DARK WEB MONITORING

Protecting your team from stolen passwords

What this service does, what it means for you, and the one step we ask of your people.

Most password leaks don't start with you — they come from the other websites and services your team uses. When one of those is breached, the stolen passwords are sold on the dark web and tried against business accounts. **Dark web monitoring watches for exactly that**, so an exposed password is fixed before anyone can use it against you.

We alert only on an exposed **password** tied to your team — not merely an email address — so every alert is real and worth acting on.

What happens when a password is found

1

We detect it

We continuously check known breaches for passwords linked to your team.

2

The person is notified

They're emailed the details and a secure link to act. Admins can be CC'd.

3

They fix it

They change the exposed password and confirm it in the learning portal.

4

It clears

The exposure moves from *unresolved* to *resolved* on the dashboard.

Who does what (and why it's almost nothing for you)

We handle it

- Monitor continuously for breached passwords
- Notify the affected person and guide their fix
- Track every exposure's status on the dashboard

Your team does one thing

- Change the exposed password — and anywhere it was reused
- Mark it complete in the learning portal

That's the whole ask — no tickets, no new logins.

Reading your status: resolved vs. unresolved

UNRESOLVED

A breached password hasn't been changed and confirmed yet. The only state that needs attention.

RESOLVED

The person changed the password and confirmed completion. That exposure is addressed.

WHAT THIS MEANS FOR YOUR ORGANIZATION

- **Caught early.** Fixed before it can be used to break in.
- **People are guided.** Each person is told exactly what to do.
- **You stay hands-off.** Full visibility, optional CCs, no queue.