# Increasing Business Security: Windows 10 and 6th Gen Intel® Core™ vPro™ Processors

In an era of cyber intrusions, security is an essential priority for every business. To address these requirements, Microsoft has introduced Windows 10—one of the most secure versions of Windows, ever.

**Sumera Baker**
Security Consultant
MPS Cybersecurity Strategy and Information Management, George Washington University

## Introduction

Why should any business invest in Windows 10? What is the added advantage of using Windows 10 with 6th Gen and above Intel® Core™ vPro™ processors?

The simple answer is *security*. We all know that security is not absolute—even with an unlimited budget there is no guarantee that an organization won't suffer a breach. Hackers are getting smarter, and advanced persistent threat (APT) hackers with state affiliations have the resources and time to breach any network or organization.

As hackers look for zero-day exploits and social engineering opportunities, technology experts have to get smarter as well. This is why businesses need to invest in better technology and hardware that helps ensure security from the core to the application layer. This way security is present not only in applications, security tools, and perimeter firewalls, but embedded in the operating system as well.

### Windows 10 Security Benefits

Windows 10 has introduced essential security features along with Windows Defender and built-in firewall. These key features are targeted identity protection, credential cache protection, and storage protection. When combined with 6th Gen or above Intel Core vPro processor technology, these features enhance the protection for identities, data, and threats.

## Security Technologies: Microsoft

### Windows Device/Credential Guard

Microsoft has introduced Device Guard to its Windows 10 system to fight zero-day exploits and malware. Device Guard relies on Intel® Virtualization Technology for Directed I/O (Intel® VT-d) and acts like a bouncer to block zero-day attacks by vetting applications that try to access a Windows 10 machine or its network.

### Windows Hello

Windows Hello is a biometric technology that uses the face, iris, or fingerprint as password alternatives to launching Windows. Another feature of Windows Hello is the password technology called Windows Passport. Passport utilizes two-factor authentication (a biometric sensor or PIN with enrolled device) and grants password-free access to applications, websites, and networks on specific enrolled devices. This is only possible on devices that have biometric sensors, such as those based on Intel® processors and technologies.

### Windows BitLocker with Azure Rights Management

Windows 10 has also enhanced the BitLocker's ability by associating it with Azure Rights Management services and Information Rights Management (IRM) in Microsoft Office. This helps protect data through automatic encryption of corporate apps, data, emails, and website content as it arrives on devices from corporate locations or when new content is created. This feature also helps prevent copying corporate data and other sensitive information. When users create new original content, this data protection solution helps users define which documents are corporate versus personal. Companies also have the option to designate all new content created on devices as corporate by policy. Additional policies also allow organizations to prevent data from being copied from corporate content to noncorporate documents or external locations on the web, such as social networks.

### Windows Patch Management

Windows 10 Professional and Windows 10 Enterprise also provide patch management automatically and continuously to fix code and security holes.

**Protect against Modern Security Threats**

## Better Together: Identity Data and Platform Protection

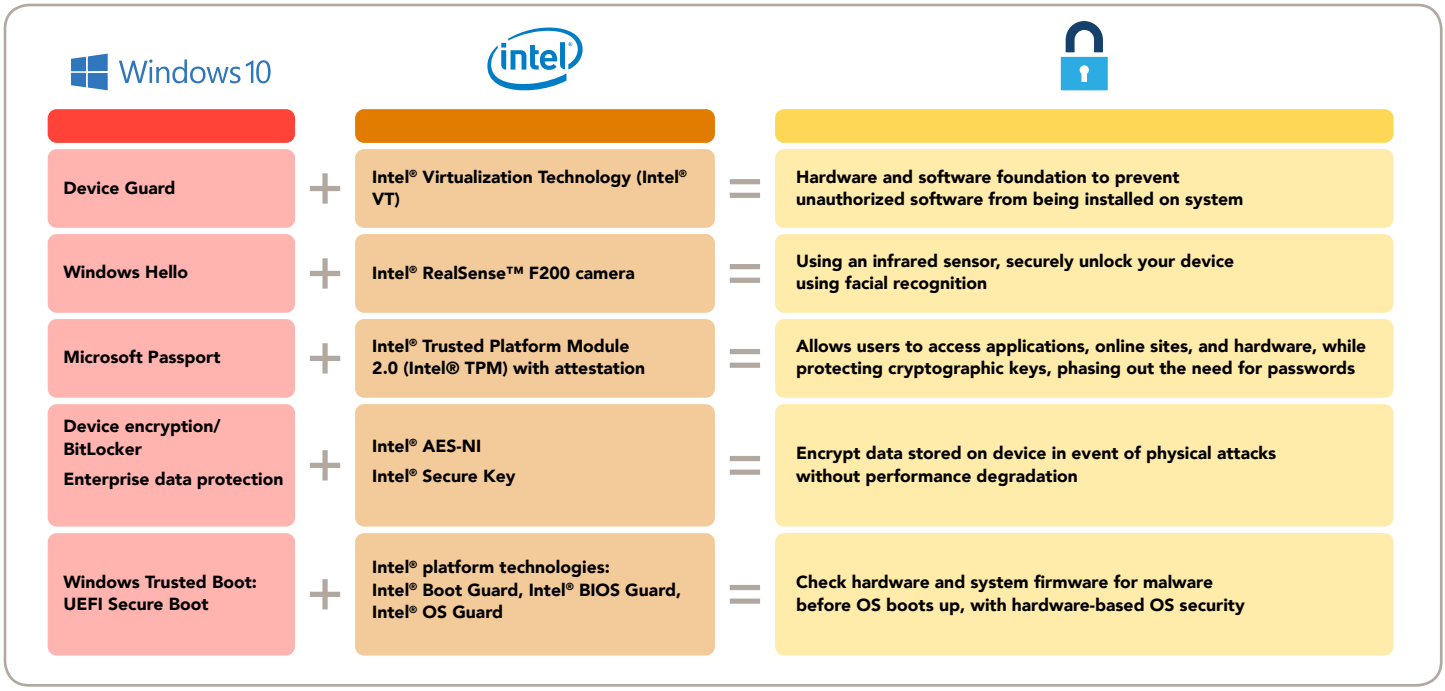


**Figure 1.** Intel and Microsoft: better together

### Windows Trusted Apps/Application Guard

Microsoft has also enhanced the Microsoft Store for Windows 10 devices. It requires apps distributed through its store to be signed by Microsoft or a trusted vendor. These signed apps are called trusted apps. Besides being vetted, these apps are sandboxed, which means that an app is partitioned in its own virtual space. If something happens, this only affects that particular app and not the whole system, making Windows 10 devices more secure.

### Windows Secure Boot

Another important security feature for Windows 10 is UEFI Secure Boot. It was created to enhance security in the preboot environment and allows only apps that are signed and trusted by administrators. This helps thwart efforts by some of the most dangerous hackers who attack computers by injecting low-level malware like rootkits during the PC boot process. The UEFI specification is an interface framework that provides firmware, operating system, and hardware providers a defense against potential malware attacks. Without UEFI Secure Boot, malware developers can easily take advantage of several preboot attack points, including the system-embedded firmware itself, as well as the interval between firmware initiation and loading the operating system.

### Windows Edge Browser

The Windows 10 system also comes with the Microsoft Edge browser designed to prevent sophisticated and prevalent attacks. The Edge provides more security by not supporting extensions that offer hackers entry through a web browser. Microsoft also adds several Edge browser security features ranging from allowing Windows to run Edge in an app controller sandbox by default (like the trusted apps in the Microsoft Store), to tightening the reins on how Edge handles website certificates. This prevents a compromised browser from giving admin-level access to the whole system.

### Windows Virtual Secure Mode

Windows 10 Enterprise and Professional editions introduce a capability called virtual secure mode (VSM) that uses a PC's CPU virtualization to protect key aspects, including data and credentials (aka tokens) on the system's hard drive. The VSM prevents the hacker from obtaining credentials and infiltrating the enterprise infrastructure. For virtualization to be enabled, the CPU has to have hardware virtualization capability, such as that in 6th Gen or above Intel Core vPro processors.

### Windows Micro-Virtualization

Microsoft partnered with Bromium to deliver micro-virtualization to Windows 10. Bromium protects PCs by automatically isolating each user's unverified tasks at the device level. It creates hardware-isolated micro-VMs that run untrusted processes without giving them access to critical parts of a PC. This helps prevent breaches that involve browser attacks, USB thumb drives, and email attachments.

## Security Technologies: Intel

### 6th Gen Intel Core vPro Processor Security Benefits

High-performing devices based on the 6th Gen Intel Core vPro processor family provide the hardware-enhanced security that enterprises demand, along with wireless convenience. New security features of Windows 10 make a compelling case for businesses to invest in this operating system. The latest Intel Core vPro processors (6th Gen and up) allow organizations to fully utilize available security features. The combined solution provides much better support for seamless and holistic security to address today's issues and threats.

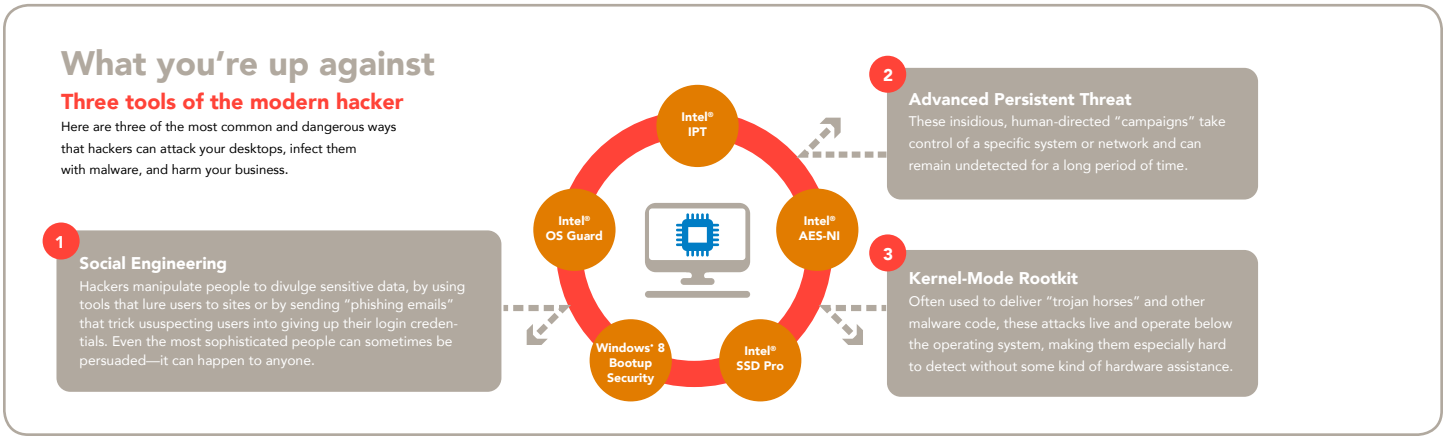


**Figure 2.** Tools of the modern hacker

### Intel® Authenticate

Intel Authenticate is a hardware-based, multifactor authentication (MFA) solution that hardens the user's PC to make unauthorized access more difficult. Intel Authenticate is designed to confirm user identity by using a combination of up to three hardened factors simultaneously. These factors include: something you know, such as a personal identification number (PIN); something you have, such as a PC or a mobile phone; and something you are, such as a fingerprint.[1]

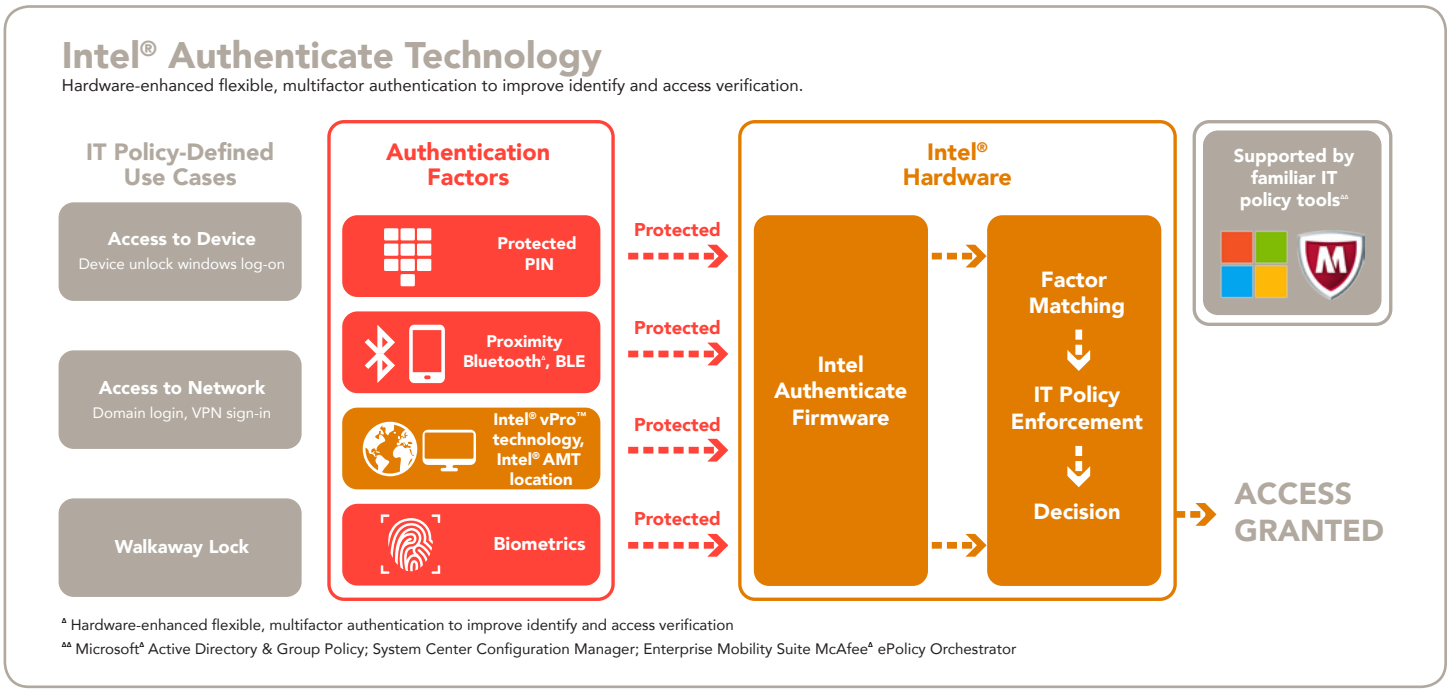


**Figure 3.** Intel® Authenticate Technology

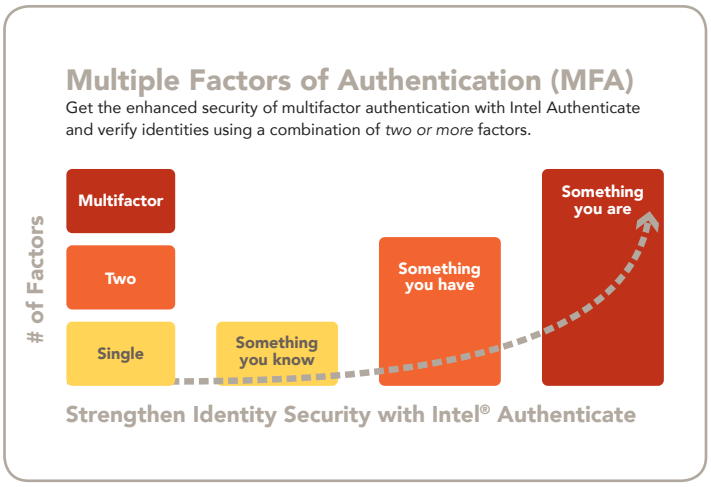


**Figure 4.** Multifactor authentication with Intel® Authenticate

### Intel® Remote Secure Erase

6th Gen Intel Core vPro processors provide hardware-enhanced security with added layers of identity safeguards. Adding Intel® Solid State Drive (Intel® SSD) Pro provides remote secure-erase capabilities, so when an employee leaves the organization and the device changes hands, IT can erase the Intel SSD Pro without having to physically remove it, while also providing an audit trail to authenticate the process. Intel also continues to lead the way with hardened application-level protection that guards against malware beyond the network perimeter and endpoint devices.[1]

### Intel® Active Management Technology (Intel® AMT)

Intel Active Management Technology allows IT or managed service providers to better discover, repair, and protect their networked computing assets. With Intel AMT, you can manage and repair PC assets, workstations, and entry servers, utilizing the same infrastructure and tools across platforms for management consistency. For embedded developers, this means that devices can be diagnosed and repaired remotely, ultimately lowering IT support costs. Intel AMT is a feature of 6th Gen or above Intel Core vPro processors and workstation platforms based on select Intel® Xeon® processors.

### Intel® Boot Guard and Intel® BIOS Guard

Intel further enhances security with Intel Boot Guard and Intel BIOS Guard. Intel Boot Guard provides hardware-based boot integrity protection and prevents unauthorized software and malware of boot blocks critical to a system's function, thus providing an added level of hardware-based platform security. Intel BIOS Guard protects the BIOS flash from modification without platform manufacturer authorization, which helps defend the platform against low-level DOS (denial of service) attacks, and restores BIOS to a known good state after an attack.

### Intel® Virtualization Technology (Intel® VT)

Virtualization solutions allow multiple operating systems and applications to run in independent partitions on a single computer. Using virtualization capabilities, one physical computer system can function as multiple virtual systems. Intel Virtualization Technology improves the performance and robustness of today's virtual machine solutions by adding hardware support for efficient virtual machines.

Intel VT-d is part of the Intel VT hardware architecture. VT-d helps the virtual machine manager (VMM) better utilize hardware by improving application compatibility and reliability, and providing additional levels of manageability, security, isolation, and I/O performance. By using the VT-d hardware assistance built into Intel® chipsets, the VMM can achieve higher levels of performance, availability, reliability, security, and trust.

### Intel® Software Guard Extensions (Intel® SGX)

Intel Software Guard Extensions helps application developers protect selected code and data from disclosure or modification. Intel SGX makes such protections possible through the use of enclaves, which are protected areas of execution. Application code can be put into an enclave by special instructions and software via the Intel® SGX Software Development Kit (SDK). The Intel SGX SDK is a collection of APIs, libraries, documentation, sample source code, and tools that allow software developers to create and debug Intel SGX-enabled applications in C/C++.

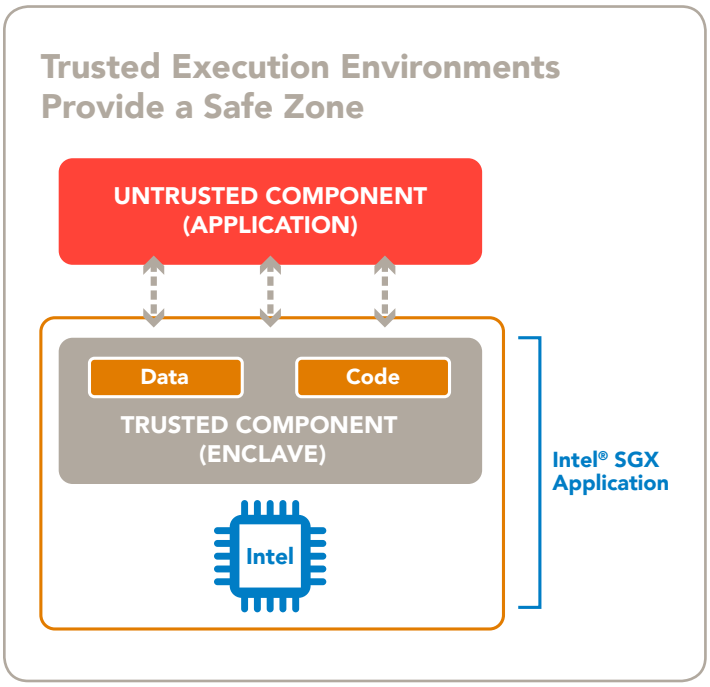


**Figure 5.** Intel® Software Guard Extensions (Intel® SGX) can reduce the attack surface of an application

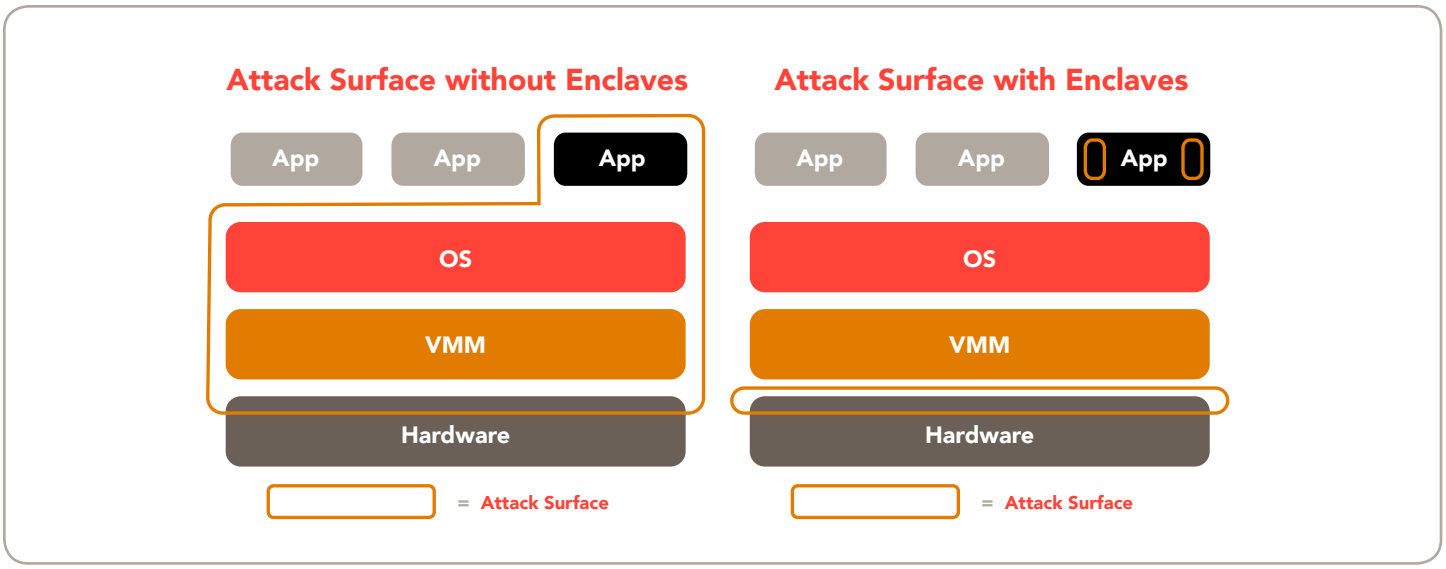


**Figure 6.** Demonstrates the dramatic difference between attack surfaces with and without the help of Intel SGX enclaves

### Intel® Trusted Execution Technology (Intel® TXT)

Intel Trusted Execution Technology provides a hardware-based security foundation, offering greater protection for information used and stored on the business PC. A key aspect is the provision for an isolated execution environment and associated memory where operations can be conducted on sensitive data. Intel TXT also provides a sealed portion of storage where sensitive data such as encryption keys can be kept, helping to shield them from being compromised during an attack by malicious code. To make sure that code is executing in this protected environment, attestation mechanisms verify that the system has correctly invoked Intel TXT.

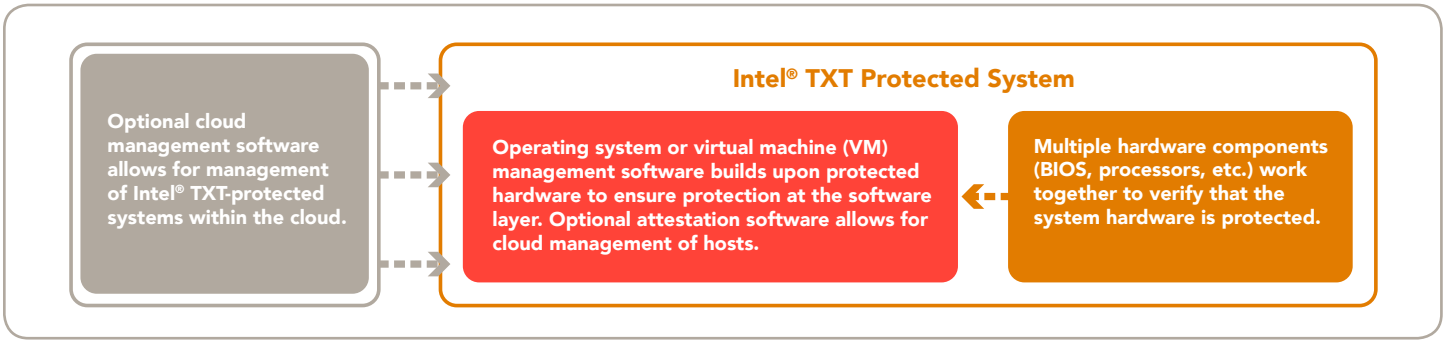


**Figure 7.** Intel® Trusted Execution Technology (Intel® TXT)

### Intel® Secure Key

Intel Secure Key is the instruction RDRAND and its underlying digital random number generator (DRNG) hardware implementation. The DRNG, using the RDRAND instruction, is useful for generating high-quality keys for cryptographic protocols. Intel Secure Key enables fast, true random number generation done in the hardware, with minimal user impact.

### Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

The 6th Gen Intel Core vPro processor family includes Intel AES-NI. These instructions are designed to implement and accelerate some of the complex and performance-intensive steps of the AES algorithm. Intel AES-NI can be used to speed the performance of an AES implementation by 3x to 10x, over a complete software implementation.[4] This helps improve the speed of applications while performing encryption and decryption.

Intel AES-NI minimizes application performance concerns inherent in traditional cryptographic processing. It provides enhanced security by addressing side channel attacks during Intel AES associated with traditional software methods using table look-ups.

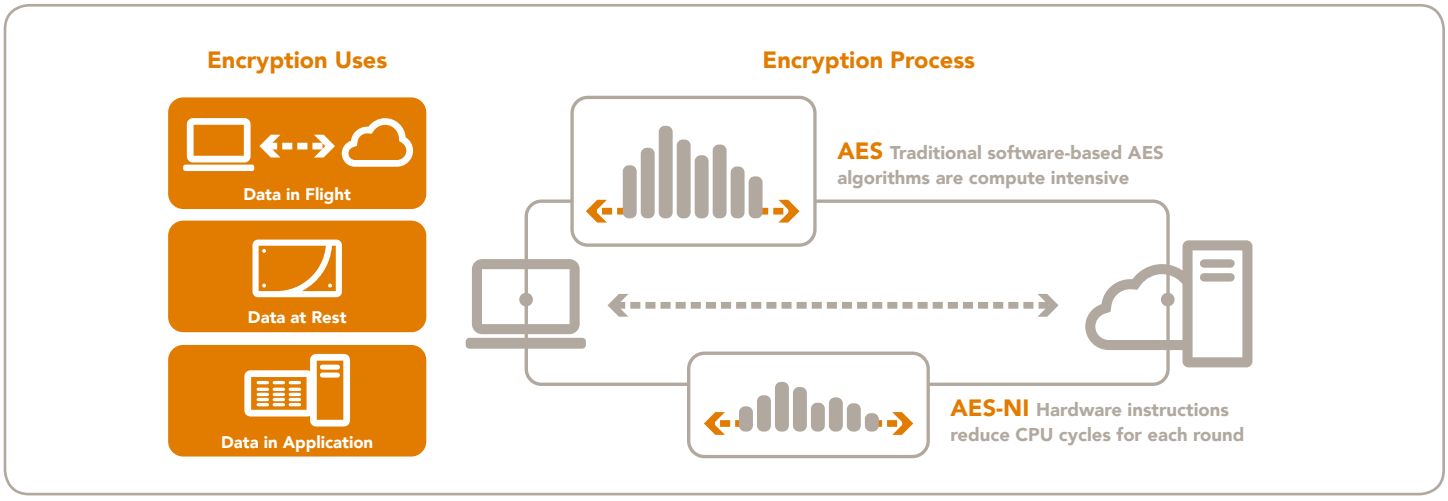


**Figure 8.** Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

## Intel® OS Guard

Intel OS Guard offers two key types of protection against escalation-of-privilege attacks:

- Malware execution protection. Prevents malware from executing code in application memory space. Instructs the processor not to execute any code that comes from application memory while the processor is in supervisor mode.
- User data access protection. Prevents malware from accessing data in user pages. Instructs the processor to block access to application memory while the processor is in supervisor mode.

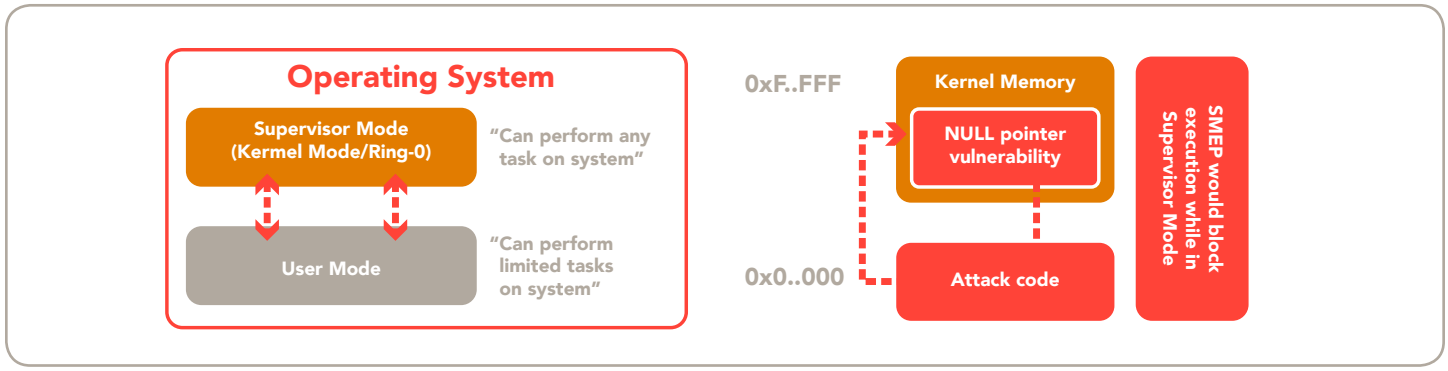


**Figure 9.** Intel® OS Guard prevents execution of untrusted application memory, while operating at a more privileged level. By doing this, Intel OS Guard helps prevent Escalation of Privilege (EoP) security attacks.

## Intel® Identity Protection Technology (Intel® IPT with PKI)

Intel Identity Protection Technology with public key infrastructure (PKI) is a second-factor authentication for business and web services that validates when a legitimate user (not malware) is logging in from a trusted PC.

PKI is a system of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. Intel IPT uses PKI certificates stored in firmware to authenticate the user and the server to each other and to encrypt and digitally sign documents.

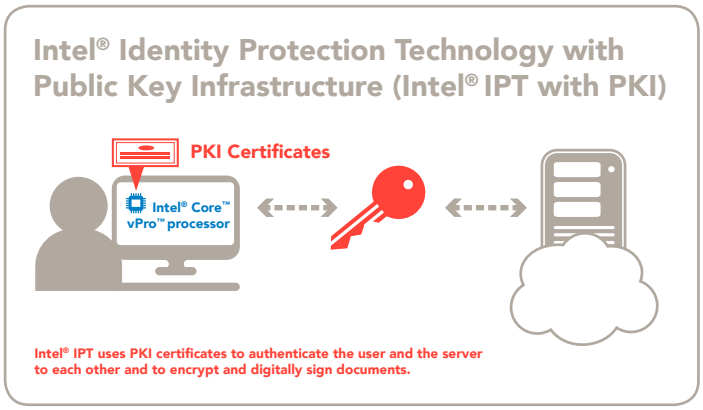


**Figure 10.** Intel® Identity Protection Technology (Intel® IPT with PKI)

## Conclusion

As technology advances, so do the skills of cyber intruders. It is prudent to take advantage of safer and more efficient technology, and for that we need to adapt to change. Business Reimagined's Dave Coplin says, "If you can't help people change, technology changing all around them won't make the slightest difference." [2]

Every day there is a new test on the security of your infrastructure, as hackers look to take advantage of zero-day exploits and social engineering opportunities to target your enterprise. To combat these threats, technology experts have to get smarter as well, and need to expand their focus from more than just perimeter security to include endpoint security in their overall strategy. Investing in Windows 10 with systems featuring 6th Gen or above Intel Core vPro processors increases security to protect your valuable systems, data, and, ultimately, your business.

---

## About Sogeti

Sogeti is a leading provider of technology and engineering services. Sogeti delivers solutions that enable digital transformation and offers cutting-edge expertise in cloud, cybersecurity, digital manufacturing, quality assurance and testing, and emerging technologies. Sogeti combines agility and speed of implementation with strong technology supplier partnerships, world class methodologies, and its global delivery model, Rightshore®. Sogeti brings together more than 25,000 professionals in 15 countries, based in over 100 locations in Europe, USA, and India. Sogeti is a wholly owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange. For more information please visit www.sogeti.com.

*Rightshore® is a trademark of Capgemini.*

## Learn More


1. Intel Transforms the Workplace with Latest 6th Generation Intel® Core™ vPro™ Processors, https://newsroom.intel.com/news-releases/intel-transforms-the-workplace-with-latest-6th-generation-intel-core-vpro-processors/.
2. Workplace Transformation: Intel's Vision for Embracing Change and Innovation, Jim Henrys, chief strategist and architect. Intel, 2016, http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/workplace-transformation-vision-paper.pdf.
3. Windows 10 Features, https://www.microsoft.com/en-us/windows/features.
4. https://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni


## Contact Sogeti for a Windows 10 Enterprise Security Briefing

Want to know more about implementing the security features of Windows 10 on modern devices? Contact Sogeti to conduct a Windows 10 Enterprise Security Briefing. Owning Windows 10 on modern devices is only the beginning. Sogeti can show you how to take a systematic approach to disrupting the attackers by ruining the economics of attacks, breaking the attacker's playbook, and eliminating the vectors of attack. During this briefing, you will discover how to implement the new security features, and be provided with a high level capability implementation timeline to strengthen your security with Windows 10.

For further information or to schedule a Windows 10 Security Briefing, contact Darren Baker, Global Business Development Director, at Darren.Baker@Sogeti.com, or visit our website at https://www.sogeti.com/contact/.

SOGETI

intel

1. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit http://www.intel.com/performance.

2. Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.