signal65

# The Intel® Core™ Ultra 200V Series with Intel vPro®: Leading Commercial System Manageability and Security

Cameron Moccari

COMMISSIONED BY

intel®

# Contents

# Intel's Commitment to Enterprise Device Management and Security

As businesses have evolved, so has the Intel vPro platform.

Intel vPro technology was introduced in 2006 as a comprehensive platform specifically engineered to address the evolving demands of business computing environments. The enterprise computing landscape at that time required solutions that could deliver enhanced security, streamlined manageability, and robust performance capabilities – requirements that traditional consumer-focused technologies could not adequately meet.

The Intel vPro platform's sustained relevance lies in Intel's commitment to continuous innovation in response to evolving enterprise challenges. As organizational requirements have shifted from traditional computing models to encompass remote workforce management, cloud integration, and sophisticated threat protection, Intel has systematically enhanced the vPro platform to address these emerging needs, ensuring that enterprise technology investments remain strategically aligned with business objectives.

The Intel vPro platform represents Intel's fully integrated approach to commercial computing, built around Intel Core processors and platform technologies that incorporate specialized business-critical features. Key innovations included Intel Active Management Technology (AMT) for remote system administration, Trusted Platform Module (TPM) support for hardware-based security frameworks, and Intel Virtualization Technology (VT) for virtualization capabilities. These components have become foundational to modern enterprise IT infrastructure.

Over the subsequent two decades, Intel has established a commanding position in the enterprise PC market, powering the majority of commercial desktops and laptops deployed across global organizations. This market leadership stems from strategic partnerships with leading OEMs including Dell, HP, Lenovo, and others, combined with Intel's consistent delivery of reliable and scalable processor architectures that are designed to meet the rigorous demands of corporate IT environments. A 2024 Forrester Total Economic Impact study demonstrates the measurable value of this leadership: organizations deploying Intel vPro as their endpoint standard achieved a 213% ROI over three years, with benefits of $4.32 million versus costs of $1.38 million for a composite 10,000-employee organization.

**Key Findings:**

- Faster recovery at scale with Intel vPro and true remote out-of-band management
- Silicon-anchored security that protects organizations from attacks and breaches
- Proven OEM ecosystem built on the trusted Intel vPro platform requirements

# Broad Ecosystem Support for Intel vPro Commercial Deployments

Just as Intel has again scored countless OEM designs with the Intel Lunar Lake architecture and the Intel Core Ultra 200V series, OEMs have long seen the value of Intel vPro technology through commercial deployments. To get the Intel vPro badge and validation, minimum system design standards must be met by each OEM partner, but each partner is also free to expand and optimize the manageability and security features available through the Intel vPro platform.

- Dell has integrated Intel vPro into their Dell Client Command Suite, which offers a unified interface combining Intel AMT with Dell's BIOS configuration utilities – enabling system administrators to manage remote system provisioning, enforce security policies, and maintain hardware inventory from a single console. (See more)

- HP's Client Management Solutions incorporate Intel vPro into their commercial device management portfolio, including tools such as HP Image Assistant and HP Client Catalog. These tools support large-scale deployments while preserving the hardware-based security and remote management benefits intrinsic to the Intel vPro platform. (See more)

- Lenovo supports Intel vPro across its ThinkPad commercial systems and other laptop lines through Lenovo Vantage Enterprise and Think Deploy. These tools provide a comprehensive management ecosystem spanning from initial imaging through ongoing fleet maintenance and security compliance monitoring. (See more)

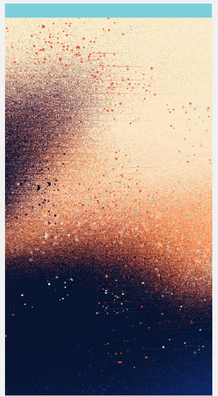
These OEM-specific implementations demonstrate the strategic value of Intel's partnership approach, as each manufacturer has developed complementary software and service offerings that amplify Intel vPro foundational capabilities while addressing the unique requirements of their enterprise customer bases. The consistent and repeated investment in the adoption of expansion of Intel vPro technology demonstrates the value that it provides to their commercial laptop product lines.

This collaborative ecosystem ensures that organizations can leverage Intel's foundational hardware management technologies through familiar, vendor-optimized interfaces that integrate seamlessly with existing IT infrastructure and operational workflows.

# Time to Value: Intel vPro Deployment Options

Intel vPro deployment architecture offers enterprises three implementation pathways, each designed to address different organizational requirements and infrastructure preferences.

- **Intel vPro Fleet Services** is a fully managed Software-as-a-Service solution that enables organizations to access Intel vPro manageability features without requiring dedicated server infrastructure, streamlining deployment complexity from traditional multi-step processes down to as few as six configuration steps.
- The **Intel Endpoint Cloud Services** approach leverages existing commercial vendor relationships, allowing enterprises to utilize established management platforms as a unified interface for accessing Intel vPro manageability capabilities natively within their current operational frameworks.
- **Intel Endpoint Management Assistant (EMA)** provides a self-hosted deployment option designed specifically for organizations requiring direct control over their management infrastructure, particularly suitable for independent software vendors and enterprises with stringent data sovereignty requirements.



## Time to Value: Intel vPro Deployment Options

This multi-modal deployment strategy addresses the fundamental challenge of enterprise fleet management at scale, enabling organizations to remediate critical system outages within hours rather than days across distributed device populations numbering in the hundreds of thousands. The architectural flexibility inherent in these deployment options ensures that organizations can integrate Intel vPro capabilities regardless of their existing IT infrastructure, vendor relationships, or operational security requirements.

Intel's mature deployment ecosystem demonstrates measurable advantages in real-world implementations. Forrester research shows that IT groups reduce device management time by 65% when standardized on Intel vPro platforms. Additionally, organizations report 99.7% application compatibility with Windows 11 transitions, supported by Intel's Stable IT Platform Program (SIPP ).

### Intel vPro Deployment Options

| **Intel vPro Fleet Services**<br>Fully Managed SaaS Solution | **Intel Endpoint Cloud Services**<br>Vendor Integration Platform | **Intel Endpoint Management Assistant**<br>Self-Hosted Solution |
|---|---|---|
| Intel-hosted Software-as-a-Service solution that provides IT administrations direct access to Intel vPro manageability hardware features without requiring dedicated server infrastructure. | Leverage existing commercial vendor relationships by utilizing established management platforms as a unified interface for accessing Intel vPro manageability capabilities. | Self-hosted deployment option designed for organizations requiring direct control over their management infrastructure, ideal for ISVs and enterprises with strict data sovereignty requirements. |
| • **Simplified deployment (6 steps vs. traditional 26)**<br>• **No server infrastructure required**<br>• **Direct access to hardware-level management**<br>• **Intel-managed security and updates**<br>• **Scalable across enterprise fleets**<br>• **Reduced operational overhead** | • **Native integration with existing tools**<br>• **Single management interface**<br>• **Preserve current vendor relationships**<br>• **Streamlined operational workflows**<br>• **Reduced training requirements**<br>• **Familiar user experience** | • **Complete infrastructure control**<br>• **Data sovereignty compliance**<br>• **Custom integration capabilities**<br>• **Enhanced security policies**<br>• **Optimized for ISV environments**<br>• **Maximum customization flexibility** |

Remediate from an outage in hours versus days across hundreds of thousands of distributed devices.

# Signal65 Testing Methodology and Analysis

This paper evaluates the manageability and security capabilities of the Intel Core Ultra 200V series and Intel vPro technology in comparison to its x86 competition. It follows a companion piece that highlights the performance and battery life of the Intel platform through hands-on testing with three representative OEM offerings. We leveraged the same three pairs of systems with our custom IT build to evaluate the real-world implications for ITDMs and system administrators with a heterogenous PC fleet.

For manageability, we focused on use cases across the device lifecycle, from deployment and device provisioning to patching and remediation. For security, we focused on the device lifecycle, from supply chain to boot to threat detection with complex AI workloads.

# Manageability Advantage: Resilient Fleet Management Anchored in Silicon

The 2024 Blue Screen event, while not a common occurrence at scale, showed the limits of software-only fleet management and the real-world impact of extended downtime. Organizations without hardware-enabled controls endured days or weeks of downtime. In contrast, enterprises equipped with hardware-enabled remote management capabilities through the Intel vPro platform saw a dramatic difference in the recovery process as systems were recovered within hours. This operational advantage illustrates the strategic value of hardware-based management in maintaining business continuity while minimizing the operational overhead often associated with distributed IT environments.

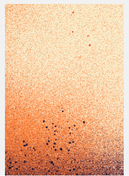
Our earlier research highlights the real-world impact of modern management on downtime and business impact through an outage scenario – where having Intel AMT activated on the Intel vPro platform would lead to significantly better business outcomes.

## About Intel Active Management Technology (AMT)

Intel AMT represents the most mature and widely deployed out-of-band management technology in the enterprise market, with nearly two decades of continuous deployment and refinement. Unlike software-based management solutions, Intel AMT operates independently of the host operating system through a dedicated microprocessor and network interface, enabling persistent connectivity even through system failure.

This hardware-based approach enables capabilities impossible with software-only solutions: remote power management from completely powered-off states, BIOS-level configurations during boot failures, and cryptographically secured administrative channels that function regardless of OS integrity. Intel AMT's integration with Intel Wi-Fi components ensures consistent functionality across wired and wireless networks – a reliability advantage that competing solutions cannot guarantee due to chipset compatibility variations.

Organizations deploying Intel vPro systems gain access to Intel AMT as part of a broader technology stack designed specifically for commercial computing environments. Intel AMT establishes a persistent, hardware-based management channel that remains operational even when the OS is down or when the device is powered off. This capability enables IT to perform critical functions – such as remote power control, BIOS access, and imaging – independently of in-band software agents.



# Hands-on with Intel vPro and AMD DASH

## Deployment and Provisioning Experience

In our test environment, we leveraged GUI management console interfaces available from Intel and AMD:

- For our three different Intel Ultra 200V Series platforms, we managed our deployment using Intel Endpoint Management Assistant (EMA) running locally on a domain-attached system.
- For our three comparable AMD Ryzen Pro platforms, we had a separate system running the AMD Management Console (AMC).

For both Intel EMA and AMD AMC, we started from a full Windows network environment featuring an Active Directory domain controller and local certificate authority.

While the GUI for AMC was only accessible on the local system where the management console was installed, Intel EMA provides a web GUI that is accessible through a login across the local network – allowing for easier fleet management across the IT management staff.

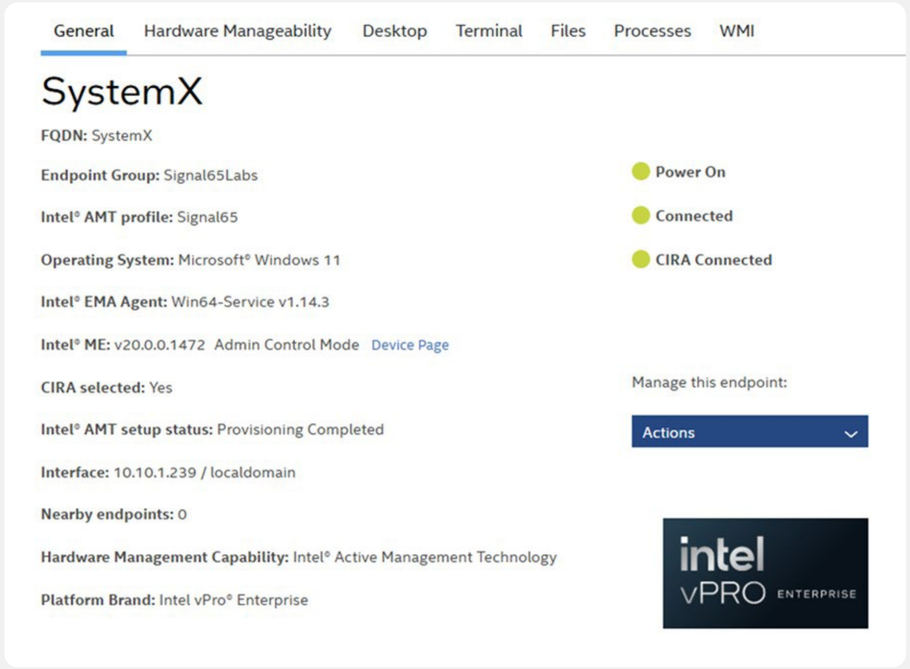
We found the deployment steps to be similar for both our Intel Core Ultra 200V series platforms with Intel vPro and our AMD Ryzen AI PRO systems with AMD DASH:

- Created a provisioning package on the system where either Intel EMA or AMC was installed.
- Installed the applicable package on the three Intel Core Ultra 200V series platforms and the three comparable AMD Ryzen AI PRO platforms.
- Completed a discovery process to add the systems to the managed inventory on Intel EMA and AMC.

While the steps were similar for both solutions, our deployment and provisioning experience was significantly better on the Intel Core Ultra 200V series platforms with Intel vPro. Utilizing Intel EMA, device provisioning and discovery was successful on the first attempt across all three OEM platforms. This initial deployment included full out-of-band management and hardware manageability features, as we will detail in the next section.

## Hands-on with Intel vPro and AMD DASH - Depoloyment and Provisioning Experience

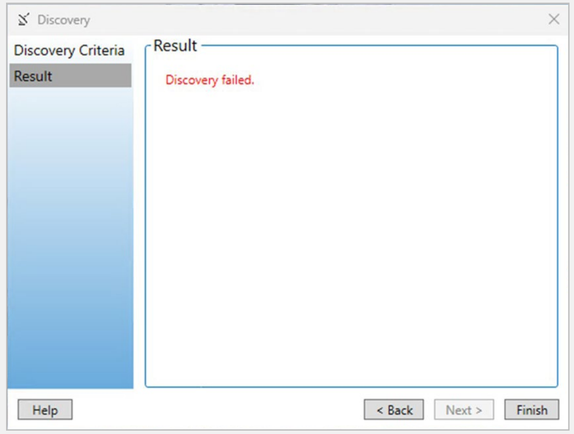
The screenshot below is from Intel EMA with confirmation that the Intel Core Ultra 200V system with Intel vPro is enrolled, discovered, and able to be managed by the IT system administrator.




Our experience with AMD DASH and the three comparable OEM platforms was an entirely different story. One of the three AMD Ryzen AI PRO platforms did not support AIM-T and was unable to be enrolled in AMC. We confirmed the lack of AMD DASH support was due to the lack of an AIM-T compatible Wi-Fi chipset.

One of the requirements for an Intel vPro platform is an Intel Wi-Fi chip, which guarantees full Intel AMT support, providing confidence that a system with the Intel vPro badge is capable of being fully integrated into the management system.

For the other two competing systems, we were eventually able to enable AIM-T management in their respective UEFI interfaces and provision the systems for AMC management. However, we experienced issues with getting the two systems to reliably discover and then populate in inventory in the AMC utility, leading us to do most of our management testing through command-line DASH which we found to be more reliable.

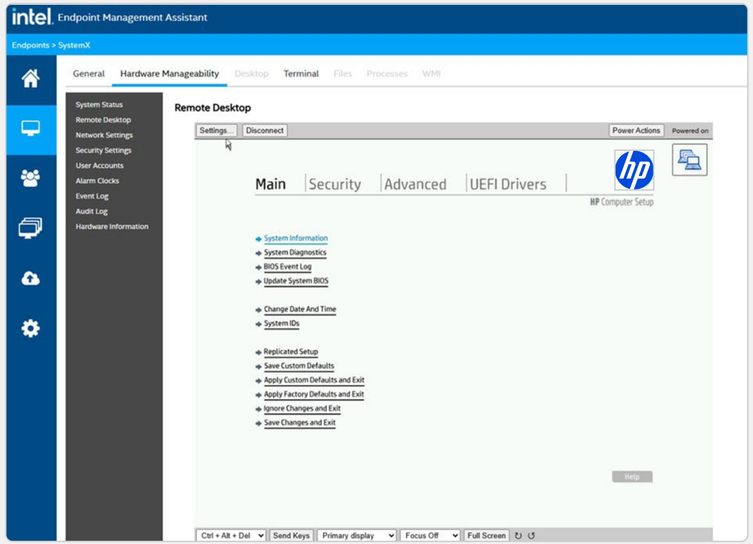


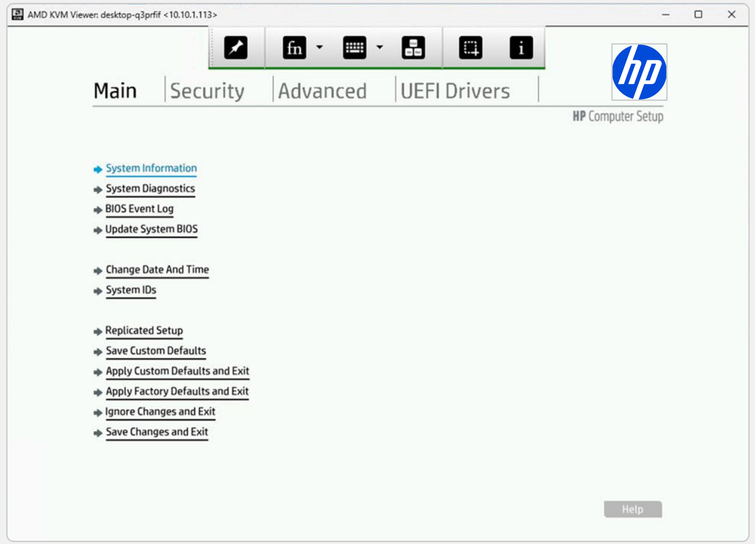
Hands-on with Intel vPro and AMD DASH - Out-of-band Remote Patching Experience

# Out-of-band Remote Patching Experience

In this test scenario, we looked at the system administrator experience for a common use case; remote patching of an operational system. We initiated the remote control session from within the operating system on the target device and then remotely rebooted the system to access the UEFI settings.

Our experience was similar for the three Intel Ultra 200V series platforms with Intel vPro and the two AMD Ryzen AI PRO platforms with AMD DASH. For the Intel platforms, starting from the Windows environment, we were able to initiate a remote session with the test system and directly reboot the system into the UEFI configuration environment. For the two AMD platforms that supported AMD DASH, we were able to maintain a remote session through a reboot, allowing each system to be remotely patched and rebooted by a system administrator. To reach the UEFI CLI, remote control must be initiated first in-band through the operating system.



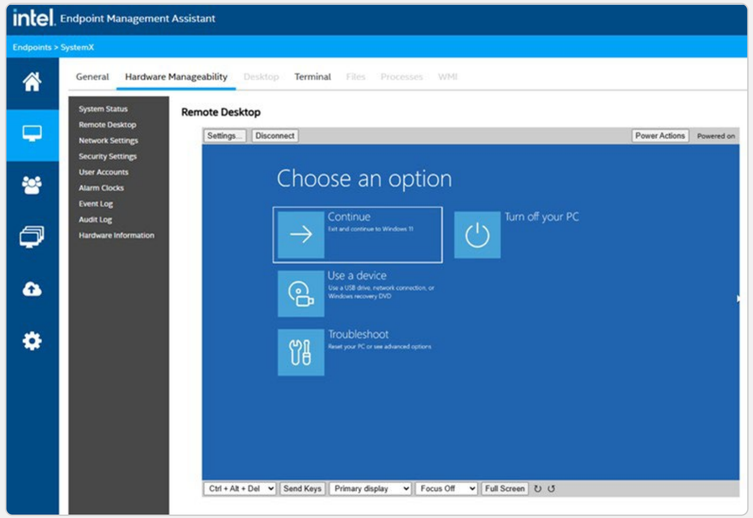
Hands-on with Intel vPro and AMD DASH - Out-of-band Issue Remediation Experience

# Out-of-band Issue Remediation Experience

In addition to the remote patching scenario, we also wanted to look at a scenario similar to the 2024 Blue Screen event, where system administrators had to remotely access the Windows Recovery Environment to manually remediate the issue and allow systems to boot. **In this scenario, initiating the remote session first while in-band is not an option.**

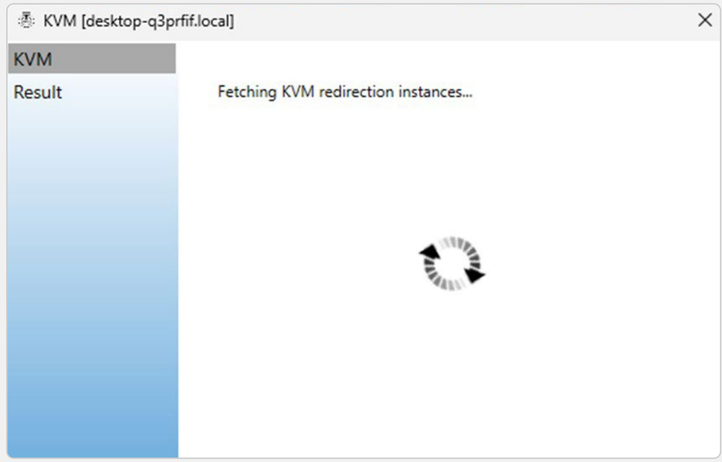
Unlike the remote patching scenario, our experience was not the same with both the Intel Ultra 200 V series platforms with Intel vPro and the two AMD Ryzen AI PRO platforms with AMD DASH. With the Intel platforms, we were able to initiate a remote control sessions from the Windows Recovery Environment, allowing the system administrator to remotely make the necessary changes and restore system functionality for the end user in a timely manner.

In contrast, we were unable to initiate the remote control session from an out-of-band




state with the two AMD Ryzen AI PRO platforms. We attempted to do so using the AMC utility, which would simply time out – leaving the test system inoperable in the Windows Recovery Environment and requiring manual intervention in person from a system administrator. For the two AMD Ryzen AI Pro platforms, this means that the system administrator would be unable to remote remediate and recover system in a 2024 Blue Screen type event.

Why It Matters: Being unable to remotely remediate and recover systems requires a manual intervention on each system – a tedious process that becomes more problematic at scale and/or when a PC fleet is geographically dispersed or behind highly controlled access points in labs, production lines, or secured buildings.



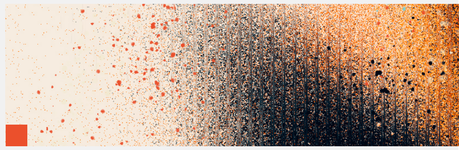
# Security Advantage: Comprehensive Enterprise Protection Anchored in Silicon

For Intel vPro platforms such as the Intel Core Ultra 200V series in our testing, Intel vPro technology provides hardware-based security designed to protect system from the silicon up. Anchored in hardware root of trust, the platform delivers a multi-layered defense that extends from the supply chain to the application layer. By addressing threats at and below the operation system, Intel vPro helps organizations mitigate risks that software-only tools can't do alone.

For IT leaders, this means stronger resilience against firmware tampering, bootkits, ransomware, and supply chain attacks – threats that can undermine trust at the foundation. Intel vPro pairs silicon-level protections with runtime resilience and ecosystem integrations such as AV/EDR solutions, enabling enterprises to validate integrity, enforce policies, and safeguard workloads and data across the fleet.

**Key areas of protection include:**

- Supply Chain Security
- Boot Integrity
- Firmware Resilience
- OS Security
- Application and Data Protection



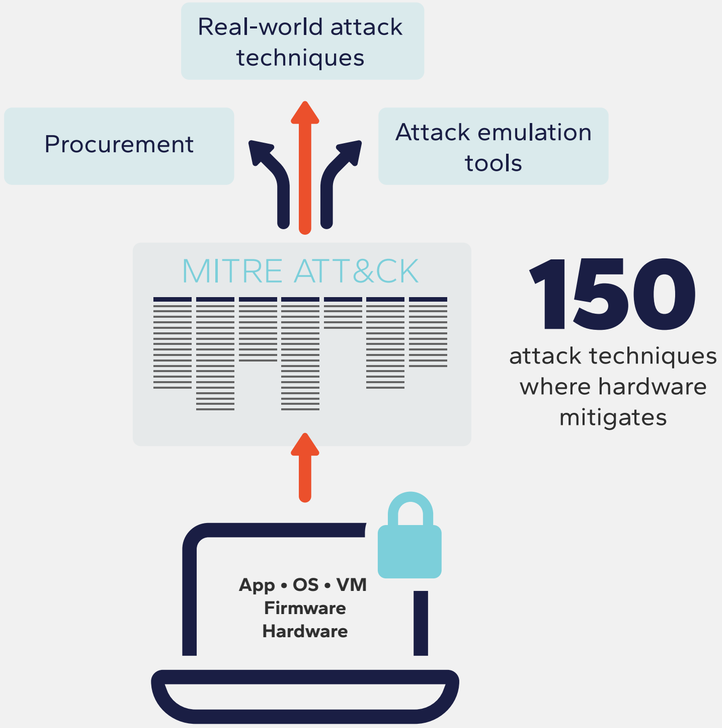
Security Advantage: Comprehensive Enterprise Protection Anchored in Silicon

## Security Ecosystem Enablement

Intel complements its hardware protections with deep integrations across the enterprise security stack, including Microsoft Secured-core PC certification, Microsoft Defender integration for accelerated memory scanning, and compatibility with leading EDR platforms such as CrowdStrike. Intel has partnered with MITRE to map the Intel vPro hardware security stack against more than 150 unique attack techniques, giving IT leaders the first comprehensive visibility into how hardware-based protections apply in real-world scenarios. Building on this, Intel Device Discovery provides a fleet-wide query interface that shows which hardware security features are present, activated, and properly configured. Together with integrations from leading Security Controls Assessment ISVs, these tools give organizations actionable insight into where gaps may exist and how to strengthen defenses.

AMD offers no comparable capability, making this a clear area of differentiation for Intel. AMD does participate in Windows security standards but provides fewer validated integrations and less prescriptive enablement guidance for enterprise environments. This disparity increases operational overhead in heterogeneous deployments.

In contrast, Intel provides tools and ISV integrations that help IT maintain every Intel vPro security feature is fully activated and aligned to real-world threat tactics. This visibility highlights misconfiguration that could leave gaps, giving organizations confidence that they are maximizing ROI from their enterprise PC investments.




**150**
attack techniques where hardware mitigates

**Why It Matters:** Security is only as strong as its operational execution. Intel's ecosystem approach simplifies enforcement and verification across large, distributed fleets.



**See the Security Ecosystem Enablement section in the Appendix for references.**

Security Advantage: Comprehensive Enterprise Protection Anchored in Silicon

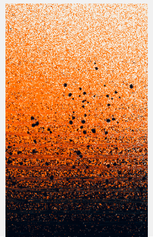
## Supply Chain Security & Attestation

Intel employs immutable device identities, OEM firmware attestation, and cryptographically enforced binding of firmware to prevent unauthorized changes after manufacturing. By embedding attestation hooks at the silicon layer, Intel ensures that organizations can verify system integrity before deployment, significantly reducing the risk of compromised hardware entering production environments. With Intel Transparent Supply Chain (TSC), Intel provides a service through a set of tools, policies, and procedures implemented at the OEM manufacturing floor that gives enterprises visibility and confidence to verify the authenticity and firmware version of systems and components.

Intel also extends protection beyond the device with its Assured Supply Chain service. This program provides a digitally attestable chain of custody for the silicon manufacturing process, anchored in pre-approved facilities located in trusted geographies such as the United States, EMEA, Vietnam, and Malaysia. For government agencies and other security-sensitive industries, this assurance helps confirm that silicon components originate from vetted, strategically aligned locations – reinforcing trust in the supply chain from the start.

AMD provides foundational secure boot but lacks end-to-end attestation and identity-binding mechanisms comparable to Intel's PSE-enabled model. This gap can leave enterprises more dependent on external audit processes and software verification for supply-chain trust – adding labor and process that requires specific expertise to execute these audits.

**Why It Matters:** Attestation-backed device integrity reduces the likelihood of introducing counterfeit or tampered components, protecting brand and regulatory standing.





**See the Supply Chain Security & Attestation section in the Appendix for references.**

Security Advantage: Comprehensive Enterprise Protection Anchored in Silicon

## Hardware Security Engine

Intel Partner Security Engine (PSE) provides a hardware-based root of trust designed to protect against firmware tampering and supply-chain compromise. It anchors trust in immutable ROM (SoftROM) and enhances it with capabilities such as key-split architecture, late binding at OEM manufacturing, and monotonic counters for replay protection. These features ensure that partner firmware executes in an isolated enclave and cannot be replaced post-manufacturing. OEM controls allow partners to manage opt-in, provisioning, and updates without undermining the integrity of the binding process. By enforcing these protections in hardware, Intel reduces the attack surface long before the operating system initializes.

AMD's approach, based on ASP 2.0 and integration with Microsoft Pluton, offers foundational verified-boot features but omits critical PSE-class protections. AMD lacks a key-split model, dedicated replay protection, and late-binding mechanisms that lock firmware identity during manufacturing. This means more assurance tasks fall back to software policy, increasing residual risk in environments where firmware integrity is critical. Note that Intel's PSE is also integrated with Microsoft Pluton, so Intel's innovation in this space is on top of Pluton support and not in lieu of it.

**Why It Matters:** Firmware-level attacks are difficult to detect post-deployment and expensive to remediate. Intel's silicon-anchored controls reduce this risk by securing the supply chain at its origin.

## Secure Boot & BIOS/FW Protection

Intel vPro anchors boot integrity in silicon using Intel Boot Guard, which validates the first block of BIOS code against cryptographic keys fused at manufacturing, and Intel Trusted Execution Technology (TXT), which establishes a measured launch environment to ensure the OS and hypervisor boot into a known-good state. Intel BIOS Guard extends these protections by preventing unauthorized updates or rollback attempts, shielding systems from persistent firmware tampering. These capabilities integrate directly with Microsoft Secured-core PC standards, giving IT teams verifiable assurance that below-OS protections are consistently enabled and compliant across the fleet.

By contrast, AMD supports secure boot and TPM-backed measurements but does not provide TXT-style dynamic runtime validation, BIOS Guard rollback protection, or OEM-verified Secured-core integrations. This can complicate compliance validation, especially in mixed-fleet deployments requiring uniform enforcement, whereas Intel has continued to innovate and stay ahead of security threats relative to a lower security posture that could leave an organization vulnerable to newer and more sophisticated attacks.

**Why It Matters:** A validated boot chain anchored in silicon ensures trust before any OS or endpoint security tools load, reducing risk from bootkits and advanced persistent threats.



**See the Hardware Security Engine and Secure Boot & BIOS/FW Protection sections in the Appendix for references.**

Security Advantage: Comprehensive Enterprise Protection Anchored in Silicon

## Post-Quantum Cryptography (PQC) Readiness

Intel is advancing security for the post-quantum era by integrating quantum-resistant cryptography directly into the platform. Today's asymmetric algorithms like RSA and ECC are expected to be vulnerable to future quantum computers, creating long-term risk for sensitive enterprise and government workloads. Intel addresses this with support for XMSS hybrid signature schemes aligned to NIST SP 800-208 and NSA CNSA 2.0 requirements, enabling quantum-safe firmware signing for critical platform components such as microcode, ISSE, and CSME. Combined with AES-256 Total Memory Encryption (TME), Intel vPro systems provide a stronger foundation against "harvest-now, decrypt-later" threats than traditional AES-128 implementations such as AMD's Secure Memory Encryption (SME). Intel's forward-looking approach helps organizations extend the security lifetime of their fleets and prepare for compliance in regulated industries.

**Why It Matters:** By embedding post-quantum protections at the silicon level, Intel vPro ensures that enterprise PCs deployed today remain trustworthy against the cryptographic challenges of tomorrow.



**See the Post-Quantum Cryptography (PQC) Readiness section in the Appendix for references.**

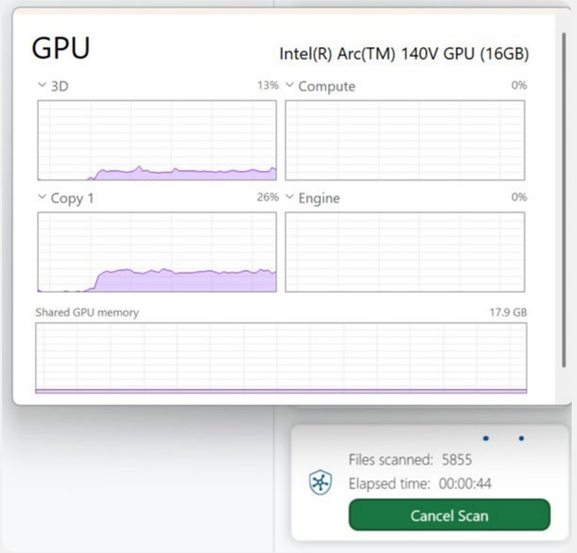
Security Advantage: Comprehensive Enterprise Protection Anchored in Silicon

## Memory Protection

As AI-driven workflows and advanced threats increasingly strain endpoint resources, Intel vPro delivers hardware-accelerated memory protections designed for both security and performance. Intel Threat Detection Technology (TDT) uses Accelerated Memory Scanning to offload memory scanning tasks from the CPU to the integrated GPU, reducing performance overhead while maintaining real-time detection of ransomware and fileless malware. In practice, this integration is already validated through partnerships with industry leading EDR solutions such as Microsoft Defender and CrowdStrike Falcon, where GPU-accelerated telemetry helps increase detection fidelity while lowering CPU utilization.

Intel vPro also incorporates Intel Control-Flow Enforcement Technology (CET) to defend against return-oriented programming (ROP) and jump-oriented programming (JOP) exploits, frequent vectors in memory corruption attacks. In our lab, we validated GPU offload with Intel TDT during Microsoft Defender scans, observing active telemetry reporting through the Intel Hardware Shield framework. These protections are pre-configured by OEMs and integrate with Windows security services, minimizing the risk of misconfiguration while strengthening overall fleet resilience.

Intel documentation and the enterprise implementation guide we have covered in the first paper in our Intel vPro series both highlight how organizations can verify these capabilities. In our lab, we verified GPU offload with Intel TDT during file scanning (as shown in the screenshot on the right).



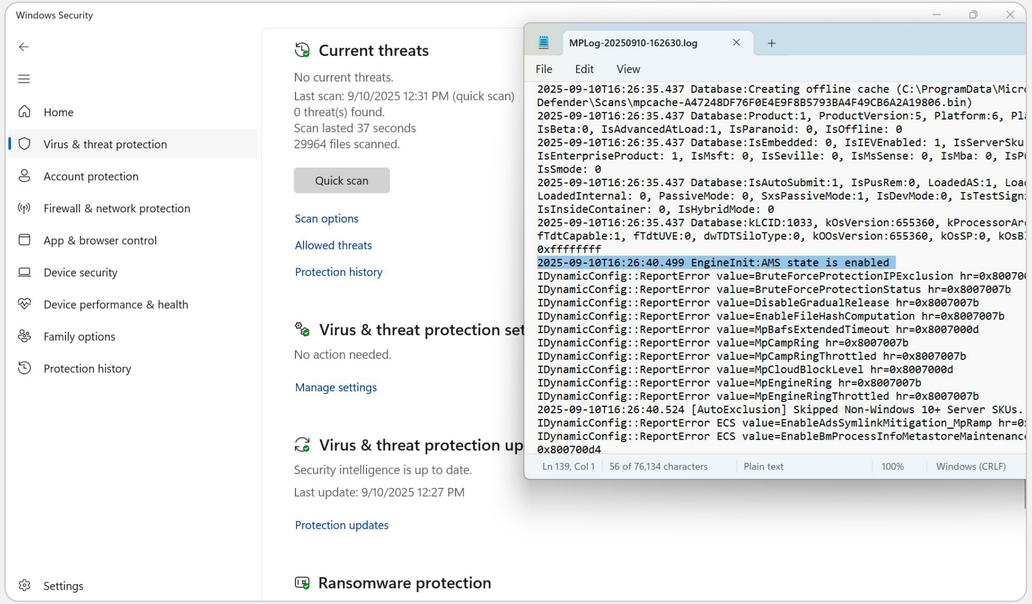



**See the Memory Protection section in the Appendix for references.**

Security Advantage: Comprehensive Enterprise Protection Anchored in Silicon

# Memory Protection (cont.)

The screenshot below shows the Intel Accelerated Memory Scanning state enabled during Microsoft Defender file scanning.




AMD does not currently provide GPU-based scanning offload or CET-class protections, relying primarily on CPU-only methods that create a trade-off between protection and productivity.

**Why It Matters:** Hardware-assisted memory protections – validated with CrowdStrike and Microsoft – help organizations scale AI and security workloads without sacrificing performance, keeping users productive while closing critical exploit paths.



**See the Memory Protection section in the Appendix for references.**

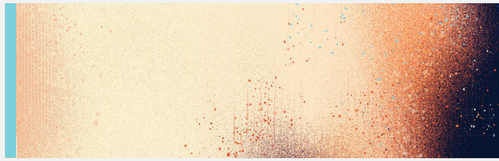
Security Advantage: Comprehensive Enterprise Protection Anchored in Silicon

## AI for Threat Detection

Intel extends its AI advantage into endpoint security with Intel TDT, which applies machine learning models to low-level CPU telemetry to identify patterns associated with ransomware, cryptojacking, and advanced persistent threats. Operating below the OS, this telemetry path is far less susceptible to tampering than software-based agents, ensuring higher fidelity alerts and faster response times. Intel Dynamic Application Loader (DAL) and Intel Security Engine integration enable ISVs to deploy additional AI-driven analytics directly onto the platform, creating a security ecosystem that evolves as threats do.

These silicon-level defenses not only improve detection accuracy but also shorten attacker dwell time—a critical factor in limiting business disruption and compliance risk. Because processing is anchored in hardware and often offloaded to integrated GPU resources, enterprises gain stronger protection without incurring significant performance penalties. For example, TDT-RSW has been found to add a 24% detection assist for EDRs over software alone. In addition, TDT-RSW was shown to catch 91% of RSW attacks vs. none for AMD.

**Why It Matters:** By embedding AI threat detection into the platform itself, Intel vPro delivers proactive defense against evolving attacks – closing gaps that software-only solutions cannot reliably address.





**See the AI for Threat Detection section in the Appendix for references.**

# Intel Ultra 200V Series and Intel vPro: the Complete Solution for Enterprise PC Deployments

Intel vPro technology represents the culmination of nearly two decades of enterprise-focused innovation, establishing Intel as the definitive leader in commercial PC management and security solutions. The comprehensive validation of Intel's approach is demonstrated through the platform's widespread adoption across Fortune 500 enterprises, government agencies, and organizations requiring the highest levels of security and manageability. Unlike competing x86 solutions that rely primarily on software-based management tools, Intel vPro's hardware-integrated approach provides unparalleled reliability and security through features such as Intel AMT's out-of-band management capabilities, hardware-based attestation, and firmware-level security enforcement that operates independently of the host operating system. This architectural advantage becomes particularly evident during critical failure scenarios, where Intel vPro-enabled systems can achieve full recovery in days rather than weeks, as demonstrated by recent industry events. Our hands-on analysis demonstrates the real-world benefits of Intel vPro technology, including true out-of-band management capabilities through Intel AMT, **for both system administrators and end users.**

The superiority of Intel's enterprise computing ecosystem extends beyond management and security capabilities to encompass fundamental performance and efficiency advantages, as evidenced by comprehensive analysis of the Intel Core Ultra 200V series processors detailed in our companion paper. These findings demonstrate Intel's continued leadership in delivering superior performance-per-watt ratios and extended battery life compared to competing x86 architectures, ensuring that enterprise organizations receive optimal productivity outcomes alongside advanced management capabilities. The convergence of Intel vPro's comprehensive security and management features with the proven performance advantages of Intel's latest processor architectures reinforces the strategic value proposition for enterprises seeking a unified, validated platform that addresses both current operational requirements and future scalability demands across their distributed computing environments. The implementation guide we covered in our first paper in the series further demonstrates Intel's commitment to the success of commercial deployments and the ongoing experience of both system administrators and end users. The Intel Core Ultra 200V series with Intel vPro technology offers a compelling value proposition and the best choice for organizations across deployment, manageability, security, performance, and battery life.

# Appendix

## References


### Security Ecosystem Enablement

https://community.intel.com/t5/Blogs/Tech-Innovation/Artificial-Intelligence-AI/Intel-AI-PCs-Deliver-an-Industry-Validated-Defense-vs-Real-World/post/1650954
https://center-for-threat-informed-defense.github.io/mappings-explorer/external/intel-vpro/

### Supply Chain Security & Attestation

https://www.intel.com/content/www/us/en/security/security-practices/transparent-supply-chain.html
https://www.intel.com/content/www/us/en/content-details/850997/2025-intel-assured-supply-chain-product-brief.html

### Hardware Security Engine

https://community.intel.com/t5/Blogs/Tech-Innovation/Client/Intel-Partner-Security-Engine/post/1661658
https://www.amd.com/content/dam/amd/en/documents/products/processors/technologies/amd-pro-technologies-security-white-paper.pdf

### Secure Boot & BIOS/FW Protection

https://cdrdv2-public.intel.com/819636/819636_Intel_Core_Ultra_Proc_PS_Datasheet__Rev001.pdf
https://www.content.shi.com/cms-content/accelerator/media/pdfs/intel/intel-client-solutions/intel-070723-below-the-os-security-white-paper.pdf
https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf
https://cdrdv2-public.intel.com/848494/windows-11-security-ebook.pdf
https://www.amd.com/content/dam/amd/en/documents/products/processors/technologies/amd-pro-technologies-security-white-paper.pdf

### Post-Quantum Cryptography (PQC) Readiness

https://www.intel.com/content/www/us/en/developer/articles/technical/post-quantum-cryptography.html
https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

### Memory Protection

https://www.intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-security/threat-detection-technology.html
https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2022-10/intel-total-memory-encryption-multi-key-whitepaper.pdf
https://www.intel.com/content/www/us/en/developer/articles/technical/technical-look-control-flow-enforcement-technology.html
https://www.amd.com/content/dam/amd/en/documents/products/processors/technologies/amd-pro-technologies-security-white-paper.pdf

### AI for Threat Detection

https://learn.microsoft.com/en-us/defender-endpoint/hardware-acceleration-and-mdav
https://selabs.uk/wp-content/uploads/2023/02/enterprise-advanced-security-ransomware-intel-threat-detection-technology-2023-02.pdf

# Important Information About this Report

**Contact Information**
Signal65 | signal65.com | info@signal65.com

## Contributors

**Cameron Moccari**
Operations Director and Client Testing Analyst - Signal65
**Ryan Shrout**
President & GM - Signal65
**Ken Addison**
Client Performance Director - Signal65

## Inquiries

Contact us if you would like to discuss this report and Signal65 will respond promptly.

## Citations

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "Signal65." Non-press and non-analysts must receive prior written permission by Signal65 for any citations.

## Licensing



## Disclosures

Signal65 provides research, analysis, advising, and lab services to many high-tech companies, including those mentioned in this paper. Research of this document was commissioned by Intel.

## Commissioned by:

intel

## About Signal65

Signal65 exists to be a source of data in a world where technology markets and product landscapes create complex and distorted views of product truth. We strive to provide honest and comprehensive feedback and analysis for our clients in order for them to better understand their own competitive positioning and create optimal opportunities to market and message their devices and services.

signal65


signal65