단말기 HW 수준의 원격 관리및 보안강화 방안

인텔코리아
상무 최원혁

AGENDA

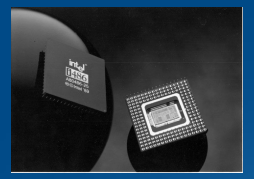
- PC의 진화 과정
- 업무용 PC 단말기에 대한 도전 과제
- 업무용 PC의 비전과 전략
  - S/W 기반의 보안의 한계, H/W 기반 보안을 포함한 풀 스택전략
  - BIOS 수준의 문제 해결을 위한 원격 제어 관리 기술
  - PC 단말기에서의 AI 기술의 발전 및 진화
  - Roadmap
- 맺음말 – AI is Everywhere, It starts with Intel

PC의 진화 과정

IBM 개인용 PC 출시

인텔 8088 마이크로프로세서를 기반으로 하며 Microsoft의 MS-DOS 운영 체제를 사용.
업계에서 널리 채택된 최초의 PC

1982



인텔 80486 프로세서

1백만 개가 넘는 트랜지스터를 포함.
2비트 정수 산술 및 논리 장치64비트 부동 소수점 장치 및 33MHz의 클럭 속도

1989

1995

1996

인텔 펜티엄 프로세서

ntel의 'x86' 마이크로프로세서 제품군의 5세대 제품. 펜티엄은 여러 명령을 동시에 실행할 수 있는 기능, 그래픽 및 음악 지원 등 프로그램 실행 속도를 높이는 여러 가지 발전된 기능을 도입

IBM ThinkPad 710C Notebooks

with Intel® Centrino® Pro processor technology support many wireless technologies, such as Wireless LAN and Gigabit Ethernet.

2003

A Wireless World

인텔® 센트리노®
프로세서가 출시되어
랩톱에 통합 무선
기능을 제공.

2008

인텔 vPro 출시

업무용 PC 브랜드, 원격 관리

2011

울트라북 출시

두께가 1.5cm 이하이고 Intel 프로세서와 SSD를 갖춘 노트북

2020

Intel® EVO

사용자 경험 중시
반응성
얇고 가벼운

2023

인텔 최초 통합 NPU

효율적인 클라이언트 AI를 위한 목적
지속적인 AI 및 AI 오프로드에 적합

AI
is Everywhere

intel

업무용 디바이스의 도전 과제

원격 근무

수 많은 근무지
대면 접촉의 감소
문제 최소화
빠른 문제 해결
쉬운 배포

사이버 보안

Zero-trust model
현대화된 위협 방어
위기 최소화

사용자 경험

직원 생산성
협업
스마트한 연결
실시간 적응

지속가능성

재활용
에너지 효율성
비용효율적인 업그레이드

인텔이 제공하는 업무용 디바이스의 임무

조직을 원활하게 유지하고 직원들이 업무에 집중할 수 있는 제품과 기술을 제공

intel

업무용 디바이스의 비전과 전략

INTEL VISION

인텔의 기술을 통해
현대적 업무환경에 맞는
비지니스 혁신 지원

고객 요구사항을 반영한 4가지 중점 사항

빠른 응답속도와 생산성

협업 툴 지원

보안과 원격 기기 관리

유지보수 비용 절감

INTEL STRATEGY

인텔은 군이 필요로 하는
첨단 전자전과
미래의 기업 환경을 위해서
최종 사용자가 필요로 하는
컴퓨팅과 보안을 제공합니다

intel

S/W 기반의 보안의 한계,

H/W 기반 보안을 포함한 풀 스택 전략

든든한 국방을 위한 최적의 인텔 vPro® 플랫폼

Learn more at intel.com/vpro

인텔 ® vPRO ™ 플랫폼은 비즈니스 컴퓨팅 엔드 포인트를 구축하는 데 사용되는 하드웨어 및 기술 세트입니다.

국방과 비즈니스를 위한 솔루션

Windows * 11 Pro / Enterprise를 활성화, 가속화 또는 보완하는 기능

광범위한 시장 지원

매년 최고 제조업체의 100개가 넘는 새로운 시스템

인증 프로그램

기능성 검증을 위한 공식 브랜드 요구사항 및 테스트 프로그램

네 가지 영역에 걸쳐 비즈니스 요구 사항을 해결하도록 설계되었습니다.

1. Based on a comparison (as of April 20, 2019) of features in the following categories: manageability, security, stability and processor performance, between vPro™ enabled platforms and other selected x86 architecture based platforms marketed for use in business PCs. Selection of manageability, security, stability and processor performance features are based on a 2018 web-based survey, conducted by Intel of more than 500 IT decision-makers to assess desired features when purchasing PC for business use. Intel will be marketing the Intel® Core™ vPro™ platforms with the tag line "Productivity Unleashed" in certain jurisdictions, including PRC and Vietnam. Intel will be marketing the Intel® Core™ vPro™ platforms with the tag line "The Intel® vPro™ platform is Intel's best business platform" in certain jurisdictions, including Argentina, Belarus, Belize, Chile, Egypt, El Salvador, Guatemala, Honduras, Italy, Japan, Panama, Peru, Saudi Arabia, Turkey, Russia, and Ukraine. If you are media or an influencer from these countries, or otherwise communicating directly to residents in these countries (e.g., on local-language social media), please only refer to the tag line Intel will be using in that country in lieu of the claim on this slide/document.

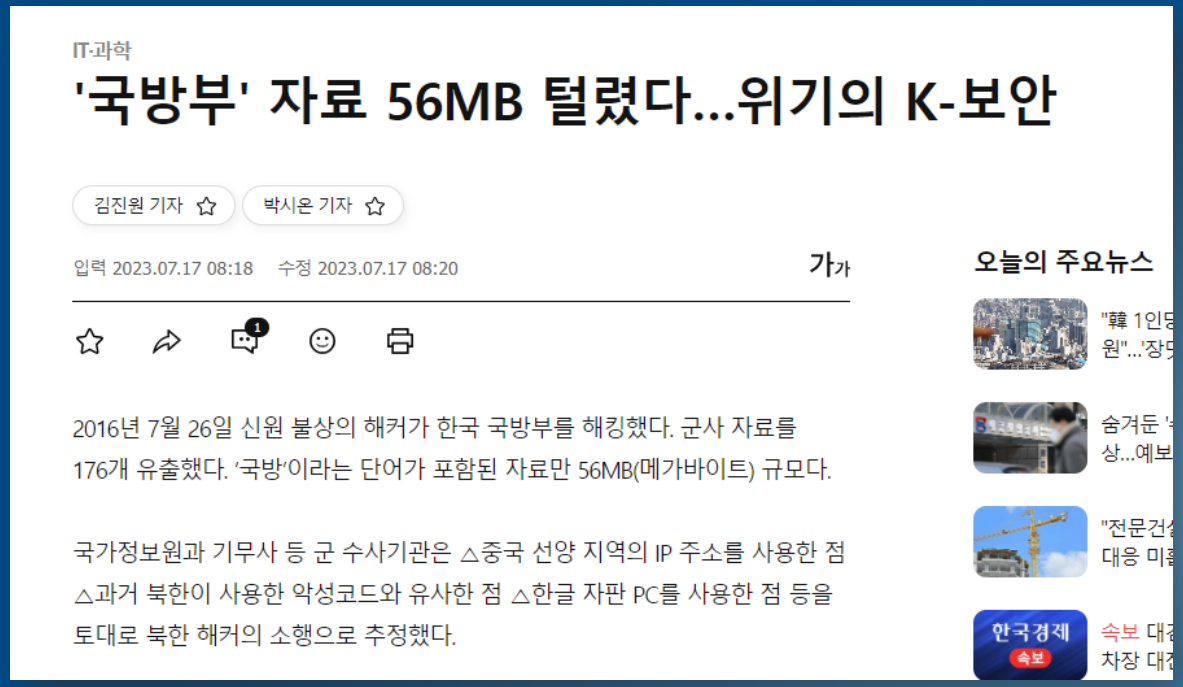
디바이스 보안 환경

- 사용자들은 이미 전통적인 보안모델로 막을 수 없는 다양한 업무 환경하에서 PC등을 이용하고 있다.
- 전통적인 보안 기술은 주로 Software방식이며 OS가 정상적으로 동작하는 상황에서 작동된다.
- 랜섬웨어는 매우 다양한 악성 Software이며 최근 공격은 HW, FW, SW에 국한되지 않고 플랫폼의 Low level 까지 침투하고 있다.
- 보안 전문가들은 최근 악성 공격이 계속해서 늘어나는 가상환경을 이용하게 많아지게 될 것이라고 예상하고 있다.

Typical Device Stack

intel

보안 사고 사례



IT·과학

'국방부' 자료 56MB 털렸다...위기의 K-보안

김진원 기자 ☆ 박시온 기자 ☆

입력 2023.07.17 08:18 수정 2023.07.17 08:20 가가

2016년 7월 26일 신원 불상의 해커가 한국 국방부를 해킹했다. 군사 자료를 176개 유출했다. '국방'이라는 단어가 포함된 자료만 56MB(메가바이트) 규모다.

국가정보원과 기무사 등 군 수사기관은 △중국 선양 지역의 IP 주소를 사용한 점 △과거 북한이 사용한 악성코드와 유사한 점 △한글 자판 PC를 사용한 점 등을 토대로 북한 해커의 소행으로 추정했다.

오늘의 주요뉴스

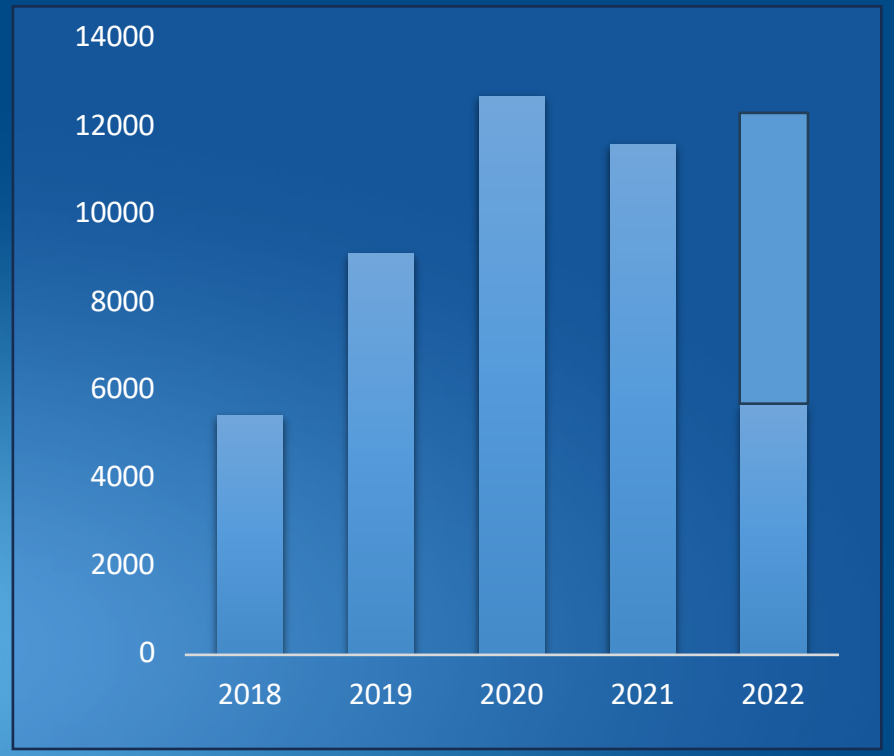
"韓 1인당 원"...'장

숨겨둔 '북 상...예보

"전문건설 대응 미흡

한국경제 속보 속보 대장 차장 대전

국방부는 해킹 피해 발생 후 국방망에 연결된 PC 19만 7038대에 대한 포맷 작업을 실시했다. 법원은 PC 1대당 포맷 작업에 들어가는 비용을 초급기술자 인건비 1만8431원으로 계산했다.



"군에 대한 사이버 공격 시도 탐지 건수는 2018년 한 해 5444건에서 2019년 9121건, 2020년 1만2696건으로 증가했다. 2021년에도 1만1600건이었으며, 2022년에는 7월까지만 5724건의 해킹 시도가 탐지됐다."

intel

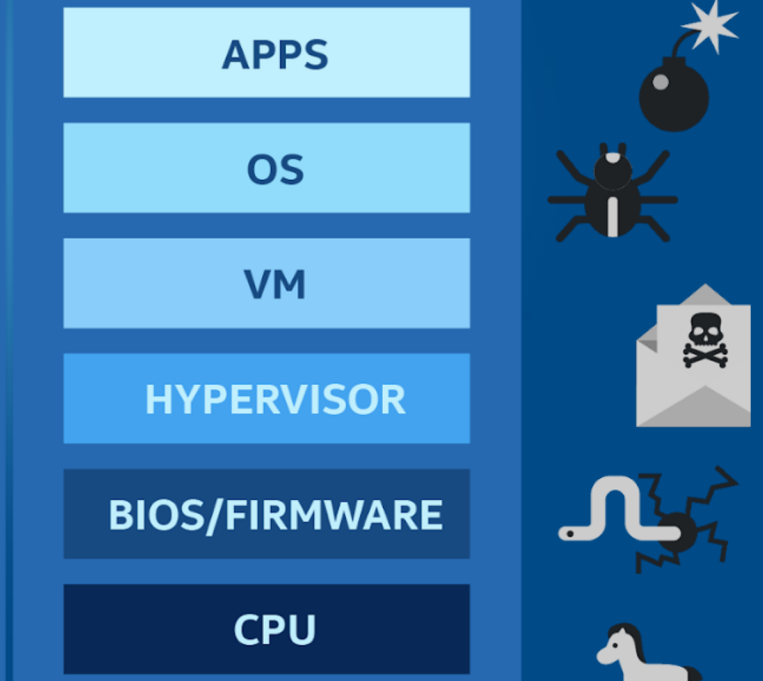
하드웨어 기반의 보안

하드웨어는 모든 보안 솔루션의 기반이며 인텔은 혁신적인 하드웨어 기반의 보안 기술 개발을 주도적으로 진행하고 있다.

➔ **Advanced Threat Detection**
CPU 성능에 영향을 주지않고, AI 기술을 이용해서 악성공격을 감지

➔ **App & OS Protection**
VT-D, VT-x 를 이용한 가상화를 통해서 Application과 Data 및 OS를 보호, Total Memory Encryption.

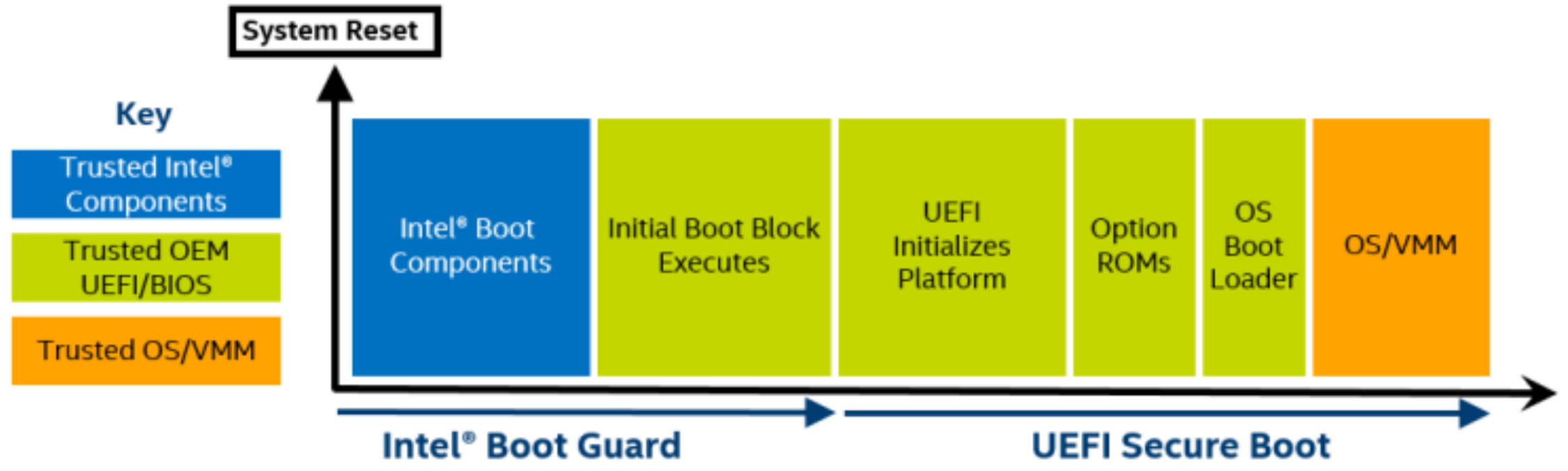
➔ **Below the OS**
Firmware 공격에 대해서 BIOS의 메모리를 Lock Down하며 하드웨어 레벨에서 안전한 Booting이 되도록 한다.



intel

INTEL® SECURE BOOT

검증된 Firmware가 설치되고 해당 Platform에서 실행되도록 하는 기술



- 부팅의 맨 처음 단계부터 Firmware의 중요한 각 요소들의 오염 여부를 확인
- 그림의 왼쪽부터 한 단계를 완료하면 바로 다음 단계의 Digital Signature를 체크

Intel® Secure Boot는
Low-level 과 높은 권한을 가진 Component들을 공격으로부터 보호한다

intel

INTEL® RUNTIME BIOS RESILIENCE

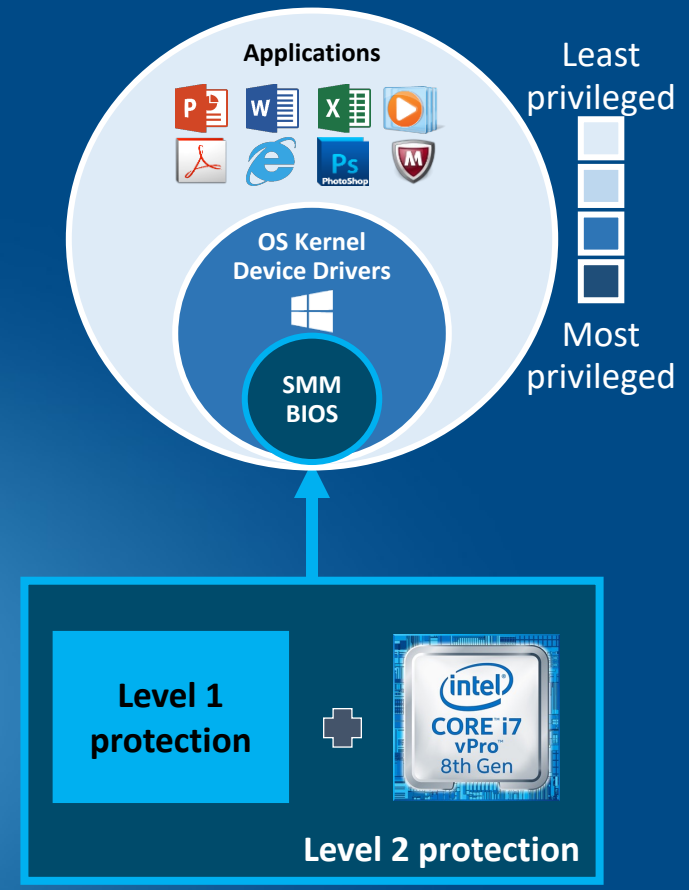
7세대와 그 이후의 Intel® Core™ & Intel® Core™ vPro™ processors 에 대해서 BIOS를 보호하는 기술

BIOS 보안은 아주 중요하다.

- BIOS는 아주 높은 권한을 가진 SW로서 최신의 보안기술로서 안전하게 보호되어야 한다.
- 일반적인 보안 Application은 BIOS의 보안 스캔을 하는데 있어서 권한이 부족한 경우가 많다.
- BIOS bug들을 통해서 spying & persistent malware/ransomware 들이 감염될 수 있다.

Intel® Runtime BIOS Resilience는 두개의 단계로 관리한다.

- **Level 1**: System Management Mode 보안 (SMM in UEFI/BIOS)
- **Level 2:** Intel® Core™ vPro™ processors로 페이지 테이블을 강화하여 Level1에 추가 강화

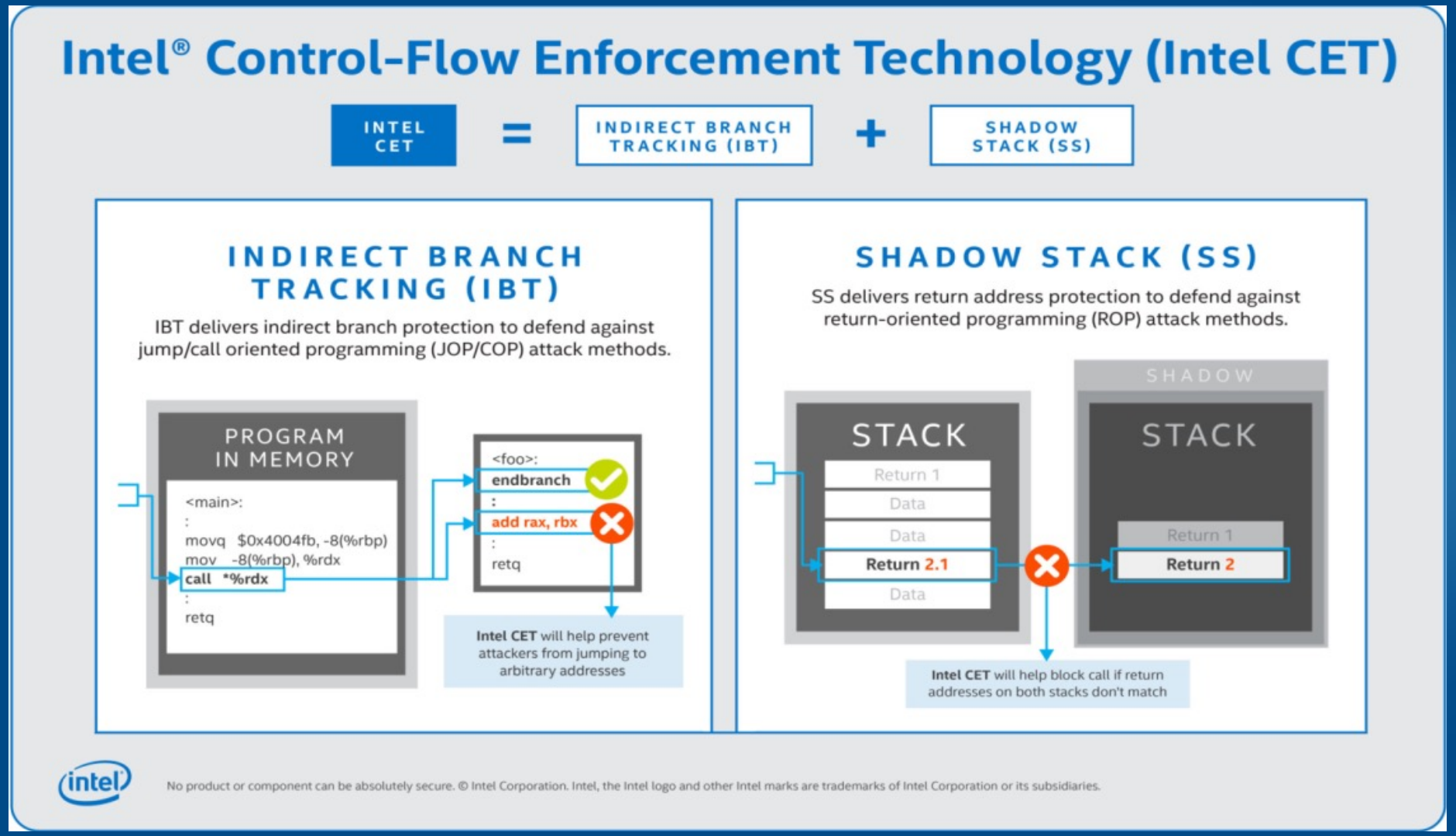


Intel® Runtime BIOS Resilience

Intel® Runtime BIOS Resilience는
BIOS Infra의 보안 레벨을 향상시킨다

intel

INTEL® HARDWARE SHIELD : CONTROL-FLOW ENFORCEMENT TECHNOLOGY



- Intel® Control Flow Enforcement Technology (Intel® CET)는 전반적인 메모리 공격에 대한 위험을 제거한다.
- Intel CET 는 하드웨어 마이크로 아키텍처에 포함되어 있으며 인텔 11세대와 그 이후의 프로세서에 사용 가능한 기술이다.

INTEL® HARDWARE SHIELD : CONTROL-FLOW ENFORCEMENT TECHNOLOGY

Forbes

EDITORS' PICK

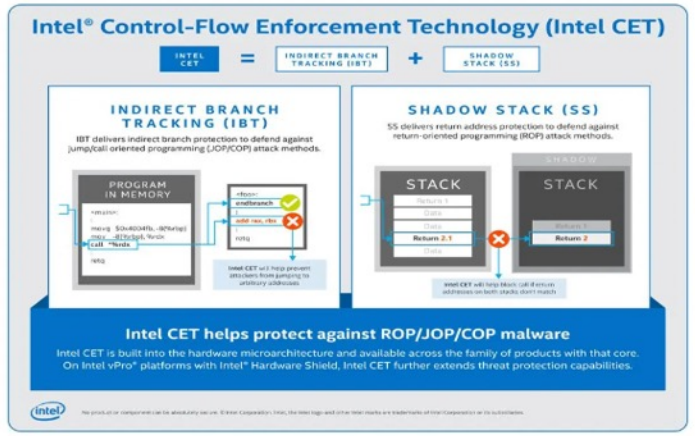
Intel CET Raises The Bar For Malware Defense

Tony Bradley Senior Contributor
I cover all things tech and the impact tech has on everyday life.

Follow

Jun 17, 2020, 03:35pm EDT

Listen to article 4 minutes



An overview of Intel Control-Flow Enforcement Technology (Intel CET) and how it works to defend ... [+] INTEL

Malware is a massive, overwhelming plague for companies and individuals. AV-Test identifies an average of over 350,000 new malicious programs and potentially unwanted applications (PUA) every day. There were over a billion malware threats identified in 2019, and that is projected to increase by nearly 600,000 in 2020. Clearly, malware is a huge problem. Intel is working to address the problem and

INTEL® HARDWARE SHIELD – ADVANCED THREAT DETECTION

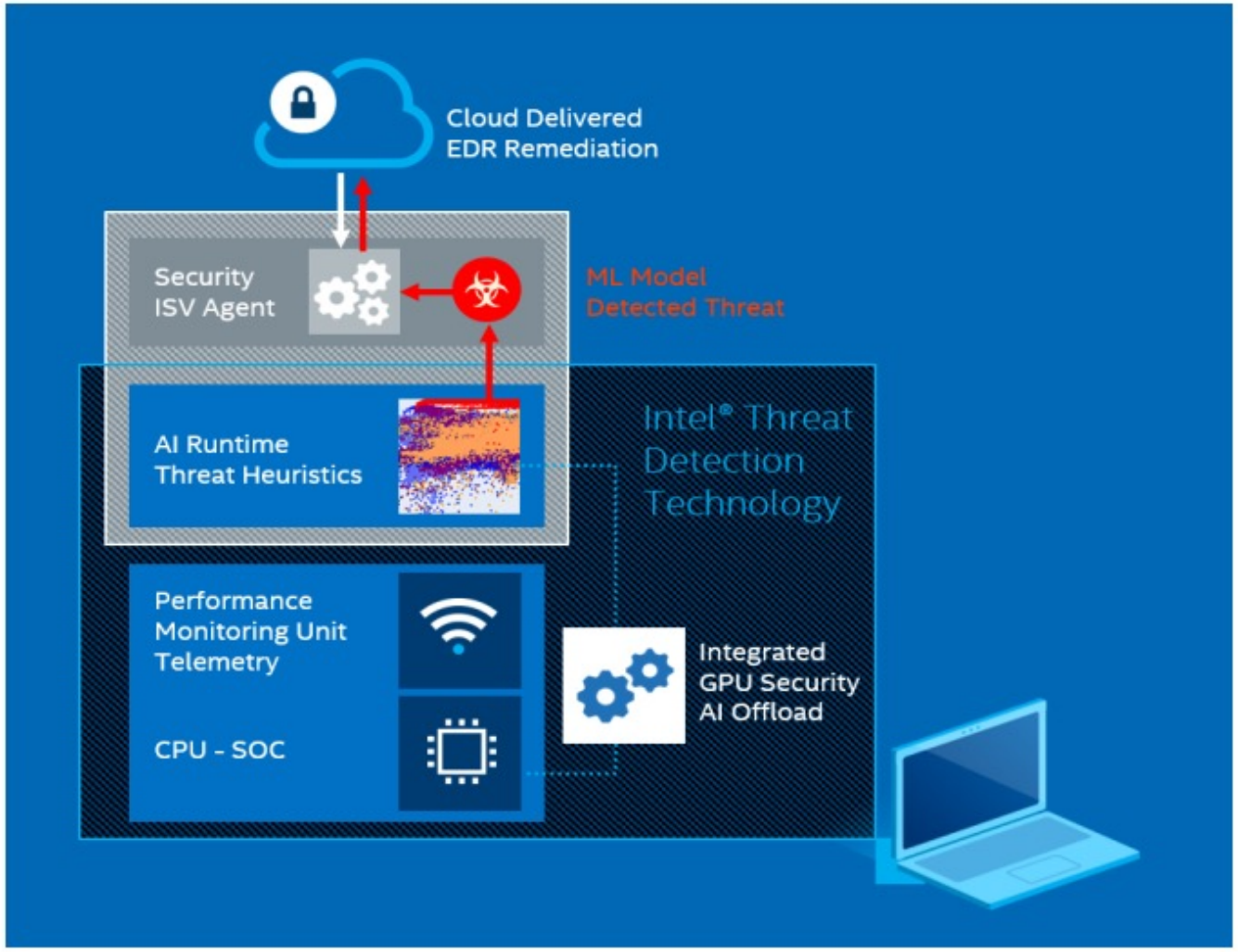
Purpose- Improves the performance and detection efficacy of anti-malware (AV, EPP, and EDR) security ISV solutions.

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.

intel

BIOS 수준의 문제 해결을 위한 원격 제어 관리 기술

intel

HARDWARE기반 원격관리의 장점

Software-based (traditional)

- 원격 PC들이 OS가 동작하는 환경에서 TCP/IP 같은 일반적인 표준 네트웍으로 관리자가 관리를 진행
- OS가 정상적으로 반응하지 못할 때는 원격에서 할 수 있는 기능이 크게 줄어든다.

Hardware-based

(Intel® Active Management Technology)

원격 PC들의 OS의 상태와 상관없이 out-of-Band connection을 이용해서 관리

- OS가 비정상이어도 많은 시스템 문제들을 해결할 수 있다.
- OS가 비정상인 상황에서도 각종 driver, application software, OS 문제들을 해결할 수 있다.
- KVM을 이용해서 원격으로 OS 업그레이드를 관리하거나 BIOS 설정 변경을 할 수 있다.

intel

REMOTE MANAGEMENT

재구성

여행&교통

방문 일정 잡기

Non-vPro Retail Platform

VS.

HW KVM

BIOS 재구성

OS 복구

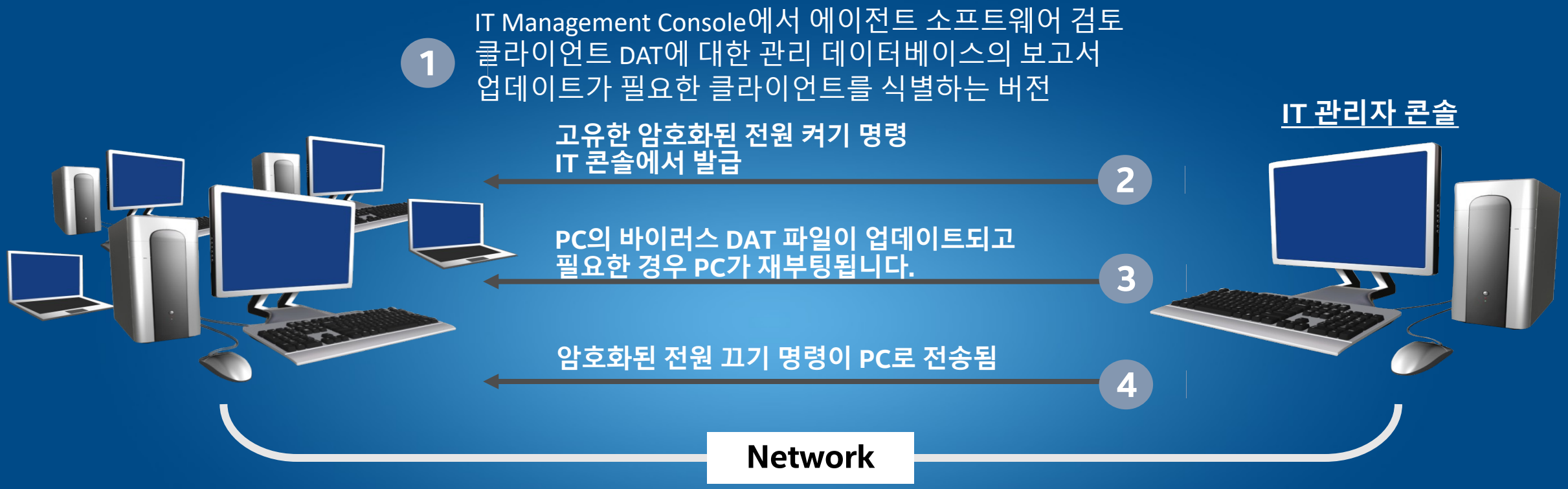
Wi-Fi/LAN

재구성

Intel vPro Retail Platform

intel

REMOTE POWER ON AND UPDATE

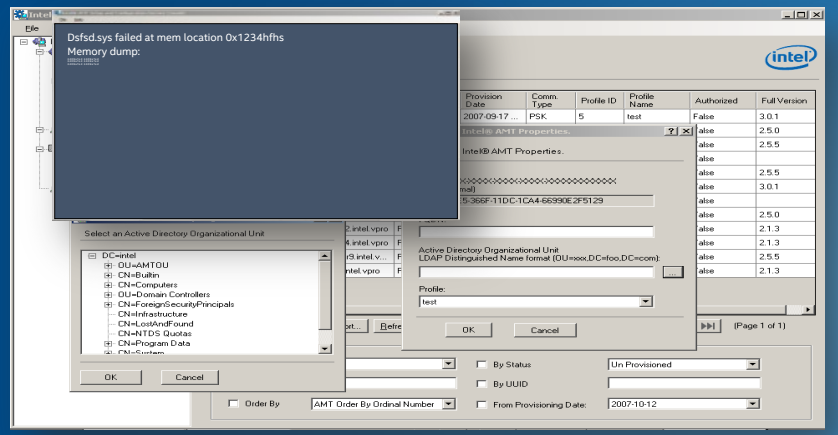


- 전원이 꺼져 있는 경우에도 클라이언트 PC에 보안 업데이트 푸시
- 사용자 중단 없이 암호화 된 패치 원격 배포

intel

KVM REMOTE CONTROL WITH INTEL® PROCESSOR GRAPHICS

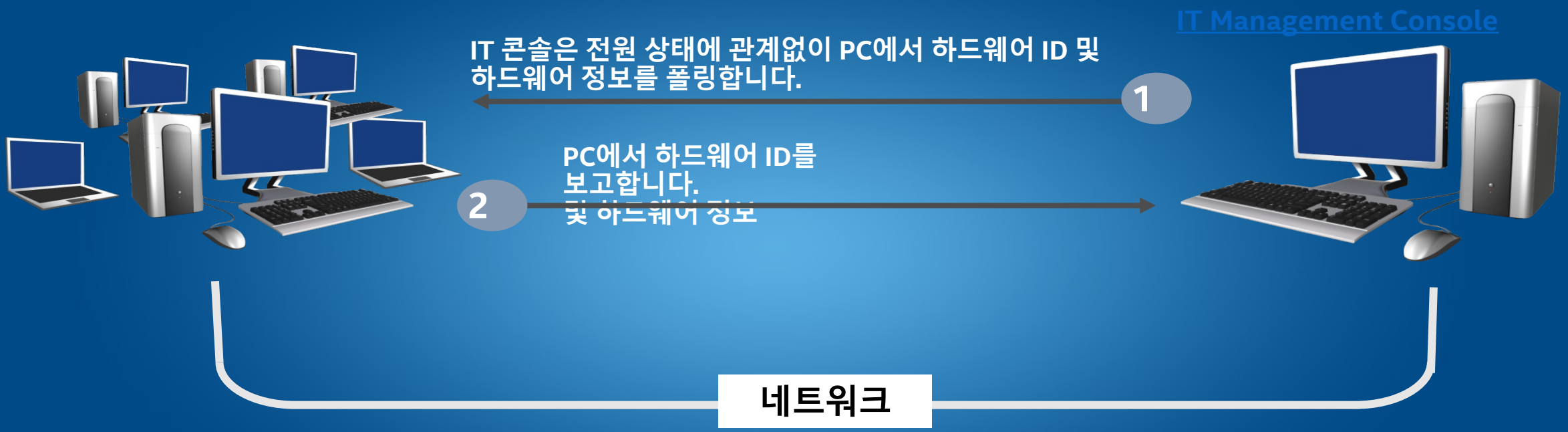
원격 관리 콘솔



- KVM 원격 제어 세션은 재부팅 후에도 지속됩니다.
- 유선 LAN과 무선 LAN에서 모두 작동

intel

HARDWARE INVENTORY



- 수동 검사보다 빠르고 정확합니다.
- CPU, 메인 보드, 메모리, 스토리지 정보

EVENT LOG

IT 콘솔은 전원 상태에 관계없이 하드웨어 이벤트 로그 데이터를 PC에 폴링합니다.

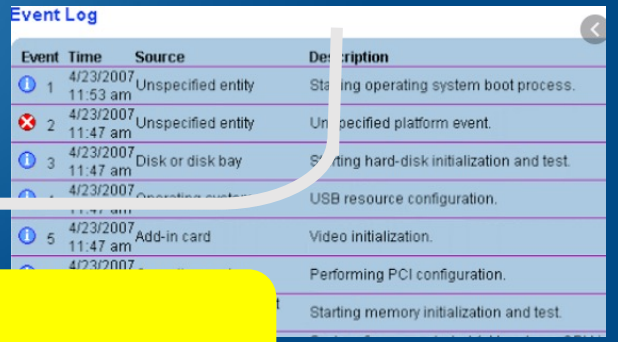
1

PC는 하드웨어 이벤트 로그 데이터를 제공합니다.

2

IT Management Console

Network



- 시스템 충돌 시 먼저 하드웨어 이벤트 로그 확인
- 빨간색 표시는 심각도가 높음을 의미합니다.

intel

INTEL VPRO® 플랫폼의 첨단 관리기술 - 사용사례

Hardware KVM
OS가 비정상이나 BIOS 환경에서도 원격에서 화면을 보거나 설정변경

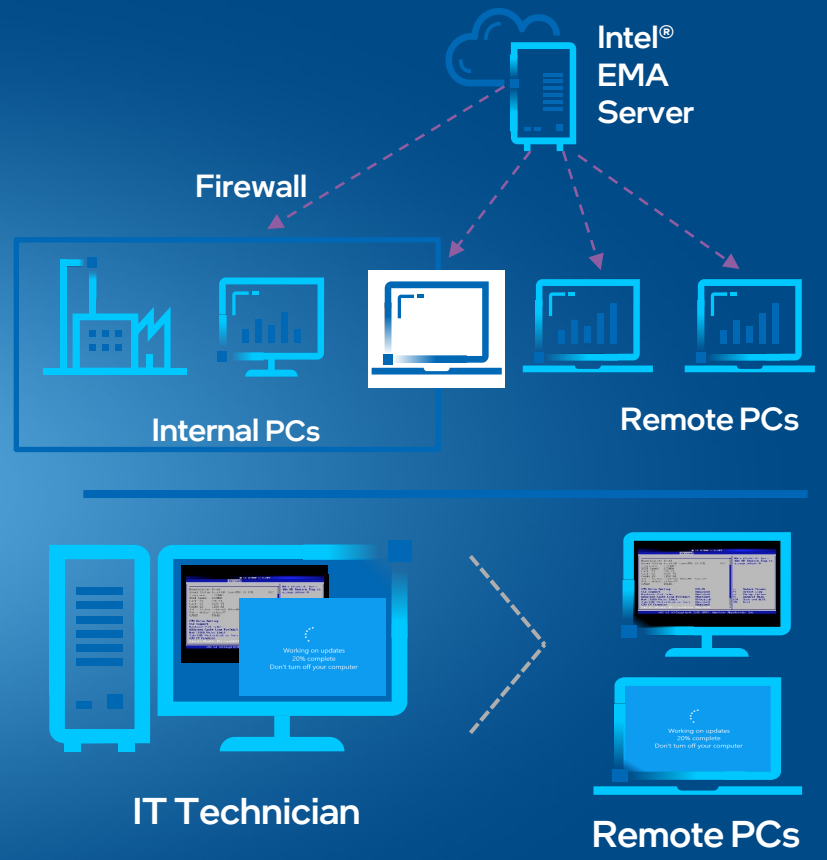
Remote Power Control
보안상 안전하게 원격 PC의 전원을 On/Off

Boot Redirection
원격의 OS 이미지로 Booting이나 설치

Upgrade Management
다수의 PC의 OS를 업그레이드 할 때 유용

Hardware Alarm Clock
Wake-up을 설정해서 한 번이나 주기적으로 PC의 전원을 On

Unattended System Control
무인 PC나 시스템을 원격으로 관리



소프트웨어의 한계를 하드웨어 원격관리로 극복

intel

13세대 인텔 코어 모바일 프로세서

리더십 플랫폼에 확장 가능한 성능을 제공

AI
is Everywhere

업무용 AI Use Case Targets for MTL Launch Moment

협업(NPU)

더 풍부한 협업 &
더 빠른 멀티태스킹,
보존된 배터리 수명

생산성(NPU)

로컬 AI Assistant를 통한
생산성 향상
AI 기반 번역

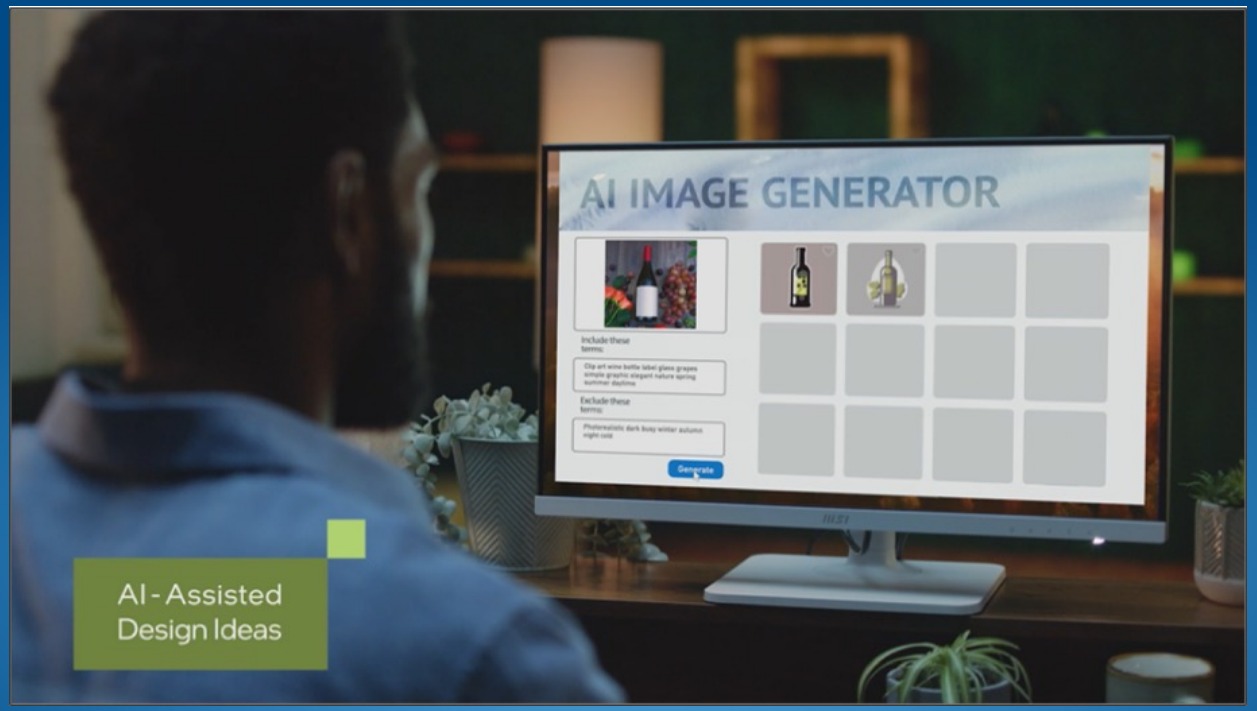


사진 편집(GPU)

더 빠른 AI 기반 사진 필터

비디오 편집(NPU)

더 높은 품질의 미리보기 및
더 빠른 비디오 내보내기

보안(GPU)

AI로 강화된 랜섬웨어 및 크립토재킹 탐지

텍스트를 이미지로(CPU/GPU/NPU)

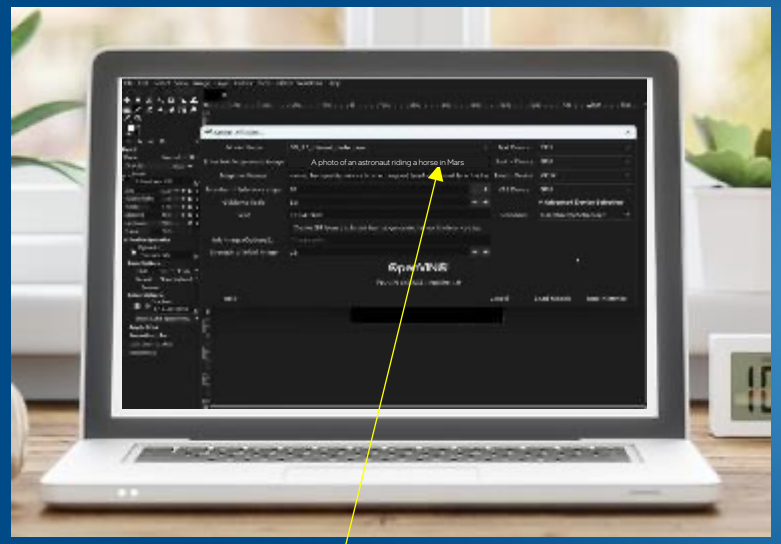
몇 가지 설명 단어를 입력하여 이미지 생성

Microsoft Teams · Windows Studio Effects · Rewind · Microsoft Defender for Endpoint · CROWDSTRIKE · Adobe · Lr · Pr · wondershare · GIMP

all while KEEPING YOUR DATA PRIVATE from the cloud

intel

텍스트 프롬프트에서 이미지 생성하기



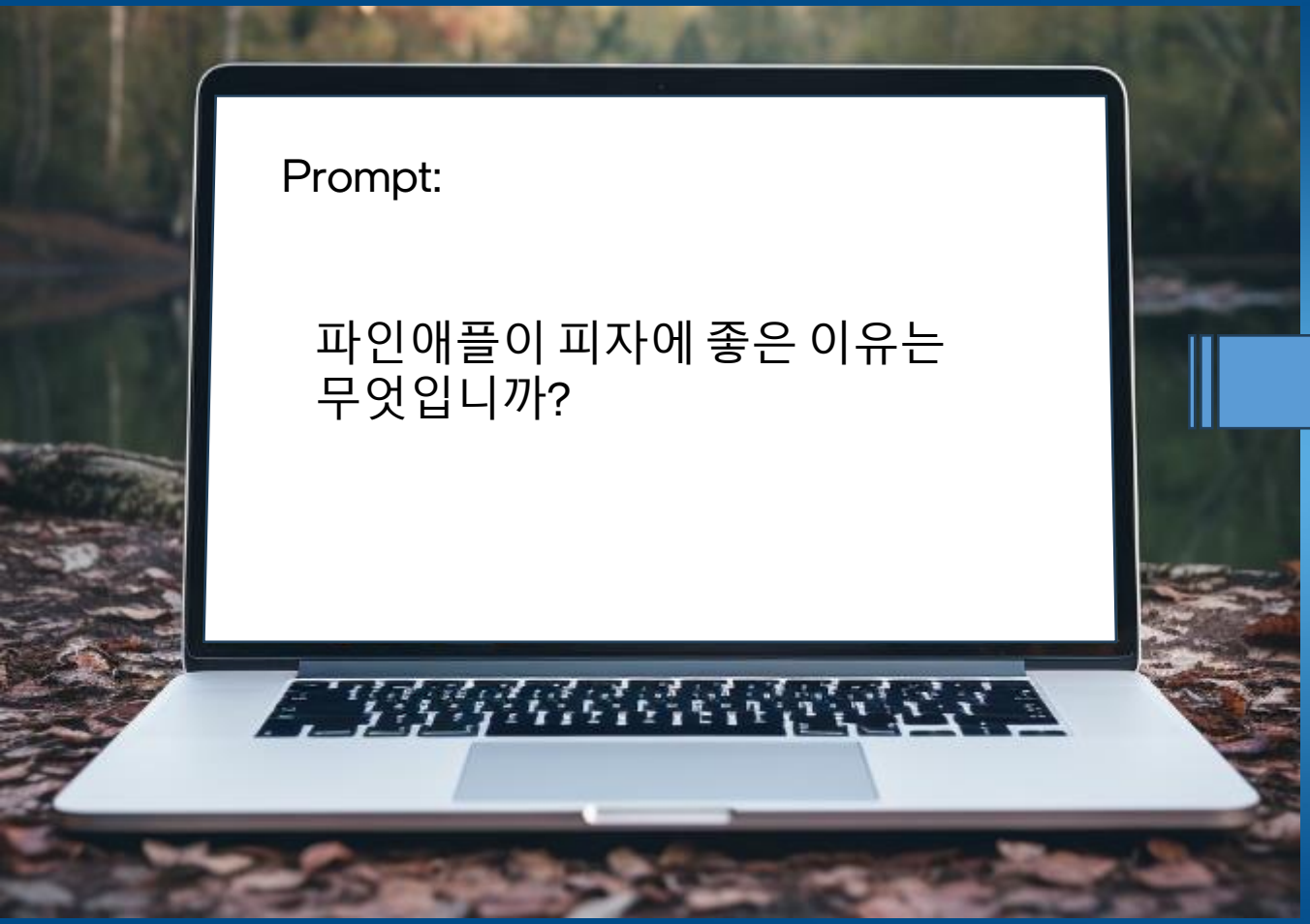
프롬프트: '화성에서 말을 타고 있는 우주 비행사의 사진'

- 출력을 구체화하기 위해 이미지 렌더링을 여러 번 반복해야 합니다.
- 특정 스타일에 대한 미세 조정을 위해 로컬 데이터 세트를 사용

Intel Core Ultra는 초당 여러 번의 반복을 렌더링할 수 있습니다.

intel.

텍스트 프롬프트에서 단락, 목록, 에세이 생성



일부 사람들이 피자에 파인애플을 즐기는 몇 가지 이유는 다음과 같습니다.

1. **달콤하고 짭짤한 대비:** 달콤하고 육즙이 많은 파인애플과 치즈, 소스 및 기타 토핑의 짭짤한 맛 사이의 대비는 일부 개인이 즐기는 독특하고 흥미로운 풍미 프로필을 만들 수 있습니다.
2. **질감의 다양성:** 파인애플은 부드럽고 약간 쫄깃한 농도로 피자에 다른 질감을 더하여 고기나 야채 토핑의 일반적인 질감에서 벗어날 수 있습니다.
3. **균형 잡힌 맛:** 파인애플의 단맛은 햄이나 베이컨과 같은 특정 토핑의 짠맛의 균형을 맞추는 데 도움이 되어 풍미의 조화로운 조화를 제공할 수 있습니다.
4. **개인 취향:** 어떤 사람들은 단순히 피자에 파인애플의 맛을 즐기며 그 조합이 만족스럽고 즐겁다고 생각합니다.

Examples for illustrative purposes

intel


intel