CyberSmart

Vulnerability Management vs Patch Management:

What's the Difference and Why It Matters

The Reality Check

In 2024, 612,000 UK businesses (43% of all businesses) reported a cyberattack. Yet only 22% have incident response plans in place.

This gap between threat reality and preparedness highlights why understanding vulnerability and patch management matters.

incident response

of all businesses

The Core Difference

Vulnerability Management = Finding and prioritising what's broken	Patch Management = Fixing what's broken
Continuous scanning with real-time visibility (up to 3× daily updates) identifies security weaknesses across your environment, assesses their severity, and tells you what matters most.	Deploying software updates to close known security gaps before attackers exploit them.

Why People Confuse Them

Many organisations assume patching alone equals complete vulnerability management. Here's why that's not the case:

- Patching addresses specific vulnerabilities → **Vulnerability management shows the complete risk landscape across endpoints, servers, and optionally networks**
- Patching focuses on remediation → Vulnerability management provides the continuous context needed to prioritise what should be patched first
- Patching requires you to know what needs fixing → Vulnerability management tells you exactly what's at risk and why it matters

What Each One Does

Vulnerability Management

- Continuous scanning with up to 3× daily updates to detect security weaknesses
- Prioritises vulnerabilities by severity, exploitability, and business impact
- Tracks vulnerabilities across your entire environment
- Provides audit-ready evidence for compliance frameworks
- Identifies gaps that patching alone won't catch

Patch Management

- Keeps software up to date with the latest security fixes
- Deploys updates across Windows and Mac devices
- Reduces vulnerabilities in third-party applications
- Minimises disruption through scheduled deployment
- Verifies patches are installed correctly

The Consequences of Neglecting Both

Data breaches
Unpatched vulnerabilities give attackers easy access. Once inside, they can steal customer data, financial information, or intellectual property.

Business disruption
Real example: In August 2025, Jaguar Land Rover was hit by a cyberattack that forced production to halt for over a month, costing an estimated £50 million per week in lost output.

Compliance failures
Under UK GDPR and the Data Protection Act 2018, businesses must take reasonable steps to protect personal data. Failing to patch known vulnerabilities can be seen as negligence, leading to investigations and fines.

Ransomware attacks
Outdated software is a common target. Attackers exploit known flaws to encrypt business-critical data and demand payment for its release.

When to Use Each Approach

Start with Vulnerability Management if:

- You need audit-ready evidence for Cyber Essentials Plus, ISO 27001, or similar frameworks
- You manage multiple clients or devices and need centralised risk visibility with continuous scanning (up to 3× daily updates)
- You're unsure which vulnerabilities pose the greatest threat
- You want to prove compliance and demonstrate continuous security improvements

Start with Patch Management if:

- You already know what needs patching (via existing vulnerability data)
- You want to quickly reduce your attack surface with minimal disruption
- You lack dedicated security resources and need straightforward remediation
- Your primary concern is keeping everyday software up to date
- **Note: Patch requires CyberSmart Active Protect**

Use Both for Complete Protection

Vulnerability management tells you what to fix and why it matters. Patch management fixes it. Using both tools through the CyberSmart platform means you can move from detection to remediation without switching systems.

Real Scenarios

- Scenario 1: Preparing for a Cyber Essentials Plus audit
  → Start with vulnerability management. **The audit checks that all high and critical vulnerabilities are resolved, and vulnerability scanning strongly supports demonstrating this compliance.**

- Scenario 2: A critical vulnerability is announced affecting software you use
  → Deploy patch management immediately. **You know exactly what needs fixing and speed matters.**

- Scenario 3: Managing security for 20+ SME clients
  → Use both. **Vulnerability management gives you visibility into risk across all clients. Patch management lets you remediate at scale. Both are accessible through the CyberSmart platform for streamlined workflow.**

- Scenario 4: Your RMM tools are missing third-party app updates
  → Add patch management. **RMM tools typically handle OS patches but miss hundreds of third-party applications that attackers commonly exploit.**

Building an Integrated Approach: 8 Practical Steps

1. Start with what you've got

You can't secure what you don't know about. Create a comprehensive inventory of all your devices, software, and systems.

2. Schedule scans before installing patches

Run vulnerability scans immediately before your monthly patch deployment windows to identify what needs attention.

3. Create a severity-based timeline

Critical vulnerabilities: patch within 72 hours	High-risk issues: patch within 2 weeks	Medium/low -risk: follow a monthly cycle

4. Expedite high-impact patches

Prioritise testing for patches that fix vulnerabilities in your most-used software.

5. Use one central tracking system

Document all vulnerability discoveries and patch deployments in a single location.

6. Test before you deploy

Always test critical patches in a safe environment first to avoid breaking production systems.

7. Focus on internet-facing systems

Scan and patch public-facing websites and applications first. These are your highest-risk areas.

8. Include mobile devices

Cybercriminals increasingly target mobile devices. Add smartphones and tablets to your regular scanning and patching schedule.

Think Like a Hacker

Not all vulnerabilities are created equal. A critical flaw in your public-facing website poses more immediate risk than a minor issue in standalone software.

Prioritise based on:

- Exploitability: Can this be weaponised easily?
- Business impact: What happens if this is exploited?
- Exposure: Is this system internet-facing or internal?

Quick Reference: What Should I Do?

Your Situation:	Recommended Approach:
• Need audit evidence for compliance • Know exactly what needs patching • Managing multiple clients/sites • RMM missing third-party updates • Preparing for CE+ certification • Want continuous security visibility	• Start with vulnerability management • Deploy patch management • Both, accessible through one platform • Add patch management • Start with vulnerability management • Use both together

How CyberSmart Helps

- CyberSmart Vulnerability Manager (CSVM)
  Enterprise-grade vulnerability scanning (99.9996% accuracy, PCI-DSS approved) with continuous scanning and up to 3× daily updates, plus prioritised remediation guidance. Built for Cyber Essentials Plus, ISO 27001, and ongoing compliance. Unlimited expert support included.

- CyberSmart Patch
  Effortless patch deployment for 350+ third-party applications across Windows and Mac. Deployed through CyberSmart Active Protect, providing minimal disruption and management from the CyberSmart dashboard.

- Used together: CSVM identifies what's vulnerable and why it matters. Patch closes the gaps. Both tools are accessible through the CyberSmart platform, allowing you to move from vulnerability detection to remediation within the same environment.

How CyberSmart Helps

Vulnerability management gives you the intelligence. Patch management gives you the action.

Focus on consistent improvement rather than perfect implementation. Cyber Essentials certification provides an excellent framework for developing essential security processes, while tools like CyberSmart Patch and CSVM make security simpler and more reliable.

If you're trying to choose between them, ask yourself: Do I know what my biggest security risks are right now?

- No → Start with vulnerability management
- Yes → Deploy patch management to close those gaps
- Want both → Use complementary tools within the same platform for complete, continuous protection

Want to see how they work together?

Book a demo or speak with your CyberSmart account team to explore how vulnerability management and patch management complement each other within the CyberSmart platform.

CyberSmart