Intel vPro® with Microsoft: the endpoint foundation for security, management and AI

The pressure on endpoint estates

IT leaders are managing more devices across more locations than the estate was designed for. Hybrid work distributed the fleet. The end of Windows 10 support created a hard deadline. AI is introducing hardware requirements that most existing devices don't meet.

The refresh happening now is the largest in a decade. Budgets are fixed and timelines are short. The decision is how much operational improvement to extract from it beyond the hardware itself.

What Intel vPro® delivers

Out-of-band management

Intel vPro® is a platform-level capability set built into the processor. It operates below and independently of the OS.

Intel AMT enables remote access to devices regardless of power state or OS health. Crashed, powered off or stuck in a boot loop: IT can still reach the machine, access the BIOS, recover the OS or reimage remotely.

The July 2024 CrowdStrike outage tested this at scale. Approximately 8.5 million Windows devices crashed from a faulty update. Organisations with AMT-enabled fleets recovered in hours. BLG, Canada's largest law firm, used Intel's endpoint management tools as part of their incident response. Banorte, Mexico's largest bank, resolved the issue across its fleet without dispatching technicians. Organisations without out-of-band access spent days on manual remediation.

Intel vPro® Fleet Services, available since 2025, surfaces AMT capabilities directly inside the Intune admin centre as a cloud-native service. No self-hosted servers. Activation reduced from 24 steps to six. Authenticated via Entra ID SSO. No extra infrastructure or licensing.

Separately, Intel® Endpoint Cloud Services provide access to vPro manageability through existing commercial tools from HP Workforce Solutions, Ivanti, Omnissa and CrowdStrike. Two routes to the same below-the-OS access, depending on the tooling already in place.

Silicon-level security

- Intel Hardware Shield mitigates firmware-level attacks and reduces the device attack surface before the OS loads.
- Intel TDT feeds silicon-level threat telemetry into endpoint protection tools including Defender.
- Up to 7x improved memory scanning performance through Intel TDT. 24% better ransomware detection efficacy.
- Three times fewer firmware vulnerabilities than the nearest competitor. 150 active mitigations across the platform.
- Intel and Microsoft co-engineered 30 silicon security features into Windows 11.
- vPro Enterprise devices exceed Secured-core PC requirements.
- Intel remains the only silicon provider with hardware security validated against MITRE ATT&CK.

All enquiries online@scc.com
Contact our team 0121 766 7000
Visit scc.com

scc | intel. | Windows 11 | Copilot+PC

Intel vPro® with Microsoft: the endpoint foundation for security, management and AI

Platform stability

The Intel® Stable IT Platform Programme holds hardware component consistency for at least 15 months from launch. Application compatibility is validated at 99.7% across OS versions. That reduces the overhead of deployment waves, driver validation and OS transitions on large estates.

vPro has been the enterprise PC standard for 20 years. The management tooling, support processes and partner familiarity are well established.

How Microsoft fits in

vPro® operates within the Microsoft environment most organisations already run.

With Fleet Services now embedded in the Intune admin centre, the management plane extends from cloud policy down to the hardware. Entra ID handles authentication and conditional access. Defender provides endpoint protection at the OS and application level, alongside Intel TDT at the silicon level.

Copilot+ PC features require a minimum 40 TOPS NPU. Intel Core Ultra Series 3 processors with vPro deliver up to ~50 NPU TOPS, meeting this requirement. Total platform performance can reach ~180 TOPS across CPU, GPU and NPU, although Copilot+ features are driven specifically by NPU capability.

Local inference capabilities, including large language models up to ~70 billion parameters with 32K context, depend on model optimisation, available memory, and runtime environment rather than representing a guaranteed baseline.

Outcomes

Designed for direct extraction into battle cards.

Reduced support costs

A Forrester TEI study commissioned by Intel, based on 500 IT decision-makers, modelled a composite 10,000-employee organisation. The findings: 213% ROI over three years. Benefits of $4.32 million against costs of $1.38 million. 90% reduction in hardware-related on-site visits. 65% less time on device management. Up to 368,000 kg less CO_2 over three years from avoided travel.

Faster crisis recovery

The 2024 CrowdStrike outage demonstrated the operational gap between fleets with out-of-band access and those without. Organisations with vPro recovered distributed estates in hours through remote remediation. Those relying on software-only management spent days on manual intervention.

Stronger security posture

Hardware-rooted security validated against MITRE ATT&CK. Three times fewer firmware vulnerabilities than the competition. Up to 7x faster memory scanning via Intel TDT. 24% better ransomware detection. 30 co-engineered silicon security features in Windows 11. 150 active platform mitigations.

Intel vPro® with Microsoft: the endpoint foundation for security, management and AI

AI readiness

Up to 50 NPU TOPS, exceeding the 40 TOPS required for Copilot+ PC. Up to 180 total TOPS across CPU, GPU and NPU. 99% AI application compatibility. Over 200 ISVs delivering AI workloads on the platform. 30% higher token rate on MLPerf Client V0.5 versus the competition.

Performance and sustainability

Up to 20% more productivity performance versus a three-year-old PC. Up to 5x faster wireless and 4x faster wired connectivity. Battery life up to 27 hours on the latest processors. A single remote support session via vPro can save carbon equivalent to up to two years of PC use. 95% of vPro devices registered on EPEAT achieve Silver or better. Intel® Platform Service Record provides device usage and event data to support residual value and reuse decisions.

How SCC helps

SCC is OEM-agnostic. We work with Dell, HP, Lenovo and every major manufacturer. We advise on the right device for the environment, the user profile and the budget.

Procurement and supply chain.

The full range of vPro-enabled enterprise devices across every major OEM.
Volume pricing, configuration and logistics.

Deployment.

Zero-touch provisioning through Autopilot and Intune.
Devices enrolled and policy-compliant before they reach the user.

Managed endpoint services.

Ongoing management, patching, security monitoring and hardware-level support through vPro.

Financing and lifecycle.

Flexible models including device-as-a-service.
Phased refresh, cost management and residual value planning.

Copilot readiness.

Licensing guidance, governance planning and deployment support for Microsoft 365 Copilot.

Next step – Call this out

Talk to an SCC specialist about your device refresh and endpoint strategy.

All enquiries online@scc.com
Contact our team 0121 766 7000
Visit scc.com

scc | intel. | Windows 11 | Copilot+PC