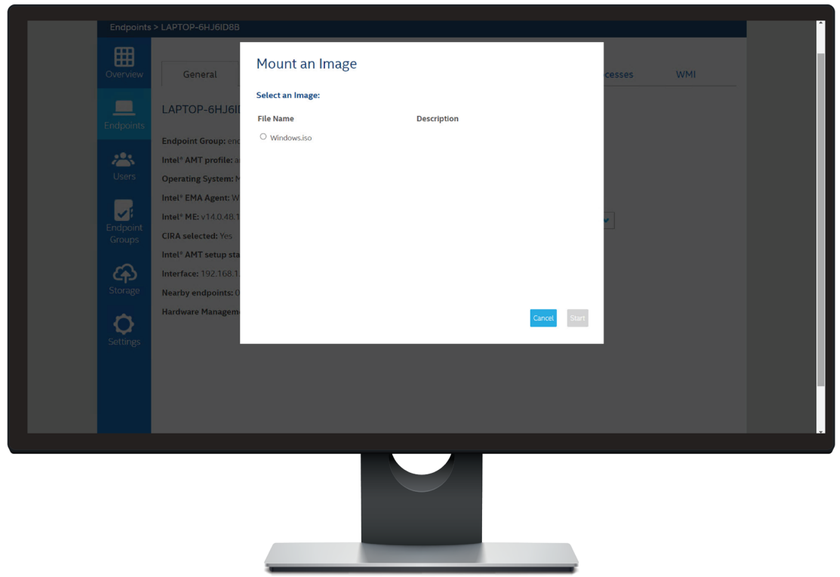

Figure 8. IT can mount an image and reboot to the image with Intel EMA

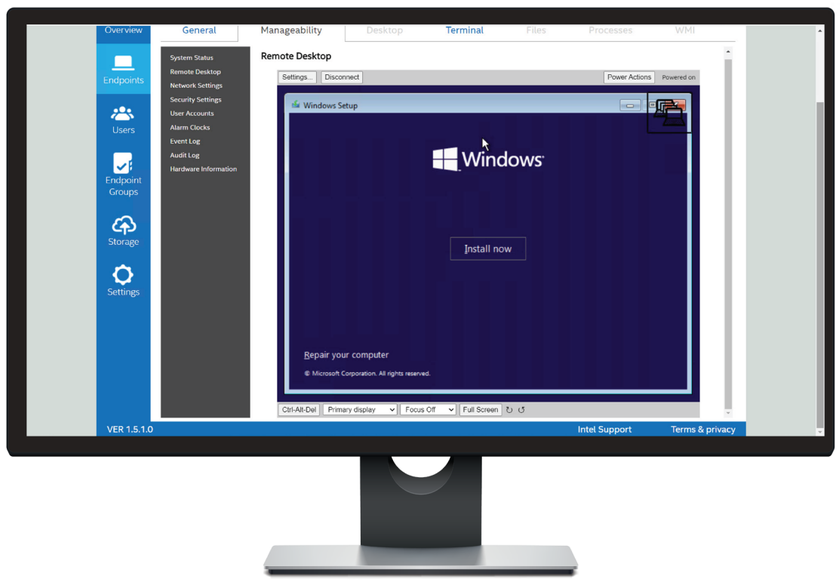

Figure 9. IT can prepare a device for a new hire by rebooting to an image and installing Windows remotely

Table of Contents

Larger benefits of Intel AMT and Intel EMA

By allowing IT to manage devices from the cloud, Intel AMT and Intel EMA help save IT time and costs and simplify their tasks. As a result, employees can stay more productive, and their devices can stay healthier, without having to travel to the office.

- 74 percent of IT decision makers (ITDMs) surveyed found that laptop- and desktop-management costs were reduced with the Intel vPro platform.[6]
- The Intel vPro platform could deliver a payback in 9 months, as estimated using a composite organization of 100,000 PCs, modeled by Forrester Consulting in a Total Economic Impact (TEI) study commissioned by Intel.[7]

Flexible for hybrid cloud environments

Intel EMA offers in-band management capabilities via its software agent to complement Intel AMT, and it supports deployment in the cloud or on premises. It can be deployed in a range of configurations to manage devices inside and outside the corporate firewall. Intel EMA communicates through a software agent or out of band through Intel AMT. This allows IT to manage devices in a hybrid cloud environment.

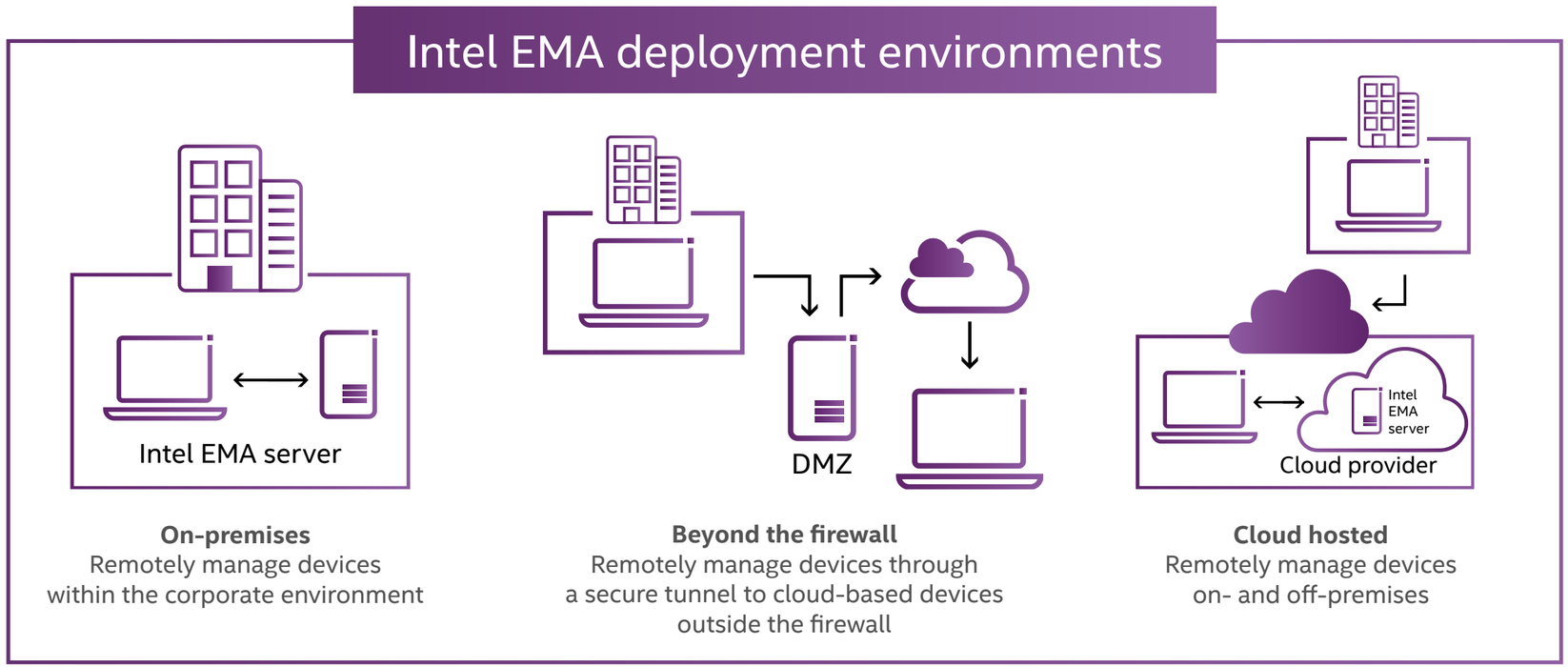

Figure 10. Intel EMA enables remote access to devices through Intel AMT, both inside and outside the corporate firewall

Table of Contents

Going beyond industry standards

Unlike other solutions, Intel vPro technology exceeds Desktop and mobile Architecture for System Hardware (DASH) standards set by the Distributed Management Task Force (DMTF). Although not all PC models implement DASH standards, Intel AMT, a superset of DASH standards, incorporates components that go beyond and enhance DASH capabilities. For instance, Intel AMT is the only wireless solution for remote manageability.[8] Other chipset manufacturer products depend on wired connectivity.

Intel EMA deployment guides for the public cloud

Intel EMA can be deployed to the public cloud by using the Intel EMA deployment guides listed below. These guides walk through the steps to set up Intel EMA on a public cloud. Configure the network, virtual machines (VMs), databases, and more with these guides:

- Microsoft Azure: intel.com/content/www/us/en/support/articles/000058623/software/manageability-products.html
- Amazon Web Services: intel.com/content/www/us/en/support/articles/000055630/software/manageability-products.html
- Google Cloud Platform: intel.com/content/www/us/en/support/articles/000058624/software/manageability-products.html

Before starting

If an organization already has an account with a public cloud service provider, then the organization's cloud administrator will need to grant access to allow Intel EMA deployment. The organization's network administrator should also be asked for the preferred address space to use. This will help avoid overlap with the corporate network to prevent routing issues if a VPN is already established to the cloud provider, or if there will be one in the future.

The network administrator deploying Intel EMA will also need to ensure that network security best practices are applied during deployment. This includes making sure that only traffic from the business public IP can be allowed to the Intel EMA web application.

Table of Contents

Conclusion

As more employees work outside the firewall and access cloud-based services rather than the intranet, IT management and support become more complicated. Current remote-management solutions don't always keep up with the relentless change of technology and shifts in workplace culture. Intel vPro technology helps IT's management capabilities reach beyond the OS, so that it can carry out modern endpoint management from the cloud.

Learn more about ways that the Intel vPro platform can support hybrid work capabilities in your organization.

Visit the Intel AMT page on intel.com to see what's possible.

Table of Contents

Printed in USA 1021/RR/PRW/PDF Please Recycle 348472-001US

[1] Rani Molla. "How remote work is quietly remaking our lives." *Recode by Vox*. October 2019. vox.com/recode/2019/10/9/20885699/remote-work-from-anywhere-change-coworking-office-real-estate.

[2] The Hill. "FBI sees spike in cyber crime report during coronavirus pandemic." April 2020. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic.

[3] As measured by December 2020 IOActive study (commissioned by Intel) comparing in-band software-based remote-management functions, out-of-band hardware-based remote-management functions, cloud-based support for these management functions, and batch management devices on PCs running Windows, including against an AMD Ryzen PRO 4000 series processor–based system. Source: IOActive. "Intel vs. AMD Comparison: Cross-Platform Manageability Comparison Research." Commissioned by Intel. December 2020. intel.com/content/dam/www/public/us/en/documents/articles/cross-platform-manageability-comparison-research.pdf.

[4] Intel AMT requires a wired or wireless network connection to provide remote management. Wireless support requires Intel AMT to be preconfigured with Wi-Fi profiles or to be configured to duplicate Wi-Fi profiles from the OS when it connects to a new Wi-Fi network. Intel AMT cannot join new Wi-Fi networks without the OS first connecting to them. Results may vary by use, configuration, and other factors.

[5] Check with your OEM manufacturer to ensure that Intel RSE is supported on your devices.

[6] Survey of 416 ITDMs at enterprises across the world using Intel vPro platform–based systems, including in the United States, UK, Germany, Japan, and China. 74 percent of respondents marked "agree" or "strongly agree" to this statement. Source: Forrester Consulting. "The Total Economic Impact of the Intel vPro Platform." Commissioned by Intel. January 2021. https://tools.totaleconomicimpact.com/go/intel/vproplatform/.

[7] Survey of 416 ITDMs at enterprises across the world using Intel vPro platform–based systems, including in the United States, UK, Germany, Japan, and China. 90 percent of respondents marked "agree" or "strongly agree" to this statement. For the purposes of this data, there are two assumptions being made to simplify analysis and explanation: 1) The composite organization assumes 100 percent laptop use—this helps simplify having to break out secondary inputs of device type counts and costs, which readers can do for their own business-case analyses; 2) The composite organization assumes no growth to avoid attributing organic growth with value gains attributable to Intel vPro technology, or complex explanation to subtract those gains from the return on investment (ROI) that is specific to the Intel vPro platform investment. Source: Forrester Consulting. "The Total Economic Impact of the Intel vPro Platform." Commissioned by Intel. January 2021. https://tools.totaleconomicimpact.com/go/intel/vproplatform/.

[8] As measured by a December 2020 IOActive study (commissioned by Intel) of in-band software-based remote-management functions, out-of-band hardware-based remote-management functions, and cloud-based support on Windows PCs. Intel AMT requires a network connection; must be a known network for Wi-Fi out-of-band management. Source: Intel. "11th Gen Intel vPro® Platform | Built for Business." intel.com/content/www/us/en/now/11thgenvpro.html.

Table of Contents