FREE GUIDE

Your First 5 Vulnerability Management Wins

Five plain-English steps that pay off fastest — what to scan first, which findings to fix first, and why.

Vulnerability management drowns teams in numbers — thousands of findings, all marked urgent. The way out is to rank by real risk, not raw counts, and fix the few things that actually matter first. These five wins get you there without buying anything new.

A free guide from Sylvan Assurance — plain-English security, without us ever seeing your data.

Win 1 — Know what you have

What it is

A working inventory of the systems, services, and software you're responsible for.

Why it's first

You can't scan — or protect — what you don't know about. The asset you forgot is the one that gets you. Every later step depends on this list.

Do this

List your internet-facing systems first, then the rest: servers, laptops, key applications, and the cloud accounts behind them. Note who owns each. Keep it somewhere it'll stay current.

Win 2 — Scan what matters first

What it is

Pointing a vulnerability scanner at your most exposed systems before anything else.

Why it matters

Trying to scan everything at once stalls. The internet-facing systems are where attackers look first, so that's where scanning pays off fastest.

Do this

Run an authenticated scan against your internet-facing systems this week. Free and built-in tools are fine to start — the goal is to see what's exposed, not to buy a platform.

Win 3 — Prioritise by real risk, not the raw score

What it is

Ranking findings by how likely they are to actually hurt you — not just their severity number.

Why it matters

A "critical" on an isolated internal box can matter less than a "medium" on a public server that's being exploited in the wild. Raw counts and scores alone send you fixing the wrong things.

Do this

Push to the top the findings that are internet-facing and known to be exploited (check whether a vulnerability is on the Known Exploited Vulnerabilities, or KEV, list). Let exposure and real-world exploitation — not just the Common Vulnerability Scoring System (CVSS) number — set your order.

Win 4 — Fix the top few, and verify

What it is

Actually remediating your highest-risk findings and confirming the fix worked.

Why it matters

A finding isn't closed until it's verified. Patching without re-checking leaves you believing you're safe when you may not be.

Do this

Fix your top few this cycle — patch, reconfigure, or remove the exposure. Then re-scan to confirm each one is gone. A short, finished list beats a long, untouched one.

Win 5 — Make it a cadence, not a one-off

What it is

Turning scan, prioritise, fix, and verify into a regular, repeating loop.

Why it matters

New vulnerabilities appear constantly. A scan from six months ago tells you about a world that no longer exists. Consistency is what actually reduces risk over time.

Do this

Put a recurring scan on the calendar (monthly is a fine start), and agree simple targets for how fast the riskiest fixes get done. Keep the loop small and steady rather than heroic and rare.

Where to go from here

The free Vulnerability Management assessment shows where you stand in a few minutes, and it runs entirely in your browser, so we never see your answers: sylvanassurance.com/free/vm/

When you're ready to turn that into a full programme with templates and runbooks, the Vulnerability Management toolkit lays it out: sylvanassurance.com/vulnerability-management

Scan for the free assessment that goes with this guide.
sylvanassurance.com/go/free-vulnerability-management