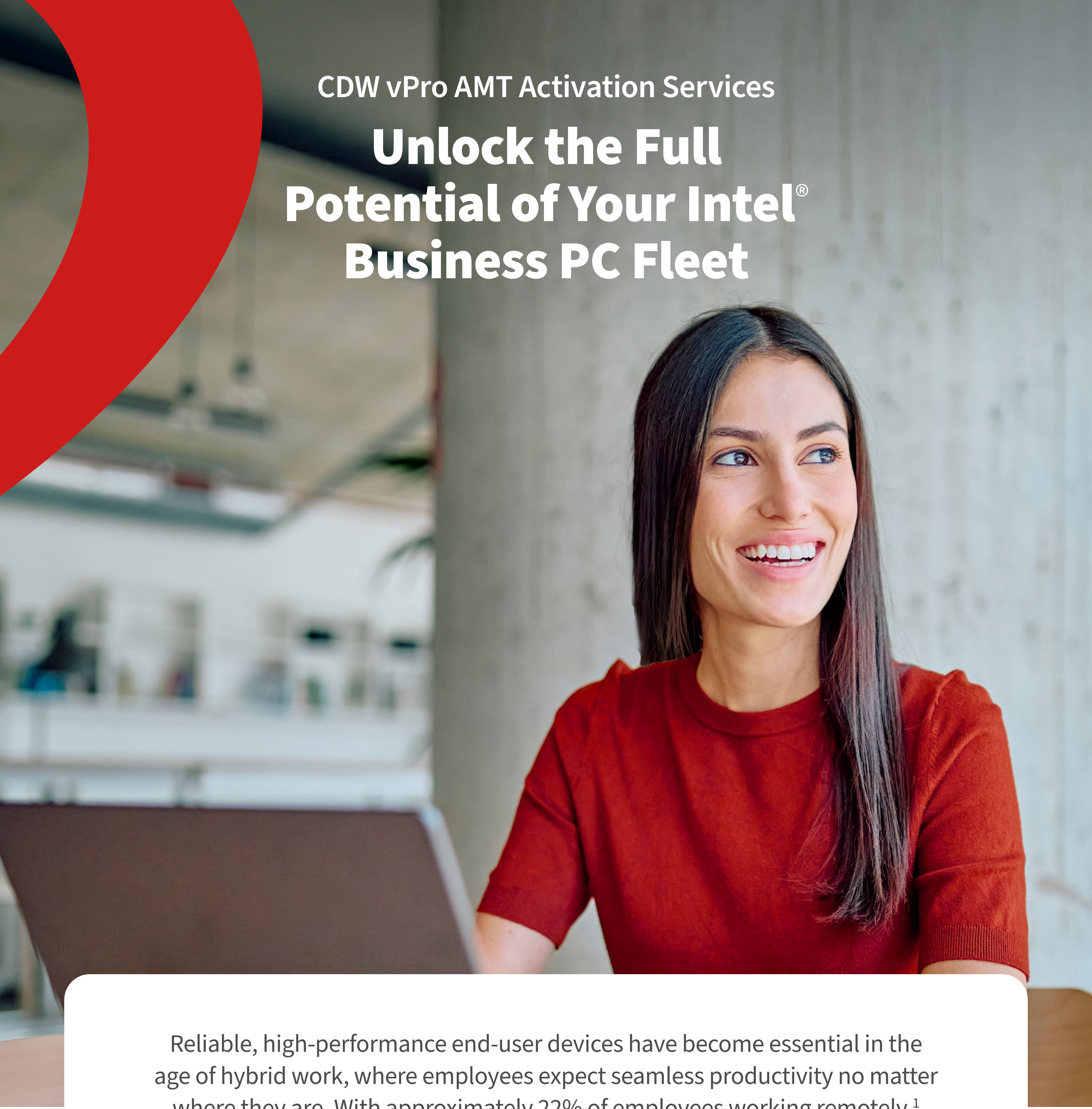
CDW vPro AMT Activation Services

Unlock the Full Potential of Your Intel® Business PC Fleet



Reliable, high-performance end-user devices have become essential in the age of hybrid work, where employees expect seamless productivity no matter where they are. With approximately 22% of employees working remotely,[1] organizations rely on these devices to deliver fast performance, secure access and consistent uptime without adding strain on IT teams.

Optimized Performance for Today's Hybrid Workforce

Many organizations today deploy Intel vPro® devices — for the exceptional performance and security they deliver right out of the box. They're realizing that Intel vPro® isn't a processor, but a comprehensive business platform available on Intel® Core Ultra™ and Intel® Core™ processors. And it's designed to deliver four key benefits:

Optimized performance

Enterprise stability

Multilayered hardware-based security

Advanced manageability

The majority of Intel vPro® features that fall under the first three of those pillars are enabled automatically when the device ships. Organizations don't need to do anything special for employees to leverage the benefits of Intel vPro® technology.

But to fully unlock the fourth — advanced manageability — organizations need to take an additional step to activate Intel® Active Management Technology (Intel® AMT). And this is a very important step in today's always-connected world of hybrid and remote work.

How Intel® AMT and Intel® EMA Work Together

Intel® AMT is the hardware-level capability built into Intel vPro® devices that enables remote power control, OS rebuilds, KVM and device recovery — even when the operating system is unresponsive.

Intel® Endpoint Management Assistant (Intel® EMA) is the cloud platform that activates and coordinates those capabilities at scale. Intel® EMA provides a secure management console, identity integration, certificate management and APIs that let you use AMT features through tools like Microsoft Intune.

In simple terms:

Intel® AMT is the capability.

Intel® EMA is how you securely use it.

Without Intel® EMA (or another unified endpoint management tool), Intel® AMT features exist in your devices but remain inactive. CDW activates and configures the platform needed to unlock the full value of Intel vPro®.

The Vital Importance of Effective Remote Manageability

To keep employees productive and engaged, IT teams need to be able to quickly troubleshoot, diagnose and repair problems remotely. For common software or configuration issues, most remote access solutions give IT teams the visibility they need to resolve issues efficiently.

But when the issue exceeds the capabilities of those tools — for instance, when the OS isn't responding — IT teams need to either travel to the device or ship the device somewhere it can be serviced hands-on, which means productivity and employee/customer satisfaction drop quickly.

Intel® AMT enables IT teams to remotely manage, patch and recover devices even if the operating system is down or the device is off the network. That's something software-only tools simply can't do.

A Real-World Example

Consider the global outage in July 2024 that left millions of PCs around the world unresponsive with blue screen errors. Enterprises with Intel® AMT activated were able to remotely power up, patch and recover their systems within hours. Those without it had to physically touch every endpoint — a process that stretched into weeks.

There were two major airlines that hit the news during that July outage. One had Intel vPro® with Intel® AMT activated and was able to recover its systems with only 1% flight cancellations. Because the other airline lacked that capability, it had to physically touch every device, resulting in a multi-week remediation plan.

Airlines weren't the only organizations that got back on track faster using the remote management capabilities of Intel vPro®. A leading healthcare provider recovered remote impacted devices quickly utilizing Intel® EMA and Intel® AMT. Devices without Intel vPro® had to be shipped for repair.

One of the largest banks in Mexico leveraged Intel vPro® remote manageability and achieved a 100% success rate in resolving the issue on Intel vPro® devices. And one of the largest retailers in Australia said, "vPro and AMT saved us," recovering its point-of-sale systems in stores to full service.

Take Control of Your Intel vPro® PC Fleet

With Intel® AMT activated, Intel vPro® transforms device management from reactive troubleshooting to proactive fleet control. IT teams can quickly diagnose and repair issues, reduce downtime and maintain compliance, all while keeping employees productive no matter where they work — from a corporate office to a home network to a retail or hospital floor.

Supporting a Multilayered Defense

In today's hybrid environments, layered protection is essential. **90% of successful cyberattacks** and **70% of data breaches** originate from compromised endpoint devices.[2] Intel vPro® provides a solid foundation along with Microsoft Pluton and Windows 11 to form a full-stack defense that secures every layer of the endpoint ecosystem.

At the hardware level, Intel vPro® delivers a trusted foundation through Intel Hardware Shield, protecting devices below the OS. Microsoft Pluton, integrated directly into Intel silicon, isolates credentials and encryption keys within the processor itself. Windows 11 builds on that base with Secure Boot, TPM 2.0 and virtualization-based security.

For companies adopting cloud-based fleet management, Microsoft Intune connects everything through the cloud for centralized management. Together, these technologies safeguard endpoints from firmware-level attacks to cloud-based threats, ensuring devices are resilient and compliant across every layer of your stack.

Intel® AMT Manageability Use Cases

Remote issue resolution
Diagnose and remedy your PC fleet remotely, including OS and image installation

Remote power control
Manage your entire PC fleet with remote power on, off and BIOS redirection

Hardware alarm clock
Set wake-up times and schedule updates for patches, drivers and apps

Hardware KVM
Take control of the keyboard, video and mouse even when the OS is down

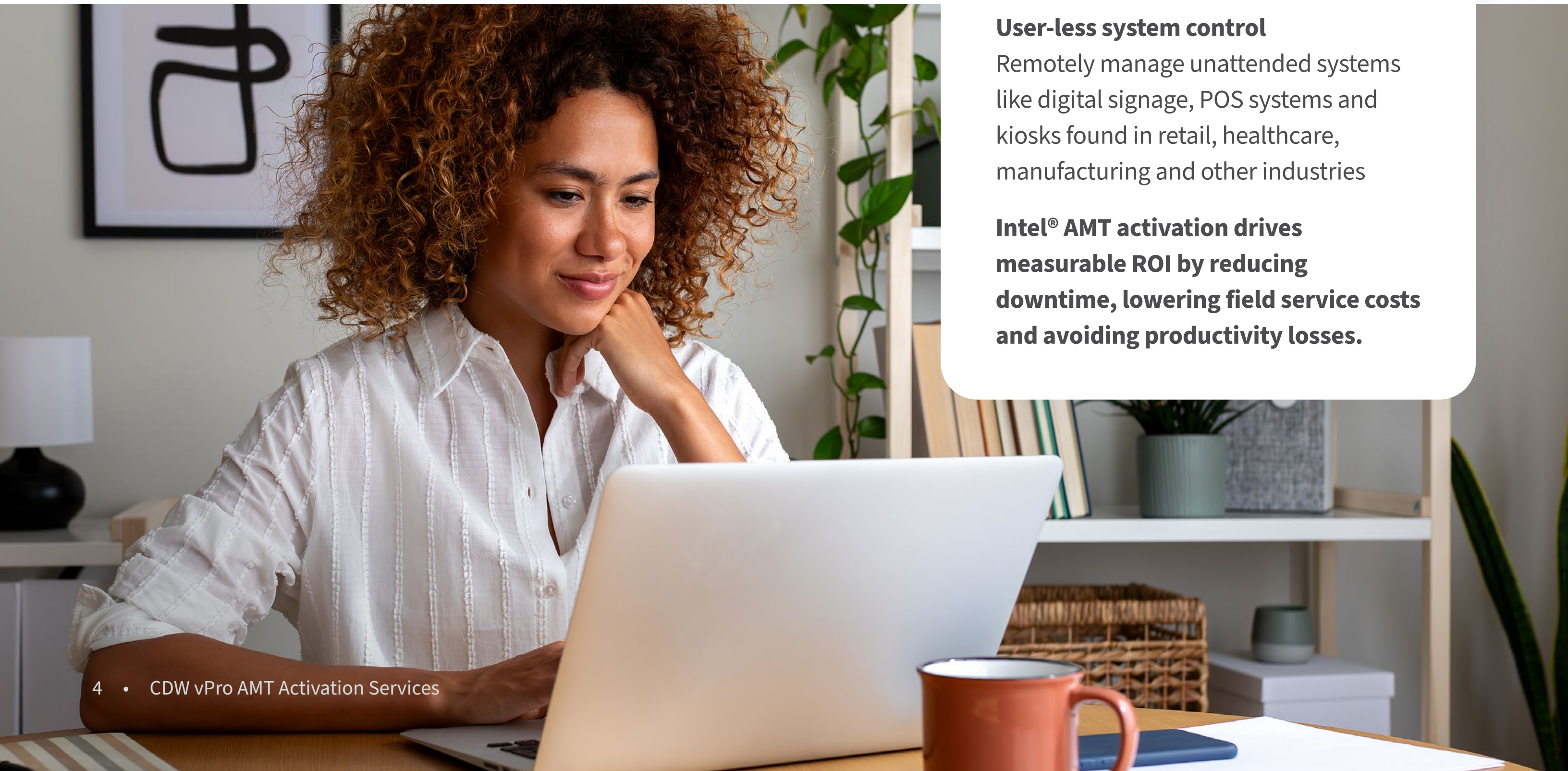
Boot redirection
Boot into temporary environments to run remote apps and diagnostic tools

Support beyond the firewall
Connect to devices inside and outside the corporate firewall

Cloud-based manageability
Manage devices from a single console in the cloud

User-less system control
Remotely manage unattended systems like digital signage, POS systems and kiosks found in retail, healthcare, manufacturing and other industries

Intel® AMT activation drives measurable ROI by reducing downtime, lowering field service costs and avoiding productivity losses.



Activating Intel® AMT on Intel vPro® Devices

Activating Intel® AMT on Intel® vPro® can be complex for IT departments to do on their own, as it requires the right configuration — executed in the right order — to integrate securely with the operating environment. That's where CDW's Digital Experience team comes in.

Our **Intel vPro AMT Activation Service** provides customers with a dedicated engineer to review your IT environment and install and configure an endpoint management platform. This can be done in the cloud using **Intel vPro® Fleet Services** (now integrated with Microsoft Intune) or on-premises with the **Intel® Endpoint Management Assistant (Intel® EMA).**

The choice depends on the organization's need for customization and control, the features required, its infrastructure capabilities, and security and compliance requirements.

Customization and Control

- **Intel vPro® Fleet Services** is a hosted Software as a Service (SaaS) solution managed by Intel, designed to provide IT professionals with an easy-to-use, Intel-hosted solution for taking advantage of hardware-level management of the Intel vPro® platform — no server investment required. CDW will configure and deploy Intel vPro® Fleet Services for customers, now available via Microsoft Intune.
- In regulated or isolated environments where cloud services aren't an option, CDW can deploy **Intel® EMA** instead of Intel vPro Fleet Services. Intel® EMA provides a customer-controlled platform for activating and managing Intel® AMT to meet specific security or compliance requirements. CDW handles the deployment and configuration so your team can manage AMT within your existing processes.

Security and Compliance

- **Intel vPro® Fleet Services** offers a secure hosted environment but may not meet all the specific compliance or security requirements of some organizations.
- **Intel® EMA** might be preferred by organizations with stringent security and compliance requirements that necessitate keeping management within their own controlled environment.

Intel® AMT can also be activated through other commercial unified endpoint management (UEM) tools like Omnissa WorkspaceOne®, Ivanti and CrowdStrike Falcon. No matter which configuration is chosen, we handle all the prerequisites, documentation and knowledge transfer, ensuring your team is ready to manage devices confidently after activation.

How CDW Activates Intel® AMT

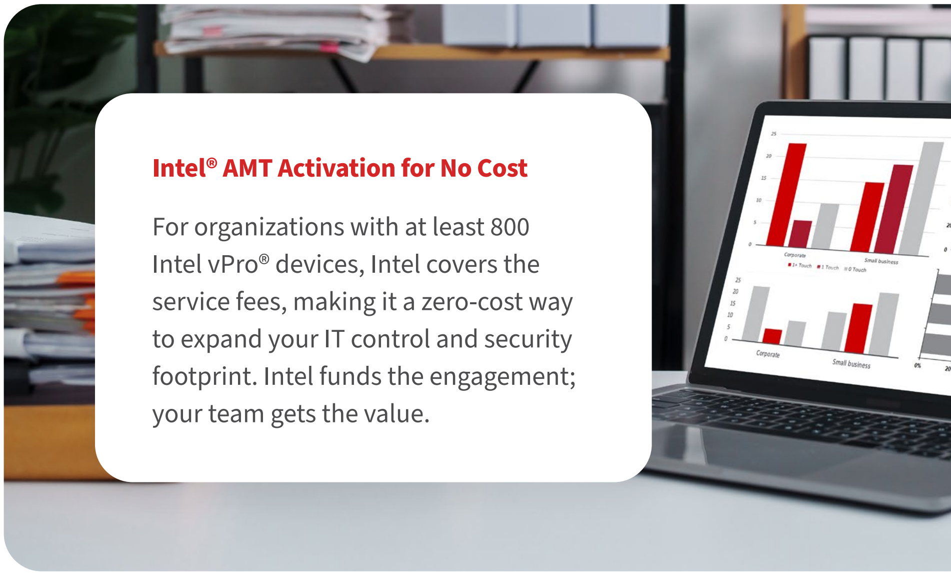
As an Intel® Prestige Partner, CDW has provided vPro AMT Activation Services since 2021, so our engineers are highly experienced in all kinds of IT environments and well versed in best practices for Intel® AMT activations. Our expertise and commitment to delivering exceptional results means you get the solution you need. Here's what you can expect:

Planning and Design Session	Our experts will review your current environment and work with you to create a detailed solution design that meets your business and technical requirements. Additionally, CDW will ensure that you meet any prerequisites and understand the features and differences between different types of control modes.
Deployment Plan	Our team crafts a deployment plan that works for you and limits interruptions and ensures a seamless integration.
Deployment and Configuration	Based on your environment, requirements and needs, we ensure that the solution is ready to set up and work for you.
Knowledge Transfer	We provide comprehensive user knowledge transfer to ensure a smooth transition to the new device management solution. Our team will also be available to offer ongoing support throughout the project and assistance with addressing any issues or concerns.

We are the only partner delivering Intel vPro® manageability activation at enterprise scale.

- More than 100,000 device activations performed from Fortune 500 customers to startups
- Deep expertise across all major MDMs
- Amplified™ Workspace Services to provide end-to-end lifecycle management

See how a U.S. home healthcare provider made remote device management faster, easier and more secure in our case study.



Intel® AMT Activation for No Cost

For organizations with at least 800 Intel vPro® devices, Intel covers the service fees, making it a zero-cost way to expand your IT control and security footprint. Intel funds the engagement; your team gets the value.

Frequently Asked Questions

Question	Answer
How do I know which devices have Intel vPro®?	We can help identify devices in your fleet with a variety of discovery tools.
Is Intel® AMT a replacement for Intune or my current endpoint management solution?	No. Intel® AMT is not a replacement — it's a force multiplier. Intune handles **in-band management** (OS is healthy). Intel® AMT handles **out-of-band management** (OS is corrupted, frozen or unreachable). Together, they give you **complete lifecycle control,** even in remote or hybrid environments.
We've had devices fall off of Intune. Will activating Intel® AMT help with that?	Yes. This is one of the most common reasons organizations activate Intel® AMT. If a device falls out of Intune or stops checking in, Intel® AMT gives you a **direct hardware-level connection** to power the device on/off remotely, rebuild or reimage the OS, and return it to Intune enrollment. Activating Intel® AMT essentially gives you **a back door** to bring the device back under management — without shipping it, touching it or sending a technician.
Will this require major changes to our environment or MDM?	Not at all. CDW handles the heavy lifting. Organizations can keep their existing MDM (Intune, Workspace ONE, Jamf, etc.) and natively access Intel vPro® features through their preferred MDM with **minimal to zero disruption** to the workflows your IT team already uses.
Why haven't we activated Intel® AMT before?	Historically, activating Intel® AMT required complex on-premises infrastructure. With modern Intel® EMA and Intel vPro® Fleet Services, activation is now fast, cloud-based and sometimes fully funded by Intel.
How long does CDW's vPro AMT Activation take?	For most customers, the average engagement is ~40 hours. CDW engineers complete the configuration, permissions, certificates and policy setup — ensuring everything works with your environment, security requirements and MDM.
Does this only work for on-premises networks?	No. Intel® AMT is designed for today's workforce. It works over Wi-Fi, outside the corporate network, from anywhere in the world, even if the OS is down. This is why most customers activate Intel® AMT — traditional tools break down off-premises, while Intel vPro® continues to work.
Does this work over home Wi-Fi and outside corporate networks?	Yes. Intel® AMT is designed for the hybrid workforce. It works over Wi-Fi, beyond the corporate firewall and even when the operating system is unresponsive. No VPN or physical touch is required.
Is Intel® AMT secure?	Yes. Intel® AMT is designed with multiple layers of security to ensure secure remote management. • Hardware-based security to protect against firmware attacks and ensure secure boot processes • Encrypted communication channels, ensuring data security during remote management • Out-of-band management that operates independently of the operating system, providing persistent connectivity even when the OS is down or the device is powered off, and ensuring secure management capabilities at all times • User authentication and role-based access controls provide additional security layers to prevent unauthorized access and allow defining of roles and permissions for different users • Intel continuously improves product security through research, vulnerability management and security updates
Will this conflict with our security model?	Intel® AMT uses a dedicated hardware security processor, isolated from the OS, with role-based access controls aligned to your identity provider. It reduces risk, not increases it.

Glossary

Advanced Manageability: One of the four pillars of Intel vPro® that enables IT teams to remotely manage, diagnose and repair devices, even when the operating system is unresponsive or the device is outside the corporate network.

Endpoint: Any user device connected to an organization's network, such as laptops, desktops, kiosks, point-of-sale systems or digital signage.

Endpoint Management Platform: A centralized system used by IT teams to manage devices across their lifecycle, including configuration, security, updates and compliance. Examples include Microsoft Intune and Intel® Endpoint Management Assistant (Intel® EMA).

Hardware-Based Security: Security features built directly into device hardware that protect systems below the operating system, helping defend against firmware-level and advanced persistent threats.

Hybrid Work: A work model in which employees operate across a mix of corporate offices, home networks and remote locations, requiring secure and reliable device access from anywhere.

In-Band Management: Device management that relies on the operating system being functional and connected, such as software updates, policy enforcement and application management.

Intel® Active Management Technology (Intel® AMT): A hardware-level capability built into Intel vPro® devices that enables out-of-band remote management, including power control, OS recovery and hardware-level troubleshooting, even when the OS is down.

Intel® Endpoint Management Assistant (Intel® EMA): A platform that activates, secures and manages Intel® AMT at scale. Intel® EMA provides a management console, identity integration and certificate handling to enable secure use of AMT capabilities.

Intel vPro® Fleet Services: A cloud-based, Intel-hosted Software as a Service (SaaS) solution that enables activation and management of Intel® AMT without requiring on-premises infrastructure. Now integrated with Microsoft Intune.

Intel vPro® Platform: A comprehensive business computing platform available on select Intel® Core™ and Intel® Core Ultra™ processors, delivering optimized performance, hardware-based security, enterprise stability and advanced manageability.

Keyboard, Video and Mouse (KVM): A remote access capability enabled by Intel® AMT that allows IT teams to view and control a device's keyboard, display and mouse at the hardware level. KVM works even when the operating system is unresponsive or during boot, enabling full remote troubleshooting and recovery without physical access to the device.

Out-of-Band Management: Hardware-level device management that operates independently of the operating system, allowing IT teams to recover, repair or reimage devices even when the OS is unresponsive or unavailable.

Remote Power Control: The ability to remotely power devices on or off, restart systems or schedule wake times, regardless of device location or OS state.

Unified Endpoint Management (UEM): A category of tools that allow IT teams to manage multiple device types and operating systems from a single platform, combining traditional device management with modern mobility management.

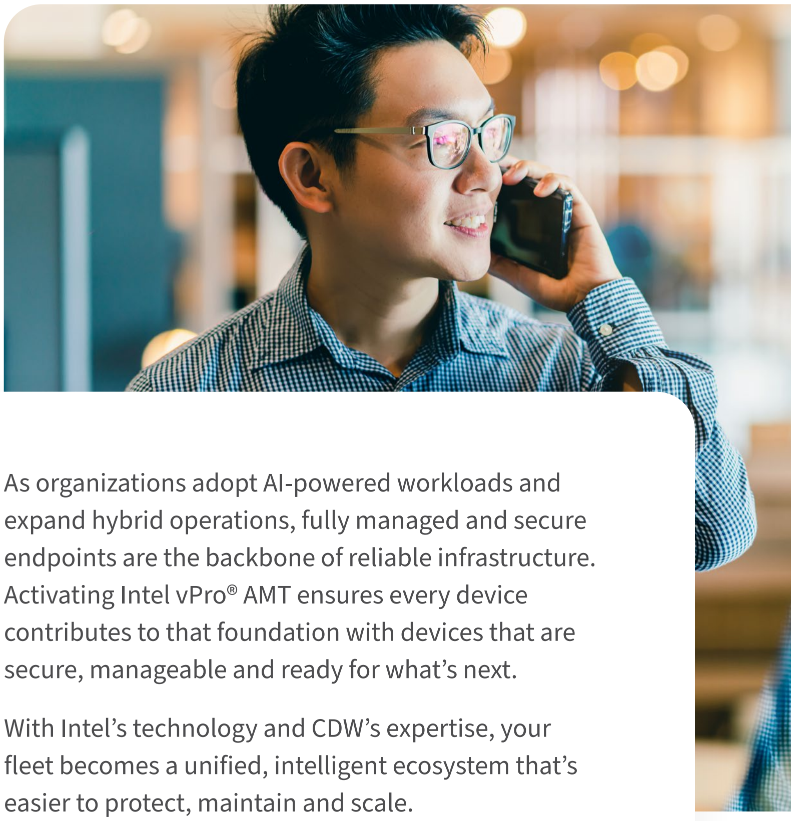
User-Less Devices: Devices that operate without a dedicated end user, such as kiosks, point-of-sale systems and digital signage, which require remote monitoring and management capabilities.

Is CDW vPro AMT Activation Services Right for You?

If you have Intel vPro® devices in your fleet, the short answer is “Yes.” With the enhanced ability to remotely manage, diagnose and restore devices anywhere in the world, your organization can save time, money and effort across your IT operations.

If you’re still not sure, consider these questions:

- Do you have a highly distributed workforce with many remote workers and sites?
- How do you manage your fleet today? What are you using for a unified platform manager? What challenges are you having with it?
- How often do you have devices that go down and need troubleshooting?
- If devices go offline, drop out of your MDM or aren’t getting patched, how do you troubleshoot and repair?
- If an employee’s PC gets a blue screen, what is your help desk’s remediation process (e.g., onsite hot swap or overnight shipments for troubleshooting)?
- Is your IT team responsible for managing remote, user-less devices like kiosks, POS systems and digital signage?



As organizations adopt AI-powered workloads and expand hybrid operations, fully managed and secure endpoints are the backbone of reliable infrastructure. Activating Intel vPro® AMT ensures every device contributes to that foundation with devices that are secure, manageable and ready for what’s next.

With Intel’s technology and CDW’s expertise, your fleet becomes a unified, intelligent ecosystem that’s easier to protect, maintain and scale.

Engage CDW for a vPro AMT Activation Workshop or Assessment to see how your existing hardware can deliver stronger security, enhanced manageability and measurable ROI. If you’d like to learn more, reach out to your CDW account team or visit **CDW.com/IntelServices#vPro.**

Sources:

[1] Neat, “The State of Remote Work: 2025 Statistics,” May 2025

[2] Market.biz, “Endpoint Security Statistics and Facts,” September 2025

intel vPRO CDW