Your First Vulnerability Management Wins

A free plain-English guide from Sylvan Assurance

Sylvan Assurance, LLC

Version 1.0 · Updated 2026-10-05

Contents

Why this guide exists 1
Move 1 — Make the list 2
Move 2 — Run one authenticated scan 2
Move 3 — Adopt the KEV habit 3
Move 4 — Set three deadlines 4
Move 5 — Write the one-page report 4
What not to do yet 5
The five moves on one page 5
The jargon translator 6
Where you stand, and where to go next 7

About This Guide **8**

A plain-English guide to the five moves that start a real programme, for the person who just inherited "the security stuff".

Why this guide exists

Somewhere between the client questionnaire, the insurance renewal, and the news story about the breach that started with an unpatched server, you concluded that your organisation should be doing something called vulnerability management: finding the security weaknesses in the things you run, deciding which ones matter, and fixing them in a sensible order.

Then you looked at the field and found a wall of acronyms, a dozen tools with four-figure price tags, and advice written for companies with a security department.

Here is the encouraging truth: a real vulnerability management programme starts with five moves, none of which needs a budget line or a specialist. Organisations that make these five moves are meaningfully better defended, and can prove it, within a month or two. This guide walks through each move in plain English: what it is, why it works, and how to do it this week.

One note before we start. Everything here is general guidance drawn from widely recognised practice. Your organisation is specific. Treat each move as a recommendation to

adapt, not a rule to obey.

Move 1 — Make the list

The win: one current list of everything you run.

You cannot assess, scan, or fix what you don't know you have. Every other part of vulnerability management sits on top of an asset inventory, and most small organisations don't have one. They have a hardware purchase log from finance, a vague memory of which laptops went to whom, and a collection of software subscriptions someone signed up for in 2021.

A spreadsheet is enough. Open one and list:

- **Devices**: servers, laptops, desktops, the firewall, switches, wireless access points, printers. If a managed service provider (MSP) looks after your devices, ask them to export their list; it is usually one email.
- **Cloud and Software-as-a-Service (SaaS)**: every online service the business uses, such as email, file storage, accounting, the customer system, the website host. Check the company card statement; it is a surprisingly good discovery tool.
- **Software that matters**: the operating systems on your servers, plus the handful of applications your business genuinely depends on.

For each entry, record four things: what it is, who owns it (a named person, not "the team"), what it touches (customer data? payments? nothing sensitive?), and whether it is reachable from the internet.

That last column deserves a sentence. Internet-facing systems (your website, a remote-access portal, anything with a public address) are the systems attackers can try without an invitation. Knowing which of your assets are internet-facing is the single most useful fact in the whole list.

Time required: one honest afternoon, plus an email to your MSP or accountant.

Move 2 — Run one authenticated scan

The win: a first, honest picture of your weaknesses.

A vulnerability scanner is a tool that examines your systems and reports known weaknesses, typically referenced by their Common Vulnerabilities and Exposures (CVE) identifier, the industry's catalogue number for "a specific flaw in a specific product".

Two things matter for your first scan.

First, run it at all. Free and low-cost options are genuinely workable at small scale: scanner free tiers cover a small estate, and many MSPs offer scanning as a modest add-on to an existing contract. Scan the assets on your list from Move 1, which is why Move 1 comes first.

Second, make it an authenticated scan if you can. An unauthenticated scan knocks on the outside of each system and reports what it can see from the doorstep. An authenticated scan (one given credentials, or run through an installed agent) looks inside: installed software, missing updates, weak settings. The difference in what you learn is large. If your MSP manages your devices, they already have the credentials; ask for credentialed scanning by name.

When the report arrives, expect a big number. Hundreds of findings on a small estate is normal and not a verdict on you. Most findings are minor, many are duplicates of one underlying issue across several machines, and a small handful genuinely matter. Sorting out which handful is Move 3.

Time required: an hour or two of setup, then the scanner does the work.

Move 3 — Adopt the KEV habit

The win: the Known Exploited Vulnerabilities (KEV) catalogue tells you what attackers actually use, and you fix that first.

Scanners rate findings by severity, usually with a Common Vulnerability Scoring System (CVSS) number from 0 to 10. Severity is useful, but it answers the wrong first question. A flaw can be severe in theory and ignored by every attacker on earth; another can look moderate on paper and be exploited in live attacks this week.

The KEV catalogue answers the right first question. Maintained by the United States Cybersecurity and Infrastructure Security Agency (CISA), it is a free public list of vulnerabilities confirmed as actually exploited in the real world. Not theoretically exploitable: exploited.

The habit, in three steps:

1. **Subscribe.** CISA's KEV update emails are free. In the UK, the National Cyber Security Centre's alerts are the natural companion subscription. Thirty minutes of setup, once.
2. **Cross-check.** When a scan report arrives, check whether any finding appears in the KEV catalogue. Many scanners flag this for you; if not, the catalogue is searchable.
3. **Act on matches immediately.** A KEV-listed finding on one of your systems, especially an internet-facing one, is the closest thing vulnerability management has to a fire alarm. The widely recommended response is to patch (or switch off, or wall off) within a day or two, not within a month.

If you have appetite for one refinement: the Exploit Prediction Scoring System (EPSS) gives each CVE a probability that it will be exploited soon. It is free, and it pairs well with severity scores. But if you adopt only one signal, make it KEV.

Time required: thirty minutes of setup, then minutes per scan cycle.

Move 4 — Set three deadlines

The win: findings stop ageing silently.

Here is the failure mode of most young programmes: the scan runs, the report lands, everyone agrees the findings are concerning, and ninety days later the same findings are still open because nothing made anyone fix them by any particular date.

The fix is a starter Service-Level Agreement (SLA), which sounds corporate, but is just three written deadlines:

- **Critical findings: fixed within 30 days.** (KEV-listed ones much faster; see Move 3.)
- **High findings: fixed within 60 days.**
- **Everything else: fixed within 90 days, or at the next maintenance window.**

Write these three lines down, agree them with whoever does the fixing (your technician, your MSP), and date the page. That is the whole exercise. The deadlines do not need to be aggressive; they need to exist, because a deadline turns "we should patch that" into "this is due on the 14th".

One companion habit makes the deadlines honest: **the exception note.** When something genuinely cannot be fixed on time (the vendor has no patch yet, or the update breaks a system you depend on), write down four things: the finding, the reason, what you are doing to reduce the risk meanwhile, and a date to look at it again. Four fields in a shared document. This small record is the difference between "risk we considered and are managing" and "risk nobody remembers accepting", and it reads impressively well when a client or insurer asks.

Time required: one conversation and one page.

Move 5 — Write the one-page report

The win: the programme becomes visible, and therefore durable.

Every quarter, write one page for whoever is in charge: the owner, the managing partner, the board. Three numbers and a sentence each:

1. **Open critical findings**: how many, and whether any are KEV-listed (the target is zero KEV, and a shrinking count).
2. **Deadline performance**: what share of findings were fixed within the deadlines from Move 4.
3. **Active exceptions**: how many four-field exception notes are open, and whether each still has a future review date.

Why this matters more than it looks: programmes run by one conscientious person have a way of evaporating when that person is busy, on leave, or gone. A quarterly page to leadership creates a rhythm someone will ask about ("where's the security summary?"), and that question is what keeps the scan running in month nine. It also builds, page by page, the evidence file that answers client questionnaires and insurance forms in minutes instead of days.

Time required: thirty minutes a quarter. The best half hour in this guide.

What not to do yet

A short list of things that can wait, offered with respect for your time and budget:

- **Don't buy a platform.** Until the five moves are routine, an expensive vulnerability management platform automates a process you don't have yet.
- **Don't chase a perfect inventory.** A 90% complete list maintained monthly beats a 100% complete list from last year.
- **Don't try to fix everything.** The goal is not zero findings. No organisation on earth has zero findings. The goal is that the dangerous few are handled fast and the rest are handled deliberately.
- **Don't wait for a quiet month.** There isn't one. The five moves are sized to fit alongside a day job.

The five moves on one page

Print this page and put it where the work happens. Tick the boxes as the moves land; the dates column is what turns intentions into a record.

```
THE FIVE MOVES                                    Done   Date

MOVE 1 - MAKE THE LIST
[ ] Devices listed (ask the MSP for an export)   [ ]   _____
[ ] SaaS and cloud services listed (walk the
    card statement)                               [ ]   _____
[ ] Each entry has: a named owner, what data
    it touches, internet-facing yes/no            [ ]   _____

MOVE 2 - RUN ONE AUTHENTICATED SCAN
[ ] Tooling chosen (MSP add-on / free tier /
    built-in platform)                            [ ]   _____
[ ] Credentials or agents in place                [ ]   _____
[ ] First scan run; report saved to a dated
    folder                                        [ ]   _____
[ ] Repeat booked in the calendar (monthly,
    or quarterly at minimum)                      [ ]   _____

MOVE 3 - ADOPT THE KEV HABIT
[ ] Subscribed to CISA KEV updates (and your
    national cyber centre's alerts)               [ ]   _____
[ ] Scan findings cross-checked against KEV       [ ]   _____
[ ] Standing rule agreed: KEV match = action
    within 24-48 hours                            [ ]   _____

MOVE 4 - SET THREE DEADLINES
[ ] Written: Critical 30 days / High 60 /
```

```
    Rest 90 or next maintenance window          [ ]   ____
[ ] Agreed with whoever does the fixing         [ ]   ____
[ ] Exception note format ready (finding,
    reason, risk-reducing measure, review date) [ ]   ____

MOVE 5 - WRITE THE ONE-PAGE REPORT
[ ] Quarterly reminder in the calendar          [ ]   ____
[ ] First report sent: open criticals (KEV
    count), deadline performance, exceptions    [ ]   ____
```

The jargon translator

The dozen terms you will meet first, in plain English. (Each is explained in context earlier in this guide; this page is for the moment a vendor or questionnaire throws one at you.)

Term	Plain English
Vulnerability	A known weakness in software or hardware that an attacker could use
CVE	The catalogue number of a specific flaw (e.g. CVE-2026-12345): an identity, not a severity
CVSS	A 0–10 score for how damaging a flaw *could* be if exploited
KEV	The public list of flaws *confirmed as actually exploited*: your “fix first” signal
EPSS	A probability estimate that a flaw will be exploited soon
Authenticated scan	A scan that signs in (or uses an installed agent) and sees what is really there
Asset inventory	The list of everything you run: devices, cloud, SaaS
Internet-facing	Reachable from the public internet; attackers can try it uninvited
Remediation	Fixing the flaw: usually patching, sometimes a setting or a switch-off
Compensating control	A risk-reducing measure used while the real fix is pending
Exception	A written, approved record that a finding will be fixed late (or accepted), and why
SLA	A written deadline per severity level: your three deadlines from Move 4

Where you stand, and where to go next

If you want to see how your current practice measures up, our free **Vulnerability Management Assessment** scores you across eight areas (inventory, scanning, prioritisation, remediation, patching, cloud workloads, exceptions, and reporting) in about ten minutes, entirely in your browser. Your answers never leave your device.

When you are ready for the working documents (an asset register template, a first-scan runbook, a triage decision path, SLA tables, exception forms, and board-report templates), the paid editions of the assessment include them as ready-to-adapt PDFs, scoped by organisation size: Solo, Team, and Enterprise.

Provided by Sylvan Assurance, LLC. This is general, plain-English guidance, not professional advice and not a security audit. Every recommendation is optional, and following it reduces common risks but does not guarantee any outcome. Responsibility for your organisation's security remains with you; verify anything here against your own circumstances and, where needed, a qualified professional.

About This Guide

This guide is produced by **Sylvan Assurance, LLC** and reflects professional experience in the relevant practice area, translated into plain-language guidance for the people who run vulnerability management - from solo operators to security teams.

It provides **general guidance and recommended practices**. It is **not** legal advice (and not a professional audit). Every recommendation is **optional** - a widely accepted way to reduce a common risk - and following it reduces exposure to common problems but **does not guarantee security or any particular outcome**. Responsibility for your business remains with you.

For full terms, see the Terms of Use provided with the Vulnerability Management Assessment.

Copyright 2026 Sylvan Assurance, LLC. Not for resale.

Free to share unchanged with credit. Terms: sylvanassurance.com/licence/free/

Where to go from here



Scan for the full toolkit that builds on this guide.
sylvanassurance.com/go/toolkit-vulnerability-management



Scan for the companion book - the full story, in plain English.
sylvanassurance.com/go/vulnerability-management