PATCH MY PC

Patch Perfect:

A Practical Guide to Securing Windows 11 Devices

PATCH MY PC

Table of Contents

This eBook outlines ten essential security strategies that security administrators, SOC teams, and MSPs can implement to mitigate risk, enforce policy compliance, and reduce attack vectors. Within this list, you will find strategies such as:

- **Patching Windows and third-party applications** to eliminate known vulnerabilities before they can be exploited.
- **Enforcing least privilege** and restricting local admin rights to prevent lateral movement.
- **Securing authentication** by eliminating passwords and leveraging Web Sign-In and FIDO2 security keys.
- **Leveraging advanced defenses** like Attack Surface Reduction, Credential Guard, and Application Control to contain and neutralize threats.

PATCH MY PC

Introduction

Patching remains one of the most effective ways to prevent cyberattacks, but many organizations struggle to keep Windows and third-party applications updated. Unpatched vulnerabilities in browsers, productivity tools, and commonly used software often serve as adversaries' initial footholds.

Patch My PC takes the manual effort out of application patching. Integrated directly with Microsoft Intune and ConfigMgr, it keeps every device updated with the latest security fixes, lowering your attack surface and reducing IT overhead.

This eBook breaks down the importance of each security measure and how it contributes to a stronger security posture. You'll also find implementation tips to get the most out of every strategy. The best place to start: *eliminating the risk of outdated software and unpatched apps.*

Updating
is critical

57%
of data breaches could have been prevented by being patched on time

11 seconds
companies are hit by ransomware attempt

ISO 27001
and Cyber Essentials certification patching is required

$4.4 Million
average cost of a data breach

Keep Devices & Applications Updated

Staying current with both Windows and application updates is essential for security. While Microsoft's Patch Tuesday provides monthly updates for Windows and some core components, it does not include Microsoft Office or any third-party apps. Those applications require separate patching to close security gaps attackers often exploit.

Who this Applies to:

Vulnerability Management Teams (tracking and prioritizing CVEs)
IT Administrators (deploying updates via Intune, ConfigMgr)

- **Patch Tuesday:** Delivers Windows security updates, which can be managed with Intune (using Windows Update client policies) or with ConfigMgr and its on-premises update management features.
- **CVE:** Vulnerabilities with high scores typically address critical flaws like remote code execution. Patches with CVE identifiers must be prioritized.
- **Patch My PC:** For third-party applications, a solution like Patch My PC automates updates for products like Adobe Reader, Google Chrome, and more. This closes off additional vectors that attackers may target.

Why it Matters:

- **Comprehensive Patching:** Attackers do not care if a vulnerability is in Windows OS or in a third-party app. Any unpatched software is a potential foothold for an attack.
- **Zero-Day Exploits:** Critical CVEs can be rapidly weaponized, which means irregular update schedules give attackers more time to infiltrate victims' systems.

Implementation Tips:

1. **Automate Where Possible:** Use Intune, and Patch My PC to automate patch deployment.
2. **Pilot Feature Updates:** Test new Windows builds on a small ring of devices before wide scale deployment.
3. **Monitor CVEs:** Subscribe to security bulletins. Apply critical patches quickly to reduce the likelihood of exploitation.

Security Impact:

- **Reduces Exploitable Attack Surface:** Unpatched vulnerabilities are the #1 entry point for ransomware and targeted attacks.
- **Zero-Day Mitigation:** Rapidly applying patches prevents attackers from leveraging high-severity CVEs.
- **Compliance Alignment:** Organizations that fail to patch within a defined SLA risk falling out of compliance with security frameworks like CIS, NIST, and ISO 27001.

Although regular updates are of utmost importance, security doesn't stop at patching. Next, we'll tackle how to lock down local admin accounts to prevent lateral movement in attacks.

Restrict Local Administrator Privileges

Local Administrator accounts, if left unsecured, present a significant security risk. Microsoft's Local Administrator Protection helps by limiting when and how these privileges are available. This ensures the powerful "Superman" token remains hidden ("Clark Kent" mode) until truly needed.

Who this Applies to:

Identity & Access Management (IAM) Teams (defining who gets admin access)
SOC/Incident Response Teams (investigating privilege escalation attempts

Why it Matters:

- **Least Privilege:** Ransomware groups like Lapsus$ and APT29 have repeatedly exploited overprivileged local admin accounts to move across networks and spread malware. Microsoft's Local Administrator Protection ensures that attackers can't easily escalate privileges, keeping your endpoints safe from these high-profile threats.
- **Reduced Risk:** If attackers breach a standard user account, they hit a security wall instead of wielding admin privileges.
- **Centralized Control:** Windows now supports policies that can rotate or disable built-in admin accounts automatically.

Implementation Tips:

1. **Disable or Rename Built-in Admin**: If you keep built-in admin at all, rename it and enforce complex passwords.
2. **Set It Up in Intune:** You can create device configuration profiles (or custom OMA-URI) to configure these local admin protection settings. Check our blog references or the Microsoft documentation on enabling local admin policies in Intune for step-by-step instructions.
3. **Maintain Break-Glass:** If you do need a local admin, ensure it's only for emergencies — not day-to-day accounts.

Security Impact:

- **Prevents Privilege Escalation:** Attackers can't quickly escalate from a standard user to admin.
- **Reduces Lateral Movement:** Local admin accounts are often abused in ransomware campaigns.
- **Protects Against Credential Theft:** Reduces attack surface for Mimikatz and other credential dumpers.

Reducing local administrator rights is critical for preventing lateral movement and privilege escalation. But what about the local admin accounts you can't remove, such as emergency break-glass accounts? Even a restricted local admin account can be a security risk if its password is static, predictable, or shared across multiple devices. That's where Windows LAPS comes in.

Secure Local Admin Passwords with New Windows LAPS

Reducing local admin privileges is crucial, but some situations still require a break-glass admin account for emergencies. However, static, shared admin passwords create security risks. If one of these static passwords becomes compromised, attackers can easily move laterally across devices undetected.

Windows LAPS (Local Administrator Password Solution) eliminates this risk by ensuring each device has a strong, unique local admin password that automatically rotates on a set schedule. These credentials are securely stored in Entra ID or on-prem Active Directory and accessible only to authorized admins, greatly reducing the risk of credential theft.

Who this Applies to:

Identity & Access Management (IAM) Teams
(enforcing privileged account security)
Security Compliance Teams (ensuring unique, rotated passwords)

Why it Matters:

- **No Shared Passwords:** Prevents attackers from using the same password across multiple machines.
- **Automated Rotation:** Reduces the risk of long-term credential exposure.
- **Emergency-Only Access:** Ideal for offline maintenance, not daily admin tasks.

Implementation Tips:

1. **Deploy via Intune:** Configure password complexity, rotation intervals, and storage location.
2. **Restrict Access:** Ensure only designated admin groups can retrieve/reset credentials.
3. **Educate IT Staff:** Reinforce that LAPS accounts are for emergency use only, not for regular administration.

Security Impact:

- **Eliminates Password Reuse Attacks:** Each machine has a unique admin password.
- **Prevents Credential Theft:** Attackers can't use compromised local admin accounts for lateral movement.
- **Supports Zero Trust:** Credentials are time-limited, reducing attack persistence

Securing local admin accounts with Windows LAPS is a crucial step in preventing lateral movement and credential theft. But passwords aren't the only security concern — what happens if an attacker gets their hands on a lost or stolen device? Even if they can't log in, could they still access sensitive files?

That's where BitLocker and Personal Data Encryption (PDE) step in.

Encrypt Your Device with BitLocker & PDE

Encryption is a non-negotiable security measure, ensuring that sensitive data remains protected even if a device is lost, stolen, or compromised. BitLocker encrypts entire drives, while Personal Data Encryption (PDE) adds an extra layer specifically for user data.

- **BitLocker:** Encrypts the entire OS and attached drives, leveraging TPM-based key storage to prevent unauthorized access.
- **Personal Data Encryption (PDE):** BitLocker encrypts the entire drive, but what if an attacker is already inside the system? Personal Data Encryption (PDE) takes it further, all of the user it personal data is locked with their own cryptographic key, meaning even an admin can't casually browse through another user his personal files.

Who this Applies to:

Security Compliance Teams (ensuring regulatory compliance)
Risk Management Teams (evaluating data protection risks)

Why it Matters:

- **Physical Security:** Prevents unauthorized data access if a device is offline or stolen.
- **Isolation of User Data:** PDE confines each user's data to unique cryptographic keys, adding defense-in-depth.

Implementation Tips:

1. **Enable BitLocker in Intune:** Configure device encryption policies, automatically storing recovery keys in Entra ID
2. **Set Up PDE:** For environments with sensitive data, Personal Data Encryption (PDE) can be enabled by creating a settings catalog policy in Intune. This ensures each user's data is protected with their own encryption key. For detailed steps, see our blog post on configuring PDE.
3. **Recovery Plans:** Always maintain a secure copy of BitLocker keys. Educate users on how to handle locked drives.

Security Impact:

- **Prevents Data Theft:** Lost/stolen devices remain inaccessible.
- **Meets Compliance Standards:** Required by GDPR, HIPAA, and PCI-DSS.
- **Protects Against Offline Attacks:** Attackers can't remove the drive and extract data.

Encryption ensures that even if a device is stolen, the data remains protected. But not all attacks require physical access; many exploits run directly on an active system, using malicious macros, scripts, or fileless malware to bypass traditional security measures.

That's where Attack Surface Reduction (ASR) rules come to the rescue. By blocking risky processes before they execute, ASR prevents attackers from using malicious scripts, untrusted macros, or credential theft techniques to compromise your endpoints.

Reduce Attack Surfaces with Attack Surface Reduction (ASR) Rules

Attackers don't always need to install malware. More often, they exploit built-in tools like PowerShell, Office macros, and script engines to gain control over a system. While traditional antivirus solutions may not catch these fileless threats, Attack Surface Reduction (ASR) rules, a part of Microsoft Defender for Endpoint, act as a preemptive shield, stopping malicious behaviors before bad actors can execute their attacks.

Beyond the original ASR rule set, Microsoft continuously expands ASR capabilities to address new attack techniques, such as credential dumping, malicious scripts, and living-off-the-land (LotL) attacks that weaponize built-in Windows utilities.

Who this Applies to:

SOC/Threat Hunting Teams (monitoring and tuning ASR rules)
Endpoint Security Teams (deploying ASR rules via Defender for Endpoint)

Why it Matters:

- **Preemptive Blocking:** ASR stops an exploit chain before malware executes, reducing attack impact.
- **Protection Against Fileless Threats:** Attackers often use PowerShell, WMI, or Office macros to bypass antivirus. ASR addresses and neutralizes these tactics.
- **Ransomware Defense:** Microsoft Defender threat intelligence reports show that ASR rules have successfully blocked ransomware payloads like LockBit and Emotet before encryption begins.

Implementation Tips:

- **Start with Audit Mode:** Identify potential false positives before enforcing policies.
- **Deploy via Intune:** Use Microsoft's preset ASR templates to avoid guesswork.
- **Use a Gradual Rollout:** Implement in rings to ensure business applications aren't impacted.

Security Impact:

- **Blocks Fileless Malware:** ASR stops script-based attacks that bypass traditional AV.
- **Prevents Phishing Payloads:** Blocks macro-based and LOLBin (living-off-the-land) attacks.
- **Reduces Ransomware Risk:** Microsoft reports ASR mitigates 75% of exploit-based attacks.

Blocking malicious scripts is just one piece of the puzzle, as even the best ASR policies won't help if attackers manage to steal login credentials. So, the next logical step after reducing attack surfaces? Eliminating passwords altogether. That's where passwordless authentication (such as Windows Hello, FIDO2 keys, and Web Sign-In) comes in.

Secure Device Logins with Web Sign-In, Passwordless Authentication & ESS

Even with Attack Surface Reduction (ASR) rules in place, attackers still have one major entry point: stolen passwords. Credentials remain one of the most widely exploited attack vectors, with phishing, credential stuffing, and brute-force attacks compromising millions of accounts every year. The best way to prevent this? Eliminate passwords entirely or make them as difficult to steal as possible.

Microsoft provides several authentication options to secure device logins:

- **Web Sign-In:** Allows users to log in using a Temporary Access Pass, eliminating the need for a password to login for the first time.
- **Enhanced Sign-In Security (ESS):** Uses hardware-backed protections like TPM and secure enclaves to protect login credentials from malware or interception.
- **Passwordless Authentication:** Solutions like Windows Hello (biometric/PIN) and FIDO2 security keys eliminate password exposure while still allowing privileged actions like Run as administrator.

Who this Applies to:

Identity & Access Management Teams (implementing passwordless authentication)
SOC Teams (investigating login anomalies and account compromise attempts)

Why it Matters:

- **Improves User Experience:** Biometric authentication (face/fingerprint) and security keys make sign-in faster and more secure.
- **Maintains Flexibility:** Passwordless methods still allow administrative actions (like "Run as"), ensuring usability.

Implementation Tips:

1. **Ensure Devices Are Updated:** The first Windows 11 24H2 release had an issue where Web Sign-In was broken. Ensure your devices are running the latest build to avoid login failures.
2. **Do NOT Disable the Password Provider:** just hide it! If the password authentication provider is disabled, users may be unable to recover access if Web Sign-In fails. Ensure that password-based sign-in remains enabled as a fallback option.

Security Impact:

- **Prevents Phishing and Credential Theft:** Having no static passwords means there is nothing for attackers to steal or reuse.
- **Strengthens MFA Adoption:** Web Sign-In, FIDO2 keys, and Windows Hello enforce hardware-backed authentication.
- **Reduces Helpdesk Costs:** Fewer password resets and phishing-related lockouts.

Even with passwordless authentication in place, attackers can still attempt to bypass security policies or tamper with device configurations. The next step in hardening Windows security? Enforcing Config Refresh to prevent policy drift and unauthorized changes.

Enforce Security Policies with Config Refresh

Even with passwordless authentication and other security controls in place, there's still a risk: what if users or attackers modify security settings when the device is offline?

Security policies are only effective if they stay enforced. However, configuration drift occurs when:

- **Users manually override settings** (e.g., disabling Defender, changing firewall rules).
- **Software updates modify security policies** unexpectedly.
- **Attackers attempt to weaken protections** by tampering with Group Policy, registry keys, or MDM settings.

Intune Config Refresh ensures that baseline security policies are automatically reapplied, reverting any unauthorized changes, even if the device is offline or hasn't checked in with Intune.

Who this Applies to:

Security Compliance Teams (ensuring policies remain enforced)
SOC Teams (detecting unauthorized policy changes and rollbacks)

How Does Congif Refresh Work?

- **Scheduled Task Execution** – Windows runs a scheduled task that triggers Config Refresh based on the cadence you configure in Intune.
- **Secure Cache Retrieval** – If the device is offline, it retrieves the last known Intune policy from a secure cache and reapplies those settings to prevent tampering.
- **Tamper Reversion** – If an attacker modifies security settings while offline, Windows automatically restores the enforced baseline at the next local refresh.

Why it Matters:

- **Offline Protection:** If a device is disconnected and someone modifies security settings, Config Refresh restores the correct policy when it comes back online.
- **Prevents Configuration Drif:** Ensures that Intune, Group Policy, and MDM settings remain enforced across all endpoints.
- **Defends Against Tampering:** Stops users or attackers from disabling critical security controls, even when the device cannot immediately sync with Intune.

SEE NEXT PAGE FOR CONTINUATION

Enforce Security Policies with Config Refresh

CONTINUED

Security Impact:

- **Prevents Configuration Drift:** Ensures security policies persist even offline.
- **Blocks Tampering Attempts:** Attackers can't disable Defender, firewall, or security baselines permanently.
- **Improves Compliance:** Ensures CIS/NIST security baselines are enforced.

Even with Config Refresh, some attacks target the device boot process before Windows security features are activated. To fully protect the system, the next step is Device Attestation, which ensures that only trusted devices can enroll and access corporate resources.

Require Device and Health Attestation for Secure Enrollment

Even with Config Refresh ensuring policy integrity, attackers can still attempt to enroll unauthorized devices or tamper with the boot process to bypass security controls. That's where Device and Health Attestation comes in. These technologies verify that a device's firmware, boot sequence, and security posture meet enterprise security standards before it enrolls in Intune.

Who this Applies to:

Identity and Access Management (enforcing secure device enrollment policies)
Risk Management Teams (evaluating device security posture before access is granted)

What is Device Attestation? (MDM Enrollment Security)

- Device Attestation ensures that only genuine, unmodified devices can enroll in Microsoft Intune.
- It verifies hardware-backed security properties, ensuring attackers can't spoof or use modified VMs, jailbroken devices, or manipulated firmware to bypass enrollment.

What Device Attestation Checks:

- **Trusted Platform Module (TPM) presence**
- **Secure Boot enabled**
- **Manufacturer-signed BIOS and firmware**

Example: If an attacker attempts to enroll a virtual machine, it will likely fail device attestation because VMs cannot provide a valid TPM or Secure Boot measurement. If platform restrictions are configured, enrollment will be blocked.

What is Device Health Attestation (DHA)?

- **Device Health Attestation (DHA)** ensures that a device remains secure post-enrollment by checking that key security settings remain enabled.
- If someone disables Secure Boot, tampers with the TPM, or removes BitLocker encryption, DHA can detect the change, mark the device as non-compliant, and restrict access to corporate resources.

What DHA Checks:

- **Secure Boot remains enabled** (protects against bootkits and firmware-level threats).
- **TPM integrity remains intact** (ensures encryption and security keys are protected).
- **BitLocker encryption is enforced** (prevents unauthorized disk access).

Example: If a user disables Secure Boot after enrollment to run unsigned OS images, DHA will detect this and revoke access.

SEE NEXT PAGE FOR CONTINUATION

Require Device and Health Attestation for Secure Enrollment

CONTINUED

PATCH MY PC

Implementation Tips:

While Device Attestation strengthens enrollment security by ensuring only genuine, unmodified devices can enroll, there are important considerations and potential restrictions to be aware of:

1. **If you configure Intune** platform enrollment restrictions to only allow TPM-attested devices, be aware that this restriction will **block Windows Cloud PC enrollment** because **vTPM is not currently trusted.** This means that **Cloud PCs provisioned via Windows 365** will **fail enrollment** if this filter is enforced.

2. **Check** that endpoints have **TPM 2.0 enabled and Secure Boot turned on** before enforcing attestation.

3. **Use the Attestation Report** to determine if **existing devices** support attestation **before** enforcing it.

Security Impact:

- **Prevents Unauthorized Enrollment:** Ensures only genuine, secure devices can register.
- **Detects Firmware Tampering:** Rejects devices with disabled Secure Boot or TPM.
- **Reduces Shadow IT:** Prevents unapproved personal devices from enrolling.

While Device Attestation secures the enrollment phase, and Health Attestation ensures post-enrollment compliance, attackers can still attempt credential theft. The next step? Virtualization-Based Security (VBS) and Credential Guard, which prevent credential dumping even if an attacker gains system access.

Strengthen Security with Virtualization-Based Security (VBS) & Credential Guard

Even with Device and Health Attestation preventing unauthorized enrollments, attackers can still utilize post-login credential theft attacks. Many modern cyberattacks, including ransomware and advanced persistent threats (APT), rely on stealing authentication secrets to move laterally across an enterprise network. That's where Virtualization-Based Security (VBS), Hypervisor-Protected Code Integrity (HVCI), and Credential Guard come into play. These technologies leverage hardware virtualization to isolate sensitive system processes, ensuring that even if an attacker compromises the OS, they cannot access high-value security components.

Who this Applies to:

Security Architects (designing endpoint security strategies)
SOC Teams (monitoring LSASS and credential dumping attempts)

What is Virtualization-Based Security (VBS)?

Virtualization-Based Security (VBS) is a security architecture that uses hardware-assisted virtualization to create an isolated environment within Windows. This secure memory space is protected by the Windows hypervisor, ensuring that even if an attacker compromises the OS kernel, they cannot access protected security processes.

Key VBS Features:

- **Hypervisor-Protected Code Integrity (HVCI):** Ensures that only signed, trusted code executes in kernel mode.
- **Credential Guard:** Moves authentication secrets (e.g., Kerberos tickets, NTLM hashes) into the isolated VBS container, blocking pass-the-hash and pass-the-ticket attacks.

Example: Even if an attacker gains local admin access to a compromised machine, they cannot extract credential hashes from LSASS because Credential Guard prevents access.

What is Hypervisor-Protected Code Integrity (HVCI)?

HVCI (also called Memory Integrity) is a VBS-powered feature that runs Kernel Mode Code Integrity (KMCI) inside the VBS secure environment rather than in the main OS kernel.

Why this Matters:

- **Prevents malware from modifying Windows kernel-mode code** (e.g., rootkits, malicious drivers).
- **Ensures only verified, signed drivers load:** blocking unsigned kernel code injections.
- **Stops exploits like WannaCry** that rely on kernel-level code execution vulnerabilities.

Windows 11 Default Security:

- **All Windows 11 devices support HVCI** by default.
- **New Windows 11 hardware ships** with **VBS + HVCI enabled** out-of-the-box.

SEE NEXT PAGE FOR CONTINUATION

What is Credential Guard?

Credential Guard is a VBS-powered security feature that isolates authentication credentials from the OS. This prevents attackers from using pass-the-hash (PtH) and pass-the-ticket (PtT) attacks, which are commonly used in ransomware campaigns.

How Credential Guard Works

- Kerberos tickets, NTLM hashes, and credentials are stored in VTL1 (VBS).
- Even local admin users cannot extract credentials from LSASS.
- Prevents lateral movement attacks by blocking stolen credential reuse.

Security Impact:

- **Stops Credential Dumping:** Blocks Mimikatz and similar tools from stealing credentials.
- **Defends Against APTs:** Microsoft enforces Credential Guard on high-risk workloads.
- **Meets Zero Trust Goals:** Protects authentication secrets, even from compromised admins.

Protecting credentials is only half the battle. Attackers don't always need stolen logins; they can just run unauthorized applications to establish persistence. The best defense? A locked-down application control strategy that prevents rogue software from running in the first place. That's where AppLocker and Application Control for Business come in.

Isolate Applications with AppLocker vs. Application Control for Business

Not all threats rely on stolen credentials. In many attacks, the end goal is to execute unauthorized code, whether through malware, rogue scripts, or unsigned applications. Application control is the final layer of defense, ensuring that only pre-approved software runs on managed endpoints.

Microsoft provides two primary solutions for application control:

- **AppLocker:** Uses rule-based allowlists or blocklists to control executables, DLLs, scripts, and installers. It's easier to manage for MSPs or organizations with frequently changing software.
- **Application Control for Business (AKA WDAC):** A more advanced, code signing-based enforcement model that provides stricter security but requires more effort to maintain (e.g., handling unsigned apps, creating code signing policies).

Who this Applies to:

Application Security Teams (enforcing software execution policies)
SOC Teams (investigating unauthorized execution attempts and policy bypasses)

Why it Matters:

- **Prevents Unauthorized Software Execution:** Blocks malware, rogue scripts, and unwanted applications from running.
- **Ensures Compliance:** Standardizes the environment, ensuring that only approved business apps execute.
- **Provides Granular Control:** Application Control for Business enables policy enforcement at the OS level, making it ideal for high-security workloads.

Implementation Tips:

1. **Start with AppLocker:** For many MSPs, AppLocker is simpler. It allows easy exceptions for new software.
2. **Consider Application Control for Business:** For advanced allow listing or highly secured devices (like kiosks or sensitive workloads), Application Control for Business delivers granular enforcement.
3. **Manage via Intune:** Both AppLocker and Application Control for Business can be deployed through Intune policies. Validate your rule sets and test them in a pilot ring to avoid blocking critical processes.

Security Impact:

- **Prevents Malware Execution:** Blocks untrusted applications, scripts, and DLLs.
- **Reduces Supply Chain Risks:** Ensures only signed applications can run.
- **Meets Compliance Standards:** Required under DoD STIG and CIS benchmarks.

Patch My PC: Closing the Gaps in Third-Party Patching

Security isn't just about locking down your environment. It's also about keeping software updated to eliminate vulnerabilities before they can be exploited.

While Windows Update Client Policies / Autopatch manages Windows OS updates, third-party applications remain one of the biggest security gaps in enterprise environments. Patch My PC plays a crucial role in this process by automating third-party application updates, ensuring that common attack vectors, such as outdated browsers, productivity apps, and runtime libraries, are patched before they become security risks.

How Patch My PC Strengthens Endpoint Security

- **Vulnerability Management:** Automates patching for third-party applications such as Adobe Reader, Google Chrome, Zoom, and Java, closing security gaps that attackers often target.
- **Attack Surface Reduction:** Keeps high-risk applications updated to prevent exploits and fileless malware attacks that rely on outdated plugins and insecure runtimes.
- **Ransomware Prevention:** Ensures that applications commonly exploited in phishing campaigns, such as browsers and PDF viewers, receive timely security updates.
- **Compliance and Policy Enforcement:** Helps organizations meet security baselines by ensuring third-party software stays up to date and supports compliance with NIST, CIS, and ISO 27001 patching policies.

While Windows OS patching is well-managed through Microsoft's update solutions, Patch My PC helps close the third-party application update gap by ensuring every application remains up to date with minimal IT effort.

Conclusion:

Building a Resilient Patch Management Strategy

Effective patch management is crucial to protecting against vulnerabilities, ensuring compliance, and maintaining system stability. By following these best practices and implementing a structured approach, organizations can safeguard their IT environments and minimize the impact of patching on daily operations.

For a third-party patch management solution that automates, schedules, and alleviates many IT team issues, consider Patch My PC. A free demo will reveal affordable pricing and endless opportunities.