White Paper

Information Technology
Cybersecurity

Intel Virtualization Technologies Help Protect Endpoint Applications & Data without Impacting the User Experience

Hardware-based security capabilities deliver the performance required to help protect applications and data, without adversely impacting the user experience.

Intel Business Client Platform Security Marketing

Virtualization at the Endpoint

The concept of virtualization began with IBM mainframes in the late 1960s and early 1970s, supporting robust time-sharing solutions that increased the efficiency of expensive computer resources while simultaneously simplifying applications/infrastructure/operations management. Virtualization techniques abstract the physical hardware to create logical resources consisting of CPUs, memory, storage, networking, etc. and provide those resources in the form of agile, scalable, consolidated virtual machines (VMs).

Although the term "virtualization" implies datacenters and cloud services to many, and the technology continues to deliver tremendous value in those environments, today's advanced business client PC systems use virtualization for productivity, software compatibility and security, but that fact is less well-known. Because VMs are sandboxed from the rest of the client system, VMs provide complete isolation from the PC OS and other VMs—useful for strong security boundaries. The spectrum of use cases range widely, including the following:

Use Applications with Different OSs in Different VMs

In the example shown in Figure 1, the user has access to a Windows 10 VM, a Windows 7 VM for legacy applications, and a Linux subsystem VM for Ubuntu and Red Hat workloads. This flexible and extensible model supports a wide range of standard or custom applications for different types of users (such as knowledge workers and developers). There might also be several instances of the same OS, like Windows 10, to run different workloads for increased security through isolation.

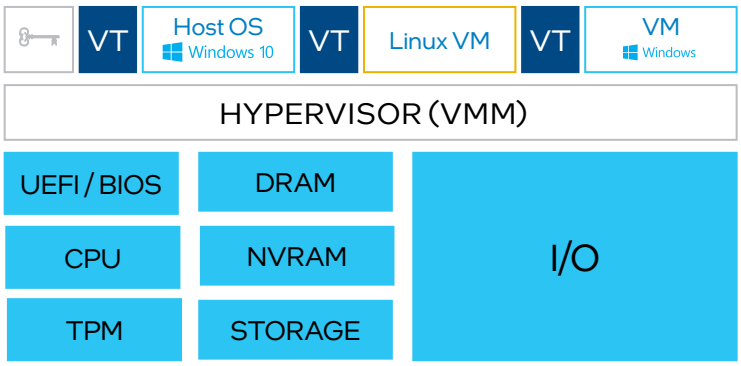


Figure 1. Virtualization helps enterprise workers achieve application compatibility and flexibility against attacks at the foundational level.

Workload isolation, enabled by the Intel® vPro platform, reduces the attack surface and the ability for malware to persist and spread across resources.

Improve Endpoint Security for Remote Workers

Isolating employees' personal and work use helps prevent business data from being exfiltrated and helps protect businesses from vulnerabilities due to personal use of social media and browsing—especially valuable as the number of remote workers continues to grow, and many organizations expect an increase in personal use of work PCs. Use cases where this approach may be most valuable include scenarios when employees and systems need to comply with industry standards and regulations like the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI) standards (see Figure 2).

Isolate Work & Personal Use

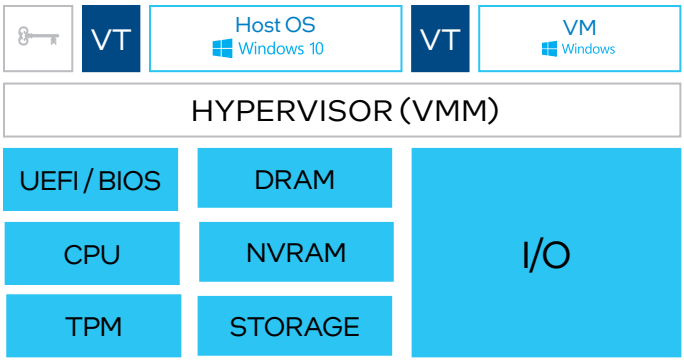


Figure 2. Virtualization helps create isolated VMs for work and personal use.

In this example, the two VMs might be running the same operating system, but one is dedicated to working with applications like SAP solutions, and the other is dedicated to working with social media and other personal applications. (PCI) standards (see Figure 2).

Virtualize Multiple Gigs

Gig workers have another reason to isolate workloads on the same PC. Virtualization supports separate workspaces for multiple gigs with private and confidential transactions, built-in security capabilities, and the right performance and user experience. Consider a psychologist contracting with different hospitals and government agencies who need to ensure that they meet the compliance requirements for each of their clients. With virtualized workloads, they can do multiple jobs on the same PC (see Figure 3).

Support Separate Workspaces for Multiple Gigs

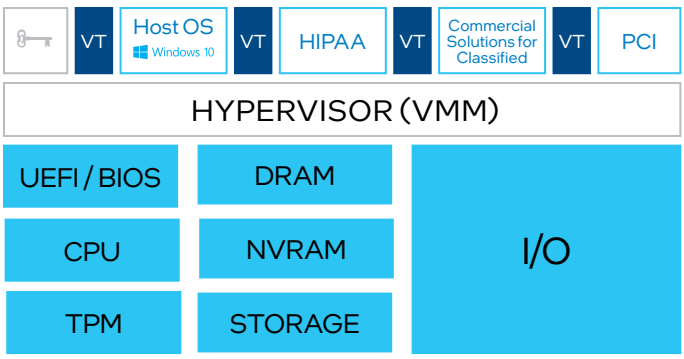


Figure 3. Gig worker with one machine but multiple jobs and personas

Recover Faster

The growing sophistication and ubiquity of cyberattacks means that it's not a question of if, but when any given system will be attacked. When such attacks occur, a primary concern is how fast you can get your systems back up and running. Virtualization supports rapid resiliency. For the virtualized workloads that are compromised, the goal is to quickly resolve matters without impacting other workloads on the same system. Having independently isolated workspaces can help reduce support costs and the overall cost of maintenance.

Increase and Accelerate Security Protection with Intel Virtualization Technology

From a business client endpoint perspective, virtualization lets organizations re-think productivity and security. Virtualization solutions allow multiple operating systems (OSs) and applications to run in independent partitions on a single computer. Using these capabilities, one physical computer system can function as multiple virtual systems. That enables isolation of workloads, reducing the opportunity for malware to easily spread, and enabling the use of hardened VMs for improved protection of credentials and other secrets, as well as for running entire workloads (browsers, applications, entire IT workspaces) in separate VMs.

Intel Virtualization Technology

Intel VT-x supports virtualization of platforms based on Intel processors, enabling the running of multiple OSs and applications in independent partitions. The virtualized platform allows for the PC to support usages for activity partitioning, workload isolation, embedded management, legacy software migration, and disaster recovery.

Hardware support for processor virtualization enables simple, robust and reliable virtual machine management (VMM) software. VMM software relies on hardware support on operational details for the handling of events, exceptions, and resources allocated to VMs. Intel VT-x provides hardware support for processor virtualization. For Intel vPro platform endpoints, this support consists of a set of VM extensions (VMX) that support virtualization of processor hardware for multiple software environments by using VMs.

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

A general requirement for I/O virtualization models is the ability to isolate and restrict device accesses to the resources owned by the partition managing the device. Intel® VT-d provides VMM software with the following capabilities:

- **I/O device assignment:** for flexibly assigning I/O devices to VMs and extending the protection and isolation properties of VMs for I/O operations.
- **Direct Memory Access (DMA) remapping:** for supporting address translations for DMA from devices.
- **Interrupt remapping:** for supporting isolation and routing of interrupts from devices and external interrupt controllers to appropriate VMs.
- **Interrupt posting:** for supporting direct delivery of virtual interrupts from devices and external interrupt controllers to virtual processors.
- **Reliability:** for recording and reporting of DMA and interrupt errors to system software that may otherwise corrupt memory or impact VM isolation.

Intel® VT-Redirect Protection (Intel® VT-rp) – Help Protect Against Kernel Memory Corruption and Page Table Attacks

Malicious attacks on the OS kernel and the page tables threaten applications and data across the platform and beyond. Intel VT-rp delivers hardware acceleration for an otherwise performance-intensive attack mitigation.

Through enhancements to the paging architecture, Intel VT-rp accelerates the use of trusted page tables. These trusted page tables are created by a hypervisor or virtual machine monitor (VMM) to enforce guest linear to physical page translations.

Intel VT-rp comprises three related components: a Hypervisor-managed Linear Address Translation (HLAT) mechanism, a new Extended Page Table (EPT) control bit called "paging-write", and another new EPT control bit called "verify guest paging." Intel VT-rp enables the VMM to ensure the integrity of guest linear to physical translations, greatly limiting an entire class of attacks commonly found in rootkits. Intel VT-rp is available on 12th gen Intel vPro platforms, but has not been enabled in any mainstream OS yet. Intel will make an announcement when Intel TV-rp is enabled.

Kernel DMA Protection

DMA-capable devices can read and write to system memory without having to engage the system processor. Once, these devices existed only inside the PC, but today, hot plug PCIe ports such as Thunderbolt™ technology give modern PCs greater extensibility.

To help protect data flowing to and from such devices, Intel VT-d provides the foundation for solutions such as Kernel DMA Protection on Microsoft Windows 10 (1803 and above). In addition, Intel VT-d based security has been supported on Mac OS since version 10.8.2 and on Linux since Kernel version 4.21. All these solutions block peripheral devices from unauthorized access to system memory.

Mode-Based Execution Control (MBEC)

MBEC virtualization provides an extra layer of protection from malware attacks in a virtualized environment. It enables hypervisors to more reliably and efficiently verify and enforce the integrity of kernel-level code.

MBEC provides finer-grain control on execute permissions to help protect the integrity of system code from malicious changes. It provides additional refinement within the Extended Page Tables by turning the Execute Enable (X) permission bit into two options: XU for user pages, and XS for supervisor pages. The CPU selects one or the other based on permission of the guest page and maintains an invariant for every page that does not allow it to be both writable and supervisor-executable at the same time. This feature enables hypervisor code integrity to share the page table between kernel and user mode without causing VMExits, which cause a large performance impact when processing unsigned user mode code. The value of the XU/XS bits is delivered through the hypervisor, so hypervisor support is necessary.

Advanced Programmable Interrupt Controller Virtualization

To virtualize interrupt delivery to virtual processors, the hypervisor uses a synthetic interrupt controller (SynIC)—an extension of a virtualized local Advanced Programmable Interrupt Controller (APIC)—a circuit that handles the priority of interrupts in a computer. Each virtual processor has a local APIC instance with the SynIC extensions. These extensions provide a simple inter-partition communication mechanism. Interrupts delivered are either external and internal. External interrupts originate from other partitions or devices, and internal interrupts originate from within the partition itself.

Interrupt delivery requires the exit and reentry of VMs—typically time-consuming and a major source of overhead. To minimize that, the Intel vPro platform emulates those activities in hardware using a feature called Advanced Programmable Interrupt Controller Virtualization (APICv). APICv eliminates the VM exits triggered by privileged register access during the handling of virtual interrupts. APIC register virtualization and virtual interrupt handling eliminate a major source of virtualization overhead.

Windows Supports Intel Virtual Technology Based Security on the Intel vPro Platform

Intel vPro platform business clients exceed the secure-core PC specification by delivering hardware-based capabilities enabling greater Windows security capacity.

Secure Biometric Authentication

Biometric authentication is becoming a mainstream use case driven by Windows Hello. Securing the entire biometric datapath is important to enable mainstream adoption of biometrics which both enhances security (by elimination of passwords) and ease of use. Enabling this capability with Virtualized Trusted I/O (VTIO) helps Intel deliver greater value for eCommerce use cases.

Microsoft Windows in conjunction with Windows Hello support VTIO with a Hyper-V based secure VM infrastructure. VTIO works in conjunction with the hypervisor and trusted I/O drivers running in a secure VM (which isolates and protects I/O data via VT Extended Page Table-based memory views). VTIO protects I/O for USB/MIPI cameras used for biometric face authentication—the camera data can be securely delivered to a biometric match engine running in the secure VM (which also protects the biometric match template). Starting with version 20H1, Microsoft Windows leverages the hypervisor-based architecture (called "VSM") to support biometric authentication.

VTIO leverages Intel VT-x and Intel VT-d for virtualization acceleration, and USB dual channel Bus Device Function (BDF) / MIPI Dual Command Channel—for concurrent use of secure and non-secure cameras for USB and MIPI cameras, respectively.

Secure Biometric Authentication

On Intel vPro platform PCs, Windows Virtualization-based security (VBS) isolates a secure region of memory from the OS and increases protection from OS vulnerabilities. VBS uses many hardware-based capabilities. The hypervisor uses

Intel VT-x, VT-x2 with Extended Page Tables (EPT) and many features used for performance optimization and security. For example, VBS uses Intel VT-d to accelerate advanced security capabilities and improve reliability and security through device isolation using hardware-assisted remapping. Intel VT-d also improves I/O performance and availability by direct assignment of devices. These features work in concert to enable virtualized workloads that prevent malicious code injection in the OS and protect data such as log-in credentials from direct memory access attacks and other modern threats.

Windows Virtual Secure Mode (VSM) uses Intel VT-x to protect key data and credentials (tokens) on the system's main storage drive. VSM and Intel VT-x help prevent hackers from obtaining credentials and infiltrating the enterprise infrastructure.

Beyond VSM, Windows Defender Credential Guard can isolate secrets so that only privileged system software can access them, preventing credential theft attacks. Credential Guard utilizes Intel VT-x to help protect credentials against OS kernel-level malware in Virtual Secure Mode enclaves. Credential Guard can be enabled via Microsoft Intune, Group Policy, editing the Windows Registry, or using the Device Guard and Credential Guard hardware readiness tool.

In addition, Windows includes a set of Intel VT-x enabled hardware and OS hardening technologies called Windows Defender Device Guard. A Device Guard feature called Configurable Code Integrity restricts devices to run only authorized applications. Simultaneously, a Device Guard feature called Hypervisor-Protected Code Integrity (HVCI) hardens the OS against kernel memory attacks.

Complement Virtualization with Encryption

A comprehensive approach requires hardware-based security capabilities at every layer, including the encryption of data and endpoint system memory.

Intel® Total Memory Encryption

Intel® Total Memory Encryption (Intel® TME) on 11th Gen Intel® Core™ vPro mobile platform business clients and on 12th gen Intel vPro platforms complements the virtualization security by extending protection against some physical attacks on DRAM. Intel TME helps protect against cold boot attacks by encrypting DRAM using NIST standard AES-XTS encryption. Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) are used by full disk encryption (FDE) solutions including Microsoft BitLocker and Google Chrome disk encryption to protect data at rest, allowing VMs to individually encrypt storage volumes.

Intel TME leverages Intel expertise in process/circuit design to help provide data protection through high-performance and low-power crypto circuits. It is an out-of-box capability that provides memory data protection for end users' sensitive/confidential data if their client system is lost or stolen. Hooks are available for anti-theft service to wipe out the keys for Intel TME.

Intel® Total Memory Encryption

Virtualized and containerized environments need granular, page-level memory encryption. Intel TME-MK enhances Intel TME for page-granular memory encryption through support for multiple encryption keys. The hardware-generated ephemeral key of TME, which is inaccessible by software or external interfaces, is still used to encrypt memory not specifically encrypted by software. Alternatively, Intel TME-MK also supports software-provided keys.

Intel TME-MK can effectively work with non-volatile memory and key provisioning services. It is also attestable, so that enterprises can inventory and enforce protection on their fleet. For virtualized workloads, a hypervisor can manage the keys to transparently provide memory encryption support for legacy OSs without modifications. Intel TME-MK is available starting on 12th gen Intel vPro platforms after the Windows 11 version 22H2 update. Check out the Intel TME-MK data sheet on Intel.com to learn more.

Intel Advanced Encryption Standard New Instructions

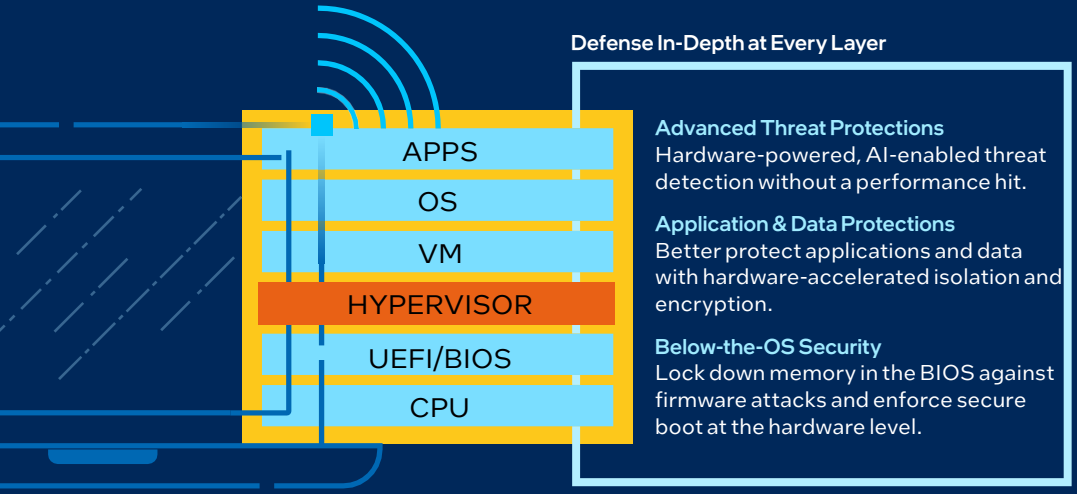
Intel AES-NI improves on the Advanced Encryption Standard (AES) algorithm and accelerates the encryption of data in the modern Intel processors for business clients and servers.

Comprised of seven new instructions, Intel AES-NI makes pervasive encryption feasible in areas where previously it was not—that gives IT environments faster, more affordable data protection, and greater security.

Intel Key Locker for ChromeOS and Linux to Help Prevent Attackers from Using System Cryptographic Keys

Attackers break-in to endpoint devices to gain access to security keys that can unlock connected data, systems and applications. Intel Key Locker helps protect AES keys on ChromeOS and Linux OS -based systems by minimizing the keys' exposure, reducing the chances they are compromised.

Intel Key Locker encrypts and decrypts data with an AES key without the raw key value being present in memory. It converts AES keys into "handles" that can perform the same encryption and decryption operations as the original AES keys, but they only work on the current system, and only until they are revoked. If software revokes Key Locker handles (e.g., on a reboot), then any previous handles can no longer be used. Once a key handle has been created, the original keys that were wrapped into those handles can be erased from memory. Intel Key Locker is available on 12th gen Intel vPro platforms for ChromeOS.



Hardware is the bedrock of any security solution, and Intel is uniquely positioned in the industry to create and deliver truly innovative hardware- based security technologies, at scale.

Figure 4. Intel® Hardware Shield is built into Intel vPro® platform business client systems to help protect against attacks at every layer.

Help Protect Endpoint Applications and Data with Intel Hardware Shield

The Intel vPro platform enables the performant execution of virtualized workloads and the protection of assets that reside in memory. The integrated platform delivers the latest PC technology in one validated solution built for both IT and end-users.

With Intel Hardware Shield, the Intel vPro platform provides hardware-based defense-in-depth to help protect every layer of the compute stack: the hardware, UEFI/BIOS, hypervisor, VMs, OS and application layers.

12th gen Intel vPro PCs feature hardware-based technologies like Intel VT-x, Intel VT-d, Intel VT-rp, Intel APICv, Intel TME and Intel AES-NI for accelerated virtualization, isolation and encryption to help protect endpoint applications, OSs and data. None of those technologies require additional hardware. Intel VT-x, Intel VT-d, Intel TME and Intel TME-MK require BIOS enabling, so IT departments should check that the UEFI/BIOS settings support them before the PCs are deployed.

Each of these Intel Hardware Shield virtualization and encryption technologies is turned "on" by default, with the exception of Intel TME—again, IT should check the UEFI/BIOS settings on 11th gen Intel vPro mobile PCs and 12th gen Intel vPro PCs.

Intel Hardware Shield Application & Data Protections Features

New on 12th Gen Intel® vPro platforms

Intel Feature	Generation Introduced	Consumer SKU?	Mobile SKU?	Intel vPro® Enterprise req't?	Intel vPro Enterprise?	Intel vPro Essentials?	Additional HW requirement? (Companion module, extra HW needed)	BIOS integration req't?	On by default?	OS enabling req't?	HW capability mapped to OS feature?	Secured core PC req't?	ISV solution needed?
Intel® Virtualization Technology (Intel® VT-x)	Pentium® 4	Y	Y	Y	Y	Y	N	Y	Y	Y	VBS, WD Credential & Application Guard,Hypervisor-Enforced Code Integrity	Y	Y, virtualization apps (e.g., VMware, VBS, HP Sure Click)
Mode Based Execution Control (MBEC)	7th Gen	Y	Y	N	Y	Y	N	N	Y	Y	Virtualization-based Security (VBS)	Y	N
Intel® VT for Directed I/O (Intel® VT-d)	5th Gen	Y	Y	Y	Y	Y	N	Y	Y	Y	VBS	N	Y, virtualization apps (e.g., VMware, VBS, HP Sure Click)
Kernel DMA Protection	9th Gen	Y	Y	N	Y	Y	N	Y	Y	N	VBS	Y	N
Advanced Programmable Interrupt Controller Virtualization (APICv)	10th Gen	Y	Y	N	Y	Y	N	N	Y	Y	VBS	Y	N
Intel® VT–Redirect Protections (Intel® VT-rp)	12th Gen	Y	Y	Y	Y	N	N	N	Y	Y	VSM Kernel Protection	Y	Y
Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)	1st Gen (Westmere)	Y	Y	N	Y	Y	N	N	Y	Y	e.g. Bitlocker	N	Y, any apps can lean on AES-NI - any other encryption application
Intel® Total Memory Encryption (Intel® TME)	11th Gen mobile	N	Y	Y	Y	Y	N	Y	N	N	N/A	N	N
Intel TME–Multi Key (Intel® TME-MK)	12th Gen	N	Y	Y	Y	N	N	Y	N	Y	Encryption for virtualization operations	N	N
Key Locker (Chrome OS only)	12th Gen	N	Y	Y	Y	N/A	N	Y	Y	Chrome OS	Y	N/A	N/A

Table 1. Intel Hardware Shield features for virtualization and encryption technologies include Intel VT-x, Intel VT-d, Intel VT-rp, MBEC, Kernel DMA Protection, Intel APICv, Intel AES-NI, Intel TME, Intel TME-MK and Key Locker.

With the exception of Intel TME, all of these technologies require OS enabling by the OS vendor. Intel AES-NI is the only one of these technologies that requires third-party security application software support—Microsoft BitLocker Drive Encryption and many other applications support Intel AES-NI.

For more information, contact your Intel sales partner.

Additional Resources

Intel vPro® Platform

- Intel.com/vPro
- Intel.com/HardwareShield
- Intel vPro Expert Center
- Enable Virtualization-Based Protection of Code Integrity
- Intel Virtualization Technology for Directed I/O Architecture Specification
- Virtual Interrupt Controller

Intel vPro

- Intel.com/vPro Platform Support
- Partners Take on a Growing Threat to IT Security

Whitepapers

- Intel® Total Memory Encryption (Intel® TME)
- Intel® Total Memory Encryption - Multi-Key

intel.

All versions of the Intel vPro® platform require an eligible Intel® Core™ processor, a supported operating system, Intel LAN and/or WLAN silicon, firmware enhancements, and other hardware and software necessary to deliver the manageability use cases, security features, system performance and stability that define the platform. See intel.com/performance-vpro for details. Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

1122/MZ/DCC/PDF