Microsoft Security

# Advance AI transformation securely

Actions you can take now.

## The adoption of generative AI (Gen AI) is accelerating across industries.

Organizations are in a sprint to incorporate Gen AI into their operations to improve productivity, business processes, and increase revenue.

**95%**

of organizations are planning to or already use and/or develop Gen AI.

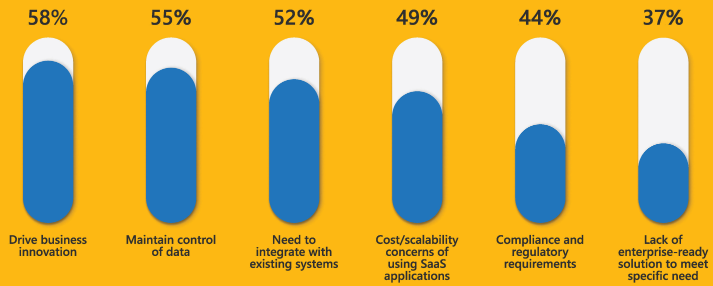
**66%**

of organizations are developing or planning to develop their own Gen AI applications

**13.9**

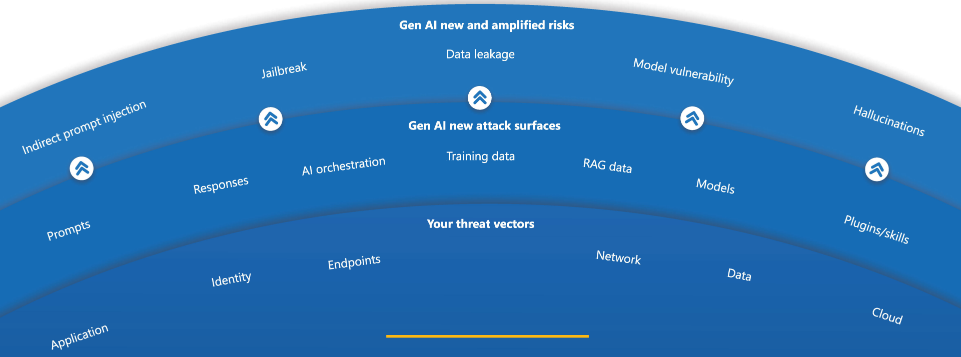
Average number of apps in development

The top reasons for developing Gen AI applications are to drive business innovation, maintain control of data, and more.



# New Gen AI risks and threats

As organizations use and develop Gen AI applications, they need to address new and amplified security risks. AI introduces new attack surfaces like prompts, responses, and models, effectively changing the risk landscape.



**Gen AI new and amplified risks**

Indirect prompt injection
Jailbreak
Data leakage
Model vulnerability
Hallucinations

**Gen AI new attack surfaces**

Prompts
Responses
AI orchestration
Training data
RAG data
Models
Plugins/skills

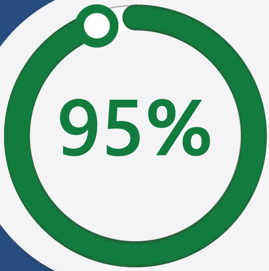
**Your threat vectors**

Application
Identity
Endpoints
Network
Data
Cloud

## The #1

## concern of companies using and developing Gen AI is data leakage

Security and risk leaders are clear they need to address data leakage, vulnerabilities, and other new and amplified threats as soon as possible.



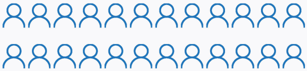
of security and risk leaders agree their company needs to have security measures in place for their AI apps—including third-party SaaS, enterprise-ready, and custom-built apps—in the next 12-24 months.

# Security and risk leaders are taking these four steps to secure and govern AI.

## Step 1

### Form a dedicated security team for AI

Dedicated security teams ensure that AI systems and sensitive data are protected, vulnerabilities are identified and mitigated, and regulatory requirements are met.



**Median team size**

**24**

80% of organizations currently have a dedicated team or plan to have to address security for Gen AI.

**80%**

**45%**

of these organizations currently have a security team for AI.

**35%**

of these organization plan to have a security team for AI.

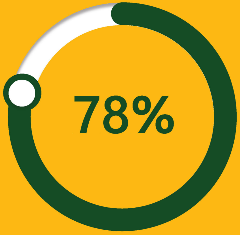
## Step 2

### Optimize resources to secure Gen AI

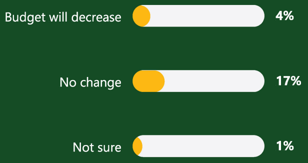
The introduction of AI applications necessitates significant changes in resource and budget allocation, especially in IT security.

### Security for AI budget expectations

Budget will increase **78%**



of security and risk leaders believe their **IT security budget** will increase with the adoption of Gen AI applications.



# Step 3

## Implement a Zero Trust strategy

Extend your Zero Trust strategy to secure and govern AI, ensuring safe and confident adoption.

### Zero Trust principles

**Verify explicitly**
Validate identities and thoroughly assess all AI applications to safeguard against unauthorized access by defining and monitoring intended and unintended activities.

**Use least privilege access**
Ensure AI can only access data required for intended uses by authorized users and AI agents operate with the least privileges to perform tasks.

**Assume breach**
To proactively design effective controls to reduce risks, operate under the assumption that AI prompts, responses, and components could harbor threats, inadvertently leak data, or possess vulnerabilities.

# Step 4

## Adopt a comprehensive security solution for AI

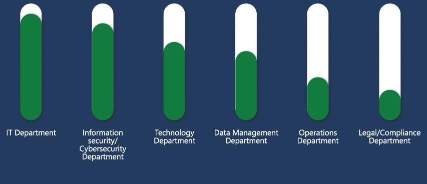
Organizations are looking for a comprehensive security solution set among new and existing solutions, with IT and Infosec being the leading departments expected to contribute their budgets towards these solutions.

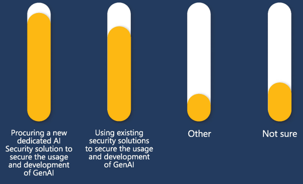
### Departments expected to contribute to Gen AI security solutions.

63% 57% 37% 23% 9% 7%

### Security plans for AI

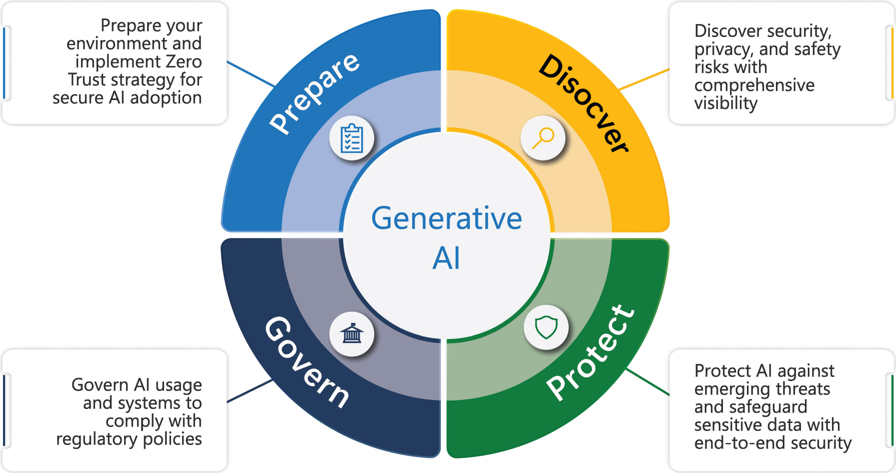
72% 64 2% 3%





## Key elements of a security solution for AI

As security and risk leaders evaluate security solutions for AI, they should consider comprehensive solutions that help companies **prepare** their environment, **discover** AI risks, **protect** AI systems, and **govern** AI to comply with regulations.



Prepare your environment and implement Zero Trust strategy for secure AI adoption

Discover security, privacy, and safety risks with comprehensive visibility

Govern AI usage and systems to comply with regulatory policies

Protect AI against emerging threats and safeguard sensitive data with end-to-end security

Microsoft Security

## Take the next step on the path toward safe and secure AI innovation.

Learn more about the actionable steps your organization can take to secure and govern AI.

Read the report.