

Risk Prioritization

Fix the few weaknesses that matter, first.

● The problem

No organisation can patch everything. A record 48,185 vulnerabilities were published in 2025, and on average companies fully fixed only about a quarter of those known to be actively exploited, taking a median of 43 days. Long lists of findings sorted only by a severity score do not tell a team where to start. What matters is which weaknesses an attacker can actually reach and use against you, and closing those first.

● Confirmed, probable or not yet known

Every weakness Cybergard reports carries a confidence label, so your team never chases noise.

Confirmed means we observed it directly: the exposed file was downloadable, the login page answered, the email policy is missing. There is no doubt it exists.

Probable means strong evidence points to it, but it was inferred rather than proven, for example a software version that is known to carry a published vulnerability. Some vendors fix flaws without changing the version number, so probable findings are worth a quick check before a large change.

Not yet known covers what could not be determined from outside, such as software whose version is hidden. These are never counted as weaknesses; they are listed separately so you know exactly what was and was not checked.

● How we rate criticality

Each weakness has a severity: critical, high, medium or low. Some conditions are treated as critical whatever their technical score, because the business impact is immediate: an abandoned web address anyone can take over, or a database open to the internet. The overall rating of your organisation is the worst severity actually present, never a count of how many findings there are, and the report always states the reason.

On top of severity, findings are grouped into business risks, such as attackers breaking in, signing in as staff or using your name for fraud. Each risk gets a likelihood from the evidence behind it: how certain it is, how severe, how many systems, and whether those systems face the internet. The report then turns this into a short "patch first" list, where one software upgrade that fixes many vulnerabilities becomes a single task.

Every vulnerability in every system

Reachable from the internet

Known to be exploitable

Confirmed or probable on your systems

Patch first

Each step narrows thousands of findings down to the few that an attacker can use against you.

● Your internal scan reports, prioritized

Most companies already run an internal vulnerability scanner, such as Qualys, Tenable, Rapid7, Microsoft Defender or OpenVAS, and receive reports with thousands of findings. You can upload that report as it comes out of the scanner. Cybergard links each internal server to what we see from the internet, by its name, its public address or the information your team provides, and suggests matches for your team to confirm.

Each vulnerability is then ranked by clear rules: whether it is being exploited in the wild, how likely it is to be exploited soon, its severity, whether the server can be reached from the internet, whether it sits on an attack path, and how long it has been open. The result is a patch plan in four groups (fix now, this week, this month and plan), with the servers, the reason and a target date for each task. The uploaded file is deleted as soon as it has been read.

Want help with the fixes? Our consultants can plan and validate remediation with your team.

sales@cybergard.app
cybergard.app

Sources: CVE data 2025; Verizon 2026 Data Breach Investigations Report (remediation of known exploited vulnerabilities).