

External Attack Surface Monitoring

See your organisation the way an attacker does, before an attacker.

● What it is

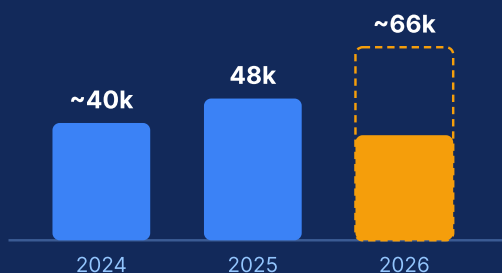
Business-critical applications now run on the internet: customer portals, online services and the systems your customers and partners log in to every day. Alongside them sit websites, login pages, cloud services, email systems and the test or legacy systems that are easy to forget. Together they are your internet edge. External attack surface monitoring continuously discovers all of it and checks it for weaknesses from the outside, exactly as an attacker would, without installing anything in your environment.

● Why it is critical now

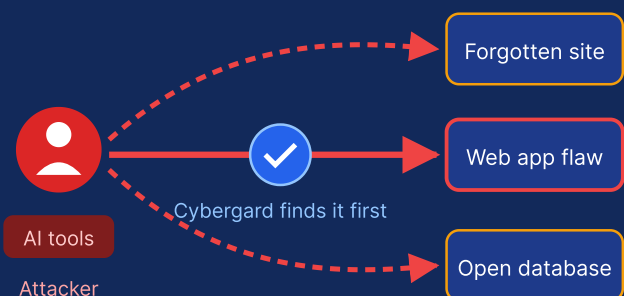
Attackers were already ahead of most defenders. AI has now given them tools that find and exploit software flaws at machine speed, and the numbers show it. A record 48,185 vulnerabilities were published in 2025, up from about 40,000 in 2024. More than 35,000 were published in the first half of 2026 alone, and close to 66,000 are expected for the year, a rise driven mostly by AI finding flaws on its own.

At the same time, weaknesses are now exploited on average a week **before** a fix is published. There is no "zero-day" safety margin any more: the window has gone negative. Knowing your external weaknesses early, and closing the ones an attacker can reach, is what keeps you from being breached.

Vulnerabilities published per year



2026: solid = first half (35k+), outline = full-year forecast.



Attackers probe every exposed system; Cybergard checks the same paths first.

● How we work

We look at your organisation strictly from the outside, the way an attacker prepares an attack, in steps that build on each other. First we map your domains and subdomains, including systems IT may have forgotten. Next we find which of those systems have open network ports and identify the services behind them. We then examine every web application we discover, and finally check all of it for known and likely vulnerabilities.

Most checks are passive: they read public records such as DNS and certificates and send nothing unusual to your systems. The active checks are safe and non-disruptive, much like a normal visitor or search engine, and deeper tests run only on the systems you approve. Results arrive as a report that leads with business risk and a short list of what to fix first.

● What we find

Subdomain takeover. A web address of yours still points to a cloud service that has been deleted. Anyone can claim that service and publish pages on your trusted name, a favourite route for phishing and fraud against your customers.

Exposed administrator panels. Internal login pages that can be reached from anywhere on the internet. They are usually protected only by a password, so stolen or guessed credentials are enough to get in.

Exposed databases and remote access. Data stores and remote-management services that should only be reachable inside your network. Attackers scan for them automatically and try passwords and known flaws at scale.

Leaked files and secrets. Backups, configuration files or keys left downloadable on a website. They hand attackers working passwords and data, and once copied they cannot be taken back.

Known vulnerabilities and outdated software. Software versions with published flaws, or versions that no longer receive security updates. These are the first things attackers look for, because working exploits already exist.

Weak or expired encryption. Certificates that have expired, or old protocols still switched on. Customers see browser warnings, auditors raise findings, and data in transit is less protected.

Email spoofing. Missing or weak email authentication lets criminals send email that appears to come from you, the basis of invoice fraud and phishing aimed at your customers and partners.

Need to go deeper? On-demand penetration testing for a critical application, by experienced testers.

sales@cybergard.app
cybergard.app

Sources: CVE publication data 2024 and 2025; FIRST 2026 CVE forecast (via Help Net Security, June 2026); first-half 2026 CVE counts; Google Mandiant M-Trends 2026 (average time to exploit).