Microsoft

Security for AI Assessment | Microsoft 365 Copilot

Detailed report

The tool provides you with a report that includes recommendations for improving your security posture when implementing AI solutions.

The report provided to you is for informational purposes only. You should not interpret the report you receive to be a commitment on the part of Microsoft; actual costs and savings may vary based on your location, purchase method, deployment, usage, and other factors. Microsoft does not make any representations or warranties, express or implied, as to the information within this website and report.

Current state of Security for AI

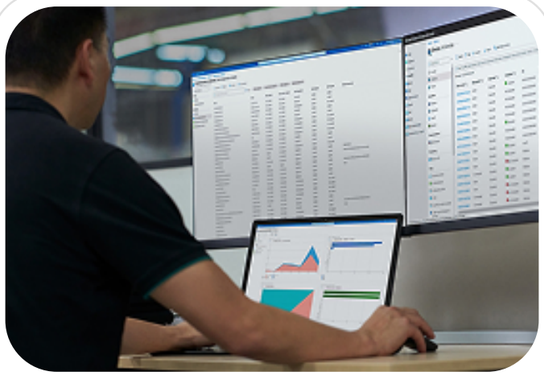
Your overall results

Initializing | **Foundational** | Optimized

Your organization has taken the initial steps to integrate security into your Generative AI adoption. You have deployed tooling to help you scale and manage, but are still primarily addressing risks and threats reactively or relying on your end users to self-manage acceptable usage.

Recommendations to Improve your AI Security

Review your Security for AI Assessment results for details and recommendations to strengthen your organization's security posture for Generative AI.



Prepare

Current state: **Initializing**

- ✓ Identify sensitive data and implement controls to enforce protections
- ✓ Identify overshared sensitive data in locations accessible by Generative AI applications
- ✓ Limit access of Generative AI applications from approved and compliant company devices

Learn More

- AI Security Essentials

Discover

Current state: **Foundational**

- ✓ Monitor and Identify the risky use of Generative AI applications
- ✓ Monitor and report on when sensitive data is being shared with Generative AI applications

Learn More

- Top 3 Challenges in Securing and Governing Data for the Era of AI

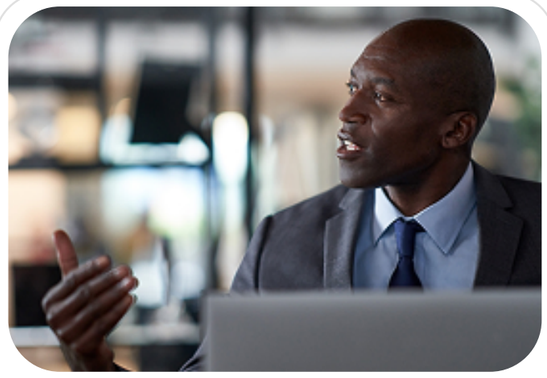
Protect

Current state: **Initializing**

- ✓ Require employees acknowledgement of acceptable usage policies before granting access to Generative AI applications
- ✓ Implement or configure an endpoint management solution to identify and respond to threats

Learn More

- Data Security as a Foundation for Secure AI



Govern

Current state: **Foundational**

- ✓ Automatically retain or delete data based on sensitivity classification
- ✓ Monitor for inappropriate or unethical use of Generative AI applications
- ✓ Track alignment to regulatory controls governing Generative AI applications and usage

Learn More

- Preparing for AI - Are you ready for the new era of work

Current state of Security for AI

AI Security dimensions

Prepare

Preparing for Generative AI focuses on implementing security protections across your digital estate. They are not unique to Generative AI and will greatly improve your security posture for your apps, data, users, and devices, inclusive of AI apps and data.

Discover

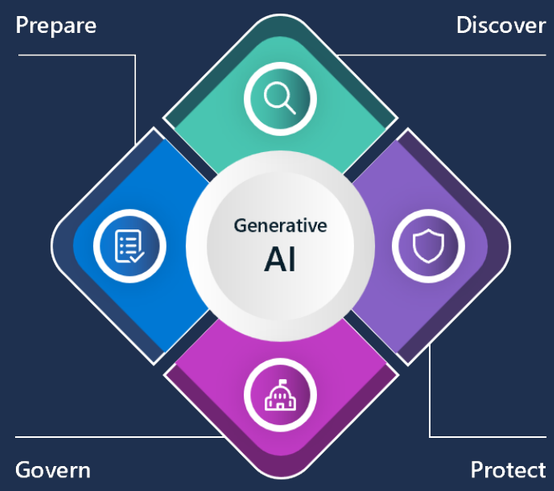
Security teams can mitigate and manage risks more effectively by proactively gaining visibility into AI usage (data, access, user, and application) and implementing corresponding controls to address vulnerabilities.

Protect

Security teams need to have the capabilities to protect AI apps and the data they interact by safeguarding existing sensitive and AI-generated data and defend against emerging AI threats.

Govern

AI regulations and standards are emerging across regions and industries. Security, and Risk and Compliance teams need to be able to assess and strengthen their compliance posture against regulations and implement controls to properly govern the usage of AI apps and data.



State definitions

Initializing

Your organization is at the early stages of your Security for AI Journey. You have limited tooling and mostly simple or manual processes to help your IT and Security teams manage Generative AI workloads.

Foundational

Your organization has taken the initial steps to integrate security into your Generative AI adoption. You have deployed tooling to help you scale and manage, but are still primarily addressing risks and threats reactively or relying on your end users to self-manage acceptable usage.

Optimized

Your organization has taken a significant step toward being prepared to secure Generative AI. Advanced tooling and processes have been implemented and operationalized to allow for automation of previously manual activities and a shift from reactive to proactive identification risks or threats.

Assessment detailed information

Review the assessment questions, including your answers and valuable links to help you learn more about how to prepare your organization into an optimized state.

Overview

1. What Generative AI solutions are currently being evaluated or deployed in your organization? Choose all that apply

YOUR ANSWER

Consumer AI Tools (e.g. Chat GPT, Microsoft Copilot, Google Gemini)

2. How far along is your organization in their Generative AI adoption?

YOUR ANSWER

We are currently researching Generative AI solutions but have not commited to any solutions.

3. Does your organization have a security team or plan to address security for Generative AI?

YOUR ANSWER

No, my organization currently has not allocated any resources to address security for Generative AI.

4. Does your organization have resources (budget, tooling, etc.) allocated to secure Generative AI Solutions?

YOUR ANSWER

We currently do not have any resources allocated to support generative AI.

Data Security and Privacy

1. How does your organization classify sensitive information when it is created or accessed by individuals or Generative AI solutions?

YOUR ANSWER

We do not have tools or processes for classifying sensitive information.

RELEVANCE

Organizations need to classify and protect their sensitive data. Information Protection solutions help customers discover, classify, and safeguard their data with sensitivity labels.

ADDITIONAL INFO

- Identify and protect sensitive business data with Zero Trust | Microsoft Learn
- How do I prepare my environment for AI security? | Microsoft Learn
- Deploy an information protection solution with Microsoft Purview | Microsoft Learn

2. How does your organization ensure Generative AI use adheres to data security policies?

YOUR ANSWER

We do not align Generative AI interactions with data security policies.

RELEVANCE

When data has sensitivity labels applied to the content, additional controls and protections can be applied.

ADDITIONAL INFO

- Learn about the Microsoft 365 Copilot location (preview) | Microsoft Learn
- Microsoft Purview data security and compliance protections for Microsoft Copilot and other generative AI apps | Microsoft Learn

Assessment detailed information

3. How does your organization assess and govern user access to sensitive information?

YOUR ANSWER

We do not have a formalized approach to governing access to sensitive information.

RELEVANCE

Knowing what is being shared and by whom helps organizations manage both inadvertent and malicious oversharing of data

ADDITIONAL INFO

- Microsoft 365 Copilot blueprint for oversharing
- Create and deploy a data loss prevention policy | Microsoft Learn
- Initiate site access reviews for Data access governance reports - SharePoint in Microsoft 365 | Microsoft Learn

4. How does your organization ensure only authorized users can access Generative AI applications?

YOUR ANSWER

We do not have any tools or processes to control how users utilize Generative AI applications.

RELEVANCE

Organizations should follow the approach of least-privilege and just-enough-access (JEA) when providing access to Generative AI workloads.

ADDITIONAL INFO

- Zero Trust identity and device access configurations - Microsoft 365 for enterprise | Microsoft Learn
- Conditional Access protections for Generative AI - Microsoft Entra ID | Microsoft Learn
- Block access for users with elevated insider risk - Microsoft Entra ID | Microsoft Learn

5. How does your organization identify risky behaviors from users or devices when working with Generative AI applications?

YOUR ANSWER

We do not have tools or processes to identify AI application misuse.

RELEVANCE

Adopting integrated and intelligent data security solutions, businesses can not only safeguard sensitive data but also empower teams to operate more efficiently, shifting focus from reactive to proactive defense.

ADDITIONAL INFO

- Insider risk management | Microsoft Learn
- Mitigating insider risks in the age of AI with Microsoft Purview Insider Risk Management | Microsoft Community Hub

6. How does your organization evaluate and control sensitive data or sites being overshared or having excessive permissions?

YOUR ANSWER

We do not identify overshared or over-permissioned sensitive data.

RELEVANCE

With the rapid adoption of Generative AI, many organizations are taking an accelerated approach to data protection-immediately prioritizing protection for the most sensitive data and then filling in gaps and building maturity over time.

ADDITIONAL INFO

- How do I prepare my environment for AI security? | Microsoft Learn
- How to use Data Security Posture Management for AI | Microsoft Learn

Assessment detailed information

7. How does your organization ensure sensitive information is only used on authorized devices or applications?

YOUR ANSWER

Our policies state that business information should only be used on approved devices, but we do not have tools to enforce this.

RELEVANCE

Managing and protecting devices is crucial for enterprise-level security. Whether implementing Zero Trust architecture, preventing ransomware, or supporting remote workers, device management is key.

ADDITIONAL INFO

- Manage devices with Intune | Microsoft Learn
- App protection policies overview - Microsoft Intune | Microsoft Learn

Vulnerabilities and Threats

1. How does your organization identify and monitor suspicious behavior by users or devices when using Generative AI applications?

YOUR ANSWER

We do not have centralized tools to identify suspicious behavior on compromised devices or identities.

RELEVANCE

Implementing a comprehensive set of detection and alert tools can help organizations use analytics to get visibility, drive threat detection, and improve defenses.

ADDITIONAL INFO

- How do I prepare my environment for AI security? | Microsoft Learn
- Implement threat protection and XDR | Microsoft Learn
- Share insider risk management data with other solutions | Microsoft Learn
- Investigate data loss alerts with Microsoft Defender XDR - Microsoft Defender XDR | Microsoft Learn

2. How does your organization govern the usage of sanctioned Generative AI applications?

YOUR ANSWER

We discourage the use of unsanctioned Generative AI applications, but do not have tools in place to control it.

RELEVANCE

As sanctioned Generative AI applications are used in the organization it is important that users understand how to safely use them, and that controls are in place to help limit misuse.

ADDITIONAL INFO

- Terms of use in Microsoft Entra - Microsoft Entra ID | Microsoft Learn
- Configure endpoint DLP settings | Microsoft Learn
- Building layered protection: New Microsoft Purview data security controls for the browser & network | Microsoft Community Hub

Assessment detailed information

Non-Compliance

1. How does your organization identify and flag risky communication and content in Generative AI interactions?

YOUR ANSWER

We do not monitor prompts and responses for risky Generative AI interactions.

RELEVANCE

Organizations should utilize tools to minimize communication risks by helping detect, capture, and act on potentially inappropriate messages, risky interactions or sharing of confidential information in your organization.

ADDITIONAL INFO

- How do I govern AI apps and data for compliance? | Microsoft Learn
- Learn about eDiscovery solutions | Microsoft Learn
- Audit logs for Copilot and AI activities | Microsoft Learn
- Configure a communication compliance policy to detect for generative AI interactions | Microsoft Learn

2. How does your organization monitor the usage of SaaS-based Generative AI applications?

YOUR ANSWER

We use tools to identify unsafe or misconfigured SaaS applications and control access based on the information being shared.

RELEVANCE

Regulatory compliance introduces extra criteria for triaging and assessing the risk of discovered AI apps.

ADDITIONAL INFO

- How do I govern AI apps and data for regulatory compliance? | Microsoft Learn
- Incident Response with XDR and Integrated SIEM | Microsoft Learn
- How do I discover AI apps and the sensitive data these use in my organization? | Microsoft Learn
- Connect apps to get visibility and control - Microsoft Defender for Cloud Apps | Microsoft Learn

3. How does your organization interpret regulatory requirements for responsible Generative AI use?

YOUR ANSWER

We have tools that maintain alignment with regulations and provide guidance on implementing controls.

RELEVANCE

AI changes the risk landscape by introducing new attack surfaces and methods of data processing, impacting regulatory compliance. These AI characteristics affect existing privacy regulations and new AI-specific regulations.

ADDITIONAL INFO

- What are new considerations for governing AI apps and data? | Microsoft Learn
- Get started with Microsoft Purview Compliance Manager | Microsoft Learn

4. How does your organization monitor data shared in Generative AI application prompts?

YOUR ANSWER

We audit Generative AI interactions and conduct manual reviews when requested.

RELEVANCE

Organizations should implement tools that help them gain visibility over how users interact with data and AI to effectively manage and mitigate insider risks.

ADDITIONAL INFO

- How do I govern AI apps and data for regulatory compliance? | Microsoft Learn
- Considerations for deploying Microsoft Purview Data Security Posture Management for AI & data security and compliance protections for Microsoft Copilot and other generative AI apps | Microsoft Learn
- Risky AI usage indicators in insider risk management | Microsoft Learn

Assessment detailed information

5. How does your organization prepare data for Generative AI while maintaining data quality and reducing risk?

YOUR ANSWER

We use tools to retain and/or delete data based on specified timeframes or revision counts.

RELEVANCE

Proactively deleting content you are no longer required to keep helps reduce the risk of data overexposure in AI tools

ADDITIONAL INFO

- How do I govern AI apps and data? | Microsoft Learn
- Learn about Microsoft Purview Data Lifecycle Management | Microsoft Learn