

Breach and Leak Monitoring

Know when your organisation's data leaks, before criminals use it.

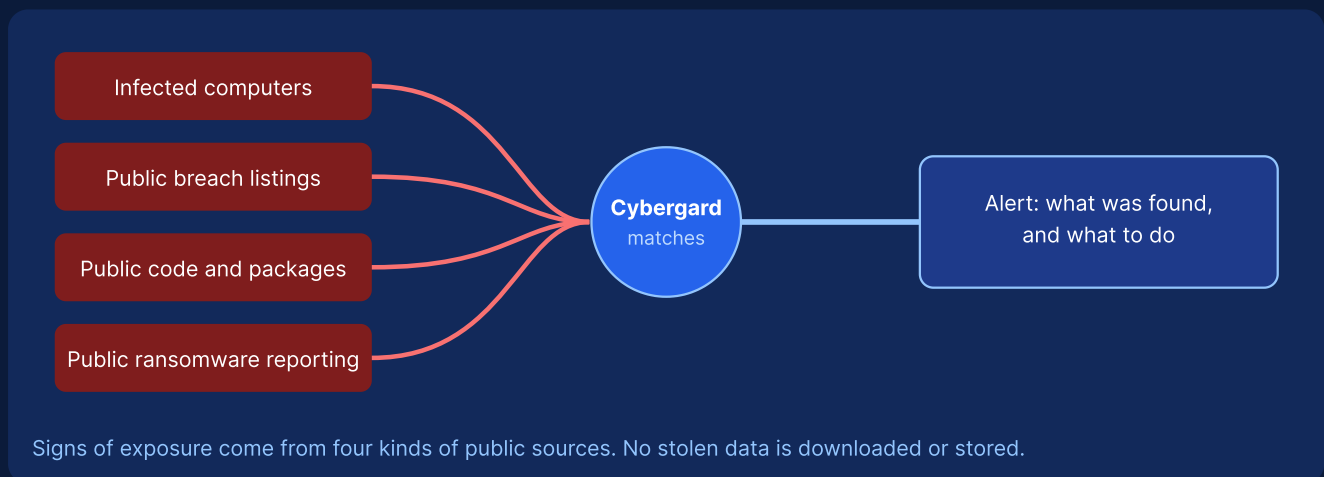
• What it is

Your organisation can be exposed without anyone attacking your systems. Malware on an employee's laptop quietly steals saved passwords, a website your staff use is breached, a developer publishes code with a live key, or a ransomware group publicly claims you as a victim. Breach and Leak Monitoring continuously watches for signs of these events that relate to you and tells you what to do about them, with nothing to install.

• Why it is critical now

Stolen credentials appear in 39% of breaches. More than half of ransomware victims (54%) had passwords exposed in password-stealing malware logs before they were attacked. In 2025, 29 million secrets such as passwords and keys were leaked on public code sites, 34% more than the year before, and code written with AI help leaks them at about twice the usual rate. Ransomware groups publicly claimed a record 7,458 victims in 2025, up 30%.

Criminals use automation and AI to try stolen passwords at scale, so a leak can turn into a breach within days. Knowing early that your passwords, keys or data are exposed gives you the time to reset, revoke and warn people before the damage is done.



• How we work

We continuously watch four kinds of sources: intelligence on computers infected with password-stealing malware, public listings of data breaches, public code and software-package sites, and public trackers of ransomware groups' victim announcements. Every new item is matched against your domains and company names, ranked by how serious it is, and shown with the steps to take.

We never download, store or buy stolen data, and we never show stolen passwords; we only report that an exposure exists, where it relates to you and how serious it is. Nothing is installed and we never touch your systems. When a key is found in public code, we check whether it is still active, without using it to reach your data, so you know whether it must be changed today.

● What we find

Stolen employee passwords. How many employee computers are infected with password-stealing malware holding logins for your systems, and which of your sign-in pages are affected, such as email, VPN or cloud consoles. Those passwords are in criminal hands and should be reset now.

Customer accounts at risk. How many of your customers' computers are infected and hold their passwords for your website. Expect account-takeover attempts and fraud against those customers.

Breaches affecting your organisation. Newly published data breaches that may include your staff or customers, so you can warn people and enforce password changes.

Leaked code and keys. Public code repositories that mention your domain, especially configuration and secret files. Keys that are still active are flagged as critical.

Public software packages and images. Packages and container images published under your name, which can carry internal code or credentials by mistake.

Ransomware leak-site listings. Your organisation, or a supplier, named in public reporting of ransomware victim announcements. This usually means a breach has already happened and needs an immediate incident response.

Found something serious? On-demand incident response and consulting, by experienced practitioners.

sales@cybergard.app
cybergard.app

Sources: Verizon 2026 and 2025 Data Breach Investigations Reports; GitGuardian State of Secrets Sprawl 2026; Searchlight Cyber ransomware research 2025.