



How to secure MSFT Copilot:

The Ultimate Guide to Data Governance Controls for Microsoft Copilot

How to Secure MSFT Copilot:

The Ultimate Guide to Data Governance Controls for Microsoft Copilot

How to Secure MSFT Copilot:

The Ultimate Guide to Data Governance Controls for Microsoft Copilot

In the rapidly evolving landscape of artificial intelligence, organizations are eagerly exploring the potential of Microsoft Copilot to transform their operations. However, this journey into the AI realm comes with its share of challenges, particularly in the domains of data security, compliance, privacy, and governance.

As security leaders, it's paramount to understand that successful Copilot adoption is not just about leveraging advanced technology; it's about doing so safely and responsibly.

Microsoft Copilot: Understanding the Risks

The early stages of Copilot adoption have highlighted significant concerns around data governance and security. The essence of these concerns lies in the importance of having a well-organized and secure data estate before embarking on the AI journey.

In order to adopt Microsoft Copilot security, you need to be able to know the data it's being trained on, control access to the data that's sensitive, and put controls in place around data that shouldn't be available for Microsoft Copilot (or any external actor) to access.

The urgency of this requirement has been underscored by numerous incidents of data leaks and breaches stemming from ungoverned use of training data.

A notable example includes Microsoft researchers inadvertently leaking 38TB of confidential information to their GitHub page -- which included passwords, credentials, private messages, and more.

To manage the overhead and risks of adopting Microsoft Copilot, organizations need a solution to address:

- **Data Inventory:** It's critical to know your data - what's sensitive, regulated, critical; what data is fit for consumption by LLMs and external parties, and what data is confidential
- **Data Governance:** Proper labeling and tagging of data are crucial to prevent unauthorized access and ensure compliance.
- **Access Control:** Overexposed data and overprivileged users present significant risks, especially in the context of AI-driven tools like Copilot.
- **Data Minimization:** Duplicate, similar, and redundant data represent unnecessary risk - delete, move, and lock down data to reduce storage costs and the attack surface.

Microsoft Copilot: How it Works

Microsoft Copilot's functionality hinges on its ability to ingest data from the extensive realms of Office 365 (or M365, depending on how up you are on Microsoft's official latest parlance). Without proper data classification, labeling, and tagging of the data that Microsoft Copilot trains on, it can inadvertently become a source of significant risk.

Incorrect access control, inefficient classification, and mislabeling can lead to unauthorized access to sensitive information, putting an entire organization at risk.

To adopt copilot securely, organizations need to implement best practices and evaluate their capabilities to:

- Conduct a comprehensive assessment of existing data estate within Office 365 - including OneDrive, Sharepoint, Outlook Online, and Teams
- Identify, map, and flag any sensitive, critical, regulated, or confidential information across their data environment
- Establish clear policies and procedures for data labeling, tagging, and access control, aligned with organizational security requirements.
- Remediate potential risks, out of policy violations, and minimize unnecessary data
- Leverage automation capabilities for efficient data management.
- Regularly monitor and audit data access and usage to identify any potential security gaps or compliance issues.

Adopt Microsoft Copilot Safely with BigID

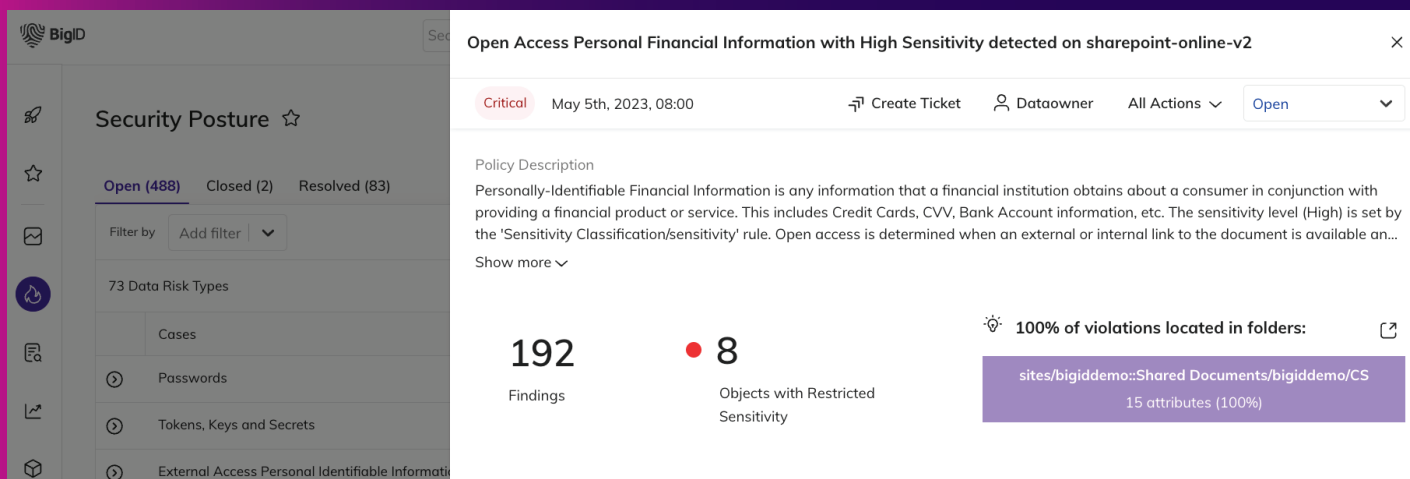
BigID's unique capabilities enable organizations of all sizes to adopt Microsoft Copilot safely, swiftly, and without additional overhead. With BigID, organizations can easily classify, tag, flag, and label data within their M365 environment - including OneDrive, SharePoint, SharePoint Online, Outlook Online, and Teams - laying the foundation for identifying data that is safe for Copilot use.

This process not only mitigates the risk of unauthorized access but also paves the way for more informed and secure AI engagements. Automated policies further enhance this security framework by flagging unsafe data: enabling companies to take necessary remedial actions, such as deletion, moving sensitive data, or marking for investigation - all within BigID.

By identifying overexposed data and overprivileged users within Office 365, BigID provides an additional layer of security. This ensures that Copilot access is limited to datasets that have been thoroughly vetted and deemed safe, thereby safeguarding sensitive information from potential misuse.

With BigID, organizations gain:

- **Enhanced Data Visibility:** Automatically inventory your data estate, find dark data, and gain insights into data assets across Office 365 (and beyond), to facilitate better decision-making.
- **Proactive Risk Mitigation:** Identify and address security vulnerabilities before they escalate, improve your data security posture, and streamline incident response
- **Compliance Acceleration:** Ensure adherence to regulatory requirements through automated data policies, robust data governance controls, and remediation and retention workflows
- **Streamlined Operations:** Automate repetitive tasks related to data classification, access control, and data minimization - freeing up resources for strategic initiatives.

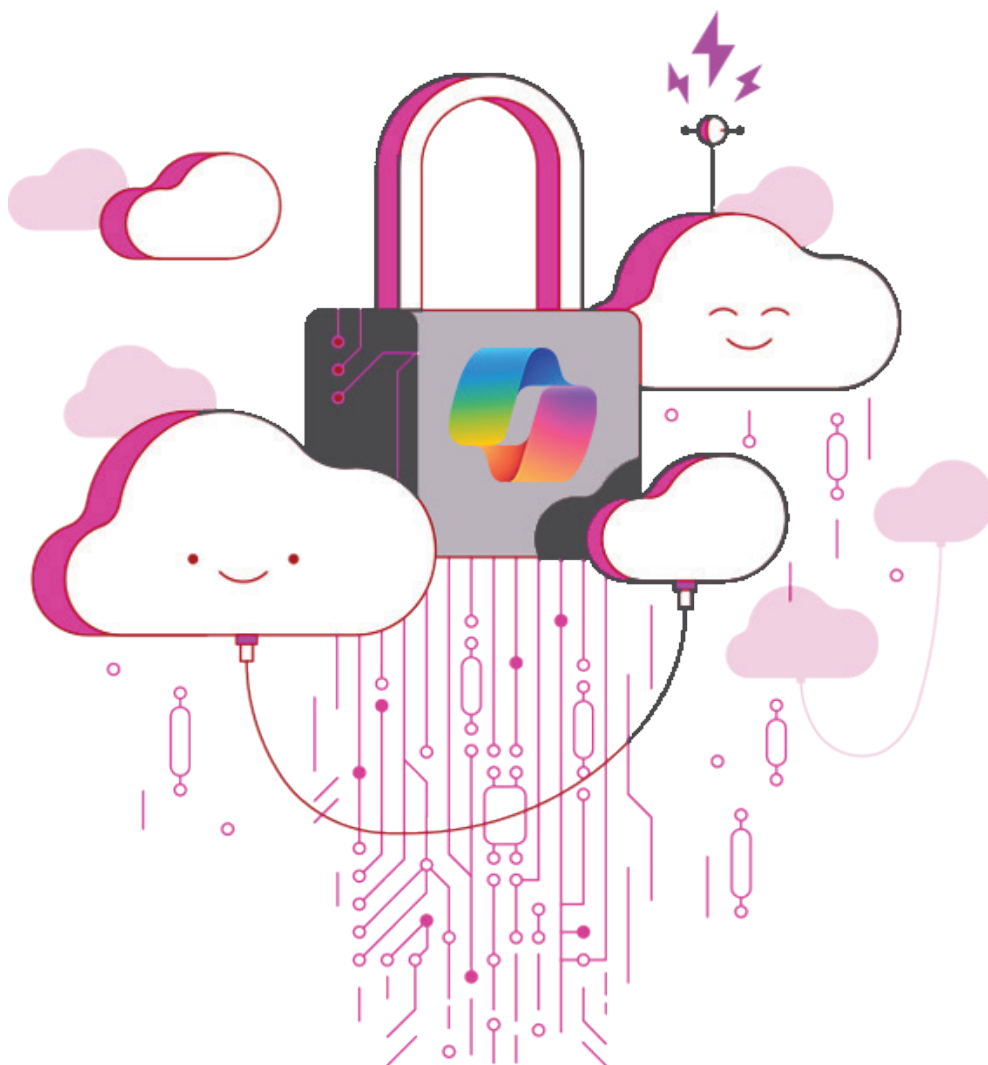


Charting a Safe Course for Microsoft Copilot

For security leaders navigating the intricacies of AI adoption, the path forward involves a strategic blend of technology and vigilance. BigID offers the tools and insights necessary to ensure that Microsoft Copilot adoption is not only successful but also secure. By prioritizing data governance and security, organizations can harness the full potential of Copilot while maintaining the integrity of their data estate.

The adoption of AI technologies like Microsoft Copilots represents a significant leap forward for organizations. However, this advancement must be approached with a keen eye on data security and governance. With BigID, security leaders have a robust ally in their quest to navigate the new frontier of AI, ensuring a safe and successful journey into the future of innovation.

Get a 1:1 demo with BigID's AI security experts and learn how to secure Microsoft Copilot today.



About BigID

BigID enables security, compliance, privacy, & governance for all data, everywhere. BigID is enterprise-ready and built to scale: enabling a data-centric approach to comprehensive cloud data security & DSPM, accelerating compliance, automating privacy, and streamlining governance. Customers deploy BigID to proactively discover, manage, protect, and get more value from their regulated, sensitive, and personal data across their data landscape.

BigID has been recognized for innovation as a 2019 World Economic Forum Technology Pioneer; named to the Forbes Cloud 100; the Inc 5000 for 3 consecutive years; the Deloitte 500 for 3 consecutive years; Market Leader in Data Security Posture Management (DSPM); Leader in Privacy Management in the Forrester Wave; and an RSA Innovation Sandbox winner.

Find out more at <https://bigid.com>.

Know Your Data, Control Your Data.

Data Security • Compliance • Privacy • Governance

Reduce risk, accelerate time to insight, and get data visibility and control across all your data - everywhere.

“Tools like BigID are the future.

Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.



Ryan O'Leary
Future of Trust: Battling Data Discovery Confusion