

Technology that grows your business, secure by design.

We build software, apps and AI automation around your goals, your budget and the way you work, with security and compliance built in from day one.

- ✓ 150+ projects delivered so far
- ✓ Build, security and compliance in one team
- ✓ We reply within one working day

We build AI and software, and we secure it.

SecWiz Technologies is an AI development and cybersecurity company in Delhi, India. Our developers build AI systems, web platforms and mobile apps. Our security engineers review and harden what they build, and systems other companies built too. Each side learns from the other.

Hire us for one service or for the whole journey. Either way, security is part of the plan from the start, not an extra at the end.



150+

projects delivered so far,
most of them short
security engagements

3-in-1

build, security and
compliance from one
accountable team

Day one

security is part of the plan
from the first sprint, not
added at the end

IN BRIEF

Who we are

SecWiz Technologies Pvt. Ltd., an AI development and cybersecurity company incorporated in India in 2024. We build AI and software systems, and we secure them.

How we work

Developers and security engineers work in one team. Security reviews what we build before launch, and you talk directly to the engineers on your project.

Where we work

From one office in Delhi, working remotely with clients in India, Southeast Asia, Europe, the Middle East and the USA.

Building and defending **teach** different lessons.

Two frustrations started this company. Some development firms hand over a build and go quiet. Some security firms hand over a PDF of findings that nobody on the client side knows how to act on. Both come from the same gap: the people who write the code and the people who secure it never talk to each other.

So we put them in one team. Our security engineers review and harden what our developers build before launch. Our developers sit in on findings meetings for systems other companies built.

- ✓ **Shipping teaches us where corners get cut.** A security engineer who has shipped a product knows which shortcuts teams take under deadline.
- ✓ **Defending teaches us what not to write.** A developer who has watched an AI agent get talked into leaking data writes different code afterwards.

HOW WE GREW: FOUR PRACTICES, EACH STARTED BECAUSE CLIENTS ASKED

01

Web, mobile and AI development

Where we started. We still build web platforms and mobile apps, and now AI systems too, from AI agents to LLM and RAG applications.

02

Defensive security and vulnerability management

Clients kept asking who was checking the software we handed over, so we built that skill in house.

03

Governance, risk and compliance

Enough clients asked us to walk them through ISO 27001 and SOC 2 that it became a practice. It now covers GDPR and risk management too.

04

AI security testing and guardrails

Clients started shipping LLM features and asking who could test them. This practice tests and hardens models, agents and the apps around them.

Vision, mission and the values behind our work.

Where Innovation Meets Secure Digital Future. We build what is new, and we make it safe to rely on.

WHERE WE ARE GOING

Vision

To be a trusted global partner for secure digital transformation: technology that helps organizations grow in a connected world, and stay resilient in it.

WHAT WE DO EVERY DAY

Mission

To build intelligent, secure and future-ready digital systems that improve how a business performs, protect its data and support steady growth, through innovation and trust.

Security

Safety built into every system we deliver.

Integrity

Trust and transparency in every engagement.

Innovation

Technology and defense that keep improving.

OUR OBJECTIVES

What we hold ourselves to

- ✓ Deliver high-performance, secure and user-centered software.
- ✓ Strengthen businesses with security and compliance programs that hold up under audit.
- ✓ Build long-term partnerships through transparency, trust and quality of work.
- ✓ Keep innovating with AI and automation, and test what we build before clients rely on it.
- ✓ Raise security awareness and resilience across our clients' teams.

Core strengths: development and cybersecurity in one team, experience across many industries, and a commitment to quality, confidentiality and client satisfaction.

Four commitments **you can hold us to.**

Each one is specific enough to check. If we miss one, tell us.

01

We tell you when not to hire us

If a product you can buy does most of what you need, we say so, even though it costs us the project.

02

The riskiest part gets built first

Every project has one part that decides whether it works. We build it in the first weeks, while changing direction is still cheap.

03

Our reports say what doesn't matter

A report padded with findings nobody can reach wastes your engineers' week. Ours flag which issues aren't worth your time.

04

You talk to the people doing the work

No account manager relays your messages. The engineer on your project answers your questions.

WHAT YOU CAN COUNT ON

- ✓ **Integrated expertise.** Software engineering and cyber defense in one team.
- ✓ **End to end.** From concept and build to protection and audit readiness.
- ✓ **Proven experience.** 150+ projects across many industries and regions.
- ✓ **Recognized standards.** OWASP ASVS and MASVS, CIS Benchmarks, NIST CSF 2.0.
- ✓ **You own the work.** Code, prompts and evaluation sets, written into the contract.
- ✓ **A fast, direct answer.** We reply within one working day.

One partner to **build, protect and comply.**



01 • BUILD

Software, apps and AI

Custom software, web and mobile apps, SaaS platforms and AI automation, shaped around your process and budget and designed secure from the first line of code.

Custom software

Web applications

Mobile apps

AI automation



02 • PROTECT

Defensive cybersecurity

Find and fix weak spots before they turn into incidents, harden your cloud and systems, and be ready to respond if something goes wrong.

Vulnerability management

Posture assessment

Cloud security review

Incident response



03 • COMPLY

Governance, risk and compliance

Get audit-ready for ISO 27001, SOC 2, GDPR and more, with policies and evidence your team can actually keep up.

ISO 27001

SOC 2

GDPR

Virtual CISO (vCISO)

AI, DONE SAFELY

Use AI with confidence.

Build AI. Assistants, AI agents and automation connected to your own data and tools.

Secure AI. We test AI apps for prompt injection and data leaks, and check that the guardrails hold.

Govern AI. Clear policies and readiness for ISO 42001, the EU AI Act and the NIST AI RMF.

Software and apps, **built around how you work.**

Portals, dashboards, SaaS products, internal tools and the APIs that connect them to your other systems. Our security team reviews and hardens what we build before launch.



WEB AND CUSTOM SOFTWARE

- ✓ **Websites:** corporate sites and online stores
- ✓ **Web applications:** portals and dashboards
- ✓ **Custom software** for processes no product fits
- ✓ **SaaS products** that keep each customer's data separate
- ✓ **APIs** and integration with your other systems
- ✓ **Enterprise software** built around the ERP or system of record you already run

MOBILE APPS

- ✓ **iOS** in Swift and **Android** in Kotlin
- ✓ **React Native** and **Flutter** when one codebase makes more commercial sense
- ✓ **Store submission** handled for you
- ✓ An **OWASP MASVS** security review before release
- ✓ **Maintenance and support** under a written agreement

AI that works with **your own data and tools.**

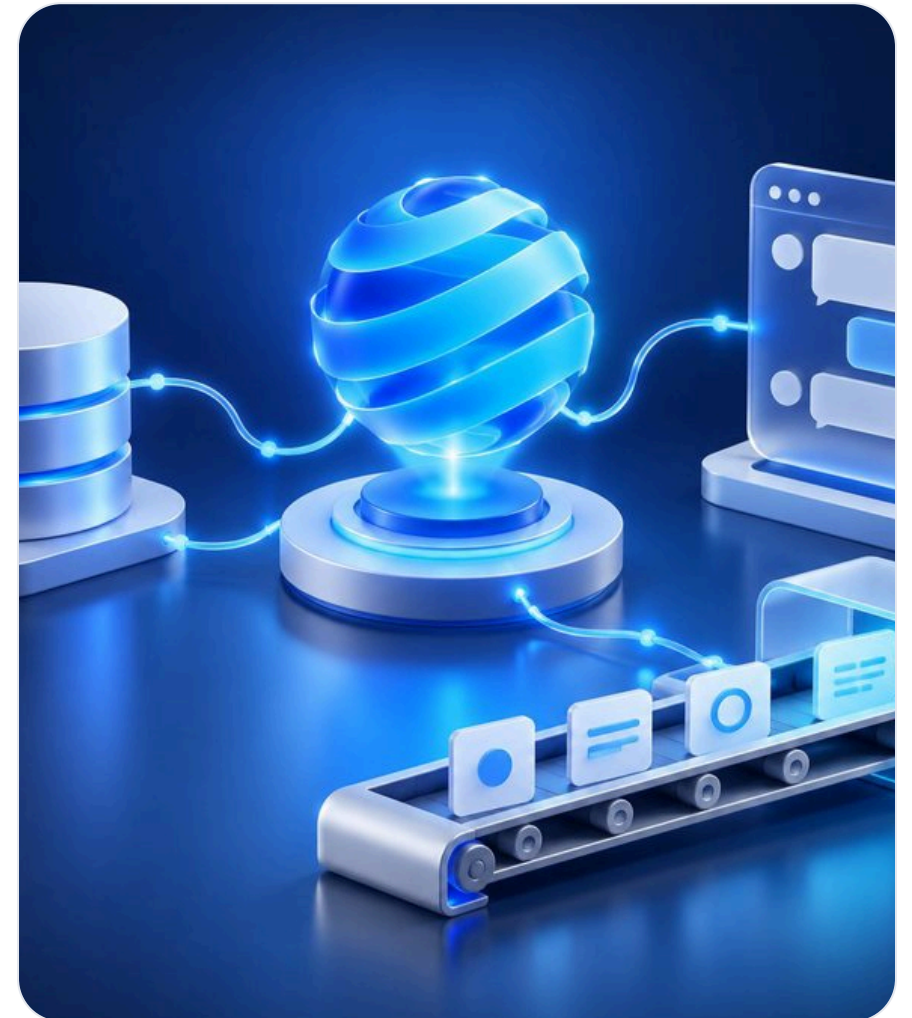
Agents, chatbots and search that answer from your own documents, and AI inside the CRM, ERP or helpdesk you already run.

WHAT WE BUILD

- ✓ AI agents that act inside your tools
- ✓ Generative AI, LLM and RAG applications
- ✓ AI chatbots that answer from your documents
- ✓ AI automation of repeated work
- ✓ AI integration into systems you already use
- ✓ LLM development, fine-tuning included

WHAT GOES INTO AN AI BUILD

- ✓ The model, the data pipeline behind it, and tests that show whether a change helped.
- ✓ Agents start read-only, so you can check every decision before granting write access.
- ✓ RAG apps give citations, and permissions are checked in the search index itself.
- ✓ You own all of it: code, prompts and evaluation sets.



MODELS AND FRAMEWORKS WE BUILD WITH

Claude

GPT

Gemini

Llama

LangGraph

LlamaIndex

pgvector

Qdrant

Find the weak spots, fix them, and be ready to respond.

The same team covers web, mobile, APIs, networks and cloud. Every finding comes with evidence and a fix, and we check your fixes.



FIND WEAKNESSES

- ✓ Continuous vulnerability assessment
- ✓ Web, mobile and API assessment
- ✓ Network configuration review
- ✓ Cloud security review
- ✓ Secure code review
- ✓ Threat modeling

FIX, HARDEN AND RESPOND

- ✓ Vulnerability management
- ✓ Posture assessment and hardening
- ✓ DevSecOps and security architecture
- ✓ Threat detection and log analysis
- ✓ Blue Team exercises
- ✓ Incident response readiness
- ✓ Security awareness training

How we work. We check your systems inside an agreed scope and confirm every finding by hand. Then we rank findings by real risk, help your team close them, and make sure an intrusion would show up in your logs.

Guardrails for AI apps and agents, **designed and tested.**

We design guardrails for AI apps and agents, then test them for prompt injection, data leakage and unsafe tool use.

SERVICES

- ✓ AI security assessment, the place to start
- ✓ LLM security testing
- ✓ Generative AI security testing
- ✓ AI guardrail design and verification

HOW WE SCOPE IT

- ✓ What an agent can call, the identity each call runs as, and the retrieval path that feeds it.
- ✓ Prompt-injection filters, personal-data redaction and tool permissions cut to each task.
- ✓ Everything that receives model output: the same output can be harmless in one place and unsafe in another.



REFERENCES WE TEST AGAINST

[OWASP Top 10 for LLM Applications](#)[MITRE ATLAS](#)[NIST AI RMF](#)

Show customers and auditors **how you protect their data.**

We run the program and prepare the evidence: gap assessment, control design, evidence collection and support through the audit. An independent auditor issues the certificate or report.



COMPLIANCE FRAMEWORKS

ISO 27001

SOC 2 Type 1 and Type 2

GDPR

India's DPDP Act

HIPAA

PCI DSS

NIST CSF 2.0

NIS2

HITRUST

AI GOVERNANCE

ISO/IEC 42001

NIST AI RMF

EU AI Act

AI risk management

AI vendor risk

RISK AND ONGOING PROGRAMS

Risk management

Vendor and third-party risk

vCISO services

Managed security and compliance

GRC as a service

Compliance as a service

Clear steps. A plan that fits your budget.

No jargon and no surprises. You always know what happens next, what it costs and who is responsible.

01

Talk

A free call about your goals, your systems and your budget. We reply within one working day.

02

Plan

A clear proposal with scope, timeline and cost, sized to your budget. For a quick number first, try the cost calculator on our website.

03

Build and secure

We deliver in short cycles with security checks built in, and report progress in plain English.

04

Support and improve

After launch we maintain, patch and improve, and keep your compliance evidence current.

150+

projects delivered so far, most of them short security engagements

3-in-1

build, security and compliance from one accountable team

Day one

security is part of the plan from the first sprint, not added at the end

Built for businesses **with data to protect.**

Every industry has its own rules, regulators and customer demands. We start from yours.



Fintech and banking

RBI or SEBI, PCI DSS and your bank customers can all ask for different evidence at once.

- ✓ Work out which rulebooks really apply
- ✓ Build and secure payment and banking apps
- ✓ Find, rank and fix vulnerabilities



Healthcare

Patient data travels through lab feeds, claims files and patient apps, and the rules follow it.

- ✓ Patient apps with audit logs
- ✓ Check each connection before real data flows
- ✓ Get ready for HIPAA and the DPDP Act



SaaS and technology

Customers' security questionnaires ask for SOC 2 or ISO 27001 before they sign.

- ✓ Evidence in place before the auditor
- ✓ Secure your product, code and cloud
- ✓ AI features your customers can trust



E-commerce and retail

How your checkout takes card payments decides how much PCI DSS work you face.

- ✓ Keep card data off your servers
- ✓ Fast, reliable stores and apps
- ✓ Customer data handled as the DPDP Act expects

WE HAVE ALSO DELIVERED FOR

Education

Hospitality and food

Real estate

Logistics and transport

Travel and mobility

Grocery and delivery

Manufacturing and trade

Recruitment

Health and fitness

Smart home

Pet care

Communications

Real projects, explained plainly.

Each case study covers the problem, what we did and two figures from the result. Client names are kept private under NDA.



AI AND AUTOMATION • HR TECH

AI recruitment platform

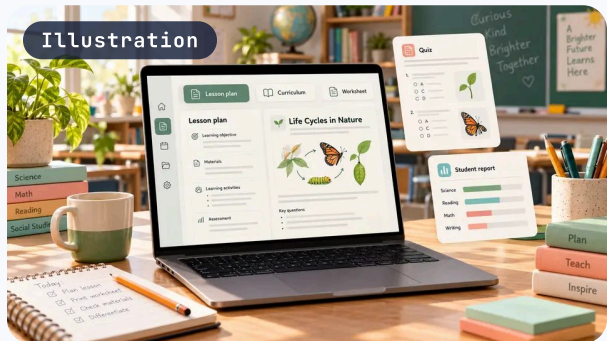
Startups lost 15+ hours per hire to CV screening, or paid an agency up to \$40,000. We built one platform that ranks candidates from three sources in a single pass.

95%

lower cost per hire than agency recruiting

<7 days

to a shortlist



AI AND AUTOMATION • EDUCATION

AI teaching platform for schools

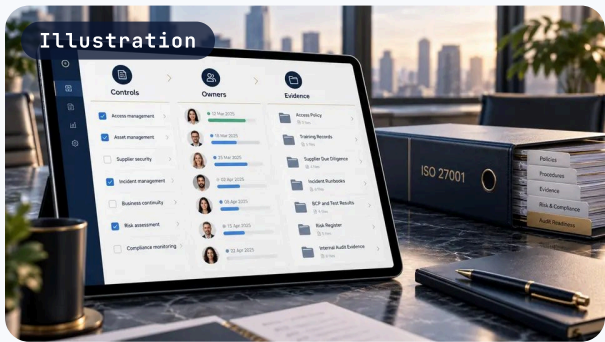
Teachers gave up evenings to lesson planning. We built curriculum-aligned lesson plans, worksheets and reports in 108 languages, with a tier for school admins.

20,000+

teacher hours saved

3.6 hrs

saved per teacher each week



SECURITY AND COMPLIANCE • SAAS

ISO 27001 certification program

A SaaS company kept losing enterprise deals because it had no certificate. We ran the gap assessment, controls and evidence as one project.

8 months

to certificate

1st

attempt audit pass



SECURITY AND COMPLIANCE • BANKING

Bank security assessment

A mid-sized bank faced a regulatory review with only automated scan results. We ran an independent assessment and a ranked plan of fixes, then verified every fix.

47

findings, every fix verified

9

of them rated critical

What each client needed, and what changed.



HEALTHCARE

Patient care management app

Appointments, prescriptions and video consultations sat in three systems. We replaced them with one Flutter app on a single backend.

15,000+
active patients

3 → 1
systems replaced by one app



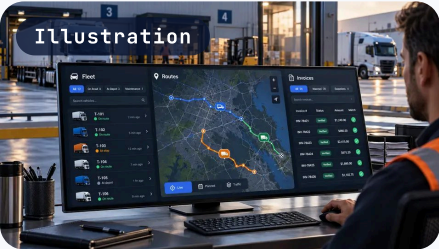
HOSPITALITY

Hotel management platform

A group of 12 hotels ran each property on its own spreadsheet. We built one system for bookings, housekeeping and occupancy, plus a guest app.

3x
direct bookings

68%
faster check-in



LOGISTICS

Logistics operations platform

Fleet logs on paper and four days of invoice matching every month. We built one platform for routes and invoices, connected to the client's ERP.

35%
lower operating cost

4 days
of manual work cut each month



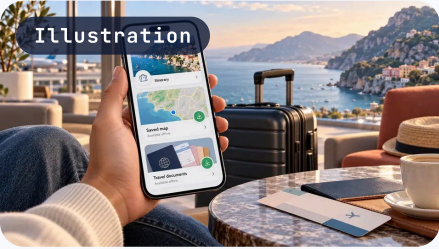
SMART HOME

Smart home monitoring dashboard

Customers were looking at device states that were already out of date. We built a Next.js dashboard over a streaming pipeline.

8,000+
connected homes

18 ms
median update latency



TRAVEL

Travel booking and itinerary app

Travelers needed their bookings in places with no signal. We built a React Native app whose itineraries, maps and documents work offline.

50,000+
monthly active users

100%
usable offline

EVERY CASE STUDY IN FULL

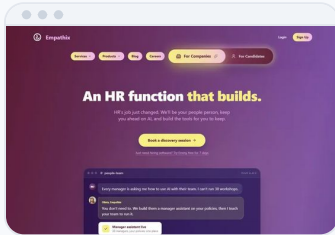
Read the hard parts, too.

Each write-up on our website covers what the client needed, what we built or checked, and the part that was difficult.

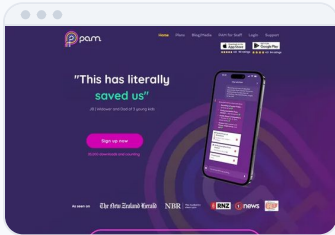
secwiztech.com/case-studies.html →

AI products from our portfolio, **live today.**

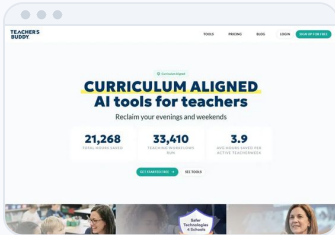
A selection of the publicly launched products, apps and sites our team has worked on. Screens captured in October 2026.



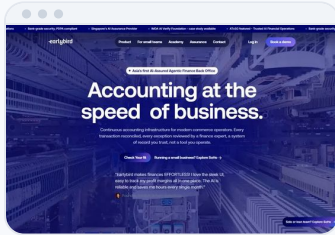
**Empathix**
AI recruitment platform that screens candidates and sources talent from several databases.
[Web](#)



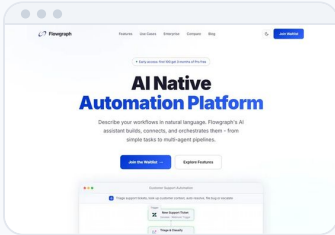
**PAM Family Manager**
NEW ZEALAND
AI family assistant that turns messages, screenshots and notes into shared calendars, tasks and reminders.
[Web](#) • [iOS](#) • [Android](#)



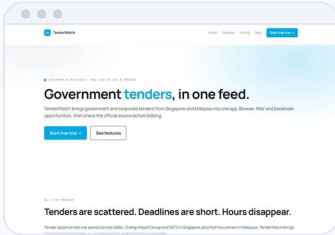
**Teacher's Buddy**
AI platform that drafts lesson plans, worksheets, assessments and reports for teachers.
[Web](#)



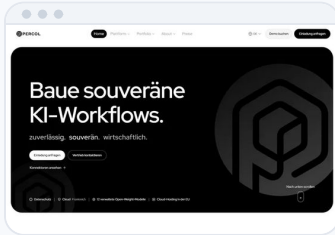
**Earlybird AI**
SINGAPORE
AI finance assistant: agentic accounting and bookkeeping for multi-channel commerce.
[Web](#) • [iOS](#) • [Android](#)



**Flowgraph**
AI-native workflow automation that builds and runs workflows from plain-language descriptions.
[Web](#)



**TenderWatch**
SINGAPORE
Gathers government tenders from Singapore and Malaysia into one feed, with alerts.
[Web](#)



**Percol**
GERMANY
AI workflow automation for enterprise processes, on European infrastructure.
[Web](#)



**mA.I Health**
NEW ZEALAND
App for storing and managing a family's health records in one place.
[Web](#) • [iOS](#) • [Android](#)



**Eloa**
GERMANY
Platform for managing AI agents across phone, email and chat.
[Web](#)

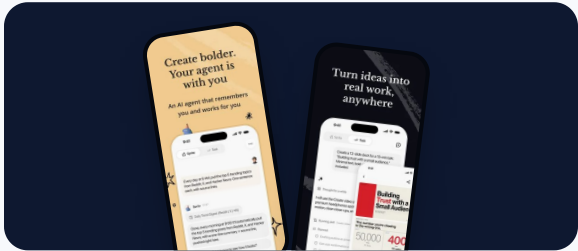
Apps in the App Store and on Google Play.

PAM, Earlybird AI and mA.I Health on the previous page are in both stores as well.



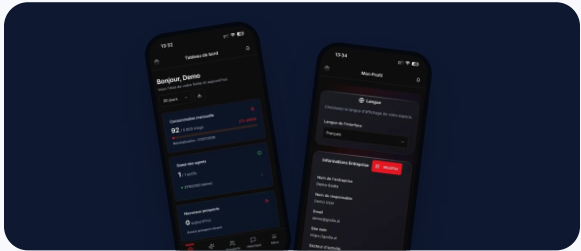
On-demand shared and private rides with professional drivers.

iOS · Android · Web



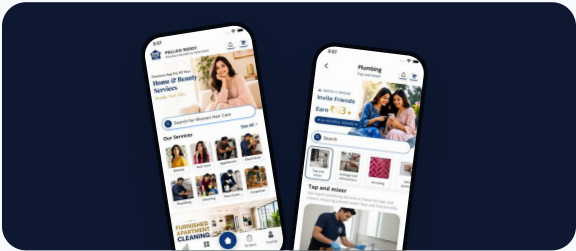
AI chat and content-creation workspace with boards and agent workflows.

iOS · Android · Web



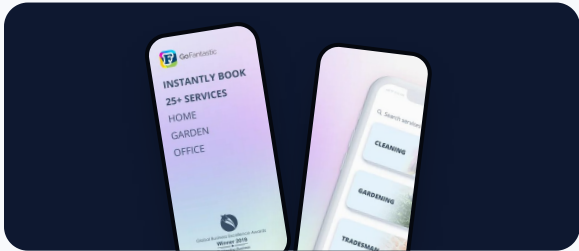
Companion app for an AI customer-conversation platform: agents, prospects and usage at a glance.

iOS · Android · Web



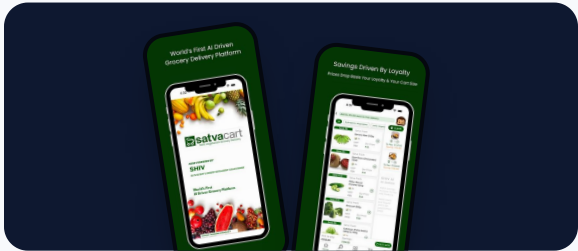
Booking home services such as cleaning, repairs and beauty treatments.

iOS · Android



Booking domestic services such as cleaning, plumbing, handyman and gardening work.

iOS · Android



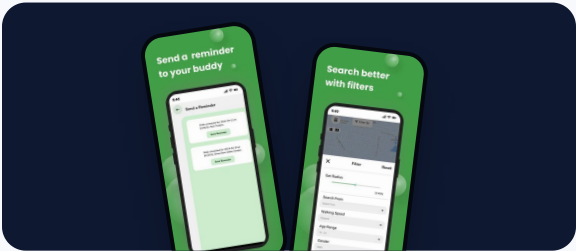
Vegetarian grocery shopping and delivery app in Gurgaon.

Android



Finding, renting and returning bikes in Niagara-on-the-Lake.

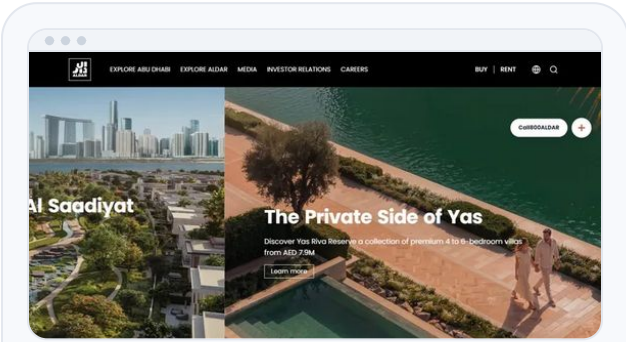
iOS



Find and match with walking buddies by location and preferences.

iOS

Web platforms and business applications.

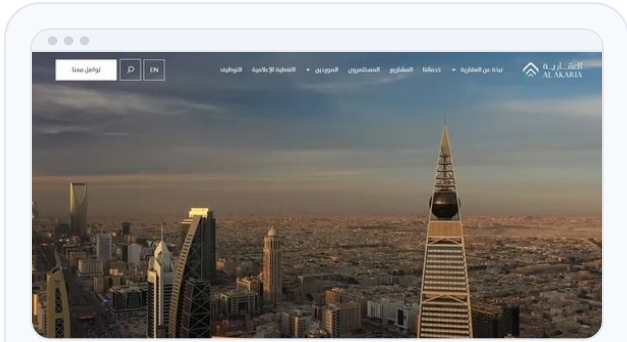




Aldar
UAE

Real estate developer and manager based in Abu Dhabi.

[Web](#)

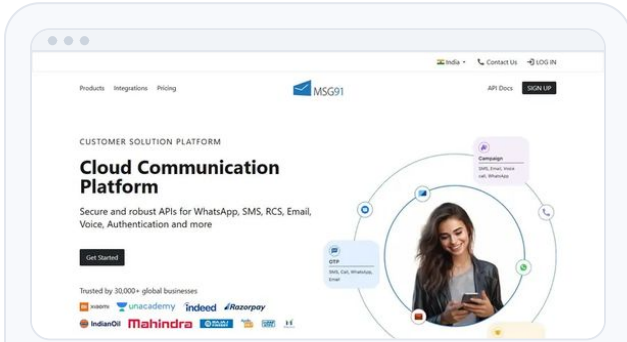




Al Akaria
SAUDI ARABIA

Real estate developer: residential, commercial and mixed-use projects.

[Web](#)

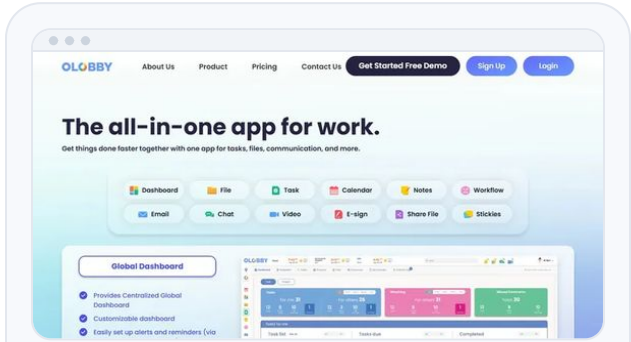




MSG91
INDIA

Cloud communication platform: SMS, email, WhatsApp, voice and OTP.

[Web](#)

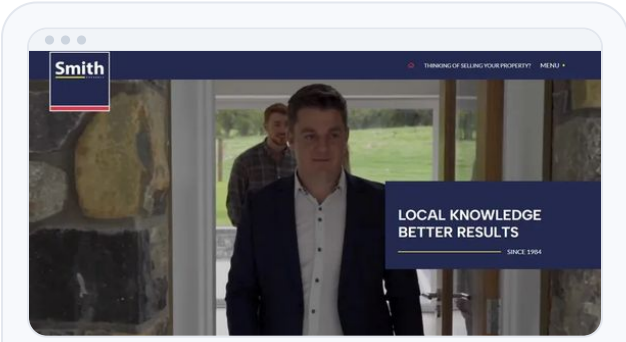




OLOBBY

All-in-one work platform: tasks, files, chat, calendar, video and e-sign.

[Web](#)





Smith Property
IRELAND

Estate agency: sales, lettings, valuations and management.

[Web](#)





Property in Sicily
ITALY

Real estate agency for residential and rural properties across Sicily.

[Web](#)

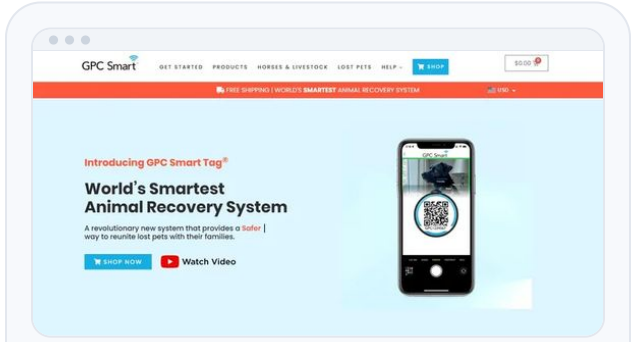




Global ID Microchip
UK

Pet microchip registration and recovery.

[Web](#)



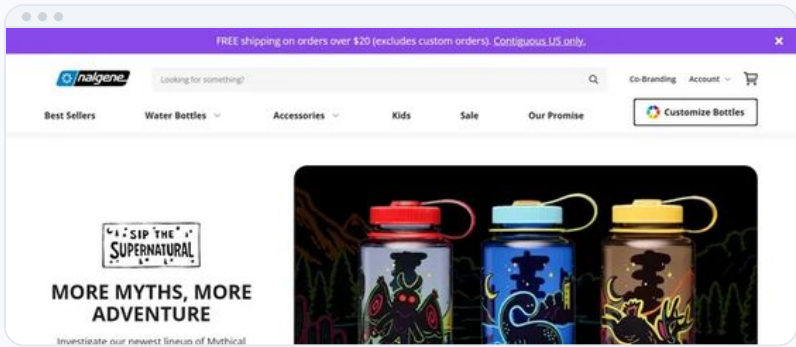


GPC Smart

Pet identification and recovery with QR and NFC tags.

[Web](#)

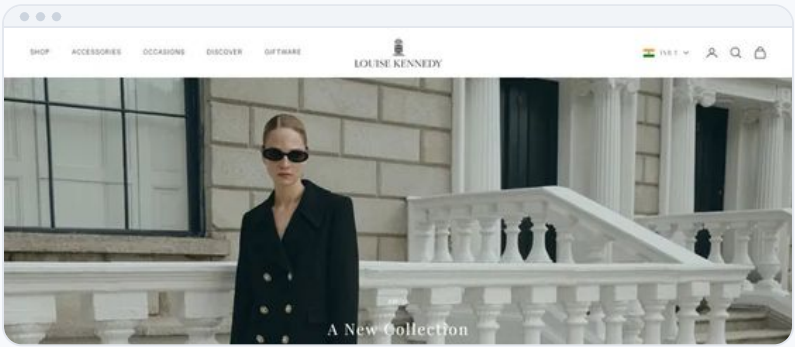
Online stores for brands and distributors.



**Nalgene**
USA

Reusable water bottles and hydration accessories.

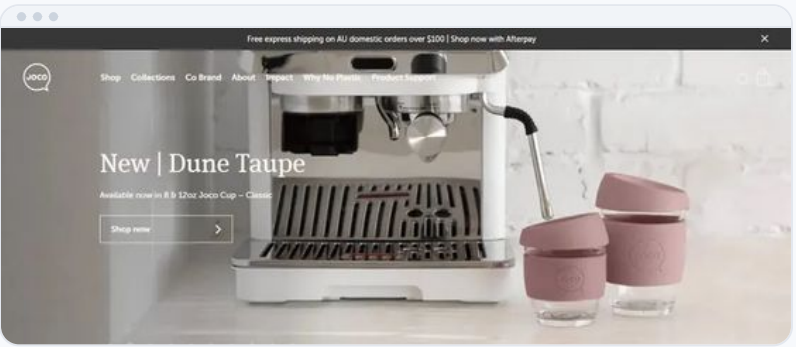
[Web](#)



**Louise Kennedy**
IRELAND

Luxury womenswear, accessories and giftware.

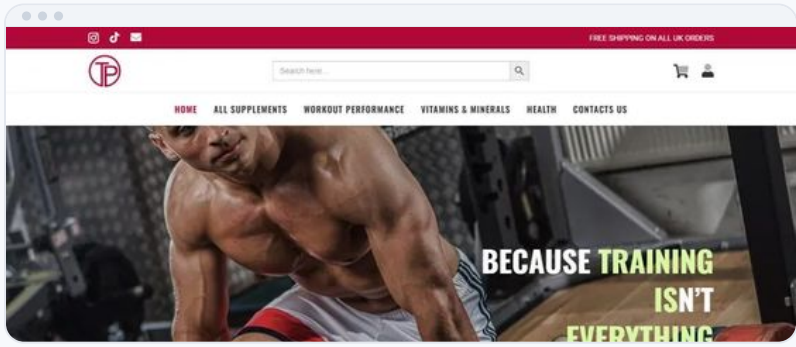
[Web](#)



**JOCO Cups**
AUSTRALIA

Reusable glass cups and bottles.

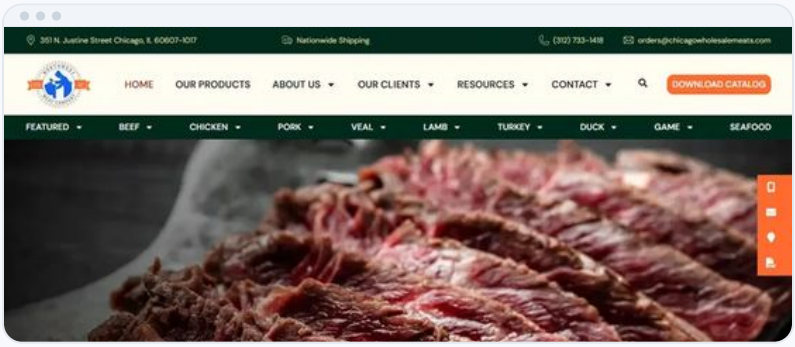
[Web](#)



**True Performance**
UK

Vitamins, minerals and workout supplements.

[Web](#)



**Northwest Meat Company**
USA

Wholesale meat distributor for restaurants and food service.

[Web](#)

WEB APPLICATIONS AND ONLINE STORES

13

across 8 countries

Retail, real estate, communications, food supply and pet care, from the United States and Ireland to the UAE, Saudi Arabia, India and Australia.

Company websites across Europe, the Gulf and Canada.



FH

FAIRHOTEL
CZECH REPUBLIC

Four-star hotel with restaurant and wellness services in Brno.

Web

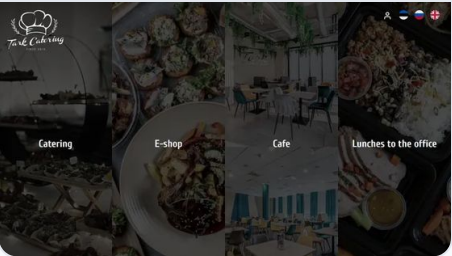




Poké Bowl
ESTONIA

Quick-service restaurant: Hawaiian-inspired poke bowls and bites.

Web





Tark Catering
ESTONIA

Catering, e-shop, café and office lunch delivery.

Web





Akban
ESTONIA

Indian restaurant serving authentic and modern cuisine.

Web

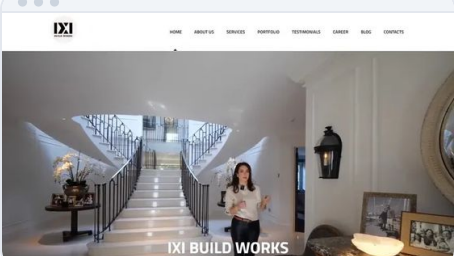


HT

Hansatrans
ESTONIA

Oversized cargo, project shipments and modular construction transport.

Web





IXI Build Works
CANADA

Carpentry and woodworking: custom furniture, restoration and installation.

Web

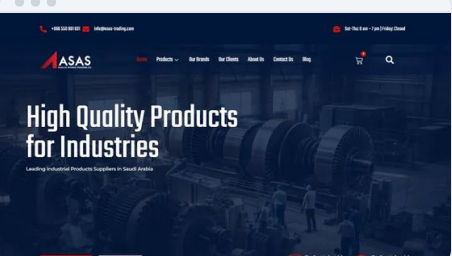


GM

Green Mining Enterprises
BAHRAIN

Manufacturer of construction, industrial, agricultural and leisure sands.

Web

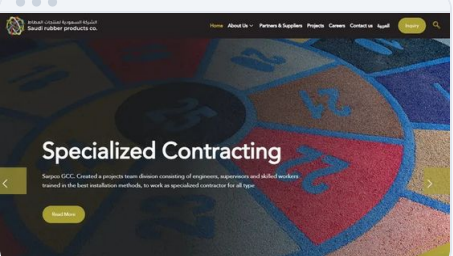


AS

Asas Al Riyadh Trading
SAUDI ARABIA

Supplier of welding equipment, cutting tools, safety gear and industrial supplies.

Web

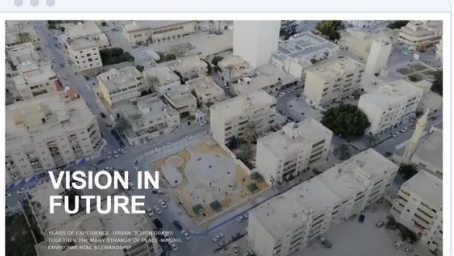




Saudi Rubber Products
SAUDI ARABIA

Waste-tire recycling and rubber products manufacturer.

Web





Alssada Co.

Construction and real estate company.

Web

The stacks we build and secure with.

FRONT END

React Next.js JavaScript
HTML and CSS Bootstrap WordPress

BACK END

Node.js Express Python Java
Supabase Firebase

MOBILE

React Native Flutter Swift
Kotlin

DATA

PostgreSQL MySQL MongoDB
pgvector Qdrant

AI

Claude GPT Gemini Llama
LangGraph LlamaIndex

SECURITY TOOLING

Semgrep Snyk Pipeline scans
Cloud posture checks



A tool flags problems. People decide what they mean.
We choose the stack that fits the job and the team that
will maintain it.

Facts you can check.

Most of these you can check without taking our word for it.



Registered company

SecWiz Technologies Pvt. Ltd. was incorporated in India in 2024 under the Companies Act. CIN U62090DL2024PTC429255, on the Ministry of Corporate Affairs portal.



Where we work

Our one office is in Delhi. We work remotely with clients across the regions we serve, and agree the hours we overlap at the start of each project.

WHAT WE WORK TO

OWASP ASVS and MASVS for applications, CIS Benchmarks for configuration, NIST CSF 2.0 for program structure, and CVSS v4.0 plus known-exploited status to set priorities. For AI work we add the OWASP LLM Top 10, MITRE ATLAS and the NIST AI RMF.



What you own

All of it: code, prompts, evaluation sets, and model weights where they exist. Ownership is written into the contract.



Confidentiality

We sign a non-disclosure agreement before anything sensitive is shared, and our published case studies name no client. Product names and screens in our portfolio belong to their owners.

STANDARDS WE HELP YOU MEET

- ISO 27001
- SOC 2
- GDPR
- HIPAA
- PCIDSS
- DPDP Act
- NIS2
- NIST CSF
- HITRUST
- ISO 42001
- EU AI Act
- NIST AI RMF

LET'S TALK

Tell us what you're building, or what you need to protect.

A free, no-obligation conversation about your goals and budget. Whether you have a detailed brief or half an idea, send it. We reply within one working day.

CALL

+91 83838 49138

Mon–Fri, 9am–7pm IST · [Chat on WhatsApp](#) →

EMAIL

info@secwiztech.com

WEBSITE

secwiztech.com

Every service in detail, our portfolio, case studies and the cost calculator

OFFICE

Building No. 11/23 Ambey Garden, Libaspur, Delhi – 110042, India

[LinkedIn](#) → [Facebook](#) → [Instagram](#) →

Where Innovation Meets Secure Digital Future



Portfolio

secwiztech.com/portfolio.html



Case studies

secwiztech.com/case-studies.html



Cost estimate

secwiztech.com/cost-calculator.html