



# Microsoft 365 Copilot: Content Risk Management

Navigating the Risks of Generative AI

## *The Challenge*

Generative AI (GenAI) is revolutionizing content creation, but its early adoption stage requires recognizing and mitigating associated risks with proper guardrails and oversight.

Microsoft 365 Copilot, a popular GenAI tool, integrates with Microsoft Office, Windows, Edge, and Microsoft 365 Business Chat. As these applications are embedded in corporate infrastructure and access various data stores, it's crucial to monitor generated content to ensure security, compliance, and trustworthiness.



**PRECISE RISK ANALYSIS**



**UNIVERSAL COMPATIBILITY**



**UNIFORM BUSINESS LOGIC APPLICATION**



**RISK DETECTION IN COMMUNICATION CHANNELS**



**AUTOMATIC RISK LABELING**



**UTILIZES CONTENT AT REST CONTROLS**

# Additional Challenges Include:

**Over-Permissive Nature of Microsoft Graph:** Microsoft Graph is a powerful API connecting various Microsoft services and devices, but its broad default access permissions can expose sensitive data to unauthorized users or applications.

**Decoupling of Content Generation and Use:** In many organizations, content created by AI tools like Microsoft 365 Copilot is often generated by one team and used by another, leading to potential risks due to a lack of context and oversight.

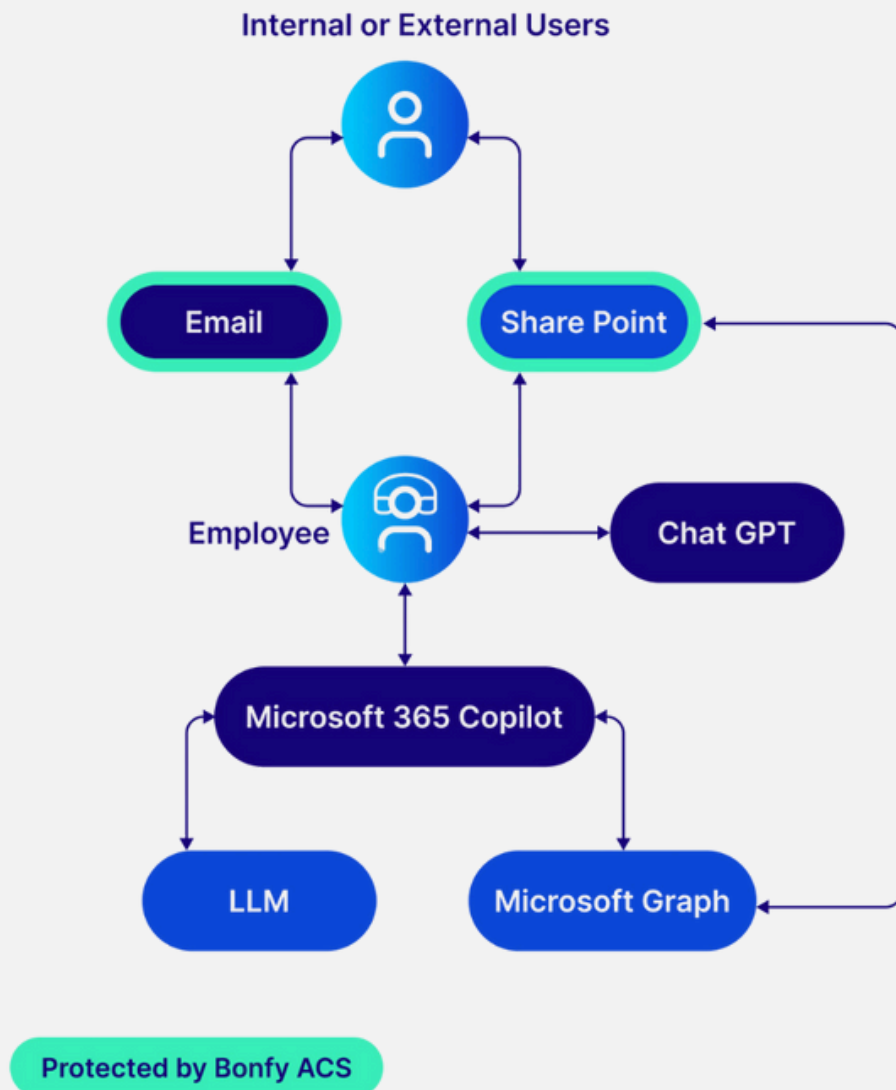
**Proliferation of Multiple Communication Channels:** Managing and securing content across diverse platforms like email, Slack, and Microsoft Teams is complex, as each channel has different security and compliance challenges.

**Complexities of a Multi-Vendor Environment:** Operating in a multi-vendor environment with different tools and services creates challenges in maintaining consistent security policies and seamless integration across all platforms.

# The Solution: Bonfy ACS™

Bonfy's adaptive content security solution, Bonfy ACS™, ensures your organization's content is always safe and compliant, instilling confidence and trust. Acting as a guardian AI, it oversees both GenAI-generated and human-generated content, detecting and preventing risks related to cybersecurity, privacy, regulatory compliance, IP protection, business liabilities, and reputational exposures.

Unlike typical AI security tools or traditional DLP solutions, Bonfy ACS™ targets content risks by analyzing the output of GenAI technologies. By applying business context and logic, it identifies risks and remediation actions across all forms of content generation and editing, including SaaS applications with GenAI (e.g., Microsoft 365 Copilot, Salesforce, Slack), internally trained models, third-party models, shadow AI, and human-generated content.



# Using Bonfy to Solve Challenges of Microsoft 365 Copilot Output

Bonfy ACS provides robust monitoring and highlights security and compliance issues in content generated using Microsoft 365 Copilot. Leveraging advanced business-context logic, it ensures your organization's content remains secure, compliant, and trustworthy across all platforms and channels.

Bonfy ACS reviews all content before dissemination, ensuring it aligns with organizational standards and policies. It alerts reviewers to non-compliant content, preventing data leakage, misinformation, and regulatory compliance risks. Bonfy ACS provides consistent protection across all tools and platforms in a multi-vendor environment.

- **Over-Permissive Nature of Microsoft Graph:** Bonfy ACS ensures that permissions are appropriately scoped and managed to mitigate these risks.
- **Decoupling of Content Generation and Use:** Bonfy ACS analyzes content in the scope of its intended use, applying business context where relevant to ensure risks are mitigated.
- **Proliferation of Multiple Communication Channels:** Bonfy ACS ensures consistent security and compliance across all communication channels, understanding the nuance of each.
- **Complexities of a Multi-Vendor Environment:** Bonfy ACS is agnostic to the channels that both create and disseminate content, reviewing the content holistically and guided by business context and logic to determine potential gaps and vulnerabilities.

By applying adaptive security principles, Bonfy ACS evolves with the changing threat landscape, offering a dynamic and responsive solution to emerging risks. Organizations can confidently leverage the power of GenAI while maintaining the highest standards of security and compliance.

# Value To Our Customers

Bonfy ACS enhances existing data security platforms like DLP, DSPM, and SSE, providing a holistic content security experience.

Benefits for Customers:

- **Accurate Risk Analysis:** Tailored risk assessments using business-context awareness.
- **Seamless Integration:** Consistent protection for both AI-generated and human-edited content.
- **Uniform Policy Enforcement:** Minimizes human error by applying security policies across all content.
- **Communication Channel Risks:** Detects and prevents risks in content in motion.
- **Alert System:** Notifies reviewers of non-compliant content for necessary changes before distribution.

# Safely Leveraging the Power of GenAI

As GenAI revolutionizes content creation, robust oversight and security are crucial. Bonfy ACS ensures customer communications generated by tools like Microsoft 365 Copilot are secure, compliant, and trustworthy.

Seamlessly integrating with existing systems and using advanced business-context logic, Bonfy ACS dynamically addresses emerging risks. Embrace Generative AI confidently, knowing Bonfy is guarding your content every step of the way.

## Contact Us

For inquiries or additional information, please contact us at [info@bonfy.ai](mailto:info@bonfy.ai).

bonfy.ai



[/bonfy-ai](#)



[@bonfy.bsky.social](#)