+44 345 094 0945
www.waterstons.com

Article

Jul 2026

# Closing the gaps: how vulnerability scanning and patching work together

Every significant cyber breach has a story. And more often than not, that story includes a known vulnerability that was never fixed. The 2017 WannaCry ransomware attack exploited a Windows flaw for which a patch had been available for two months. The Equifax breach exposed the personal data of 147 million people through an unpatched Apache Struts vulnerability. These were not zero-day attacks. They were failures of process.

This is something that keeps senior IT and cyber security leaders up at night. But the lesson is clear: knowing about a vulnerability, and doing something about it, are two very different things. Vulnerability scanning and patch management are the twin pillars of any credible vulnerability management programme. Yet in many organisations they operate in silos, at different cadences, owned by different teams. That disconnect is where risk lives.

### What scanning tells you

Vulnerability scanning is the process of systematically checking your environment, including endpoints, servers, network devices, cloud workloads and applications, to identify known weaknesses. These might be unpatched software, misconfigured services, exposed ports, or outdated components carrying published Common Vulnerabilities and Exposures (CVEs).

Modern scanning tools such as Qualys, Tenable Nessus, and Rapid7 InsightVM can provide near-continuous visibility across complex, hybrid environments. But a scan result is not remediation. It is a list of problems. Without a structured, timely response, that list simply grows, and so does your exposure.

The value of scanning is not the report it produces. It is the action that report drives.

### What patching achieves

Patch management is the discipline of acquiring, testing, and deploying software updates to address known vulnerabilities. Done well, it is one of the highest-return security investments an organisation can make. Done poorly, or not at all, it leaves the door open to attacks that are, by definition, entirely preventable.

The challenge for most organisations is not a lack of patches, but volume and prioritisation. Microsoft alone releases dozens of patches every month. Across a typical enterprise estate, the number of outstanding vulnerabilities at any given time can run into the thousands. Without a clear framework for deciding what to fix first, teams either patch everything indiscriminately, burning resource on low-risk items, or patch nothing consistently, leaving critical gaps unaddressed.

### The integration imperative

This is where the relationship between scanning and patching becomes strategically important. Scanning without patching creates awareness without action. Patching without scanning creates activity without assurance.

The two functions must operate as a continuous, integrated cycle:

1. Discover: Scan the full asset estate to identify vulnerabilities across all systems
2. Prioritise: Use risk-based scoring, drawing on CVSS severity ratings, real-world exploitability data, and asset criticality, to determine what requires urgent attention
3. Remediate: Apply patches, configuration changes, or compensating controls within defined SLA timeframes
4. Verify: Re-scan to confirm that vulnerabilities have been successfully resolved
5. Report: Track trends, measure performance, and provide leadership with meaningful metrics

This cycle should not be a quarterly exercise. Threats don't wait for a schedule, so it needs to operate continuously, with clear ownership, defined timelines, and executive visibility.

**Prioritisation is the strategic lever**

Senior leaders should pay particular attention to how their organisations prioritise remediation. Not all vulnerabilities carry equal risk. A critical vulnerability on an internet-facing system actively being exploited in the wild demands a fundamentally different response to a medium-severity finding on an isolated internal server.

Frameworks such as the CISA Known Exploited Vulnerabilities (KEV) catalogue provide clear intelligence on which vulnerabilities are being actively targeted. Integrating this threat context into your prioritisation model ensures that your patching effort is directed where it matters most, rather than simply working through a queue by severity score alone.

**The leadership imperative**

Vulnerability management is not a technical problem that can be delegated entirely to operations teams. It requires leadership commitment: defined policies, agreed SLAs by severity, adequate tooling, and the organisational alignment to ensure that security and IT teams are working from the same playbook.

The organisations that manage this well treat scanning and patching not as periodic tasks, but as a continuous, measurable programme. They know their asset estate. They know their exposure. And when a new critical vulnerability emerges (because it's 'when', not 'if'), they have the processes in place to respond with speed and confidence.

The question is not whether your organisation has vulnerabilities (it does), but whether you have the visibility and the discipline to close them before someone else finds them first.

Our Cyber Assurance and Managed Services teams scan and patch environments like this every day, and can work with you to build a programme that keeps you protected.

Contact info@waterstons.com.au to find out more.