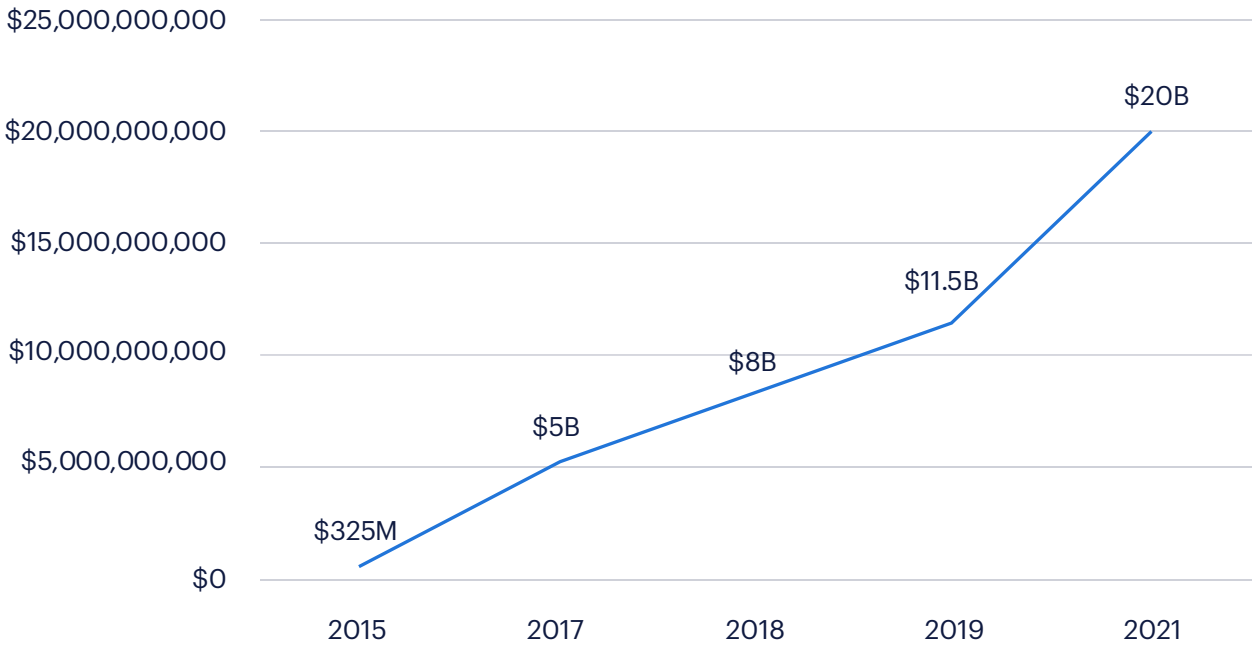
windows 11 — why its security features make upgrading worthwhile.

randstad
technologies

On the cusp of releasing Windows 10 in 2015, a Microsoft developer evangelist speaking at a company event prematurely claimed that "Windows 10 is the last version of Windows." One of the major reasons that prediction did not come to pass is the cybersecurity landscape. As the chart below indicates, ransomware attacks alone in 2021 were anticipated to be more than 60 times the cost compared to when Windows 10 was released in 2015.

predicted ransomware damages 2015-2021



Source: https://securityboulevard.com/2020/02/20-ransomware-statistics-youre-powerless-to-resist-reading/

Because of its widespread use, system vulnerabilities and its reliance on users to enable various security features in Windows 10, 83 percent of all malware attacks in the first three months of 2020 were directed toward Windows computers. Increasing security is one of the primary, if not the primary reason Windows 11 was developed. To achieve this, Windows 11 has strict hardware and configuration requirements that might require hardware upgrades or replacement.

This short paper addresses how Windows 11 enhances cybersecurity, facilitates remote work and can potentially reduce costs stemming from security incidents. A follow-up piece to this one will elaborate on new features and capabilities of the new OS.

windows 11 highlights security

Windows 10 offered users an array of "optional" security tools. Windows 11 takes the options out of the users' hands. Windows 11 smoothly integrates core security features by default. The system's updated hardware requirements mean these features are enabled out of the box.

Here's a brief overview of the new — or automatically enabled — Windows 11 security measures.

the trusted platform module (TPM)

The TPM, or Windows 11's hardware root of trust, serves as a hardware-based foundation for the operating system's security. A TPM chip is a secure crypto-processor that helps with generating, storing and limiting the use of cryptographic keys. A TPM includes multiple physical security mechanisms that make it tamper-resistant. Malicious software is prevented from tampering with the TPM's security functions. These hardware requirements should significantly reduce risks from malware and ransomware.

UEFI secure boot

The PC industry created secure boot to help ensure that when a device boots it only uses software verified by the Original Equipment Manufacturer. As the PC boots, the firmware validates each piece of boot software including the operating system. After the validity is verified, the firmware gives control to the operating system. Secure boot is intended to prevent the bad guys from hijacking the boot process and replacing the intended software with malicious software.

core isolation features

Although these features are available in Windows 10, in 11 they are automatically enabled. Here are short descriptions of the five components of this functionality:

- Virtualization-based security (VBS) – An isolated region of memory is created for security features or data and kept separate from the rest of the operating system, making it more difficult to tamper with and providing an additional layer of protection.
- Hypervisor-protected code integrity (HVCI) – The code integrity (CI) decision-making function is isolated from the rest of the Windows operating system using virtualization-based security and hardware technology, protecting the kernel memory and virtual environment.
- Memory integrity – This is a feature of core isolation which runs inside the hypervisor-protected container that verifies the integrity of the code, making it nearly impossible to gain access to the Windows kernel.
- Memory access protection – PCI hot plug devices connected to external PCIe capable ports (e.g., Thunderbolt™ 3) protect PCs against drive-by direct memory access (DMA) attacks, preventing access to sensitive information or malware attacks that bypass the lock screen or remotely control PCs.
- Device-level firmware protection – Firmware and hardware security mechanisms are in place offering protection before the PC is even booted up, removing vulnerabilities that give access to systems – often without users knowing it.

growth in remote work spurred windows 11 development

There are almost as many surveys about organizations' policies regarding remote work as there are remote workers, but one thing appears certain, even if hybrid work-from-home/in-office models become the norm, remote work is here to stay. Remote work has been embraced by the workforce, with some workers making it a prerequisite for prospective employers — but it's not a panacea for cybersecurity issues.

Home-based Windows 10 users were exposed to a number of risks that are significantly reduced by using Windows 11:

reduced risks in moving from windows 10 to 11 for home-based workers

vulnerability	Windows 10	Windows 11
OS security settings	• Many security settings are optional or user enabled • Bolt-on security approach	• Built-in security by default — improved security baselines • Device Health Attestation (DHA) capabilities
Phishing	• Accidental clicking on malicious link leads to multiple threats and risks to the user/device	• Improved application isolation using container virtualization • Improved passwordless integration reduces risk
Ransomware	• Many ransomware mitigations required advanced configuration	• Data protection improvements including virtualization-based security (VBS) as default • Hypervisor-protected Code Integrity (HVCI) as default
Improperly secured VPN/home network	• Network-based security threats • Local network often trusted by default	• Chip-to-cloud security • Zero Trust principles • Protected access to encryption keys and user credentials behind a hardware barrier
Open/unsecured wireless network	• Network-based security threats • Local network often trusted by default	• Chip-to-cloud security • Zero Trust principles • Protected access to encryption keys and user credentials behind a hardware barrier
Data exfiltration/data loss	• Optional protections required advanced configuration	• No user or device access until safety and integrity is proven • Improved controls over application access/isolation
Malicious software	• Software only protections may not guarantee security	• Isolates software from hardware to provide improved security assurances • Device Firmware Control (DFCI) capabilities

According to a study published by HP, global cyberattacks increased by 238 percent early in the pandemic — and many of these attacks were directed at remote workers. One aspect of remote work is especially troubling for those responsible for cybersecurity — the propensity of people working from home to use personal devices for work. The HP study also found that 88 percent of information technology decision makers said they worry their risk of a breach has risen because employees are using personal devices for work that were not built with business security in mind. Some of this risk can be mitigated if the personal device uses Windows 11 (which we recommend if the device can run the new OS). Not only does Windows 11 enable an enterprise-class operating system on tablets and phones offering a consistent cross-platform user experience, but it also maintains an enterprise OS security profile for BYOD, which might allow the security team to get a better night's sleep.

Windows 11 also provides home home based workers access to Microsoft Azure Attestation, which supports what we have termed "Zero Trust at Home." Attestation is a unified solution for remotely verifying the trustworthiness of a platform and the integrity of internal software binaries. It enables advanced security features such as Azure Confidential Computing and Intelligent Edge protection. Attestation offers confidence both to the home user and the IT department that only legitimate software is running on trusted hardware.

how windows 11 reduces the costs of security incidents

Early in 2018, the Specter and Meltdown hacks allowed bad players access to protected data. These two vulnerabilities were remedied through a hardware fix — but not before an estimated $18 billion was spent to mitigate the vulnerabilities found as a result. To protect users against these types of "transient execution" attacks that target hardware design flaws, Windows 11 requires the TPM 2.0 security chip, as well as a CPU released within the past four years.

In giving users guidance for Windows 11, Microsoft is encouraging users to enable the system's Tamper Protection feature to protect themselves against ransomware. The software giant claims that Windows 11 will prevent 60 percent of malware attacks. Given the cost of recovering from a cybersecurity attack, Windows 11 has the potential for helping organizations realize significant savings. In 2020, the average total cost of recovery from a ransomware attack was $761,106. By 2021, that number had grown to $1.85 million. The average ransom now paid is $170,404, and even after paying a ransom, only eight percent of organizations retrieved all their data — and nearly a third only got back less than half.

As noted earlier, threat protection in Windows 11 is not solely focused on hardware-based countermeasures. As the following chart indicates, Windows 11 offers multiple layers of security protection including elements that defend against potential vulnerabilities posed by cloud services, user identity and privacy, applications and the operating system, as well as the computer's hardware.

layers of protection in windows 11

cloud

Cloud Services

OneDrive & OneDrive Vault, AAD, MSA, Attestation, Modern Device Management (MDM) (e.g., Intune)

identity and privacy

Secured Identity

Windows Hello
Biometrics
Fast Identity Online (FIDO)
Authenticator Application
Smart Cards
Access Control
Credential Protection

Privacy Controls

Transparency and Audit Trail
Location, Camera and Microphone

application

Application Security

Application Control
User Account Control (UAC)
App Isolation (inc Office + Edge)
Secure Apps

operating system

Encryption and Data Protection

BitLocker
Encrypted Hard Drive
Email Encyption

Network Security

Transport Layer Security (TLS)
DNS Security
Bluetooth Protection
Wi-Fi Security
VPN
Windows Defender Firewall
SMB File Services

Virus and Threat Protection

Microsoft Defender Antivirus
Microsoft Defender SmartScreen
Microsoft Defender for Endpoint

System Security

Trusted Boot
Cryptography
Certificates
Code Signing and Integrity
Device Health Attestation
Security (setting) App

hardware (chip)

Hardware of Root-of-Trust

TPM 2.0
Microsoft Pluton Security Processor

Silicon Assisted Security

Secured Kernel
Identity Protection
Firmware Protection
DMA and Memory Protection

security foundation

Security Assurance

SDL
Bug Bounty

Certification

CC, FIPS

Secure Supply Chain

Software Bill of Materials (SBOM), Code Signing

Source: Windows 11 Security Guide: Powerful security from chip to cloud.

The bottom line on Windows 11 is that although this new operating system has a heavy security focus, this is only one of its many strengths. Tom Ruden, senior solutions architect at Randstad Technologies, brings perspective to the necessity of creating a new version of Windows: “The advances in Windows 11 from the OS aspect are significant — like supporting non-PC form factors and providing a consistent experience across devices, while offering support for Android applications on devices from the Microsoft Store. However, for the enterprise, we see security and management as the main drivers for Windows 11 adoption including aligning with and accelerating the M365 security stack, providing a hardware root-of-trust to prevent malware and ransomware and facilitating the adoption of a passwordless environment.”

conclusion: randstad's microsoft partnership on windows 11

Windows 11 is the most secure Windows OS ever. It's built for the cloud and offers the best of the cloud: contextual security, collaboration and user experience. We recommend that you plan your upgrade to Windows 11 now. The "modern workplace" is here to stay, and Windows 11 provides your company the security and collaboration updates you need to operate from anywhere in the world now and in the future.

The barriers to entry for this version are the lowest of any Windows OS to date, and the benefits are significant. Users can easily adapt to enjoy the smooth UI benefits on their PCs and collaborate securely while moving smoothly from PC to tablets and phones. From a licensing standpoint, it's a no-cost upgrade for Windows 10. From a hardware standpoint, most modern PCs will qualify, and more likely will require a simple UEFI BIOS settings change. Finally, an OS upgrade to Windows 11 is a great time to implement the Zero Trust objectives that are likely on your priority list already.

As a longtime Gold-Competency Windows and Devices partner, Randstad has a proven delivery methodology specifically for OS upgrades that is focused on minimal interruptions and maximum impact while working with an enterprise's users and their devices. This means building a roadmap and a comprehensive zero- or one-touch approach that considers both today's requirements and tomorrow's features, and includes security, collaboration and device management.

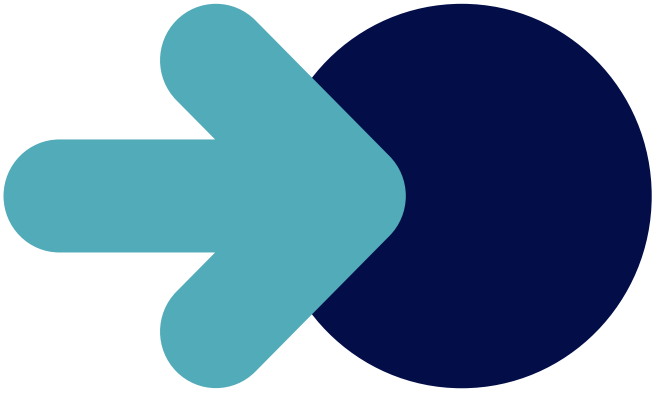
To enable adoption of the M365 Platform, and specifically Windows 11, Zero Trust Security and Microsoft's Security Solutions, Randstad offers fully funded M365 Accelerator Workshops for our clients. These week-long engagements provide best-practice guidance, hands-on experience and actionable recommendations to help our clients execute, and enjoy the value of their investment in Microsoft M365 modern workplace, security and collaboration solutions.

Randstad Technologies, is a Microsoft Gold Certified Partner and has achieved this status by demonstrating to Microsoft that it has the resources and proven experience needed to address the complexities inherent with these types of implementation projects. Randstad's experience, proven framework, methodologies and knowledge within the M365 Ecosystem makes Randstad a great partner to work with on this important initiative.

For more information, visit our Infrastructure Services page or contact us today:

Phone: 866.808.9595

Email: RT-TechnologySolutions@randstadusa.com



randstad®

human forward.

671820175_2-316_22