PROWESS

Client Security Showdown: Intel® Core™ vPro® Mobile Processors vs. AMD Ryzen™ PRO CPUs

Which client processors provide the security foundation your business needs?

Your Client PCs Need Hardware-Based Protection

Until recently, CIOs could plan and define their cybersecurity strategies separately from their client-PC purchasing decisions, but those days are now gone. PCs today need a multi-layered approach to security that is rooted in hardware. If adequate security isn't built into client systems from the CPU upwards, no amount of software can later fix that fundamental weakness.

Below-the-OS Attacks

The most direct reason for this change is that malware attacks are increasingly targeting the system below the operating system (OS), making them "undetectable" to applications that run above the OS. For example, the recently reported TrickBot botnet seeks out and exploits firmware vulnerabilities.[1]

To block attacks such as these, that take aim below the OS, organizations need a comprehensive security model rooted in hardware. First, the integrity of the hardware must be validated to establish a root of trust. The hardware must then adequately defend the firmware against tampering and attest to its integrity. Acting through the established chain of trust, the authenticated firmware must then adequately protect the operating system and hypervisor and attest to their integrity. Only then does software have a chance to protect the operating system and the applications that run on top of it.

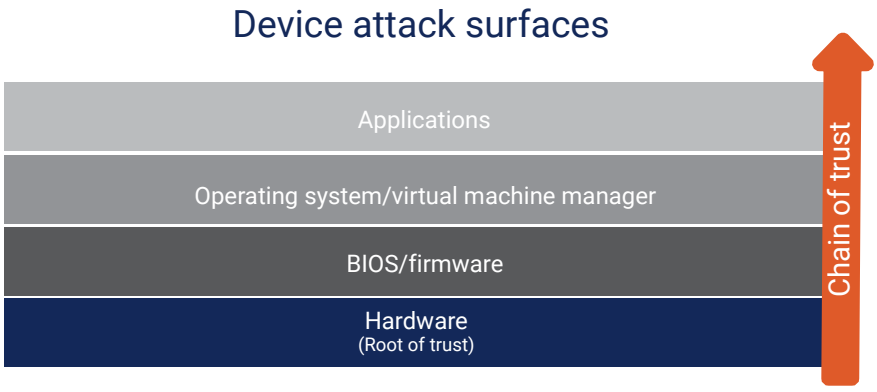

Figure 1. Effective client protection must be based on a secure hardware foundation

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

Highlights

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® mobile processors deliver more robust protection from attacks.

Additional Malware Protection Through Hardware-Based Detection

Another reason why hardware-based security is needed for business PCs is to provide additional protection against attacks that produce distinctive signatures in hardware activity. Hardware-based security features, such as CPU telemetry–based detection through machine learning (ML), can offer a second line of defense against malware that otherwise would escape detection by antivirus (AV) software.

Ransomware offers an urgent example. 56 percent of organizations reportedly suffered a ransomware attack in the last year.[2] Ransoms paid for ransomware attacks averaged 1.1M US dollars (USD) in late 2020, and they have recently been reported as high as 34M USD.[2,3] These exploits are no mere nuisance; they're now potentially an existential threat to business.

Ransomware also produces cryptographic activity that can potentially be detected through hardware telemetry. As a result, some ransomware attacks can be thwarted before they can completely encrypt a system's files. But this crucial extra layer of defense relies on features built directly into the CPU. For your client PCs to benefit from telemetry-based protection, you need to make sure that they are equipped with CPUs that support this capability out of the box.

Is All Hardware-Based Security the Same?

Client platforms need hardware-based protection against modern attacks. Given the nearly undetectable nature of many of today's threats and the severity of the damage that they can cause, it's critical that you investigate the security features available on the hardware platform of any client PCs you might purchase.

To this end, Prowess has done some of the legwork for you. To help you understand the security differences between vendors and help you make an informed decision about which client PCs to buy, we conducted research comparing the hardware-based security features of two families of CPUs that are commonly used for business client platforms: Intel® Core™ vPro® mobile processors and AMD Ryzen™ PRO 4000 Series processors.

What We Found: The Intel Core vPro Platform Delivers a More Complete Defense

Our conclusion? Both Intel Core vPro mobile processors and AMD Ryzen PRO 4000 Series processors include crucial security features, but the latest available Intel vPro® platform–based mobile processors, 11th Generation Intel Core vPro mobile processors, deliver a more comprehensive and layered security model than the most recent AMD Ryzen PRO processors. We also found that Intel security features are documented in far more detail, along with the company's overall security strategy. This gave us more confidence that the Intel security approach in practice was similarly thorough and well-considered.

In particular, we found the security capabilities shown in Table 1 were available on 11th Generation Intel Core vPro mobile processors, but not in the latest AMD Ryzen PRO 4000 Series processors.

Table 1. Security capabilities and features found on Intel® Core™ vPro® mobile processors and not on 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	✓ (Intel® Control-flow Enforcement Technology [Intel® CET])	✗
Comprehensive program to help ensure platform integrity throughout the entire compute lifecycle	✓ (Compute Lifecycle Assurance [CLA])	✗
Use of hardware telemetry and acceleration capabilities to help identify threats and detect anomalous activity	✓ (Intel® Threat Detection Technology [Intel® TDT])	✗
Feature that blocks modification of system memory policy during runtime	✓ (Intel® Runtime BIOS Resilience)	✗
Feature that ensures least-privileged access for System Management Mode (SMM) to critical system resources	✓ (Intel® System Resources Defense)	✗
Feature that provides visibility for the OS to determine which system resources can be accessed from within SMM	✓ (Intel® System Security Report)	✗
Platform-recovery capabilities to help increase the adoption of firmware updates without fear of bricking the system	✓ (Intel Firmware Update/Recovery)	✗

The following section gives more details about the security capabilities listed in Table 1.

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

As we investigated the security capabilities of the 11th Generation Intel Core vPro mobile processors and AMD Ryzen PRO 4000 Series processors, we found a number of features that were unique to the Intel vPro platform.

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

This feature, which is new to 11th Generation Intel Core vPro mobile processors, helps protect against control-flow hijacking attacks. Control-flow hijacking includes return-oriented programming (ROP) and jump-oriented programming (JOP) attacks, and it aims to manipulate items in the program-execution stack in memory to eventually gain control of a system. Intel® Control-flow Enforcement Technology (Intel® CET) defends against these control-flow hijacking attacks through the use of a shadow stack, which checks the integrity of the execution stack, and an indirect branch tracking feature to block JOP attacks. (More information about the Intel CET feature is available **here**.)

At the time of this writing, AMD Ryzen PRO 4000 Series processors do not yet offer any protection against control-flow attacks.

Compute Lifecycle Assurance (CLA)

Intel has put in place a comprehensive program to help protect the integrity and security of platforms (including hardware platforms) throughout their entire lifecycles. CLA includes more assurances of design security and privacy, product support, transparency and communications, and platform updates. For example, as one small piece of the overarching CLA strategy, a framework called Transparent Supply Chain (TSC) is used to create a set of tools for PC manufacturers to help enable enterprises verify the authenticity and integrity of systems and their components. Intel also uses bug-bounty programs and security red teams as part of CLA to proactively identify and help mitigate threats to its platforms and provide remediation guidance to customers. (The benefits of this program apply to Intel vPro platform–based systems, in addition to other Intel®-based systems.)

AMD, like Intel, has bug-bounty programs to find and publicize security flaws in its platform. However, AMD has not published any information about a comprehensive approach to security for its hardware systems throughout their lifecycle.

Intel® Threat Detection Technology (Intel® TDT)

Intel® Threat Detection Technology (Intel® TDT) encapsulates a set of features that uses hardware to help improve malware detection. AMD has not yet revealed any similar capability, and in this age of ransomware and stealth cryptominers, the feature—in our view—represents a significant advantage for the Intel vPro platform over AMD Ryzen PRO 4000 Series processors. For now, Intel TDT includes two sub-features:

- *Advanced Platform Telemetry* uses ML-based runtime algorithms to analyze CPU usage, and it notes when behavior is consistent with malware, such as cryptomining or ransomware. It then passes a warning signal into an Intel partner's anti-malware application, which can remediate before all of a platform's files have been encrypted (in the case of ransomware) or before the hidden cryptomining app has a chance to consume so many resources that it disrupts the performance of legitimate software. Currently, Microsoft® Defender and BlackBerry® Optics both use Advanced Platform Telemetry to detect cryptomining activity.
- *Accelerated Memory Scanning (AMS)* offloads computationally intensive algorithm processing to the on-board integrated Intel graphics processing unit (GPU), which minimizes the impact on system performance. This offloading also allows the anti-malware software to perform scans quickly and more frequently. Currently, AMS can be used by Windows® Defender, SentinelOne®, and Cylance Smart Antivirus®, with support from other anti-malware applications expected soon.

System Management Mode (SMM) Security Through Intel® Runtime BIOS Resilience, Intel® System Resources Defense, and Intel® System Security Report

Intel® Runtime BIOS Resilience, Intel® System Resources Defense, and Intel® System Security Report work together to restrict System Management Mode (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. Used by firmware for many important background tasks, SMM can also be exploited to gain control of the system, and it is a potential basis for firmware attacks. Intel Runtime BIOS Resilience helps mitigate some of the dangers posed by the broad powers of SMM. It provides an enforcement mechanism for the policy determining which memory addresses SMM can access at runtime, and with which access rights. Intel System Resources Defense then extends Intel Runtime BIOS Resilience by creating least-privileged access to other critical system resources, such as model-specific registers, memory-map input/output (I/O), and more. Intel System Security Report provides visibility to the OS about whether Intel Runtime BIOS Resilience is correctly implemented, and also about which system resources are accessible from within SMM. This capability gives the OS a more accurate assessment of device security.

Collectively, these three features work alongside another feature, the cryptographically verified launch environment called Intel® Trusted Execution Technology (Intel® TXT), to help prevent attacks that exploit the powers of SMM during the boot process.

We have not been able to confirm whether AMD Ryzen PRO 4000 Series processors include these same features to limit SMM and block SMM-based exploits.

Intel Firmware Update/Recovery

Some IT departments hesitate to apply firmware updates to clients in a timely manner because of the perceived risk of bricking systems. Intel Firmware Update/Recovery is intended to address this problem by providing resiliency from flash corruption errors and bad firmware updates, in addition to the capability to recover to a last known-good firmware image.

Intel is shipping firmware resiliency for boot-critical firmware on client platforms starting with 11th Generation Intel Core mobile processors. By 2023, all firmware on Intel client systems will have complete firmware resiliency.

AMD has not published any information about similar firmware resiliency features in its AMD Ryzen PRO 4000 Series processors.

Hardware-Based Security Capabilities on Both Intel Core vPro Mobile Processors and AMD Ryzen PRO 4000 Series Processors

As part of our review of publicly-available references found on the Intel and AMD websites, we also found that 11th Generation Intel Core vPro mobile processors and AMD Ryzen PRO 4000 Series processors shared a few hardware-based security features in common:

Full Memory Encryption

AMD Ryzen PRO 4000 Series processors include a feature called **AMD Memory Guard**, which uses encryption via a single key to help protect against attacks on the integrity of main memory. With 11th Generation Intel Core vPro mobile processors, which are available in the latest client systems, Intel offers a similar feature called Total Memory Encryption (TME). TME, when enabled via BIOS configuration, helps ensure that memory accessed from the Intel CPU is encrypted, including customer credentials, encryption keys, and other intellectual property (IP) or sensitive information on the external memory bus. Memory encryption helps prevent RAM scraping attacks, cold boot attacks, and other threats that can arise when a malicious party is able to physically access a system.

Virtualization-Based Security

Virtualization-based security (VBS) is a Windows® feature that relies on hardware-virtualization (hypervisor) capabilities that are supported on both Intel and AMD® processors. Through CPU-assisted virtualization, a Windows feature called Virtual Secure Mode can isolate and protect an area of system memory to run the most sensitive and critical parts of the OS kernel and user modes, or to protect assets such as security credentials. Thanks to the protections enabled by VBS, even if malware is able to gain access to the OS kernel, the hypervisor can prevent that malware from executing code or accessing platform secrets. Virtual Secure Mode is also used to perform code-integrity checks, which enables stronger protections against kernel viruses and malware.

Dynamic Root of Trust for Measurement (DRTM)

Modern computing systems provide a degree of platform security through the Secure Boot feature of the Unified Extensible Firmware Interface (UEFI) 2.3.1 specification. (UEFI is a modern and more secure version of the system BIOS.) Through Secure Boot, the UEFI firmware uses public key cryptography to verify the digital signature of each piece of boot software, including firmware drivers and the OS. Only if the signatures are valid will the firmware allow the PC to boot and give control to the OS. Both Intel Core vPro mobile processors and AMD Ryzen PRO 4000 Series processors support UEFI Secure Boot. However, Secure Boot is not failsafe—in fact, it has been successfully compromised through malware (such as Sednit) that allows hackers to gain access to systems.[4]

Whereas UEFI Secure Boot runs only at system startup, a Dynamic Root of Trust for Measurement (DRTM) enables a second round of system validation before OS launch to help ensure that the environment has not been compromised. Intel provides a DRTM with authenticated launch through Intel TXT, and AMD provides a similar capability with the help of AMD DRTM Service Block, which is made up of the SKINIT CPU instruction, the AMD Secure Processor, and the AMD Secure Loader.

While both platforms can claim to offer a DRTM and an authenticated launch environment, this fact doesn't mean that their boot sequences are equally secure. What makes a boot process secure are the specific methods and features used to protect and verify the integrity of the environment. With this in mind, it's worth noting that Intel publishes much more detailed information about Intel TXT (see, for example, this **179-page** guide and this **8-page summary**) than AMD does about its launch environment.

Remember also that Intel includes features such as Intel Runtime BIOS Resilience and Intel System Resources Defense to protect against SMM-based attacks designed to bypass a DRTM and secure launch. Other features such as Intel® BIOS Guard and Intel® Boot Guard (both **documented here**) also help ensure a safe boot environment. More specifically, Intel

BIOS Guard helps protect the BIOS flash from modification without platform manufacturer authorization, and Intel Boot Guard verifies the integrity of the initial boot block (IBB), which executes immediately after system reset. The combination of these features enables Intel Core vPro mobile processor–based devices to provide robust below-the-OS security and a more secure launch platform for the OS.

Our Findings: The Intel vPro Platform Offers More Complete Hardware Protection for Client PCs

Overall, Intel paints a comprehensive picture of defense against below-the-OS attacks and other attacks that are not detectable through traditional software-based strategies. The completeness of this security feature set is especially significant for 11th Generation Intel Core vPro mobile processors, which have added important security features such as TME and Intel CET.

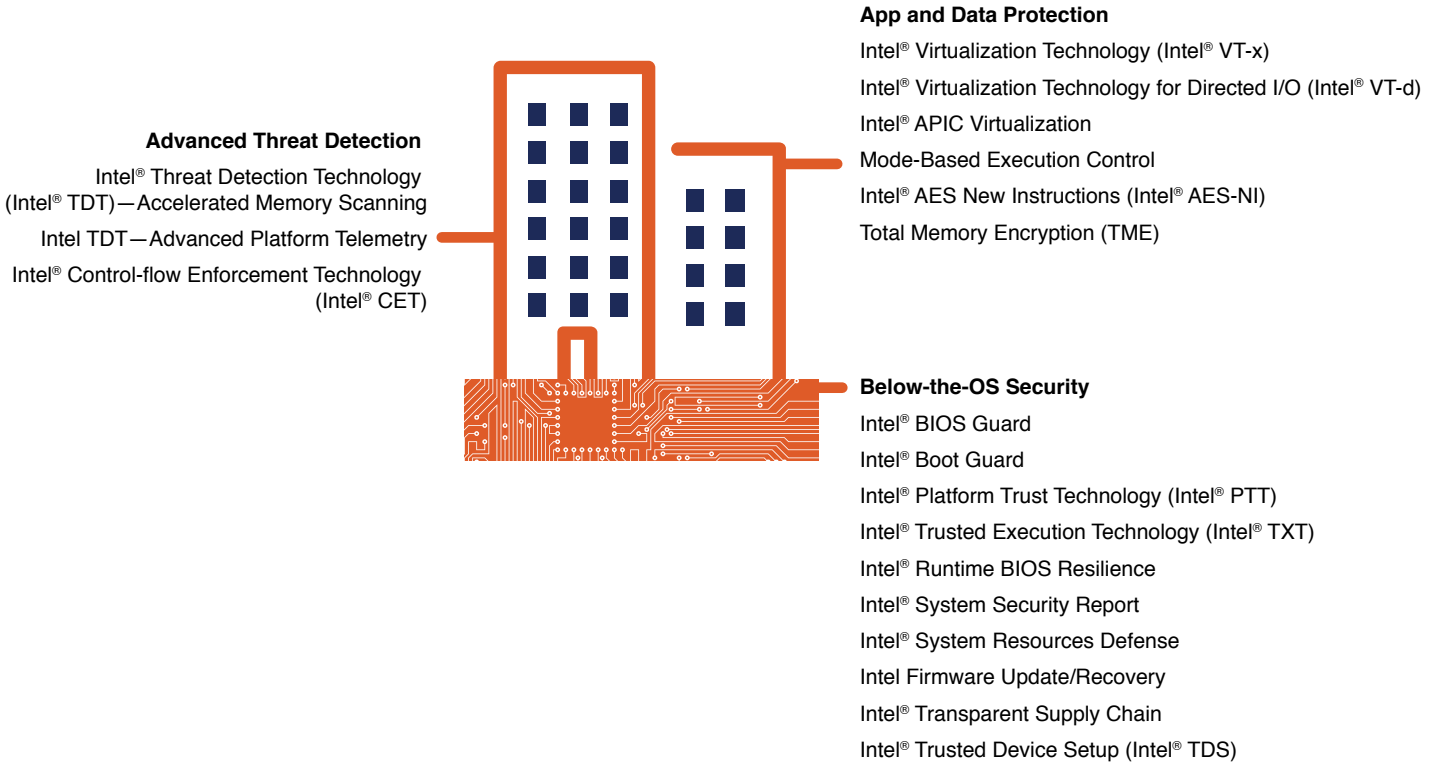

Figure 2. Hardware-based security features in Intel® Core™ vPro® mobile processors

Beyond the top-to-bottom nature of this protection, and clear security advantages over AMD in capabilities such as telemetry-based threat detection, Intel also provides much more documentation about features that address potential weaknesses in its chain of trust. This full accounting of the Intel security platform helps inspire confidence about its thoroughness and efficacy. Even better, these features require little or no configuration or setup. Intel collaborates with its OEM and OS partners to help ensure that these security features are enabled when devices ship, which makes your job easier. With so much at stake in the strength of PC defenses, we can confidently recommend 11th Generation Intel Core vPro mobile processors as a secure hardware foundation for your clients.

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

[1] Wired. “The Internet’s Most Notorious Botnet Has an Alarming New Trick.” December 2020. www.wired.com/story/trickbot-botnet-uefi-firmware/amp.

[2] Help Net Security. “56% of organizations faced a ransomware attack, many paid the ransom.” November 2020. www.helpnetsecurity.com/2020/11/20/faced-ransomware-attack/.

[3] Bleeping Computer. “Foxconn electronics giant hit by ransomware, $34 million ransom.” December 2020. www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/.

[4] MakeUseOf. “What Is UEFI And How Does It Keep You More Secure?” December 2019. www.makeuseof.com/tag/what-is-uefi-and-how-does-it-keep-you-more-secure/.