packets

by BreakNCo Global

REFERRAL PARTNER GUIDE

Packets is a human–AI agency that makes growing companies digitally resilient by owning and running their security and privacy governance system.

Most growing companies have no structured programme governing how their data is protected, who is responsible for it, and whether it meets the standards clients and regulators expect. Packets fills that gap completely: a specialist inside your team, supported by an AI platform that does the routine work automatically.

For growing companies with **20–500 employees**.

WHAT TRIGGERS COMPANIES TO COME TO US

An urgent vulnerability needs a safe fix.

Can the team identify exposed systems, deploy a tested patch, verify the result and roll back if needed?

A security incident would overwhelm the team.

Who leads the response, brings in specialists and keeps customers informed? Has this been practised?

Backups exist, but recovery is unproven.

Can critical systems actually be restored, and can the business keep operating? When was this last tested?

A customer needs proof before buying or renewing.

Certificates, SOC 2 reports, questionnaires or stronger security, privacy and AI requirements are holding up the deal.

The founder, CTO or small team owns everything.

Governance and compliance compete with delivery. Follow-up and evidence depend on a few overstretched people.

WHAT PACKETS DOES ABOUT IT

Towards Governance on Autopilot

We start from where the company is today, build and run its governance system, and strengthen its security and privacy posture as business needs and customer expectations grow.

01 · UNDERSTAND AND BUILD

Connects your tools and builds governance

Reads the real environment across AWS, GitHub, Okta and HR systems. Packets intelligently builds and maintains company context, then establishes policies, responsibilities, controls, evidence and a risk register around it.

No spreadsheets, no manual uploads, no homework for your team.

02 · IMPLEMENT AND OWN

Places a Forward Employee inside your team

A Packets specialist owns the programme, implements controls, runs internal audits and keeps work moving. AI handles routine work; experts bring judgment, specialist skills and long-term accountability.

03 · DEMONSTRATE AND MATURE

Makes you audit-ready and keeps maturing

Aligns controls and evidence with relevant ISO, SOC 2 and privacy requirements, closes gaps and supports assessments. Keeps context, risks, controls and evidence current, strengthening security and privacy as the business grows.

Your referral rewards

ON QUALIFIED INTRODUCTION

Recognition + thank you gift

A warm intro to a company that takes a discovery call with our team.

ON SIGNED ENGAGEMENT

5% of the first year's contract value

Your referral becomes a Packets customer—paid on contract signing.

ON RENEWAL OR EXPANSION

Ongoing relationship credit

Referrals that grow with Packets keep your partner relationship active.

shalini@packets.build

REFERRAL PROGRAMME

Who to refer. How to introduce them.

Growing companies with 20–500 employees whose security and governance needs have outgrown their time or expertise.

The right referral looks like this

- A founder, CTO or small team carrying security and compliance alongside product delivery.
- A company facing customer security requirements, an approaching audit or a need to practise incident response and recovery.
- A company that evaluated Scrut, Sprinto or Vanta but found the pricing or upfront commitment did not fit—or adopted a tool and still needs implementation and ongoing operations.

A practical starting foundation that we recommend

Assess the company's starting point and establish the controls that support its security, privacy and customer trust.

Threat modelling

Identify priority threats around systems, data flows and critical services, and use them to guide controls.

Penetration testing

Assess vulnerabilities and security weaknesses, then connect findings to remediation and risk decisions.

Mobile device management (MDM)

Set up device management and the agreed device-security controls.

Automated core controls

Implement the agreed core controls through Packets automation and specialist execution.

A Trust Portal for the company

Deploy a portal to share approved assurance material with customers and make the company's security and privacy work visible.

> **Audit readiness is a milestone in the continuing journey.** Independent certification bodies and auditors determine external assessment outcomes.

How to make a referral

1. Send Shalini the company name, relevant contact and a line about the immediate need.
2. Make a warm introduction over email or WhatsApp. Packets explores the priorities and agrees the delivery scope.
3. We acknowledge the introduction and keep you updated through the conversation.

Introduce a company ↗

Shalini · Packets
shalini@packets.build
packets.build

More questions to ask

Emergency production changes

Who checks testing, approvals, implementation and rollback arrangements—and reviews the result afterward?

Repeated RFPs and supplier reviews

Can the team answer security questionnaires and enterprise onboarding questions with current evidence and clear ownership?

Expanding customer requirements

Have buyers introduced stronger security, privacy or AI expectations that the company cannot yet demonstrate?

Manual evidence coordination

Are control reviews, evidence requests and follow-up actions still coordinated manually? Who keeps them current between audits?

Introduce the company and the need. The Packets team takes the conversation forward.

CONVERSATION SCRIPTS

Words you can use.

Different people have different starting points. Use the explanation that fits the conversation.

NETWORKING · A SHORT INTRODUCTION

"I know the team at Packets. They own and run security and privacy governance for growing companies. They take a company from its current position towards Governance on Autopilot: define the governance system, implement controls, align frameworks, prepare for audits and keep strengthening its posture as it grows. Their platform builds company context, AI handles routine work, and experts provide judgment and specialist execution."

Follow with: "Do you know a founder or CTO who is carrying this alongside their main job, or has a customer asking for stronger security evidence?"

WHEN SOMEONE ASKS WHAT PROBLEM PACKETS SOLVES

"A growing company wins an enterprise opportunity, then gets asked for an ISO certificate, a SOC 2 report or evidence of how it protects customer data. Packets starts from where it is today and progresses it towards Governance on Autopilot. The work builds practical security foundations, aligns controls and evidence with relevant requirements, prepares the company for independent assessment and continues to mature its posture."

Also listen for: a customer renewal, security questionnaire, approaching audit or an existing tool that still needs an implementation team.

FOUNDER OR CTO · SECURITY UNDER PRESSURE

"If a serious vulnerability affected production tomorrow, could your team identify what is exposed, deploy a safe fix and verify it worked? If an incident followed, who would coordinate the response and keep customers informed? Have you tested restoring critical systems and keeping the business operating?"

"Packets builds and runs the governance system around those needs, with a phased path towards Governance on Autopilot. Practical foundations include threat modelling, penetration testing, MDM, automated core controls and a Trust Portal for customer assurance. A conversation would establish your starting point and priorities."

INVESTOR, ANGEL OR ACCELERATOR

"Do any of your portfolio companies have enterprise customers asking for stronger security evidence, or founders and CTOs stretched across governance, compliance and incident readiness? Packets focuses on growing companies with 20–500 employees. It starts from each company's current posture and progresses it towards Governance on Autopilot, building controls, preparing for assessments and strengthening security and privacy as demand grows."

Good referral: companies that evaluated Scrut, Sprinto or Vanta but could not proceed because the pricing or upfront commitment did not fit their stage—or bought a tool and still need implementation support.

AI TOOLS AND AGENTS IN THE BUSINESS

"As your company introduces AI tools and agents, do you know what is running, what data it can access, which actions it takes and what it costs? Packets is working across AI inventory, risk assessment, policies, identity, observability, data access, gateways, guardrails, cost governance and security testing."

Follow with: "They are speaking with companies about these needs to shape delivery priorities. I can introduce you to discuss your immediate risks and what support would fit."

A MESSAGE YOU CAN FORWARD

Hi Shalini, introducing [name], [role] at [company].

They are a growing company with around [employee count] people. Their immediate need is [customer security requirement / audit readiness / ongoing governance / urgent patching and incident readiness / tested recovery / AI governance].

[Name], Packets is a human–AI agency that makes growing companies digitally resilient by owning and running their security and privacy governance system.

I thought a conversation would help establish what support fits your priorities. I will leave you both to connect.

Email or WhatsApp the introduction. Contact shalini@packets.build.

Use a warm introduction to connect the company with the Packets team.

MORE WAYS TO HELP A GROWING COMPANY

How we can help

Use these areas to recognize demand. Conversations help shape what we build and how we deliver it; discovery establishes the priorities and agreed scope.

The Packets platform intelligently builds and maintains an understanding of each company's operations, systems and governance needs. AI agents use that context to identify gaps and carry out routine work. Experts provide judgment and specialist execution, while leadership sees risks and progress, sets priorities and makes business and risk decisions.

Governance and continuous compliance

Establish responsibilities, policies, controls and recurring governance operations. Maintain the system as the company and its obligations change.

Risk and control assurance

Assess risks, agree treatment, evaluate control execution and effectiveness, and track remediation, decisions and evidence.

Audit readiness and framework expansion

Prepare for independent assessments, coordinate evidence and internal reviews, address gaps and reuse relevant work across requirements.

Customer assurance and Trust Center

Support customer security reviews and questionnaires, organize approved trust material and make evidence easier to share with the right audience.

Security controls and specialist execution

Vulnerability assessment and penetration testing (VAPT), threat modelling, device and endpoint controls, access reviews, patching and agreed remediation work.

Augmented security incident response

Coordinate security experts, application teams, customer communications, technical remediation, production-change reviews and incident follow-up.

Continuity and recovery

IT service continuity management (ITSCM), disaster recovery (DR) and business continuity management (BCM), including business continuity plans (BCPs), restore tests, continuity exercises and remediation.

Change Review Board as a Service

Review change risk, assign implementors and reviewers, check testing and approvals, confirm rollback arrangements and complete post-implementation reviews.

Privacy governance and operations

Processing records, privacy impact assessments, data-subject request workflows, privacy incidents, policies and continuing operational responsibilities.

Vendor and third-party risk

Assess suppliers, understand access and data dependencies, review supporting assurance and track risks and follow-up actions.

AI governance and runtime controls

AI inventory, risk and impact assessments, policies and ISO 42001 readiness; gateways and guardrails; agent identity and observability; data access; baselines and drift; policy enforcement; cost governance; AI security testing, VAPT and specialist tools.

Governance onboarding and migration

Understand the existing program, bring relevant policies, controls, registers and evidence into Packets, and work with incumbent teams and consultants.

Bring us the need, the current approach, where it falls short and when help is needed.

packets.build · 04