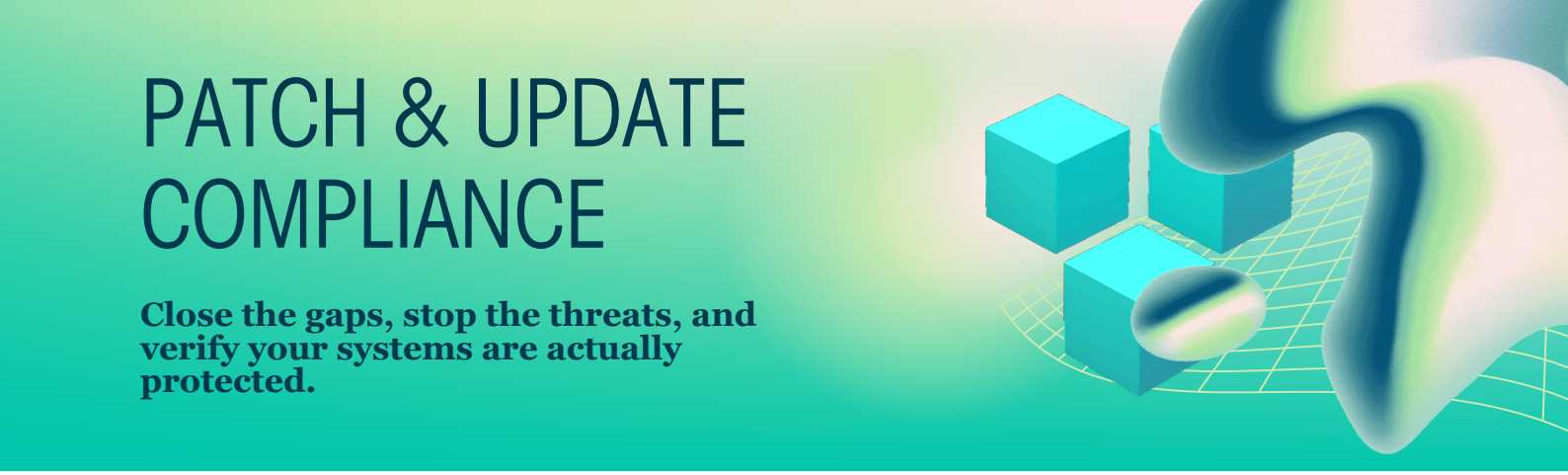

Patch & Update Compliance Checklist for Small Businesses (2026 Edition)

This checklist helps you verify your systems are not just updating but fully compliant and protected.

Patch & Update Compliance Checklist

1. Operating System (OS) Patch Compliance

- ☐ Automatic updates are enabled and enforced
- ☐ Devices install updates without relying on user action
- ☐ Systems are online during update windows
- ☐ Servers follow a scheduled patch cycle
- ☐ End-of-life systems are identified and replaced
- ☐ Patch status is logged and reviewed

Why this matters:
Unpatched operating systems are one of the fastest ways attackers gain access.

2. Third-Party Application Updates

- ☐ All installed applications are inventoried
- ☐ Browsers are updated regularly
- ☐ Tools like Adobe, QuickBooks, Zoom, and Java are current
- ☐ Unused or outdated apps are removed
- ☐ Auto-update is enabled where possible
- ☐ Update success is verified

Why this matters:
Unpatched third-party apps are a primary entry point for ransomware and credential theft.

3. Firmware and Infrastructure Updates

□ Firewall firmware is up to date
□ Routers, switches, and access points are updated
□ Hardware vendor security advisories are reviewed
□ Network devices are included in patch cycles

Why this matters:
Outdated infrastructure creates hidden vulnerabilities that bypass endpoint security.

4. Certificates, Domains, and License Renewals

□ SSL certificates are monitored for expiration
□ Domain renewals are tracked
□ Security licenses (AV, backup, etc.) are active
□ Renewal alerts are in place

Why this matters:
Expired certificates or licenses can cause outages without any attack.

5. Centralized Patch Monitoring and Visibility

□ A centralized dashboard shows update status
□ Failed or missing updates trigger alerts
□ Compliance is reviewed regularly
□ Non-compliant devices are identified quickly

Why this matters:
If you cannot see your patch status, you cannot confirm your protection.

6. Automated Patch Enforcement

□ Updates are deployed automatically
□ Users cannot bypass required updates
□ Critical patches are prioritized
□ High-risk devices are isolated if non-compliant

Why this matters:
Manual patching is unreliable and inconsistent at scale.

7. Regular Compliance Reviews

□ Weekly patch status is reviewed
□ Monthly compliance reports are evaluated
□ Missing updates are resolved quickly
□ Offline devices are checked manually

Why this matters:
Patch compliance is not a one-time task, it requires continuous verification.

8. Maintain a Patch Compliance Score

□ OS compliance is tracked
□ Application updates are tracked
□ Firmware and infrastructure are tracked
□ Verification and auditing are tracked

Why this matters:
A scoring system helps identify weak areas quickly and track improvement over time.

Patch Compliance Scorecard (Self-Assessment)

Score each section from 0–5:

Operating Systems: _____
Applications: _____
Firmware & Infrastructure: _____
Verification & Monitoring: _____

Total Score (0–20): _____

How to Interpret Your Score

18–20: Low Risk
Systems are well-maintained and monitored

14–17: Moderate Risk
Some gaps exist that should be addressed

10–13: High Risk
Multiple vulnerabilities are likely present

0–9: Severe Risk
Systems are highly exposed to attack

(Adapted from score model on page 5 of the original guide)

What True Patch Compliance Looks Like

Updates are automatic and enforced
Every device is monitored centrally
Missing patches are identified immediately
Compliance is verified—not assumed

Quick Rule of Thumb

If you're relying on users to install updates, you are not fully protected.

SofTouchSystems.com
No-Surprise IT — Predictable. Proactive. Proven.