PROWESS

Which Hardware Platform Best Protects Client PCs?

Software alone can't defend against modern threats. To help you determine the safer choice for your business, Prowess compared the security features built into Intel® Core™ vPro® mobile processors and AMD Ryzen™ PRO processors.

Modern attacks increasingly target vulnerabilities below the operating system (OS), beyond the view of antivirus software. Only hardware-based security can defend against these threats, so it is now imperative that IT decision-makers (ITDMs) consider the security features built into the hardware before purchasing PCs.

The client hardware platform, and especially the CPU, can uniquely offer a number of security protections against below-the-OS attacks. For example, the processor can initiate integrity checks that help ensure the safety of the firmware and also include features designed to thwart any attempts to bypass this security. The CPU can also help protect against attacks that use assembly language to manipulate the execution stack in ways that software cannot. CPUs can also be built with telemetry capabilities that expose low-level statistics about usage; software can then use these capabilities to detect behavior that is typical of ransomware and other attacks. Finally, built-in CPU capabilities can use encryption to protect system memory.

What We Found: Intel Core vPro Processors Deliver a More Complete Defense

To help ITDMs determine which client platform offers a more secure foundation for business PCs, Prowess compared the security features in 11th Generation Intel® Core™ vPro® mobile processors and AMD Ryzen™ PRO 4000 Series processors. Our conclusion? Intel Core vPro mobile processors offer a more comprehensive and layered security model.

Client PCs need a comprehensive security model rooted in hardware.

Hardware features, such as the ability to collect telemetry data, can provide extra layers of defense against modern threats.

Prowess found that Intel® Core™ vPro® processors deliver more complete protection from modern attacks.

Intel® Processor–Based Client Security Advantages Compared to AMD® Processors

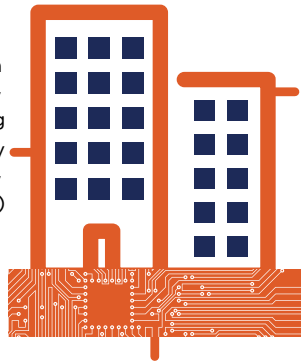
We found the security capabilities shown in this table were available on 11th Generation Intel® Core™ vPro® mobile processors, but not in the latest AMD Ryzen™ PRO 4000 Series processors.

Security Capability or Feature	Intel® Core™ vPro® Mobile Processors	AMD Ryzen™ PRO 4000 Series Processors
Protection against control-flow attacks	✓	✗
Comprehensive program to help ensure platform integrity throughout the entire compute lifecycle	✓	✗
Use of hardware telemetry and acceleration capabilities to help identify threats	✓	✗
Platform-recovery capabilities to help increase the adoption of firmware updates	✓	✗
Comprehensive restrictions on system management mode (SMM)	✓	✗

Hardware-Based Security Features Unique to the Intel vPro® Platform

In our investigation, we found no security capabilities in the AMD Ryzen PRO 4000 Series CPUs that were not also present in 11th Generation Intel Core vPro mobile processors. But importantly, we did find a number of security features that were exclusive to the Intel vPro® platform, including the following:

- **Intel® Control-flow Enforcement Technology (Intel® CET).** Uses integrity checks to protect the execution stack from tampering in control-flow programming attacks.
- **Compute Lifecycle Assurance (CLA).** A wide-ranging program to protect the integrity of system components throughout their lifecycles.
- **Intel® Threat Detection Technology (Intel® TDT).** A set of features that uses hardware capabilities to help detect malware. These features include Advanced Platform Telemetry, which uses machine learning (ML)-based runtime algorithms to detect behavior consistent with cryptomining or ransomware. They also include Accelerated Memory Scanning, which enables anti-malware software to do more scans, faster, by offloading work to the on-board Intel graphics processing unit (GPU).
- **Intel® Runtime BIOS Resilience, Intel® System Resources Defense, and Intel® System Security Report.** These features work together to restrict SMM and report the restrictions to the OS for visibility. (SMM is a privileged execution mode of the processor that is invisible to the OS and is a potential basis for firmware attacks).
- **Intel Firmware Update/Recovery.** This feature encourages adoption of firmware updates by providing resiliency from flash corruption errors and bad firmware updates. It also allows a system to recover to a last known-good firmware image.



Advanced Threat Detection

Intel® Threat Detection Technology (Intel® TDT)—Accelerated Memory Scanning

Intel TDT—Advanced Platform Telemetry

Intel® Control-flow Enforcement Technology (Intel® CET)

App and Data Protection

Intel® Virtualization Technology (Intel® VT-x)

Intel® Virtualization Technology for Directed I/O (Intel® VT-d)

Intel® APIC Virtualization

Mode-Based Execution Control

Intel® AES New Instructions (Intel® AES-NI)

Intel® Total Memory Encryption

Below-the-OS Security

Intel® BIOS Guard

Intel® Boot Guard

Intel® Platform Trust Technology (Intel® PTT)

Intel® Trusted Execution Technology (Intel® TXT)

Intel® Runtime BIOS Resilience

Intel® System Security Report

Intel® System Resources Defense

Intel Firmware Update/Recovery

Intel® Transparent Supply Chain

Intel® Trusted Device Setup

Figure 1. Hardware-based security features in Intel® Core™ vPro® mobile processors

Intel vPro Platform Delivers Full-Scale Protection

Intel delivers a multi-layered defense against attacks that are not detectable through traditional software-based strategies. It offers clear security advantages over AMD in capabilities such as telemetry-based threat detection, the CLA program, Intel CET, and firmware resiliency.

The security landscape today includes a growing number of attacks that target clients below the OS, so it's important to choose client PCs with hardware-based protections against these threats. In our study, we found that 11th Generation Intel Core vPro mobile processors include a number of unique capabilities that make them especially well-suited to protect clients from modern exploits below the OS.

Learn More

Download the full paper: https://prowesscorp.com/project/client-security-showdown

For more information about the hardware-based security in Intel Core vPro mobile processors, see "A New Level of Built-in PC Security."

The analysis in this document was done by Prowess Consulting and commissioned by Intel.