WHITEPAPER

Laying the Foundation for AI: Why IAM and Zero Trust Principles Are Critical to Securing Copilot

RKON®

Introduction

The security concerns surrounding AI in the enterprise aren't exactly new—they're just a lot harder to ignore now. As organizations embrace Microsoft Copilot to enhance productivity, securing its access to sensitive data is critical. Copilot's deep integration with Microsoft 365 and use of tools like Microsoft Graph and the Semantic Index create new identity-based risks. Strong Identity and Access Management (IAM) and Zero Trust principles such as least privilege, continuous verification, and contextual access are essential to prevent unauthorized data exposure and ensure Copilot operates securely within the enterprise.

Potential Security Risks

- **Unauthorized Data Exposure:** Copilot can surface sensitive content from across Microsoft 365 via tools like Graph API and the Semantic Index. Without strict identity-based access controls, users may unintentionally gain access to documents, emails, or chats they shouldn't see.
- **Privilege Escalation and Lateral Movement:** If roles and permissions are not tightly managed, Copilot may act on behalf of users with excessive access, increasing the risk of internal misuse or compromise by threat actors leveraging Copilot's integrations to move laterally across systems.

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

Attack Scenarios

- **Compromised Identity Leveraging Copilot Access:** An attacker who gains control of a user's account can use Copilot to quickly search, summarize, and extract sensitive business data across emails, files, and collaboration tools accelerating data exfiltration without needing to manually navigate systems.
- **Tricking Copilot Through Malicious Content:** Attackers can hide harmful prompts inside shared documents or messages. If Copilot reads and responds to these inputs, it might generate misleading answers, expose sensitive data, or influence users with false or manipulated information.

To prepare for a secure Copilot rollout, Microsoft emphasizes strong IAM practices like least privilege access, role-based controls, and continuous authentication. These measures help prevent attackers from exploiting Copilot's broad data access if an identity is compromised.

Microsoft also advises improving content governance to guard against malicious prompts embedded in shared documents. By applying Zero Trust principles and using tools like Purview and Defender, organizations can reduce the risk of manipulated outputs and accidental data exposure through Copilot.

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

Practical First Steps to Copilot Implementation

To avoid real-world risks like data leaks from compromised accounts or Copilot surfacing something it shouldn't, Microsoft urges organizations to get their house in order before turning it on. Two of the most practical and impactful steps include:

- **Audit and Limit Data Access:** Don't let Copilot become a supercharged search engine for everything. Take time to clean up who has access to what, and make sure users can only see what they are supposed to. Least privilege isn't just best practice, it's a safety net.
- **Classify, Protect, and Manage the Semantic Index:** If you haven't labeled or protected your sensitive data, now's the time. Since Copilot draws from indexed content, using tools like Microsoft Purview to classify sensitive information—and controlling what's included in the Semantic Index—is essential to prevent unintentional exposure of confidential data. Review and restrict which SharePoint sites, Teams, and file repositories are part of the index to keep access aligned with your security policies.

RKON

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

Deploying Microsoft Copilot is more than just flipping a switch—it requires ensuring your environment is prepared for a tool that can access and surface large volumes of organizational data. Without the right guardrails in place, Copilot can unintentionally expose sensitive content or be misused if an identity is compromised. Solid IAM practices and Zero Trust foundations should start from day one.

Realistically, the first steps are about tightening up your access controls and cleaning up old permissions. If users can see too much, Copilot will too. Similarly, labeling and protecting sensitive information with tools like Microsoft Purview ensures the AI only interacts with data that's been properly classified, keeping it out of the wrong hands and maintaining compliance.

Ultimately, secure Copilot implementation comes down to preparation. Review who has access to what, protect your most important data, and educate users on how the tool works. With those basics in place, organizations can unlock the benefits of AI-powered productivity without opening the door to new security risks.

Ultimately, secure Copilot implementation comes down to preparation.

RKON

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

IAM TIPS & PITFALLS

REMOVE UNNECESSARY ACCESS ACROSS THE BOARD

IMPLEMENT REGULAR ACCESS REVIEWS

Identity & Access Management

Regarding access, what else can technology teams do without unindexing everything? There are a couple other solutions:

1. **Remove Unnecessary Access Across the Board:** If unindexing everything isn't realistic, the next best move is to reduce what users can see in the first place. Review group memberships, shared mailboxes, and legacy permissions especially on SharePoint and Teams. This is important because if content is indexed, Copilot can't surface it to the wrong people.
2. **Implement Regular Access Reviews:** Make access certification a routing process. Set up periodic reviews to validate who still needs access to what and involve business owners to confirm relevance. This helps keep the semantic index exposure in check.

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

Recommendations for Labeling

Apply Encrypted Sensitivity Labels to Protect High-Risk Data: Use Microsoft Purview (if available) to apply encrypted sensitivity labels to your most sensitive data such as financials, legal documents, or executive communications. Encryption ensures that even if Copilot surfaces metadata or file references, the actual content remains protected unless the user (and Copilot acting on their behalf) has the proper rights. This adds a critical layer of control for limiting exposure through indexed content.

Use Encryption to Limit Copy and Extract Rights When Appropriate: As a protective strategy, configure certain encrypted labels to exclude copy and extract rights. This effectively prevents Copilot from summarizing or presenting sensitive content in its responses. This approach helps enforce guardrails around business-critical data while still allowing general Copilot use elsewhere. Use this selectively for data that must never leave its original context.

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

Importance of MFA and Zero Trust

As organizations adopt Microsoft Copilot, securing access to the vast data it can reach becomes essential. Strong IAM practices, anchored by Multi-Factor Authentication (MFA) and Zero Trust, help to ensure that only the right people can use Copilot to interact with the right information.Without these controls, a single compromised account could lead to broad and unintended data exposure.

- MFA adds an extra layer of security by requiring users to verify their identity beyond just a password, helping prevent attackers from exploiting stolen credentials to access Copilot and its connected data sources.
- Zero Trust ensures Copilot only accesses what a user is explicitly authorized to see, based on continuous verification, least privilege, and contextual access controls.

These measures help prevent overexposure of data and reduce the risk of misuse, even if a user’s account is compromised.

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

Why Zero Trust Matters for AI-Driven Tools Like Copilot

Zero Trust is a modern security framework built on the principle of “never trust, always verify”. Instead of assuming users of devices are safe just because they are inside the network, Zero Trust requires continuous validation of identity, device health, location, and behavior before granting access. It also enforces least privilege access, ensuring users, and tools like Copilot, only have access to the specific data and resources they need.

For AI-driven platforms like Microsoft Copilot, Zero Trust helps control the scope of what the AI tool can access and share. By combining granular access controls, real-time policy enforcement, and strong identity verification, organizations can reduce the risk of data leakage or misuse, even if an identity is compromised. Zero Trust doesn’t just protect against external threats; it is a critical safeguard against over-permissioned users and AI overreach.

RKON

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

Conclusion

As AI tools like Microsoft Copilot become deeply integrated into daily business operations, securing their use is no longer optional, it's a strategic imperative. Copilot has the ability to access, summarize, and surface vast amounts of organizational data, which makes it both a powerful productivity tool and a potential security risk. Without strong Identity and Access Management controls and a Zero Trust foundation, organizations risk exposing sensitive data, violating compliance requirements, or enabling misuse through compromised or over-permissioned accounts.

To safely harness the benefits of Copilot, organizations must go beyond technical controls and focus on building a sustainable governance framework. This includes understanding what data Copilot can access, setting clear usage policies, aligning with existing data protection strategies, and engaging both IT and business stakeholders. There are two actions companies should take now:

1. **Establish clear governance for Copilot and AI use across the organization:** Define ownership, policies, and controls for how data is accessed, labeled, and protected in AI interactions.
2. **Conduct an assessment to identify and prioritize critical IAM and data protection gaps:** Focus on access rights, sensitivity labeling, Semantic Index exposure, and Zero Trust alignment to guide phased improvements.

RKON

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661

The Value of an IT & Cybersecurity Partner

For over 25 years, RKON's human brilliance has driven our technology solutions, guiding customers to a fortified IT environment. At RKON, we do that through a security-first approach that meets our customers where they are in their digital journey. Security is seamlessly integrated into every aspect of our work, ensuring peace of mind and proactive protection for your organization. Where others see challenge, we see opportunity.

RKON's trusted advisors deliver strategic guidance, advanced technical knowledge and realistic assessments to give your organization the competitive advantage it requires in today's environment of rapidly evolving technologies. Here at RKON, we understand that our client's success starts with our organizational cohesion.

Are you looking for a proactive approach to fortifying your digital environment? Get rid of the unknown and control, secure, and monitor your business for a better peace of mind. Talk to a cybersecurity expert today.

ABOUT RKON

Founded in 1998 in Chicago, RKON has grown to become one of the nation's leading IT advisory practices. Our comprehensive understanding of execution strategies, technology, business processes, operations analytics, risk and compliance, and planning and integration supports hundreds of organizations.

Recognizing that no two companies have the same IT challenges, RKON takes a truly customized approach. We serve as trusted advisors to our customers, providing strategic guidance, technical resources, and honest assessments to address competitive challenges and meet long-term goals.

CONTACT US

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661