# Windows 11 Upgrade

## The Hardware Security Focused Refresh

VERSION 1.0
Commissioned by Intel

IOActive®

The impact of Windows 11 on **IT and SecOps represents a major inflection point**, moving from a software-based security model to a best-of-both-worlds hardware-and-software-based model. By pairing **Windows 11** with **Intel vPro®**, organizations can go beyond compliance and **exceed Secured-core PC requirements with hardware-enhanced capabilities.**

# Table of Contents

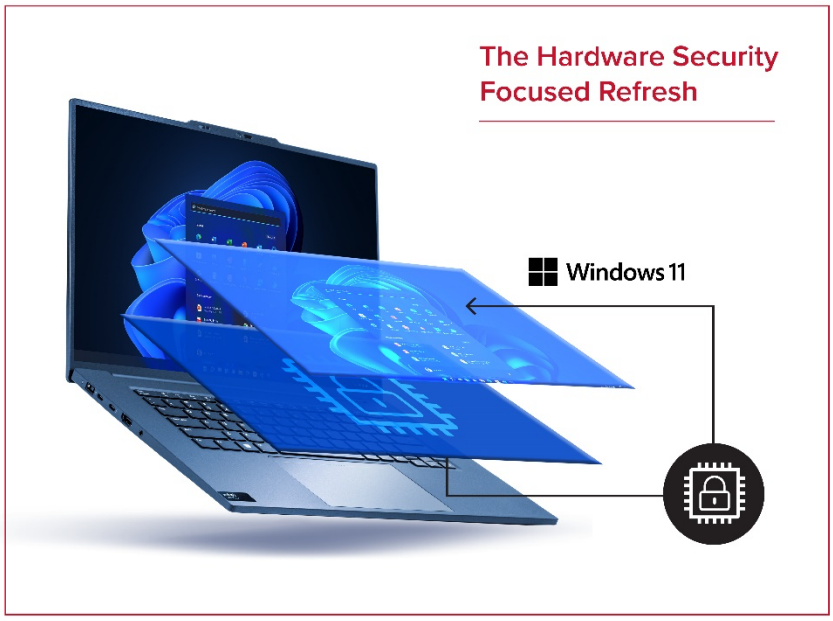
# Introduction

As a leading cybersecurity research house, IOActive produces whitepapers to reflect on notable events in security. The impact of Windows 11 on IT and SecOps presents a major inflection point that deserves our attention. IOActive works closely with both Microsoft and silicon security vendors. In this whitepaper, we focus on how PCs powered by Intel® Core™ Ultra processors and Intel vPro® offer a compelling strategy for Windows 11 upgrades.

Windows 10's End of Life (EoL) is slated for October 14th, 2025. After this date, it will no longer be supported, and businesses are expected to upgrade to Windows 11; however, this upgrade is entirely unlike previous Windows upgrades in that strict hardware requirements are needed to support Windows 11.

Oftentimes, such "forced" hardware upgrades could simply be seen as "planned obsolescence;" however, in this case, the hardware requirements are there to help with overall cybersecurity, as Windows moves from a primarily software security model to a best-of-both-worlds hardware and software model.

Windows 11 represents a significant opportunity to improve the overall enterprise security posture. As we will explore, there are different PC hardware strategies that can be taken with different security outcomes.



# Understanding the Evolution of Security Models from Windows 10 to Windows 11

Windows 10 was launched in 2015 with a comprehensive software-based security feature list,[1] including Windows Defender Antivirus, Windows Firewall, and data encryption technologies like BitLocker. These solutions have been effective in protecting systems from a plethora of cyber threats; however, software-based solutions can only take you so far in protecting data and systems and can still be vulnerable to sophisticated malware, zero-day attacks, and other Advanced Persistent Threats (APTs). Software, by its very nature, relies on the trustworthiness of the underlying hardware, which, if compromised, can render software defenses useless.

Enter Windows 11, shifting focus from software-only to a best-of-both-worlds software-and-hardware-based security solution.[2] Providing a more robust, tamper-resistant security posture. Windows 11 is built with layers of hardware and software defenses, helping ensure "secure by default" and "secure by design" principles. Microsoft's latest eBook shows this approach works: out-of-the-box security features in Windows 11 led to a reported 62% drop in security incidents.[3]

Modern Copilot+ PCs, such as those powered by Intel Core Ultra Processors (200v Series), are built with security at their foundational level. At the heart of this enhanced security is the Microsoft Pluton security processor. Enabled by default, the Microsoft Pluton Security Processor is a secure crypto-processor integrated directly into the CPU's System-on-Chip (SoC), providing a hardware-based root of trust, secure identity, attestation, and cryptographic services. On Copilot+ PCs, Intel Partner Security Engine (IPSE) hosts the Pluton firmware, offering hardware-based isolation like AMD and Qualcomm implementations. Allowing Intel PCs to leverage Pluton's enhanced security (firmware patching, key protection, and tamper resistance) while maintaining ecosystem-wide standardization across hardware vendors.

Pluton is designed to protect sensitive assets like credentials, encryption keys, and user identities by isolating them from potential attackers, even if they gain full access to the system. Pluton also supports the Trusted Platform Module (TPM ) 2.0 industry standard, enabling secure use of Windows features such as BitLocker, Windows Hello, and System Guard. Unlike traditional TPMs, Pluton receives firmware and feature updates directly from Microsoft via Windows Update, reducing the risk of supply chain attacks and ensuring consistent, up-to-date protection.

Complementing Pluton, Windows 11 includes several layered security features:

- **Secure Boot**: Ensures only trusted, signed software is loaded during the boot process, protecting against rootkits and other low-level threats.
- **Virtualization-Based Security (VBS)**: Leverages hardware virtualization, such as Intel vPro security features, to isolate critical components like credentials and system processes. This isolation helps meet regulatory standards like PCI-DSS and HIPAA, offering robust data protection even if the operating system is compromised.

[1] https://learn.microsoft.com/en-us/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10

[2] https://www.microsoft.com/insidetrack/blog/hardware-backed-windows-11-empowers-microsoft-with-secure-by-default-baseline/

[3] https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/MSFT-Windows11-Security-book_Sept2023.pdf

Taking this to the next level, Microsoft designed Secured-core PCs to provide an "On-By-Default" security for businesses and users to provide three core pillars of protection:

- Protecting identities from external threats
- Securing the operating system from malware
- Defending against hardware and firmware attacks

To properly support these secure pillars, specific hardware security requirements are necessary.

# To Standard and Beyond: The Essential Secured-core PC Hardware Security Requirements

Microsoft Secured-core PCs are designed to provide an extra layer of protection against firmware, hardware, and software attacks. By integrating hardware, firmware, and operating system security features, these PCs, available from all major OEMs,[4] offer greater protection against cyber threats across three capability levels.

| Standard Hardware Security | Enhanced Security All Standard Hardware | Exceeds Enhanced Security |
|---|---|---|
| Secure Boot | All Standard Hardware Security Features | All Enhanced Security Features |
| TPM 2.0 | HVCI Enabled – Memory Integrity | DRTM |
| HVCI Capable | | SMM |

## Standard Hardware Security: A Foundation for Operational Confidence

These baseline security features are essential for SecOps teams aiming to reduce attack surfaces and ensure system integrity:

- **Secure Boot** ensures systems start in a known-good state, blocking unauthorized or malicious code at the earliest stage. This simplifies threat hunting and incident triage by ensuring a clean, verifiable baseline from power-on.
- **TPM 2.0** provides hardware-based protection for sensitive assets like encryption keys and credentials. For SecOps teams, this enables stronger authentication, secure storage, and reliable attestation, crucial for zero trust architectures and compliance.
- **Hypervisor Code Integrity (HVCI) Capable (Memory Integrity)** provides the ability to enforce kernel-level code integrity, helping prevent advanced malware and kernel exploits. Even if not enabled by default, its availability lays the groundwork for stronger runtime protections.

## Enhanced Hardware Security: Raising the Bar on Endpoint Protection

To meet the enhanced hardware security requirements, all of the standard hardware security features must be enabled as well as HVCI. By enforcing code integrity at runtime, HVCI boosts SecOps teams' ability to prevent exploits that could bypass traditional security controls, which is especially valuable in environments with elevated risk or compliance demands.

[4] https://www.microsoft.com/en-us/windows/business/windows-11-secured-core-computers

## Exceeds Enhanced Security: Advanced Defenses for Modern Threats

For organizations with high security requirements, these advanced capabilities offer deeper resilience:

- **Dynamic Root of Trust for Measurement (DRTM)** allows systems to shift from an untrusted to a trusted state during boot. This provides a flexible but secure boot process that enables trusted attestation, even in environments with complex firmware stacks or potential supply chain concerns.
- **System Management Mode (SMM) Protection** isolates critical system functions from the operating system, offering a defense layer even if the kernel is compromised. This is particularly important for protecting against firmware-level attacks that traditional tools might miss.

By building security directly into the hardware and enabling these advanced protections, SecOps teams can better defend against APTs, streamline incident response, and maintain confidence in the integrity of their endpoint fleet.

Understanding the technical details behind hardware-based security can be complex, but what truly matters is the operational value these features can deliver. With Windows 11 devices that exceed enhanced hardware security, organizations gain tangible security and compliance advantages.

Here's a quick look at how these capabilities translate into real-world benefits:

- **Ransomware and Malware Resistance** - Intel Boot Guard and the Converged Security and Management Engine (CSME) ensure trusted firmware execution and Secure Boot. These features, combined with HVCI supported by Intel VT-x for virtualization-based security, work together to block untrusted software at startup and ensure only verified kernel-level code runs. This reduces attack surfaces, giving adversaries fewer entry points and providing SecOps teams with a clean, trusted baseline—crucial for rapid remediation. Additionally, Hardware-Enforced Stack Protection delivers runtime mitigations, while Microsoft Edge and Windows Defender offer further layers of software protection.
- **Credential Protection & Zero Trust Foundations** - Intel Platform Trust Technology (PTT) provides embedded TPM functionality, while Microsoft Pluton integrates security directly into the CPU, reducing the attack surface compared to traditional discrete TPMs. By safeguarding cryptographic keys and identity assets in hardware, these technologies create strong defenses against credential theft. This foundation supports secure authentication and conditional access models. Credential Guard, LSASS, and Windows Hello work in tandem with these hardware-based protections to further enhance security.
- **Firmware Attack Mitigation** - Enabled through Intel TXT, validating boot processes at the hardware level, DRTM dynamically establishes a trusted state during boot, even if early firmware is untrusted, closing a major gap often exploited in supply chain or rootkit-style attacks.
- **Advanced Threat Detection & Response (SMM Protection)** - By isolating system-level checks from the operating system, SMM adds a protective layer that can catch and respond to threats that evade operating-system-level security tools.
- **Regulatory & Compliance Readiness (All Features Combined)** - From HIPAA to PCI-DSS, these combined protections support policy enforcement, audit trails, and secure configuration baselines, helping reduce both risk and audit fatigue.

The exceeds enhanced hardware security features work in concert with the operating system and software security features provided by Windows 11. Devices with Windows 11 exceeds enhanced hardware security features aren't just more secure, they're operationally smarter, giving SecOps teams the visibility, control, and assurance they need in today's evolving threat landscape.

# Inside Intel vPro


PCs built on Intel vPro are specifically engineered to deliver the superior performance, robust security, and enhanced manageability demanded by high-assurance enterprise deployments. In today's enterprise environment, security is no longer optional, it's foundational. Intel vPro delivers 30 hardware security features that enable Win 11, Pluton, and Defender hardware usages referenced in this paper. Together this offers a robust, integrated platform engineered for organizations that demand high assurance, regulatory compliance, and zero-compromise productivity.

**01. Out of Box - Security at First Boot**

Every Intel vPro-based system with Windows 11 ships with essential security features pre-enabled. This "secure by default" approach ensures rapid deployment without sacrificing protection, ideal for enterprise IT environments that require scalability and consistency.

**02. Intel vPro Surpasses Microsoft Secured-core PC L3 Requirements**

Intel vPro goes beyond even the higher requirements of Secured-core PC, with additional security features and services to help SecOps teams with the deployment and support of their hardware fleet.

- **Intel Total Memory Encryption - Multi-Key (TME-MK)** helps prevent data exposure from physical memory attacks, ensuring sensitive data (e.g. credentials, encryption keys, IP) remains protected even if an attacker gains physical access to a system. Intel TME-MK support adds layered protection, limiting potential exposure in targeted attacks.
- **Intel Virtualization Technology – Redirect Protection (VT-rp)** hardens virtual environments against memory redirection attacks. Intel VT-rp reduces the risk of lateral movement between virtual machines and improving isolation and containment, which is critical for breach response and multi-tenant environments.

- **Intel Threat Detection Technology (TDT)** enhances endpoint threat visibility using hardware-level telemetry. Intel TDT detects advanced threats (e.g. ransomware behavior) that software-only tools might miss, enabling earlier detection and more accurate response through AI-powered insights.
- **Intel Active Management Technology (AMT) – BSOD Recovery** enables remote recovery from system crashes, even if the operating system is down. Intel AMT – BSOD Recovery minimizes downtime and accelerates incident response during outages or mass-impact software failures, keeping operations resilient and recoverable at scale.
- **Intel Innovation Platform Framework (IPF) – Device Discovery** offers real-time visibility into device configurations and status. Intel IPF – Device Discovery supports proactive asset hygiene, vulnerability management, and policy compliance by ensuring systems stay aligned to best-known secure configurations.

Deploying Intel vPro-based systems with Microsoft Pluton on Windows 11 ensures your business is not only compliant but also strategically prepared for tomorrow's cybersecurity challenges. This is more than just protection; it's long-term operational resilience.

**03. Third-Party Assessed for Compliance**

The security capabilities of Intel vPro are assessed against eight globally recognized compliance standards, reducing audit burdens and accelerating certifications across industries like finance, healthcare, and government.

A study by Coalfire[5] showed the effectiveness of silicon-enabled security features in helping achieve federal and public sector security control standards. They validated how each Intel vPro security feature addressed key compliance standards, including NIST SP800-193 Platform Resiliency Guidelines, NIST SP800-147 BIOS Protection Guidelines, and TCG PC Client FIM Specification (a.k.a. NIST SP800-155).

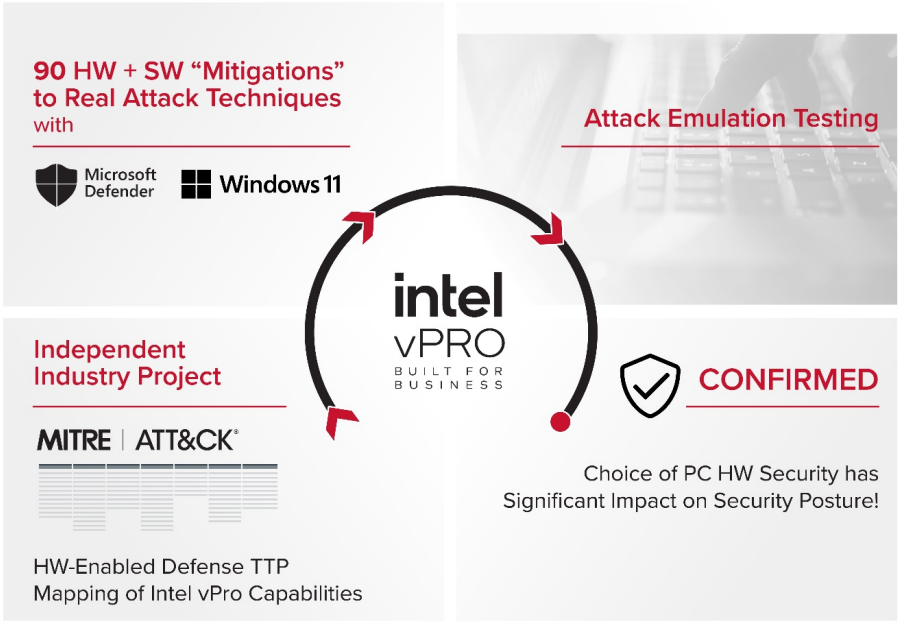
[5] https://www.intel.com/content/www/us/en/content-details/756188/intel-vpro-platform-security-product-applicability-for-federal-public-sector.html

### 04. Industry Driven Validation

With threat models mapped and validated through MITRE ATT&CK frameworks, Intel vPro and Microsoft Windows provide real-world protection aligned with advanced adversary tactics. The following diagram shows a real-world attack kill chain, threat vectors, and the Intel and Windows security features that deliver impact.

| Kill Chain Stage | Threat Vector | Intel Security Features | Windows Security Features | Sample Attacks |
|---|---|---|---|---|
| Initial Access | Phishing email, malicious links or USB | Intel Boot Guard, TPM /Intel PTT, Intel TME, CET | Secure Boot, HWESP - Shadow Stack | Phishing kits, malicious Office macros, exploit kits (e.g., Rig), removable media |
| Execution | User opens a malicious document or executable | Intel CET, Intel Thread Director, Intel CFG Support | HW Enabled Shadow Stack | Office macros, PowerShell, Windows Script Host (wscript), mshta, LOLBins |
| Persistence & Privilege Escalation | Malware drops persistence mechanisms or drivers, malicious drivers / rootkits | Optional - TDT AMS | Optional - MDE<br>VBS/HVCI, Secure Boot | Startup registry keys, scheduled tasks, service creation, DLL sideloading |
| Defense Evasion | Attacker disables AV or modifies memory | Intel VT-x/EPT<br>Intel SGX, TPM + Boot Guard, Intel ME Protections | MDE | Process injection tools (e.g., Cobalt Strike), obfuscated scripts, disabling AV via scripts |
| Credential Access | Memory scraping, LSASS dump, registry read,<br>Unsecured Credentials | VT-d (DMA Protection), TPM 2.0/PTT | Windows Hello / Credential Guard | Mimikatz, LaZagne, ProcDump, LSASS access tools, SAM/SECURITY hive extractors |
| Lateral Movement | RDP, SMB, or remote execution | Intel PTT, Intel VT Networking Isolation | Credential Guard | PsExec, RDP, SMB, WMI, remote PowerShell, Impacket , pass the hash |
| Collection | Keylogging, Credential in file | intel-aes-ni / Intel PTT | Windows Hello | Credential harvesting , internal spearphishing |
| Impact | Ransomware, data exfiltration, disk wipe | BitLocker (TPM/PTT), Intel Boot Guard, Intel TDT (ransomware detect/AMS) | MDE | Ransomware (e.g., Ryuk, LockBit), data wipers, exfiltration tools like Rclone or MEGA-cli |

Earlier this year, in collaboration with Microsoft, CrowdStrike, and AttackIQ, Intel mapped and ranked the hardware-optimized software security features against MITRE ATT&CK framework[6] using the full set of Intel vPro security protections, some 30 hardware features, on a typical enterprise security software stack. This provided, in total, 90 hardware mitigations against real-world attacks when using Windows 11 and Windows Defender.




**05. Achieve Enterprise-Class Security Posture**

Together, Intel vPro and Pluton form a layered defense strategy that empowers IT leaders to confidently enforce zero-trust architectures, ensure business continuity, and scale securely in hybrid or cloud-native environments.

[6] https://attack.mitre.org/

# Conclusion

Upgrading from Windows 10 to Windows 11 is more than a user experience refresh, it's a strategic opportunity to modernize your organization's security architecture. With built-in protections like TPM 2.0, Secure Boot, VBS, HVCI, and Windows Hello, Windows 11 sets a new baseline for device security. Integrated tools such as Microsoft Defender Antivirus, SmartScreen, and Application Control offer additional layers of real-time threat protection.

Intel vPro hardware features go beyond the requirements needed for the Windows 11 hardware refresh and the requirements for Secured-core PC; however, when looking at the security controls and compliance standards required in many verticals, the enterprise-grade validation that Intel vPro-based devices receives is a benefit that provides real dollar savings and long-term value.

For enterprises, the transition brings a clear advantage: by pairing Windows 11 with Intel vPro, organizations can go beyond compliance and exceed Secured-core PC requirements with hardware-enhanced capabilities like Intel TME-MK, Intel VT-rp, Intel TDT, and Intel AMT. These features offer operational benefits for SecOps teams, from accelerated recovery and advanced threat detection to improved device visibility and remote manageability.

Unlike traditional security projects that require complex deployments and change management, this upgrade delivers an out-of-the-box uplift to enterprise-grade security. It's a rare opportunity: a fast, impactful win for security, IT, and business leadership alike.

# References

Advanced Micro Devices, Inc. (2023). *AMD Product Security*. Retrieved from https://www.amd.com/en/resources/product-security.html

Intel Corporation. (2023). *Bug Bounty Program*. Retrieved from https://www.intel.com/content/www/us/en/security-center/bug-bounty-program.html

Li, M., Zhang, Y., Wang , H., Li, K., & Cheng, Y. (2021). CIPHERLEAKS: Breaking Constant-time Cryptography on AMD SEV via the Ciphertext Side Channel. *30th USENIX Security Symposium* (pp. 717-732). Virtual: USENIX Association.

NIST. (2023). *National Vulnerability Database*. Retrieved from https://nvd.nist.gov/

# Appendix A: Additional Information

## About IOActive

IOActive, a trusted partner for Global 1000 enterprises, provides research-fueled security services across all industries. Our cutting-edge cybersecurity teams provide highly specialized technical and programmatic services including full-stack penetration testing, program efficacy assessments, and hardware hacking. IOActive brings a unique attacker's perspective to every engagement to maximize cybersecurity investments and improve the security posture and operational resiliency of our clients. Founded in 1998, IOActive is headquartered in Seattle with global operations, including state of the art hardware hacking labs in Seattle, WA, Madrid, Spain and Cheltenham, UK.

For more information, visit: http://www.ioactive.com/

Read the IOActive Labs Research Blog: https://www.ioactive.com/resources/research/

Follow IOActive:

Facebook: https://www.facebook.com/IOActive

LinkedIn: https://www.linkedin.com/company/ioactive-inc/

X: https://x.com/IOActive