10 Takeaways!

SCALE AI WITHOUT LEAKING DATA?

Practical lessons
for MSPs &
IT leaders

1

Start with a workflow. Not an AI tool.

AI cannot fix a process nobody understands.
Before automating, document:

- What triggers the work
- What information is needed
- Who makes each decision
- What the final result should be

Do this next

Pick one repetitive process and map it step by step.

2

Build for the outcome, not the capability

Build for what you want to achieve, not for what the technology can do.

- Faster ticket triage
- Better client reports
- Fewer manual tasks
- Quicker root cause analysis

Do this next

Define the result before choosing the model or platform.

3

Turn tribal knowledge into documented workflows.

When one employee knows how everything works, the business has a risk.

Documented workflows can be taught to an AI agent and reused across the company.

Do this next

Ask: "What process breaks if one person leaves tomorrow?"

4

Treat an AI agent like a brand-new employee.

Give it:

- One clear role
- Only the access it needs
- Rules for what it can share
- A defined approval process
- Ongoing monitoring

Do this next

Write the agent's job description before connecting it to data.

5

Start with read.
Be careful with write.

Reading and summarizing are lower-risk.

Sending emails, editing records, or deleting files can create expensive mistakes.

Begin with: Read > Summarize > Recommend.
Add execution only after the process is proven.

Do this next

Limit AI to read-only until you trust the workflow.

6

Shadow IT has become Shadow AI.

Employees may be using:

- Personal AI accounts
- Unapproved browser tools
- Local coding agents
- AI connected to company files
- Tools IT cannot see

Do this next

Inventory which AI tools are being used, by whom, and for what.

7

An AI policy won't prevent every mistake.

Someone will paste the wrong email thread.
Someone will include credentials or customer data.
Training matters. Technical guardrails matter more.

Do this next

Define the result before choosing the model or platform.

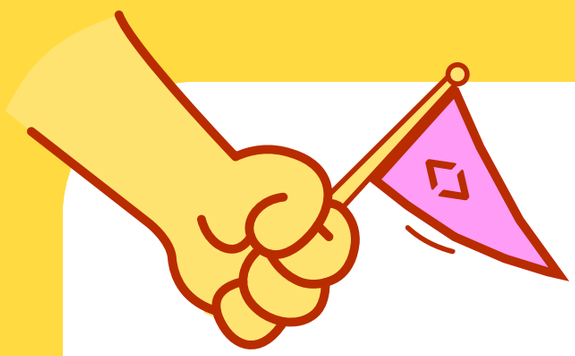
8

AI accounts are a new target for attackers.

An AI account can contain:
• Prompts and files
• Internal conversations
• Business context
• Connected systems
• Sensitive company knowledge
An attacker can query all of it in plain language.

Do this next

Protect AI accounts with MFA, monitoring, and limited integrations.



9

AI account takeovers are becoming a new target for attackers.

A provider may agree not to retain your prompts. But other features like web search or connected services can create different risks.

Do this next

Review each feature separately. One setting is not a complete plan.

10

ZDR Helps. It Is Not a Free Pass

Zero Data Retention means the AI provider processes your data without keeping it. That is a strong privacy control, but it does not cover every risk.

Web search, integrations, caching, and connected tools may behave differently.

Do this next

Check each feature separately. Anonymize sensitive data before sharing it whenever possible.

11

Keep a human in the loop.

AI can draft, summarize, classify, and recommend.
A person should approve decisions that affect:

- Customers
- Money
- Security
- Legal obligations
- Production systems

Do this next

Define where human approval is mandatory.

Security Awareness Simply Explained

wizer-training.com