VPRO® PLATFORM introduction

Notices & Disclaimers

All products, computer systems, dates and figures specified are preliminary based on current expectations, and are subject to change without notice.

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 www.intel.com/benchmarks.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

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

Statements in this document that refer to future plans or expectations are forward-looking statements. These statements are based on current expectations and involve many risks and uncertainties that could cause actual results to differ materially from those expressed or implied in such statements. For more information on the factors that could cause actual results to differ materially, see our most recent earnings release and SEC filings at www.intc.com.

Celebrating 10+ Years of Intel vPro®

2008

- Reach and manage beyond firewall

2010–2012

- Hardware KVM remote control
- Host-based configuration
- KVM resolution enhancements (1920x1200, three displays)

2013

- KVM resolution enhancements (2560x1600)
- Graceful OS shutdown

2015

- Remote provisioning for wireless platforms
- Remote screen blank
- Microsoft InstantGo support

2016

- KVM resolution enhancements (4096×2160@8bpp)
- Intel® Remote Secure Erase with Intel® SSD Pro
- USB-R storage redirection

2017–

- Intel® Manageability Commander
- Intel® Active Management Technology (Intel® AMT) location for Intel® Authenticate
- Support for KVM headless devices
- Web app hosting in Intel AMT firmware

2019

- Intel® Endpoint Management Assistant (Intel® EMA)
- Client-initiated remote access proxy

2020

- Manage Intel AMT devices beyond the firewall from the cloud
- Support for Intel® Thunderbolt™ docking stations
- Intel® Trusted Device Setup

Intel® vPro™ platform extensibility


Desktops


Laptops


2 in 1s


AIOs


Point-of-sale devices


Digital signage


Workstations


Vending machines


Intel Unite® solution hub PC

The Intel vPro® Platform is Built for Business

BUSINESS-CLASS PERFORMANCE AND EXPERIENCES

New – Leap in overall performance with new 11th Gen Intel® Core® vPro® Platform

New – Immersive collaboration with Intel® Iris® Xe graphics

New – Low power Neural Noise Cancellation with GNA2.0

New – Stay connected with increased efficiency with integrated Thunderbolt™ 4, Discrete WiFi 6E** and CPU-attached PCIE Gen 4

New – Amazing system responsiveness with Intel® Optane™ memory H20 with SSD **

New – Balancing size, cost & user experience with IPU6 to generate aesthetically pleasing image quality for collaboration

New – Making PCs smarter & user aware with low power context sensing technology with Clover Falls

Improved – Optimized system performance with Intel® Adaptix™ Technologies

A BUILT-IN, MORE SECURE FOUNDATION

New – Intel® Hardware Shield features for built-in enhanced security, including:

- Protect against control-flow hijacking malware attacks with Intel® Control-flow Enforcement Technology(Intel® CET)
- *Prevention of memory data exposure from physical attacks such as cold boot attacks with Intel® Total Memory Encryption (Intel® TME)
- Advanced threat detection for enhanced security without compromising performance with Intel® Threat Detection Technology (Intel® TDT)

*New – FIPS 140-2 Level2 Certification(crypto block) for Intel® vPro® based platforms

intel vPRO PLATFORM

BUILT FOR BUSINESS

MODERN MANAGEABILITY FOR IT

*New – Modern Manageability with Intel® AMT powered by Intel® EMA, Remote Secure Erase expansion to remotely erase Intel and 3rd party SSDs

**New – Enhanced manageability and simplified user experience with Intel® Active Management Technology (AMT) over Thunderbolt™ 4 dock support

RELIABLE, STABLE PLATFORMS

*Enhanced – Intel® SIPP for Enterprise-class validation & efficient IT platform qualification supplemented with reliable updates with Chasm Falls 2

- *Indicates feature only available on Intel vPro eligible SKUs
- ** Intercept TGL commercial in Q1 2021

MODERN MANAGEABILITY

The Value of Hardware-based Remote Management

Software-based (traditional)

- Consoles communicate with devices using standard networking capability (an in-band link)
- When the OS cannot respond, the types of problems that can be fixed remotely are significantly reduced

Hardware-based (Intel® Active Management Technology)

Uses an out-of-band connection that operates independently of the OS and provides persistent connectivity

- Fix a wider range of systems issues, even when the OS is down
- Remotely repair corrupted drivers, application software, or the OS for a nonresponsive system that won't run or boot
- Use KVM to remotely monitor OS upgrades or boot to the system BIOS

6

Intel vPRO ® Platform Modern Manageability Use Cases

REMOTE POWER CONTROL

Manage your entire PC fleet with remote power-on

HARDWARE ALARM CLOCK

Set wake-up times and schedule updates

HARDWARE KVM

See it remotely—even when it's down

Boot Redirection

Boot into temporary environments

Beyond Firewall Support

Connect to devices inside and outside the corporate firewall

CLOUD-BASED MANAGEABILITY

Manage devices from the cloud

UNATTENDED SYSTEM Control

Remotely manage unattended systems

UPGRADE MANAGEMENT

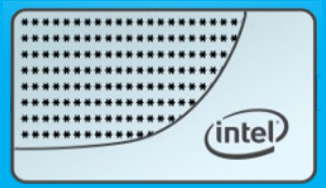
Assist with OS upgrades

Enabling expanded set of endpoint Devices with Intel® Remote Secure Erase

New

Before

Remotely erase SSDs with Intel® Remote Secure Erase[1]



Usages:
(i) for Reissue systems to different user
(ii) End of life/dispose of the system

out-of-band remote erase capability over Intel® AMT
Supports Intel Pro series Solid State Drives

With Tiger Lake vPro Platform

Intel® Remote secure Erase expanded to work with all drives that support the secure erase standards[2]

Usages:
(i) for Reissue systems to different user
(ii) End of life/dyspose of the system
(iii) All compliant SSDs are supported

Enables an expanded set of endpoint devices which can be remotely erased out-of-band over Intel® AMT

*Other names and brands may be claimed as the property of others
1 Requires enabling in UEFI as noted in Intel® BIOS Writer's Guide
2 Requires compliance with INCITS Technical Committee T13* standards for ATA drives, or Compliance with NVM Express* standards for NVMe drives

Empowering the Workforce 24/7

Modern manageability requires tools that support workers wherever they are.

The Intel vPro® platform

The Intel vPro platform helps businesses achieve modern manageability by evolving continuously in ways that bring value to customers.

Intel® Active Management Technology (Intel® AMT)

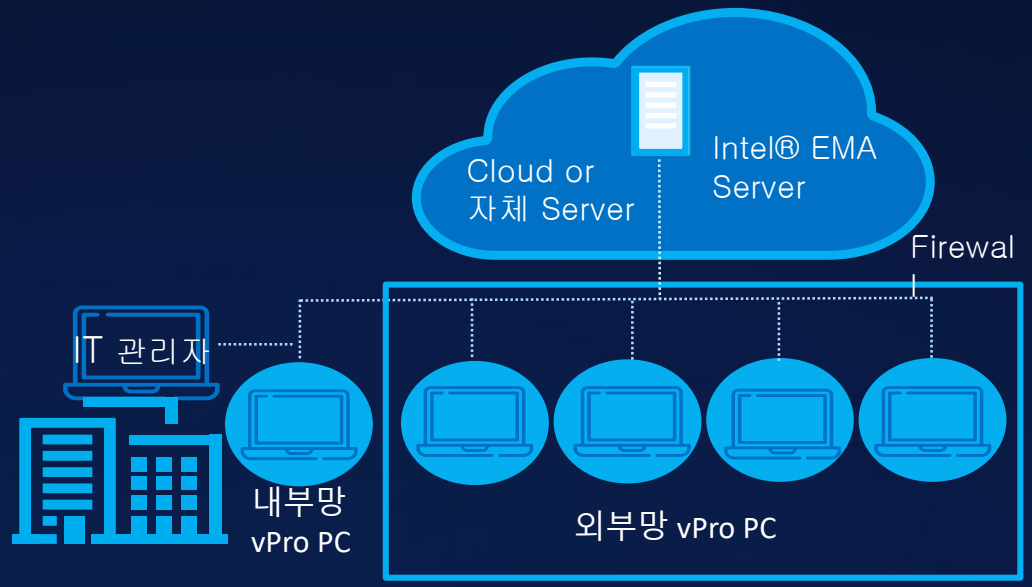
Intel AMT on the Intel vPro platform brings remote manageability where it's needed—even those working outside the corporate firewall.

Intel® Endpoint Management Assistant (Intel® EMA)

Intel EMA is one of the tools that lets IT remotely and securely manage Intel AMT devices beyond the firewall from the cloud.

9

Intel Remote Client Management Tools

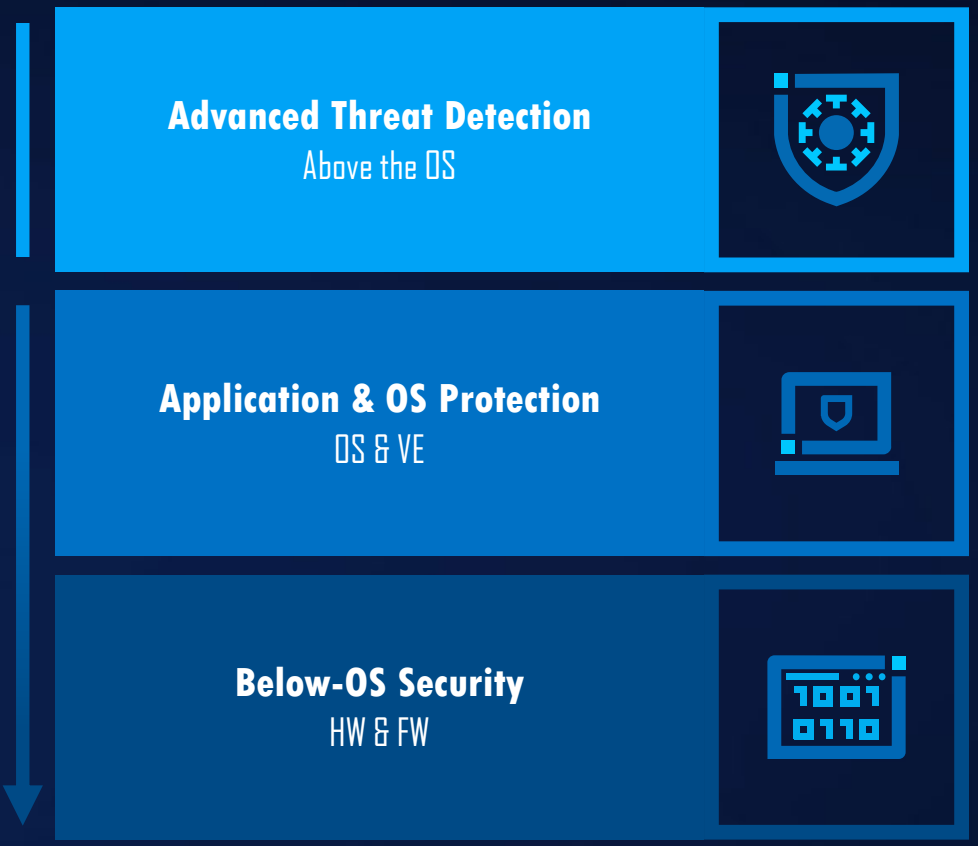


- EMA Server 구축 시에는 내부망 외부망 모든 vPro PC를 관리 가능
- 기본적인 Hardware 기반 AMT 기능과 더불어 OS 기반의 Software KVM, 파일 양방향 전송 등이 가능
- Web 으로 편하게 관리 페이지로 접속가능
- 여러 대의 PC/Server 화면을 한번에 볼 수 있는 기능을 제공

Enhanced Security with Intel® Hardware Shield

Why Intel® Hardware Shield?

- Commercial users have adopted a workplace culture that cannot be protected by the traditional security model
- Traditional security has been software-only and operates "above the OS"
- Ransomware is the top variety of malicious software and threats are "moving down the stack"→ traversing between HW, FW & SW
- Industry security experts anticipate that cyber attackers will exploit the increased use of virtualized environments as a result of the COVID-19 pandemic



Typical Device Stack

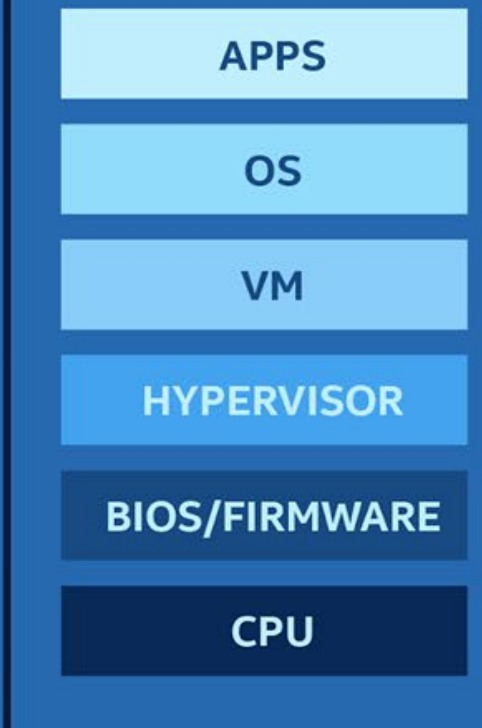
Intel® Hardware Shield's strong feature roadmap

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.

➔ **Advanced Threat Detection**
Hardware-powered, AI-enabled threat detection without a performance hit.

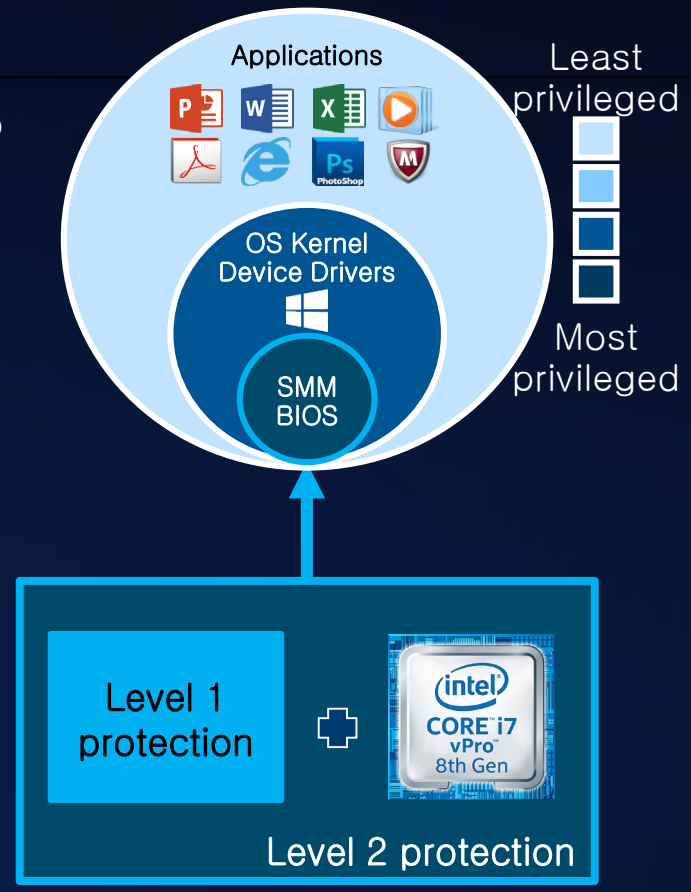
➔ **App & OS Protection**
Eliminates an entire class of attacks that evade current software solutions. Hardware-powered virtualization-based security for applications and operating system with performance enhancements.

➔ **Below the OS**
Lock down memory in the BIOS against firmware attacks and enforce secure boot at the hardware level.



Intel® Runtime BIOS Resilience

Protects platform BIOS from attacks on 7th & 8th Gen Intel® Core™ & Intel® Core™ vPro™ processors



Intel® Runtime BIOS Resilience

Protecting BIOS is critical:

- BIOS is the most privileged SW and must be protected with the latest security
- Security applications lack privilege to scan BIOS for threats
- BIOS bugs can be exploited for spying & persistent malware/ransomware[1]

Intel® Runtime BIOS Resilience offers 2 levels:

- Level 1: Protection to System Management Mode (SMM in UEFI/BIOS)
- Level 2: Adds further hardening to Level 1 by hardening the page table with Intel® Core™ vPro™ processors

Intel® Runtime BIOS Resilience improves the security of the BIOS infrastructure

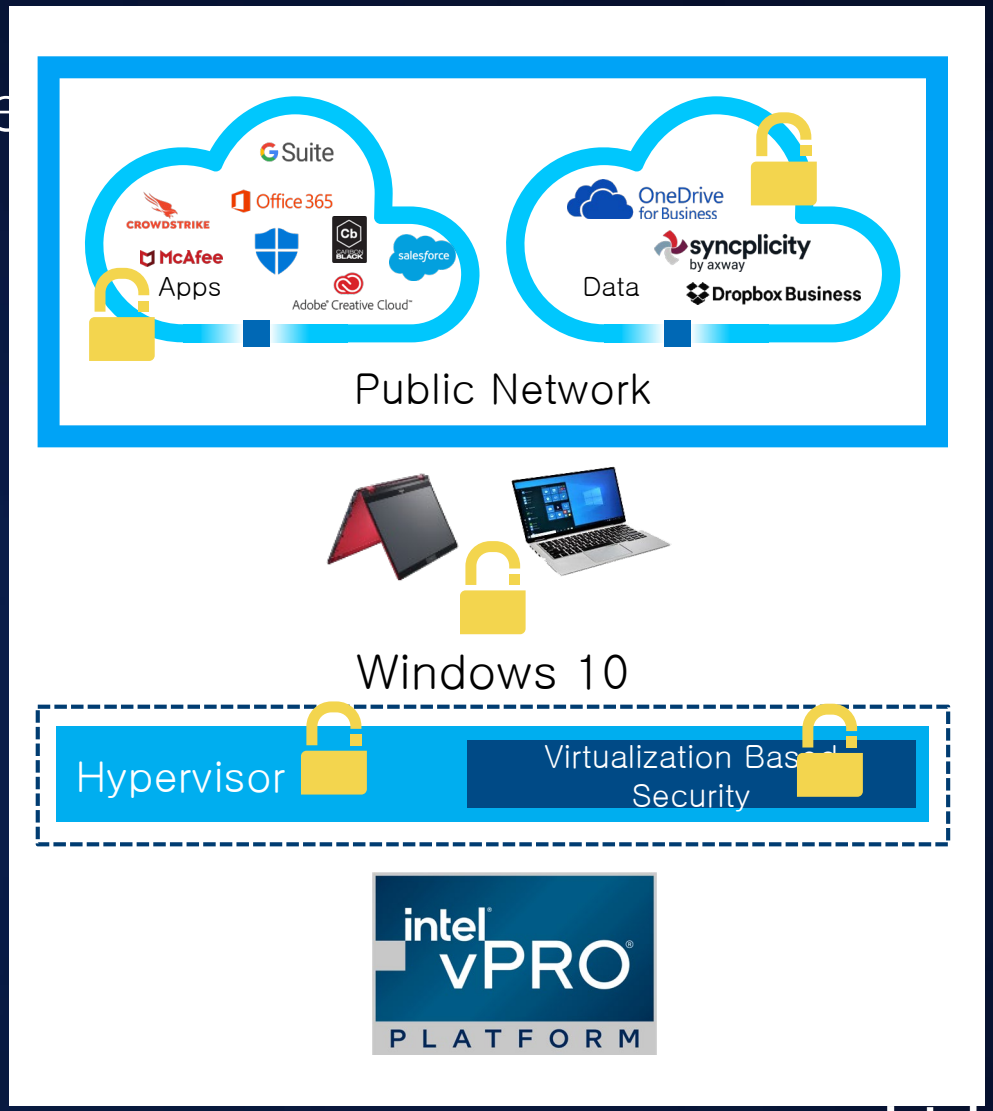
Intel® Hardware shield helps protect applications and data

Provides hardware resources for With hardware-integrated operating system se optimizing virtual work loads

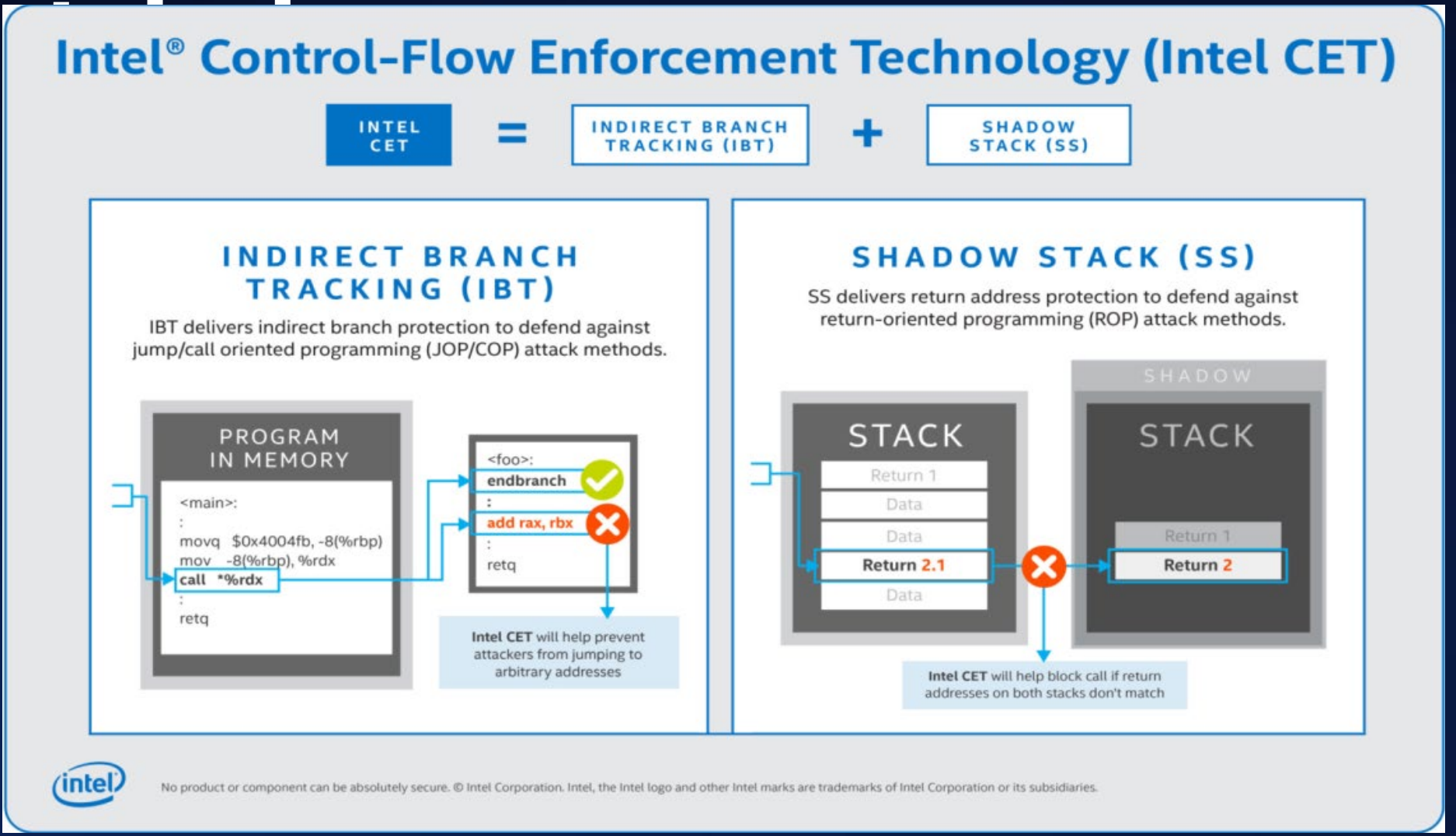
Helps prevent malware injection and protect user log-in credentials with hardware-enforced isolation

Eliminates an entire class of memory safety vulnerability issues

Helps protect data from physical tampering attacks with silicon-level memory encryption



Intel® Hardware shield : control-flow enforcement



- Intel® Control Flow Enforcement Technology (Intel® CET) helps eliminates an entire class of memory attacks
- Intel CET is built into hardware microarchitecture and available across the family of products starting with TGL

Intel® Hardware shield – advanced threat

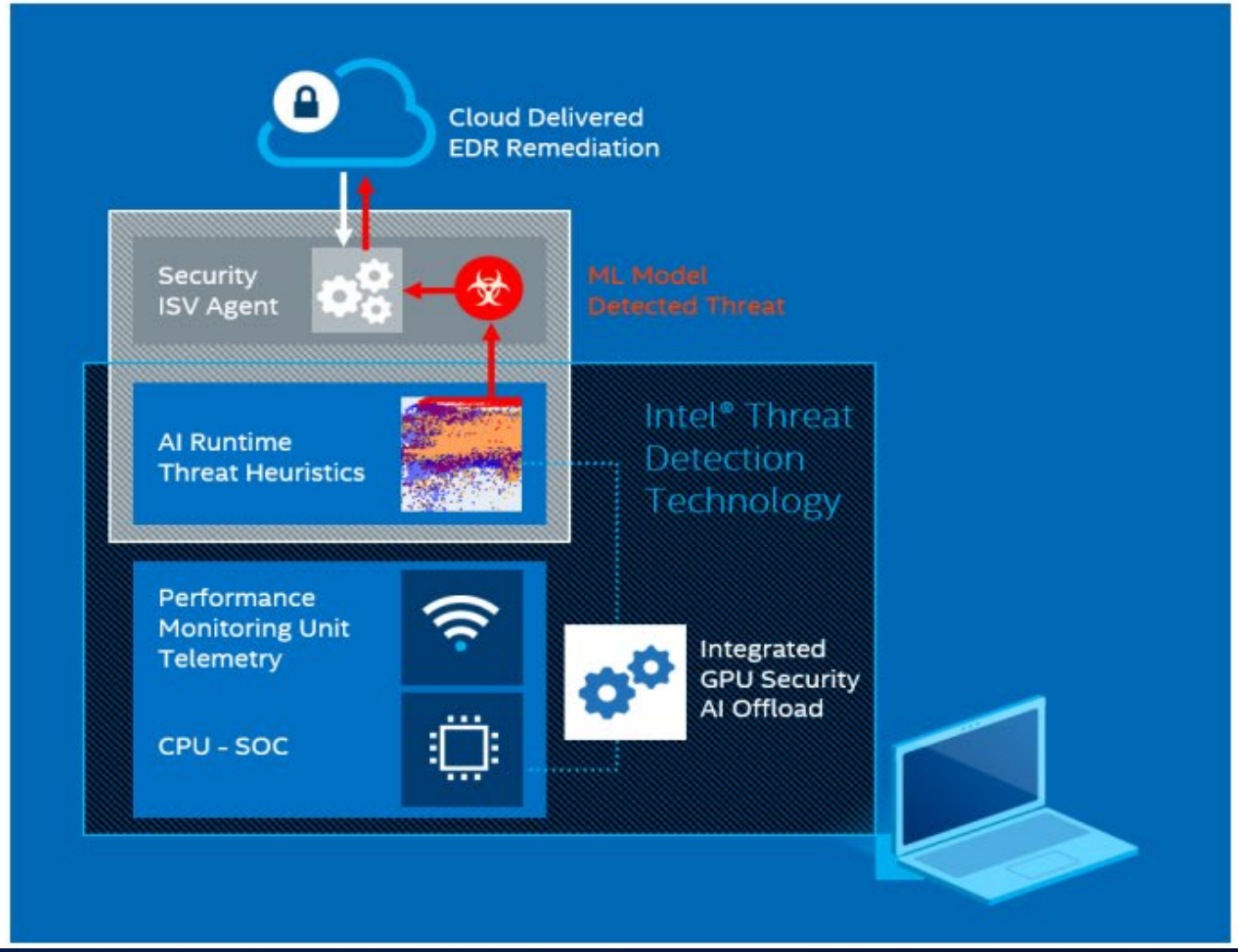
Purpose- Improves the performance and detection efficacy of anti-malware (AV, EPP, and EDR) security ISV solutions.

CPU Threat Detection. Goes beyond signature & file based static behavioral techniques with CPU malware behavior monitoring.

Cross-layer Visibility- Close blind spots to expose Ransomware & Crypto-mining from legitimate data encryption, as it avoids detection in memory, or hides in virtual machines.

Unleash AI for Better Security- Accelerate performance intensive AI security algorithms with offload to Intel's integrated GPU. Boost security capacity to analyze more data & do more scans.

Security without Compromise- Bolster the performance of security ISV agent processing on the client for a better user computing experience.



Intel® Hardware shield – advanced threat detection

인텔, '크립토재킹' 피해 방지 위해 마이크로소프트와 협력

이진우 기자 2021-04-27 화 17:26 댓글 [81]

인텔과 마이크로소프트가 크립토재킹(cryptojacking)에 대항하기 위해 손을 잡았다.

크립토재킹은 사이버 범죄자들이 컴퓨터에 악성 프로그램을 설치해 컴퓨터의 전력과 리소스를 이용해 암호화폐를 채굴하거나 암호화폐 지갑을 훔치는 것을 뜻한다

일부 악성 프로그램은 다른 장치와 서버를 감염시킬 수 있는 기능도 있다. 피해자 모르게 리소스 자원을 사용하기 때문에 CPU 사용량이 급증하는 특징이 있다.

Platform Stability

Intel® SIPP for Tiger Lake

INTEL® STABLE IT PLATFORM PROGRAM

Industry platform validation that aims for zero hardware changes for at least 15 months or until the next generational release

1. Intel® vPro Platform ingredients
2. BKC
3. Win 10 Validation
4. OEM Platform
5. IT Validation
6. IT Buying Cycle

11th Gen Intel® Core™ Mobile Processors (U Series)

Intel® Platform Controller Hub

FPO

Intel® Iris® Xe

6GHz Intel® Wi-Fi 6E (Gig+)
2.5GbE Ethernet

Intel® Thunderbolt™ 4 & Drivers

Intel® Optane™ Memory H20 with SSD * FW/Drivers

Corporate Intel® Management Engine firmware, BIOS, platform ingredients drivers and firmware

- Supplement with RELIABLE UPDATES
- Chasm Falls Gen 2: offers two use cases A) auto restart of interrupted firmware update B) auto recovery of failed update
- Windows Capsule Updates for ME firmware also required for vPro

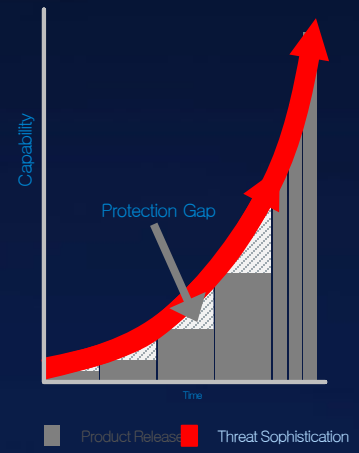
Chasm Falls Firmware Update Program

Help Minimize System Vulnerability and Update Support Issues

Background

- Delays in deployment of vulnerability mitigations
- Attach rate of mitigations for end-user systems is very low

= Platform Less Secure



Reduced validation time for OEM's

+

Increased confidence for end user adoption

= Improved Platform Security

(Part of Hardware Shield features)

Help reduce OEM validation time

- BIOS modules validated by Intel
- Increasing OEM collaboration

Help increase confidence in update adoption

- Automated recovery
- Common update format (capsule)
- FW updates done via push model

Greater Stability with improved Platform Security


intel