ENTERPRISE

Protect your workforce.

It starts with one tired person and one good email. The spoofed CEO. The vendor whose bank details changed. The payroll form that is not from payroll. Give every employee a second opinion in seconds, at work and at home.

What lands in their inbox

`From "Dana Whitfield (CEO)" · 4:52 PM`

Are you at your desk? I need gift cards for a client dinner. Keep this between us.

`From "HR Payroll Portal" · 9:14 AM`

Action required: re-verify your direct deposit before Friday's run.

`From "Vendor accounts team" · Mon`

Please note our updated banking information for invoice 4471, due this week.

Three patterns, aimed at whoever is busiest. Each one gets checked before anyone replies.

Built for

Companies where money moves on an email: finance and payroll teams, professional services, property, construction, healthcare admin. Anyone with a shared drive of invoices and a busy accounts inbox.

How it is deployed

Every employee gets a seat

The Chrome extension in the browser, the mailbox approved once by your admin and connected by each person in one click through Google Workspace or Microsoft 365, and the Carmen app on their phone. Their work inbox and their personal phone, because attackers do not respect office hours.

Provisioned from your directory

Single sign on and directory provisioning (coming soon): added when people join, removed when they leave.

Run from one place

People, seats, alerts, usage and billing in one admin page. High risk alerts emailed to the address you choose, so they land in your ticket system.

WHY IT GETS USED

Security training gets skipped.

A button that answers "is this real?" gets pressed.

What your security team gets

Fewer "is this phishing?" tickets

Employees ask Carmen first. The helpdesk gets the cases that need a person, not the screenshots that do not.

Every flag, with its evidence

What was flagged, who received it, the verdict and the reasons, in the admin page and by API.

Coverage after hours

The Carmen app screens texts from unknown numbers on personal phones. The protection follows people home.

How it is priced

Per seat, on a contract, with audit logs included. Single sign on and directory provisioning are coming soon. Deep checks draw from a shared pool sized for your headcount. There is no public price at this size. Tell us the headcount and we come back with a number.

How it starts

1. A call to scope the rollout.
2. One team first, real inboxes, two weeks, then everyone.
3. The numbers at the end: what was screened, what was flagged, what people asked. Then the contract.

What it is not

- No person reads your employees' messages. Screening is software.
- It does not block email or pages. It warns, and the person decides.
- Texts from people in their contacts are never touched. Personal phones stay personal.
- Message contents are kept 30 days for the case record, then deleted. The verdict and who received it are kept for the log.

Questions

Does it read our employees' personal messages?

It screens texts from unknown numbers only and keeps nothing. Contacts are never touched.

Can we turn parts off?

Yes. Mail, browsing and phone screening are each a switch, per person.

Where do alerts go?

The admin page, and by email to an address you choose.

Does it replace our email security?

No. It sits behind it and checks what gets through, then tells the person what to do.

Do you support single sign on?

Coming soon, SAML and directory provisioning.

Talk to sales

sales@backgrounder.com. Tell us the headcount and we will come back with a plan and a number.