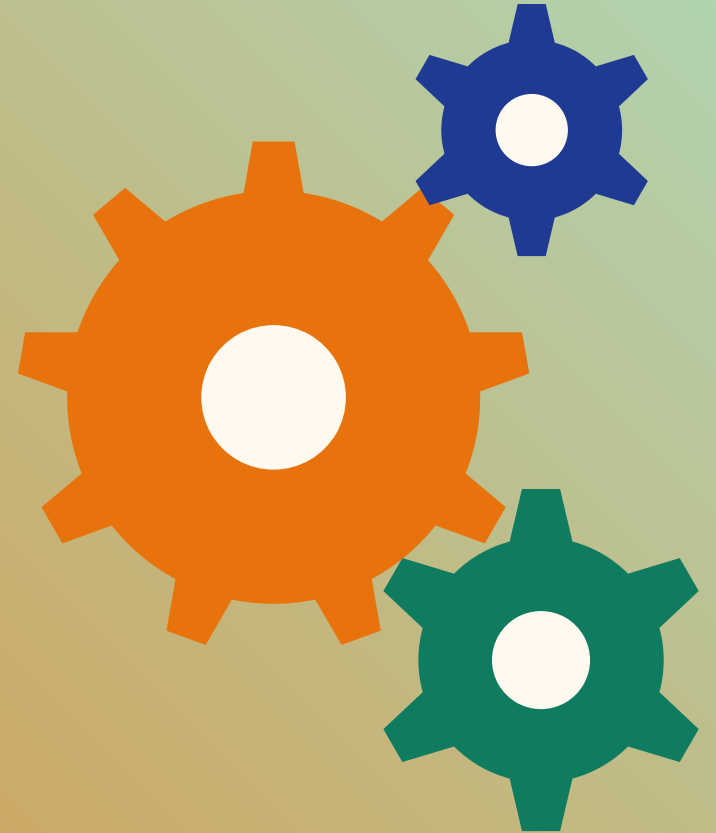


TECH COURSE

Technology Essentials Course

Every topic explained, from basics to best practice



Course map

01

Internet of Things (IoT)

02

Blockchain Explained

03

Cloud Computing 101

04

Cybersecurity Basics

05

Generative AI at Work

01

INTERNET OF THINGS (IOT)



Connected devices that sense, think and act

Module 1 · Internet of Things (IoT)

Overview

- IoT connects sensors and devices to the internet
- Data from devices drives automation and insight
- Used in homes, farms, factories and cities
- Security and power are key design challenges

KEY IDEA

Design for low power and secure updates from day one.

How it works

1 Sense

Sensors measure the world

2 Connect

Wi-Fi, BLE, LoRa or cellular

3 Analyse

Edge or cloud processing

4 Act

Alerts and automatic control

Core components

01

Devices

Sensors and actuators.

02

Connectivity

Networks and protocols.

03

Platform

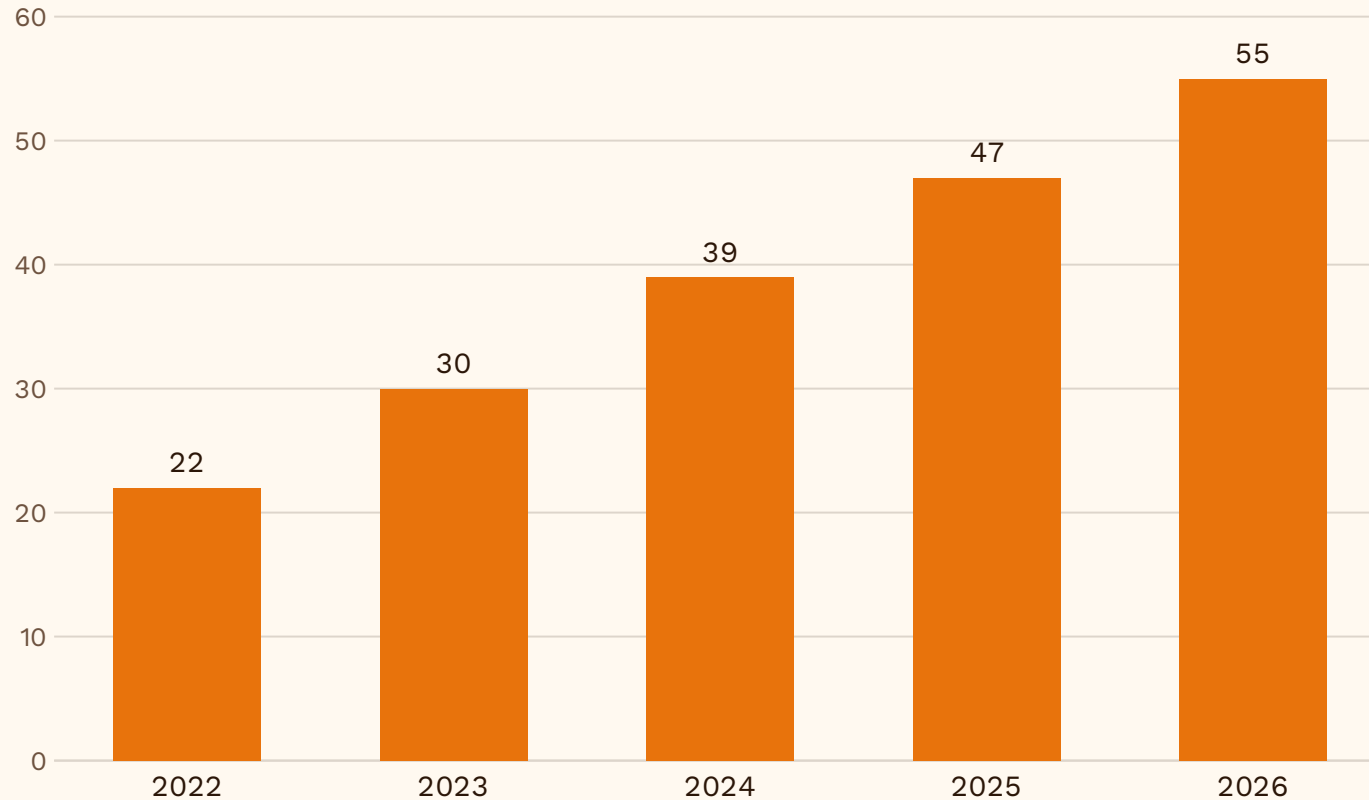
Data, dashboards and rules.

Tools and options

Layer	Popular choices	Notes
Boards	ESP32, Raspberry Pi	Cheap prototyping
Protocols	MQTT, HTTP, CoAP	Lightweight messaging
Platforms	Dashboards and rules engines	Start with open source

Generic examples; pick what fits your project.

Adoption over time



Adoption keeps rising as tools mature (sample data).

Sample data for illustration — replace with your own figures.

Use cases



Image 1

Smart agriculture

Soil and weather sensing



Image 2

Smart homes

Lights, locks and energy



Image 3

Industry

Predictive maintenance

Benefits and risks

Benefits

- Real-time visibility
- Automation saves cost
- New services possible

vs

Risks

- Security vulnerabilities
- Battery and power limits
- Interoperability gaps

Best practices

01

Secure by default

Unique credentials per device.

02

Plan updates

Over-the-air firmware.

03

Collect less

Only the data you need.

Getting started roadmap

Week 1

Learn

Core concepts and a tutorial

Week 3-4

Pilot

One real use case

Week 2

Prototype

Small proof of concept

Month 2

Scale

Standards, monitoring, training

02

BLOCKCHAIN EXPLAINED



Ledgers, blocks and real use cases beyond crypto

Module 2 • Blockchain Explained

Overview

- A blockchain is a ledger copied across many computers
- New records are grouped into blocks and linked
- Tampering is hard because every copy must agree
- Uses include supply chains, certificates and payments

KEY IDEA

**Not every problem
needs a blockchain
— a database is
often enough.**

How it works

1 Transact

A user submits a transaction

2 Validate

Nodes check it against rules

3 Block

Valid transactions form a block

4 Chain

Block is linked and shared

Core components

01

Ledger

Append-only shared record.

02

Consensus

How nodes agree on the truth.

03

Smart contracts

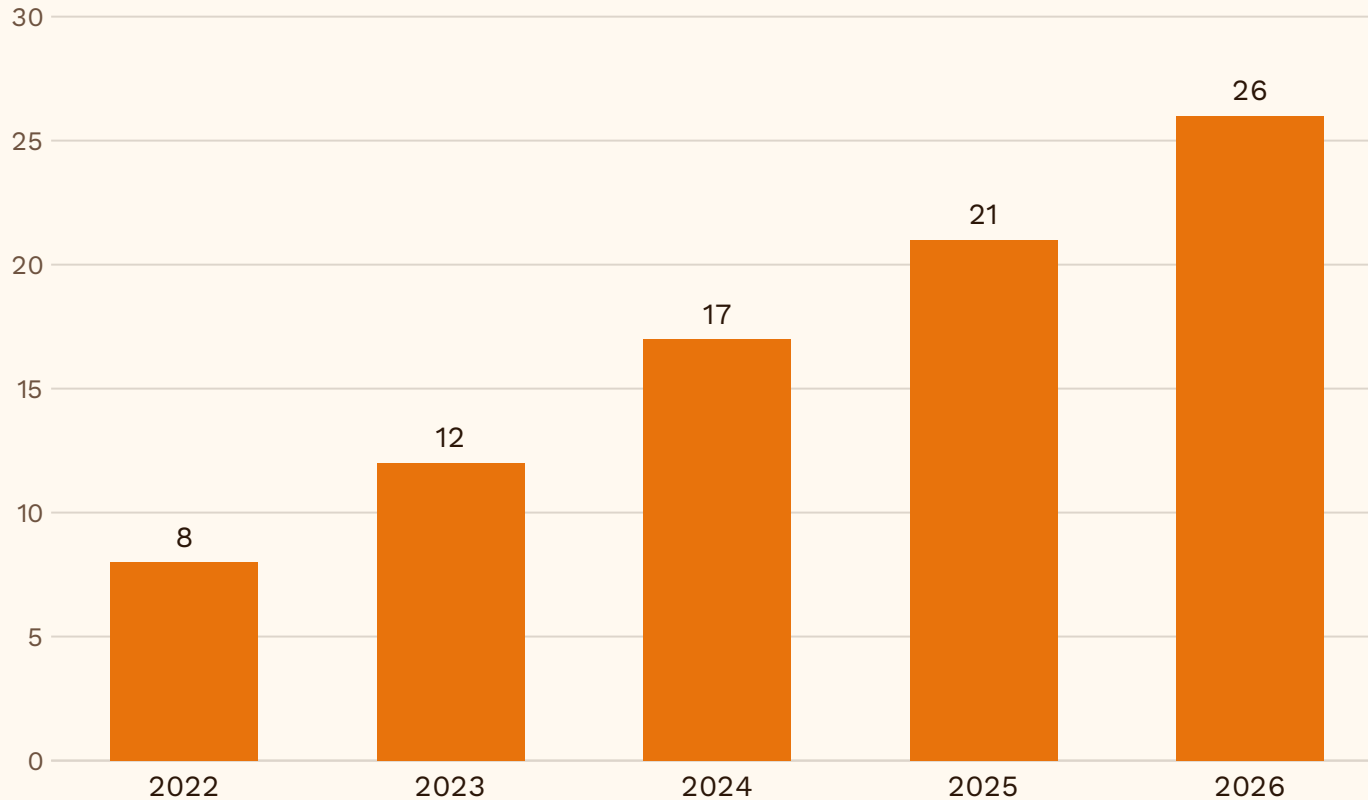
Code that runs on the chain.

Tools and options

Layer	Popular choices	Notes
Public chains	Open networks	Anyone can join
Private chains	Permissioned networks	Known participants
Wallets	Key management apps	Protect private keys

Generic examples; pick what fits your project.

Adoption over time



Adoption keeps rising as tools mature (sample data).

Sample data for illustration — replace with your own figures.

Use cases



Image 1

Certificates

Tamper-proof degrees



Image 2

Supply chain

Track goods end to end



Image 3

Land records

Transparent ownership

Benefits and risks

Benefits

- Tamper-evident records
- No single point of control
- Transparent audit trail

vs

Risks

- Energy and cost concerns
- Hard to fix mistakes
- Regulation still evolving

Best practices

01

Start small

Pilot one use case.

02

Mind privacy

Keep personal data off-chain.

03

Plan governance

Who decides upgrades?

Getting started roadmap

Week 1

Learn

Core concepts and a tutorial

Week 3-4

Pilot

One real use case

Week 2

Prototype

Small proof of concept

Month 2

Scale

Standards, monitoring, training

03

**CLOUD
COMPUTING 101**



From servers in a room to services on demand

Module 3 • Cloud Computing 101

Overview

- Cloud computing delivers servers, storage and software over the internet
- Organisations rent capacity instead of buying hardware
- Services scale up and down with demand
- It enables faster launches and global reach

KEY IDEA

Most savings come from switching off what you are not using.

How it works

1 Choose

IaaS, PaaS or SaaS

2 Deploy

Apps and data to the cloud

3 Scale

Auto-scale with demand

4 Optimise

Monitor cost and performance

Core components

01

Compute

Virtual machines and containers.

02

Storage

Object, block and file storage.

03

Networking

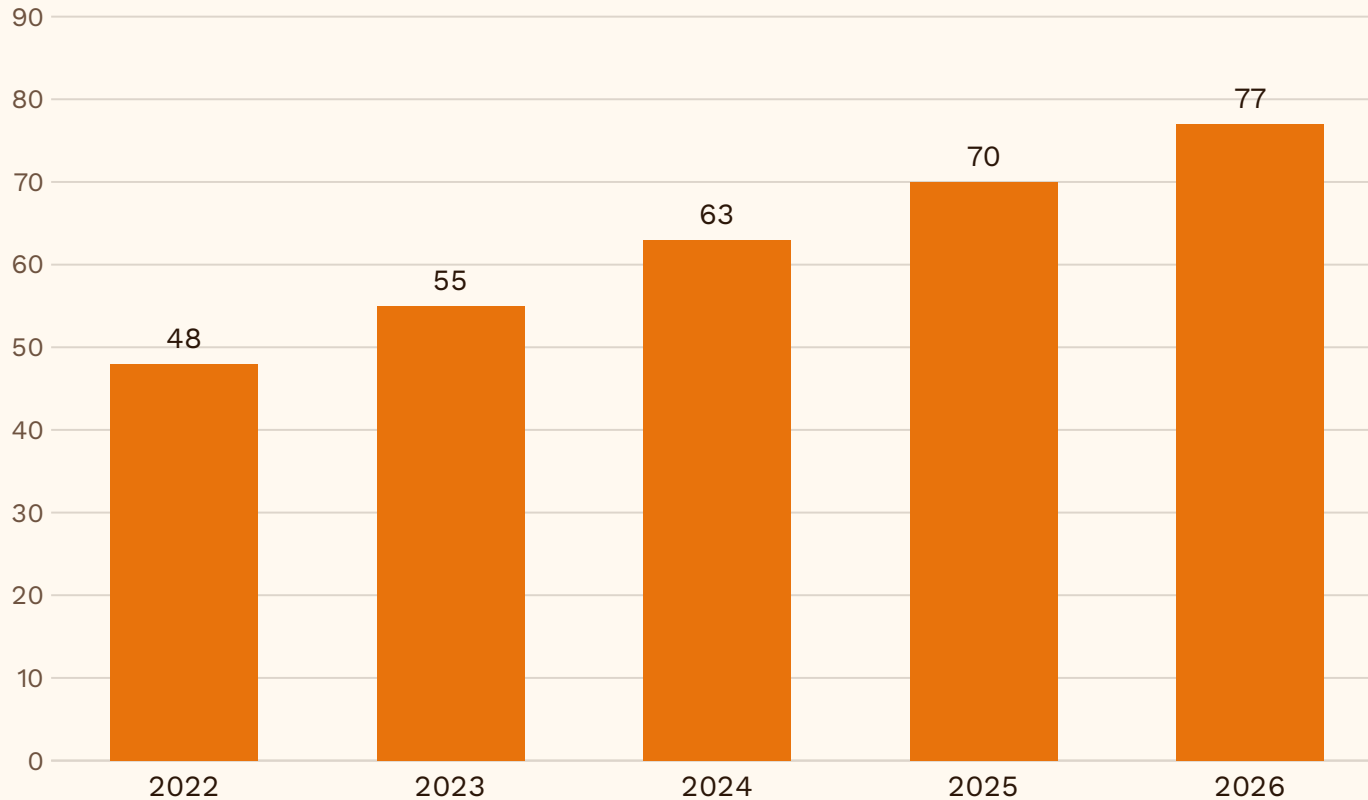
Load balancers, CDNs, VPNs.

Tools and options

Layer	Popular choices	Notes
Compute	VMs, containers, serverless	Match to workload
Data	Managed databases	Backups included
Ops	Monitoring, IaC	Automate everything

Generic examples; pick what fits your project.

Adoption over time



Adoption keeps rising as tools mature (sample data).

Sample data for illustration — replace with your own figures.

Use cases



Image 1

Websites

Hosting that scales with traffic



Image 2

Analytics

Big data on demand



Image 3

Backup

Off-site disaster recovery

Benefits and risks

Benefits

- No upfront hardware cost
- Scale in minutes
- Global availability

vs

Risks

- Costs can creep up
- Vendor lock-in
- Needs new skills

Best practices

01

Tag resources

Know who owns what.

02

Set budgets

Alerts before overspend.

03

Automate

Infrastructure as code.

Getting started roadmap

Week 1

Learn

Core concepts and a tutorial

Week 3-4

Pilot

One real use case

Week 2

Prototype

Small proof of concept

Month 2

Scale

Standards, monitoring, training

04

CYBERSECURITY BASICS



Protecting people, devices and data

Module 4 · Cybersecurity Basics

Overview

- Cyber attacks target individuals and organisations of every size
- Phishing, weak passwords and unpatched devices are the top risks
- Simple habits prevent most incidents
- Security is everyone's job, not just IT's

KEY IDEA

Enable two-factor authentication on every important account.

How it works

1 Identify

Know your assets and data

2 Protect

Passwords, updates, backups

3 Detect

Monitor for unusual activity

4 Respond

Report and recover quickly

Core components

01

People

Awareness and good habits.

02

Process

Policies and incident response.

03

Technology

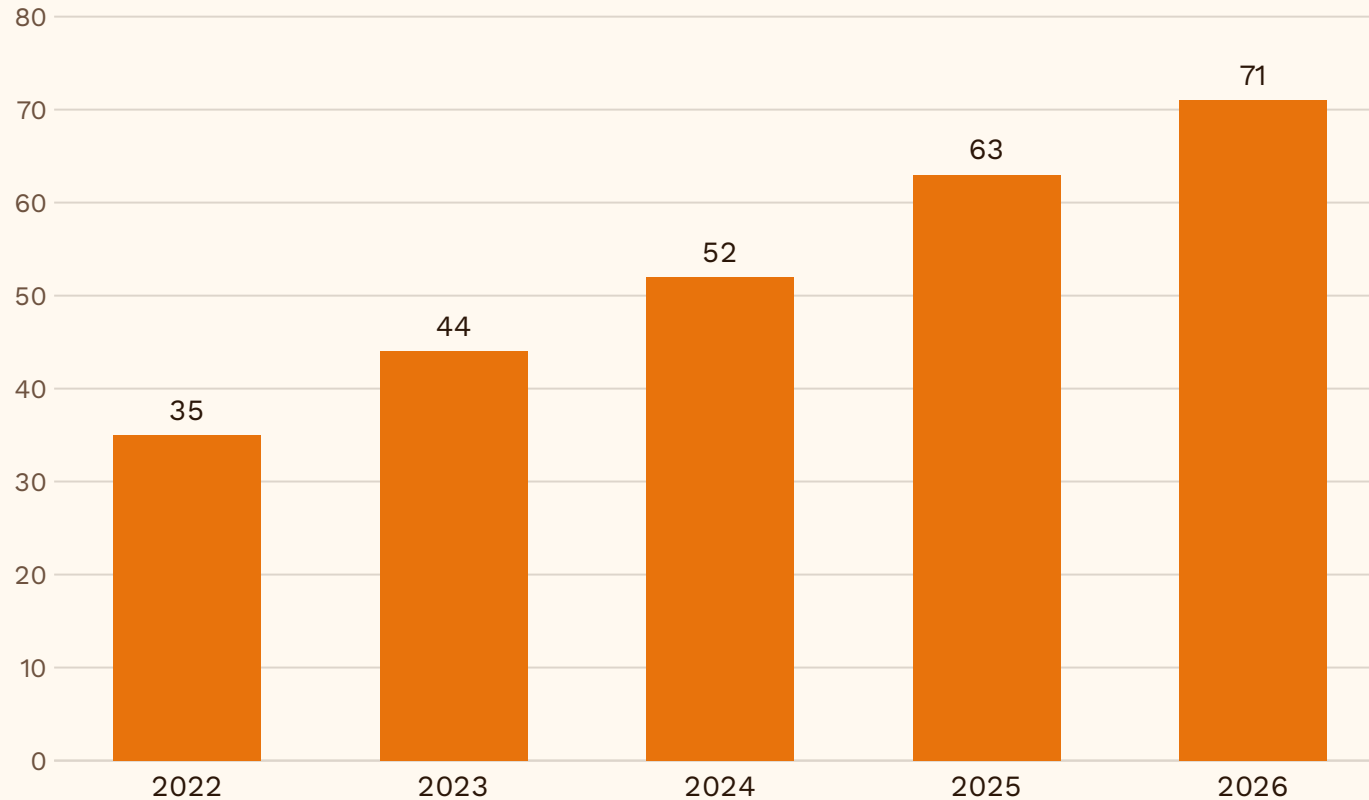
Firewalls, antivirus, encryption.

Tools and options

Layer	Popular choices	Notes
Identity	Password managers, 2FA apps	Unique password per site
Devices	Antivirus, auto-updates	Patch within days
Data	Encrypted backups	Test restores regularly

Generic examples; pick what fits your project.

Adoption over time



Adoption keeps rising as tools mature (sample data).

Sample data for illustration — replace with your own figures.

Use cases



Image 1

Phishing defence

Spot fake emails and links



Image 2

Safe remote work

VPN and secure Wi-Fi



Image 3

Data protection

Backups and encryption

Benefits and risks

Benefits

- Prevents costly incidents
- Builds customer trust
- Meets compliance needs

vs

Risks

- Needs ongoing effort
- Users find rules inconvenient
- Threats keep evolving

Best practices

01

Think before clicking

Check sender and links.

02

Update everything

Phones, laptops and apps.

03

Back up

Follow the 3-2-1 rule.

Getting started roadmap

Week 1

Learn

Core concepts and a tutorial

Week 3-4

Pilot

One real use case

Week 2

Prototype

Small proof of concept

Month 2

Scale

Standards, monitoring, training

05

GENERATIVE AI AT WORK



What it is, how it works and how to use it responsibly

Module 5 • Generative AI at Work

Overview

- Generative AI creates text, images, code and audio from prompts
- It is trained on large datasets to predict likely outputs
- Teams use it for drafting, summarising and ideation
- Quality, privacy and accuracy still need human review

KEY IDEA

Treat AI output as a first draft, not a final answer.

How it works

1 Prompt

Describe the task clearly

2 Generate

Model produces a draft

3 Review

Check facts and tone

4 Refine

Edit, iterate and finalise

Core components

01

Models

Large language and image models.

02

Data

Your documents and knowledge base.

03

Guardrails

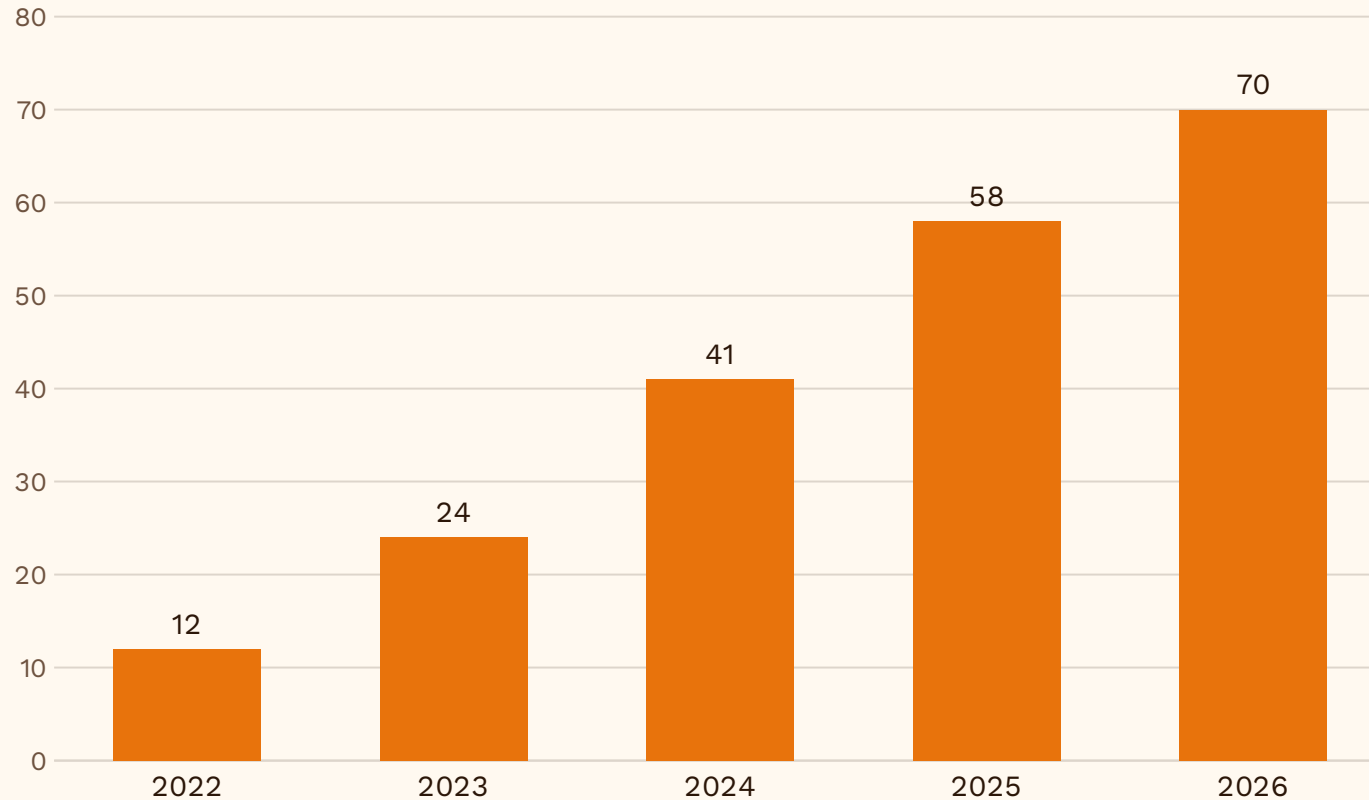
Policies, filters and review steps.

Tools and options

Layer	Popular choices	Notes
Models	Hosted APIs, open models	Compare cost and privacy
Retrieval	Vector databases	Ground answers in your data
Apps	Chat, plugins, agents	Start with one workflow

Generic examples; pick what fits your project.

Adoption over time



Adoption keeps rising as tools mature (sample data).

Sample data for illustration — replace with your own figures.

Use cases



Image 1

Customer support

Draft replies and summaries



Image 2

Marketing

Copy variations and ideas



Image 3

Engineering

Code suggestions and tests

Benefits and risks

Benefits

- Faster first drafts
- Scales knowledge work
- Helps non-experts start

vs

Risks

- Can be confidently wrong
- Privacy and IP concerns
- Over-reliance risk

Best practices

01

Be specific

Give context, examples and format.

02

Verify

Check facts before publishing.

03

Protect data

Never paste confidential data into unknown tools.

Getting started roadmap

Week 1

Learn

Core concepts and a tutorial

Week 3-4

Pilot

One real use case

Week 2

Prototype

Small proof of concept

Month 2

Scale

Standards, monitoring, training

Thank you

Questions and discussion.

Presenter Name

hello@yourdomain.in

