The Hidden Risk of "Stable" Systems - Disabling or Deferring Windows Updates Leaves You Exposed

Executive Summary

Across dozens of our recent customer wins, one pattern stands out: automatic Windows updates are disabled or deferred indefinitely. Legacy Managed Service Providers (MSPs) often justify this as a way to maintain stability, claiming that patching "breaks" systems or disrupts users. In isolated cases, that caution made sense years ago. But in today's threat landscape—where exploits are operationalized within hours—indefinite deferral equals exposure.

Modern security frameworks assume that updates happen continuously, with validation, automation, and oversight. This paper examines why legacy MSPs disable or defer Windows updates, the partial truths behind their reasoning, and why failing to ensure timely patching remains one of the biggest cybersecurity failures in 2025.

The Legacy MSP Mindset: Stability Over Security

Traditional MSPs built their businesses around uptime and ticket volume, not threat mitigation. Automatic updates introduced unpredictability—sometimes causing driver conflicts or brief downtime.

> **So they made a trade off: "If it ain't broke, don't patch it."**
> That philosophy once minimized phone calls; today, it maximizes risk. In a cloud-connected ecosystem, unpatched equals broken. Choosing stability over security is a false economy.

Why MSPs Turn Off or Pause Updates — and Where They Go Wrong

There are legitimate operational reasons an MSP might manage or delay Windows updates. But the intent to "control risk" often turns into a permanent pause, leaving endpoints months or years behind.

Common Justifications and Rebuttals

1. **"We manage patches manually for quality control."**
   a. Valid concern: Manual approval can prevent a bad patch from breaking production apps.
   b. Problem: Without a documented cadence, "manual control" becomes "no control." Many MSPs simply never circle back to approve.

2. **“Automatic updates can break systems.”**
    a. True in rare cases. Some updates have caused printer or VPN issues.
    b. Modern reality: Microsoft’s ring-based deployment, rollback protection, and telemetry now mitigate that risk. Deferring indefinitely does more harm than good.
3. **“We patch manually during maintenance windows.”**
    a. Good in principle.
    b. Reality: Many of those windows are skipped or inconsistently executed, leaving endpoints running builds months behind.
4. **“We control updates through Group Policy.”**
    a. Appropriate for standardization.
    b. Risk: When GPOs block Windows Update without a modern replacement (e.g., Windows Autopatch), updates are effectively disabled.
5. **“We use our RMM to manage patches.”**
    a. Fine—if done correctly
    b. But: Most RMMs default to deferring Microsoft updates until approved. If those approvals stall, you’re frozen in time.

The Modern Reality: Exploits Don’t Wait

Attackers now weaponize vulnerabilities within hours of Microsoft’s disclosures. According to Microsoft telemetry, 90% of successful ransomware attacks exploit known, unpatched vulnerabilities. When updates are delayed or blocked:

- Zero-day fixes never reach endpoints
- Exploits remain viable indefinitely
- Compliance frameworks (HIPAA, NIST, SOC 2, PCI) are silently violated

“Stable” systems that haven’t been patched in 60 days are quietly compromised systems waiting to happen.

Misaligned Incentives in Legacy Models

Legacy MSPs still operate under reactive SLAs. Fewer tickets = higher margins. Automatic updates generate tickets, so they’re often suppressed—not for security, but for support convenience. This reflects a dangerous misalignment: customer security taking a back seat to internal efficiency.

How to Verify Your Patch Status

You can verify your own Windows Update configuration in under two minutes:

1. Open Settings → Windows Update -> Update History
2. If your last “Cumulative”, “Security”, or “Quality” update is older than 30 days, you’re behind.
3. Click Check for updates. If it’s greyed out or errors, updates are being blocked by policy.

The Modern Work Approach: Control Without Complacency

T2M Works uses intelligent automation—not manual guesswork—to ensure continuous patching without destabilizing systems.

Our approach combines:

- Windows Autopatch for ring-based rollout
- Make sure feature updates, quality (security) updates, driver updates, Microsoft 365 application updates, and Microsoft Edge updates are all installed and regularly monitored
- Enable 'hotpachting' which allows capable updates to install without the need to restart
- AI-driven telemetry to detect abnormal patch outcomes
- Integration with Entra ID and Microsoft Secure Score for compliance validation
- Zero-touch deployment with staged reboots and real-time reporting

This ensures both stability and security—no trade-off required.

The Cost of Deferred Security

Each unpatched device becomes an open door:

- Exposure to every exploit patched since your last update
- Cyber-insurance noncompliance (many policies require 30-day patch cycles)
- Regulatory violations across HIPAA, NIST, or ISO frameworks
- Increased risk of ransomware and credential theft

Security that waits for "maintenance windows" isn't security—it's delay disguised as discipline.

Conclusion

Before you finish this paper, verify your patch compliance. It takes 2 minutes. If you are behind, schedule a 30 minute call with us @ (214) 932-1500 or email at sales@t2mworks.com.

Disabling or indefinitely deferring Windows updates once seemed prudent. In 2025, it's an outdated practice that trades visible stability for invisible risk. Modern Work demands intelligent control, continuous automation, and AI-backed assurance that updates are applied safely and consistently.

Security isn't about avoiding change—it's about managing it intelligently.
That's the Modern Work difference.
That's T2M Works.