Copilot Adoption

Forcepoint DSPM: Empowering secure and responsible Microsoft Copilot Adoption in your enterprise

Forcepoint

Brochure

This brochure introduces Forcepoint DSPM powered by Getvisibility, designed to seamlessly integrate with Microsoft Copilot within your organization. Our comprehensive set of dashboards and widgets empowers you to leverage the power of Copilot while mitigating security risks and ensuring responsible AI adoption.

Unleashing Copilot's Potential with Confidence

Microsoft Copilot offers a revolutionary AI-powered coding assistant, boosting developer productivity. Forcepoint equips you to harness this potential securely by providing:

- → **Enhanced Security:** Proactive threat detection and data protection for a secure Copilot environment.
- → **Improved Compliance:** Ensure adherence to data privacy regulations and internal security policies.
- → **Responsible AI Development:** Foster responsible Copilot usage by understanding code generation and data interactions.
- → **Actionable Insights:** Gain valuable data to optimize Copilot workflows and improve developer experience.

A Comprehensive Overview: Forcepoint DSPM Secures Copilot

Forcepoint delivers a robust solution categorized into three key areas:

Continuous Data Discovery and Monitoring:

- → **Data Discovery and Classification:** Forcepoint continuously scans and classifies all data Copilot interacts with, including code, comments and API calls. Identify sensitive data types (e.g., PII, credentials) for enhanced protection.
- → **Contextual Code Analysis:** Analyze data generated by Copilot, understanding its functionality and potential security implications based on the surrounding workflow.
- → **API Call Monitoring:** Monitor and analyze API calls made through Copilot, ensuring they adhere to security best practices and data access controls.

Risk Management and Threat Detection:

- → **Vulnerability Detection:** Continuously scan Copilot-generated content for sensitive data leakage.
- → **Real-time Threat Detection and Response:** Forcepoint's AI engine continuously monitors for anomalous behavior and suspicious code generation, enabling real-time threat detection and response.
- → **Least Privilege Monitoring:** Ensure developers only have access to the data and functionalities of Copilot required for their specific tasks, minimizing the attack surface.

Responsible AI Development and User Behavior Insights:

- → **Bias Detection in Code Generation:** Identify potential biases within code suggested by Copilot, promoting fair and ethical AI development practices.
- → **Developer Activity Monitoring:** Gain insights into developer usage patterns within Copilot, identifying potential misuse or risky behaviors.
- → **Compliance Reporting and Audit Trails:** Generate comprehensive reports demonstrating adherence to data security regulations and internal policies.

Leverage Forcepoint to

- › **Strengthen your organization's security posture by proactively mitigating Copilot-related risks.**
- › **Foster a culture of responsible AI development by promoting secure and ethical coding practices.**
- › **Gain valuable intelligence to optimize Copilot workflows and maximize developer productivity.**
- › **Simplify compliance with data security regulations and internal security policies.**

Ready to unlock the full potential of Microsoft Copilot with a secure and responsible approach?

Contact **Forcepoint** today to learn more about how we can secure data in Copilot and how we can help your organization harness the power of AI for a more secure and productive development environment.

Forcepoint DSPM: Widget Use Cases for Business Copilot Users

This outlines 12 use cases for Forcepoint DSPM widgets, showcasing how they enhance security and responsible use of Microsoft Copilot for any business user.

Data Discovery and Classification (Uncovering Sensitive Information):

Use Case

→ A marketing team member uses Copilot to draft an email campaign. Forcepoint identifies and classifies personal data (PII) like email addresses within the Copilot suggestions. This alerts the user to ensure they have consent to use the data and adhere to relevant privacy regulations.

Document Sharing Monitoring (Securing Information Sharing):

Use Case

→ A customer service representative uses Copilot to draft a response containing confidential customer information. Forcepoint monitors document sharing permissions, ensuring the recipient has the necessary access level before the document is sent.

Contextual Analysis (Understanding Copilot Suggestions):

Use Case

→ A sales representative utilizes Copilot for writing a complex proposal. Forcepoint analyzes the generated text, identifying legal disclaimers or warranty information suggested by Copilot. This prompts the user to review the suggestions for accuracy and ensure alignment with company policies.

Phishing Detection (Identifying Malicious Content):

Use Case

→ A user receives an email seemingly written by a colleague, suggesting edits to a document via Copilot. Forcepoint analyzes the email content and identifies suspicious language or link redirection attempts. This alerts the user to potential phishing and prevents them from falling victim to a cyberattack.

Real-time Threat Detection and Response (Proactive Security):

Use Case

→ A user unknowingly installs a malicious browser extension that interacts with Copilot. Forcepoint's AI detects anomalous behavior and suspicious text generation patterns triggered by the extension. An alert is issued, allowing the user and IT department to investigate and remove the extension immediately.

Bias Detection in Suggestions (Ensuring Fairness):

Use Case

→ A recruiter utilizes Copilot to write job descriptions. Forcepoint identifies potential bias within the suggested language that might favor or disfavor candidates based on irrelevant factors. This allows the recruiter to adjust the job description and ensure a fair opportunity for all applicants.

Least Privilege Monitoring (Minimizing Data Exposure):

Use Case

→ A new team member utilizes Copilot for various tasks within different departments. Forcepoint monitors access controls, ensuring the user only has access to the specific Copilot functionalities required for their assigned role. This minimizes the risk of unauthorized access to sensitive information.

User Activity Monitoring (Identifying Risky Behavior):

Use Case

→ Forcepoint monitors user activity logs, identifying a user who frequently uses Copilot to generate text containing potentially offensive or discriminatory language. This allows for targeted training or further investigation if necessary.

Data Leakage Detection (Preventing Sensitive Information Leaks):

Use Case

→ A user utilizes Copilot to write a report containing internal financial data. Forcepoint identifies suspicious text snippets attempting to leak the data through external links or file-sharing platforms. This enables the organization to take immediate action and prevent a data breach.

Integration with Existing Security Tools (Streamlined Workflow):

Use Case

→ Forcepoint seamlessly integrates with existing Security Information and Event Management (SIEM) systems, consolidating security alerts and logs related to Copilot activity within a single platform. This streamlines the security workflow and allows for centralized threat analysis.

Compliance Reporting (Demonstrating Adherence):

Use Case

→ During a compliance audit, Forcepoint provides comprehensive reports on Copilot usage, access controls and detected threats. This allows the organization to demonstrate adherence to data privacy regulations and internal security policies.

User Education and Security Awareness Training (Empowering Users):

Use Case

→ Forcepoint insights are leveraged to create targeted security awareness training for Copilot users. These training sessions educate users on responsible Copilot usage, data security best practices and how to identify potential risks within Copilot suggestions.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-DSPM-MS-Copilot-Brochure-US-EN] 28May2024