WCRG WORLD COMET RESEARCH GROUP

World Conference on Modern Engineering, AI, and Innovation
WCMEAI25-Conference Proceeding | IJETMR
Doi: 10.67228/30715636/WCMEAI-2025P109
PP. 138-150

Original Article

Microsoft 365 Premium: Integrating Copilot AI with Advanced Security Features

Rajarshi Krishna Muppaneni

Senior Programmer at Broadminds Inc, USA.

ABSTRACT

Microsoft 365 Premium integrates Copilot AI with a sophisticated, cloud-based security ecosystem to enable companies to smartly work and remain secure in a digitally complex environment. As enterprises face the challenge of increased cyber threats, a broader attack surface, and the need to securely manage hybrid workforces, the platform provides an integrated solution that combines smart productivity tools with security measures of the highest level. First, this article uncovers the problem environment that includes phishing, identity compromise, data leakage, and device vulnerabilities, and then shows how Microsoft 365 Premium AI-supported design addresses these problems using automated insights, policy-driven controls, and real-time threat detection. By integrating Copilot AI into routine operations with Word, Excel, Outlook, Teams, and SharePoint, companies get the benefit of a context-aware assistant that not only speeds up the creation of content and improves decision-making but also decreases the manual security work. Theoretically, the paper describes the way Microsoft's Zero Trust principles, threat analytics, conditional access, and unified endpoint management work together with Copilot's generative intelligence to form a layered, preemptive security model. The paper also points out that the platform constantly strengthens its defenses through learning from worldwide telemetry and provides non-intrusive personalized security recommendations to the user. The primary result indicators are that the overall operational efficiency will be improved, the number of security incidents will be lowered, the threat response will be accelerated and the compliance posture will become more resilient, i.e., all these benefits will be there at the same time, as employees will be empowered with an easy-to-use AI companion that is able to adapt to their working style. These features make Microsoft 365 Premium not just a productivity tool but an intelligent security-first ecosystem committed to customer data protection, collaboration facilitation, and AI-augmented work confidence-raising.

KEYWORDS

Microsoft 365 Premium, Security, Copilot AI, Zero Trust, Threat Protection, Cloud Security, AI Automation, Data Governance, M365 E5, Compliance, Enterprise Security, Generative AI.

WCRG
Global Research
ISSN: 3071-5636
PP: 138-150.

1. INTRODUCTION

1.1. Challenges

Organizations are rapidly transitioning to cloud services, and Microsoft 365 has in large part become a platform of collaboration, communication, and productivity. Besides, this fast-paced cloud adoption has increased the threat surface to a large extent, especially with identity being the new security perimeter. To put it differently, attackers use more and more credential theft, social engineering, and token-based exploitation in order to have unauthorized access to systems, thereby making identity-based threats the hardest problems that modern enterprises face. Whereas, simultaneously, data is spreading all over the M365 ecosystem consisting of emails, Teams chats, shared files, OneDrive folders, and SharePoint libraries, as well as numerous third-party integrations. Even though this interdependent environment is a great way to improve the productivity of the team, it has also become a very challenging task for organizations to track, classify, and protect sensitive information when it is moving so fast across the different workloads.

Compounding this issue is the phenomenal growth of AI-generated content. Workers are now dependent on AI instruments to produce documents, take the minutes of meetings, write emails, and perform data analysis. These features by themselves are a powerful way to increase the speed of the work process; on the other hand, they also raise some risks with respect to data correctness, content faithfulness, and the unintentional revealing of sensitive information. In the absence of well-established rules, the AI-generated deliverables may open up the route to leaks of confidential data or spread inaccuracies to the organization.

The situation is further aggravated by compliance requirements. Enterprises have to comply with a constantly increasing number of regulatory mandates—GDPR, HIPAA, SOX, ISO, NIST Frameworks, and industry-specific standards. It is quite a Herculean task to keep track of compliance all the time when data is scattered over numerous apps, devices, and users working from various locations. On the other hand, endpoint, and device vulnerabilities are still among the major causes of concern Laptops, mobile devices, virtual desktops, and unmanaged personal devices that are used in a hybrid work setup can be the places from which malware, phishing attacks, and data exfiltration operations are initiated. The overlapping issues above are indicative of the requirement for a smarter, AI-powered security strategy to be implemented that not only fits in with the work style of employees today but also takes into account the nature of modern threats.

1.2. Problem Statement

Businesses of the day need security measures that can keep up with the speed, the intricacy, and the volume of the cyberattacks of the modern era. Although traditional security programs are still a must, they have a hard time keeping up with such things as advanced social engineering tactics, the widespread use of the cloud, and the shift towards identity-focused attacks. Many old systems are running in isolation and have minimal integration among identity management, endpoint security, email protection, and data governance. Hence, IT teams get fragmented visibility and slower reaction

ISSN: 3071-5636
PP: 138-150.

times that make it almost impossible to find coordinated attacks or uncover hidden anomalies spanning multiple systems.

Simultaneously, companies are forced to keep up with productivity while also having to meet the growing demands for rapid content creation, seamless collaboration, and remote workforce enablement. Security teams, if not equipped with AI-assisted tools, are often left in the dark due to being bombarded with alerts, logs, and data signals that require manual analysis. Besides that, security team members become prone to exhaustion, and there is a higher risk of missing threats. Another aspect is the lack of a single AI reasoning system that can look through enterprise data and understand it. Though organizations might have AI capabilities spread out in different applications, they hardly have one intelligent system that can check the signals from identities, devices, apps, emails, documents, and teams. This fragmented strategy deprives enterprises of the contextual understanding that is crucial for early recognition of risks.

Furthermore, identity and threat detection systems are, for the most part, separate and hence unaware of each other's findings. As such, they cannot see the links between user behavior, access patterns, device health, and data movement. Consequently, the disjointed landscape leads to slow investigations, inconsistent policies, and little automation. To sum it up, enterprises need a future-proof AI-driven and integrated security platform as a solution to not only deal with the evolving threats but also, at the same time, comply with productivity requirements of the digital-first workforce of today.

1.3. Motivation

Microsoft 365 Premium becomes a compelling proposal to close the productivity-security divide with the introduction of Copilot AI and a unified, cloud-native protection model. In an environment where threats are escalating, security resources are limited, and the complexity of monitoring vast digital environments is increasing, enterprises are embracing AI-powered solutions that can detect patterns, uncover insights, and suggest actions in real time. Copilot AI essentially extends this power to the user's everyday workflows, be it creating documents, summarizing meetings, or checking for risks in the shared content.

Where the maximum benefits of Microsoft 365 Premium with Copilot AI lie is in the platform's consolidated security architecture. The union of identity, data protection, compliance, and endpoint security through a single platform is what organizations achieve when they do away with the strategy of patching up several vendors' standalone tools. Besides the fact that this unified strategy dramatically lowers the effort of the management, it also ensures that security signals are linked throughout the tenant. In short, this arrangement provides security staff with broader context and correspondingly accurate threat detection. Armed with a comprehensive view rather than isolated alerts, IT and security teams can take more effective actions.

ISSN: 3071-5636
PP: 138-150.

Furthermore, influenced by the current threat landscape, the enterprises have begun demanding more anticipative and predictive functions from the security systems. They require real-time awareness of user behavior, device risk, data access trends, and areas where the rules could be breached. By adopting Microsoft's Zero Trust framework, Copilot can effectively deliver such capabilities, where the enterprise dashboard is always a step ahead to prevent, rather than to handle, risks. The mistake of being reactive is thus replaced with proactive enforcement, which, among other things, helps in backing up the security breach prevention, getting quicker incident-response times, and enhancing compliance posture.

At the end of the day, what really pushes companies forward is the promise of a safer, more effectively operated, and more intelligently managed work environment that can result from AI-enabled decision-making, relief from manual work, and the ability of both employees and IT teams to stay a step ahead of threats while concurrently achieving the full potential of Microsoft 365 Premium.

2. LITERATURE REVIEW

2.1. Evolution of Microsoft 365 security frameworks

Initially,one of the main focuses for Microsoft's cloud productivity stack was securing the identity using Azure Active Directory, multi-factor authentication, and basic access controls. In the last ten years, this strategy has developed into a full security framework for Microsoft 365, which sees identity as the main control plane. Microsoft Entra Conditional Access is thus the Zero Trust policy engine that brings together user, device, location, and risk signals to decide in real-time if access to Microsoft 365 resources should be granted or not. Microsoft Learn+1

These features are connected to device compliance via Intune and are supported by Microsoft 365 Defender, Microsoft Purview, and other services, thus representing the organization's move away from perimeter-based controls towards continuous, signal-driven authorization.

The M365 Zero Trust deployment plan, among other things, turns this transition into detailed "swim lanes" that help identity, endpoints, data, applications, and infrastructure to conform to Zero Trust principles. Microsoft Learn The most recent versions also secure AI apps and data as a separate lane, thus suggesting that generative AI workloads have become one of the primary elements in Microsoft's security model.

2.2. Previous AI implementations in enterprise productivity

Before the arrival of large language models in the mainstream, AI in productivity suites was mostly limited to narrowly focused, assistive scenarios—spam filtering, malware detection, "smart compose," and personalized recommendations in collaboration tools. Both Microsoft 365 and Google Workspace used machine learning to identify threats in email, detect unusual sign-ins, and suggest relevant documents, but these models were working behind the scenes and on very limited problem spaces.

ISSN: 3071-5636
PP: 138-150.

The research for those earlier systems is mostly about the improvements of phishing detection, anomaly detection, and user behavior analytics, and not about content generation or reasoning. In fact, with generative AI, both Microsoft 365 Copilot and Google's Duet AI/Workspace AI are no longer just classification tools but also content synthesis and automation ones. Google publications highlight that Duet AI operates within the security and privacy limits of Workspace and that customer data is not utilized for training foundation models outside the tenant without permission. Google Workspace + 1 Microsoft, on the other hand, also describes Copilot as being within the Microsoft 365 data security, privacy, and compliance controls. Microsoft Learn

2.3. Zero Trust architecture research

Zero Trust Architecture (ZTA), as defined by NIST SP 800-207 changes the emphasis from network location to resource-centric protection, continuous verification, and least privilege. A+1 A follow-up work by Microsoft and NIST NCCoE illustrates feasible Zero Trust implementations in general-purpose enterprise IT, thereby revealing how identity, device health, and telemetry may be integrated for making policy decisions.

Microsoft's Zero Trust adoption framework directly implements these ideas in Microsoft 365 by linking Conditional Access, information protection, and SIEM/XDR telemetry together. Most of the Zero Trust-related materials, however, were written before the widespread adoption of generative AI. They generally consider "applications" and "data" as standard resources without explicitly defining AI copilots and agents that can cross multiple scopes, combine sensitive content, and behave as users' representatives. This results in a conceptual gap in the way the Zero Trust control planes should interact with AI-powered intermediaries.

2.4. Comparison with Google Workspace Enterprise AI + Security

Google has set out a similar parallel route for Workspace, where AI is embedded in productivity with a focus on zero-trust enforcement and digital sovereignty. According to Google’s releases, the most notable changes due to AI are classification of Drive-assistant, context-aware data loss prevention (DLP), and improved zero-trust and sovereignty features—like local data residency and encryption choices—to secure AI-augmented collaboration. Their security position highlights that Duet AI is operating under the same contractual commitments as Workspace, with customer content being kept within the organization's control and not used for external model training by default.

In comparison to Microsoft 365, the published materials for Google Workspace emphasize more strongly data sovereignty and AI-assisted DLP, whereas Microsoft's literature is more deeply integrated with a wider Zero Trust, XDR, and SIEM story. However, both ecosystems mostly consider AI as a further trust layer from existing boundaries; thus, they do not treat it as a new security entity requiring separate identity, policy, and monitoring.

ISSN: 3071-5636
PP: 138-150.

Table 1: Literature Review Table

Authors / Year	Focus Area	Key Findings / Contribution	Relevance to This Study
Brinkhoff et al., 2024	Windows 365, Intune, Copilot & cloud PCs	Describes deployment and management of Windows 365, Intune, and Copilot integration for secure, manageable cloud PCs.	Provides background on endpoint and device management, showing how Intune + Copilot can underpin secure M365 Premium deployments.
Zbořil, 2024	Security risks of AI deployment in organizations	Identifies organizational, technical, and governance risks when introducing AI solutions into enterprise environments.	Justifies the need for AI-aware security controls and governance in M365 Premium with Copilot AI.
Shargorodsky, 2024	Dynamics 365 AI for business insights	Explores practical use of AI modules in Dynamics 365 to improve business processes and decision-making.	Shows how Microsoft's broader AI strategy (beyond M365) leverages enterprise data, aligning with Copilot's Graph-based insights.
Homoliak et al., 2024	Security of GitHub Copilot code synthesis	Proposes prompt-engineering techniques and mitigations for security risks in AI-based code generation.	Highlights AI-assistant attack surfaces and aligns with the need for policy-aware, secure AI copilots in M365.
Sheggam & Zhang, 2024	Security risks in AI code helpers	Analyzes vulnerabilities, misuse, and mitigation strategies for AI coding assistants.	Reinforces the importance of threat modeling and controls for Copilot-like assistants used across enterprise content.
Akbar et al., 2024	Reverse engineering GitHub Copilot endpoints	Describes building OpenAI-compatible endpoints mimicking Copilot to integrate with developer workflows.	Emphasizes how AI endpoints become security-sensitive interfaces, comparable to Copilot endpoints in M365.
Asare et al., 2024	User-centered security evaluation of Copilot	Evaluates how developers interact with Copilot, including security-relevant behaviors and misuses.	Supports the human-factor argument that user education and guidance (e.g., Copilot warnings) are essential for secure AI usage.
Horne, 2023	Trust issues with AI code assistants (Pwnpilot)	Considers "trusting trust" problems and potential for hidden vulnerabilities in AI-generated code.	Motivates Zero Trust-style scrutiny of AI outputs and the need for robust telemetry and monitoring of AI-assisted workflows.
Arsal et al., 2024	Security & privacy threats of ChatGPT, Gemini, Copilot	Surveys emerging threats (prompt injection, data leakage, model misuse) in modern LLM assistants.	Frames the AI-specific threat landscape that M365 Premium + Copilot must address with integrated security.

ISSN: 3071-5636
PP: 138-150.

Sheggam & Zhang, 2024 (duplicate ref)	AI code helpers – risks & mitigations	Provides taxonomy of risks and practical mitigation strategies in AI-assisted coding.	Strengthens the argument for governance frameworks (e.g., Copilot Control System, SAM, Purview) to manage AI risks.
Alhur, 2024	AI (ChatGPT, Gemini, Copilot) in healthcare	Explores AI contributions and risks in highly regulated healthcare settings.	Illustrates how AI in regulated sectors demands strict compliance, mirroring financial services' needs in your case study.
Thompson et al., 2023	Enterprise-scale AI-augmented SDLC	Discusses GitHub Copilot, automated testing, and intelligent review for SDLC acceleration.	Shows how AI copilots can be deeply woven into enterprise pipelines, similar to M365 Copilot's role in office workflows.
Dincă et al., 2024	AI tools in software development	Analyses code quality, security, and productivity impacts of AI tools.	Supports your productivity–security trade-off discussion and need for metrics to measure both.
Veluru & Manchala, 2024	LLMs as incident prevention copilots in cloud	Proposes using LLMs to proactively detect and prevent incidents in cloud infrastructure.	Closely aligned with Copilot for Security in your paper, underpinning the AI-augmented SOC narrative.
Sai et al., 2024	Generative AI for cybersecurity	Surveys applications of generative AI (ChatGPT, DALL-E, etc.) in improving cyber defense.	Provides conceptual support for using generative AI in threat detection, triage, and predictive defense within M365 Premium.

3. PROPOSED METHODOLOGY

3.1. System Architecture Overview

The method presented in the document basically revolves around a consolidated system design that integrates the functionalities of Microsoft 365 Premium with the smartness of Copilot AI to generate an adaptive, security-first productivity environment. The core of this system design is the smooth integration of AI-powered assistance with Microsoft's enterprise-grade identity, threat protection, compliance, and endpoint management layers.

M365 Premium acts as the base platform, allowing enterprises to combine productivity applications with a sophisticated security stack. Copilot AI is the one who, by user prompts, can creatively work with the user and be the security-conscious reasoning engine that can analyze the contextual signals by email, documents, Teams, and tenant telemetry well beyond the scope of the conversation.

In fact, it is the identity layer, fueled by Microsoft Entra ID, that plays a deciding role in the architecture. Along with Microsoft Entra ID it contains multifactor authentication, Conditional Access,

ISSN: 3071-5636
PP: 138-150.

Privileged Identity Management, and identity governance features that ensure verified users and devices remain the only ones with access to sensitive data. Conditional Access policies are indeed the real-time gatekeeper. They inspect the user's location, application type, device health, risk score, and session context to implement Zero Trust principles. The identity-focused layer is the one responsible for this, which integrates with Copilot's risk-aware reasoning to ensure that every access request is not just authenticated, authorized, and continuously evaluated but also accounted for.

Microsoft Defender is the mainstay of the threat protection layer. It includes Defender for Office 365, Defender for Endpoint, Defender for Identity, and Defender for Cloud Apps, which, when combined, provide a layered defense across email, endpoints, identities, cloud apps, and data. These security measures provide abundant security signals that Copilot can use to perfect its replies, identify anomalies, and offer suggestions. Besides, the overall security posture at any point in time is also reflected through Microsoft Secure Score, Defender XDR's correlated insights, and the wider analytical capabilities of Microsoft Sentinel SIEM. Together they form a comprehensive architecture where proactiveness, the involvement of AI, identity, and threat protection all culminate to create security of a higher order.

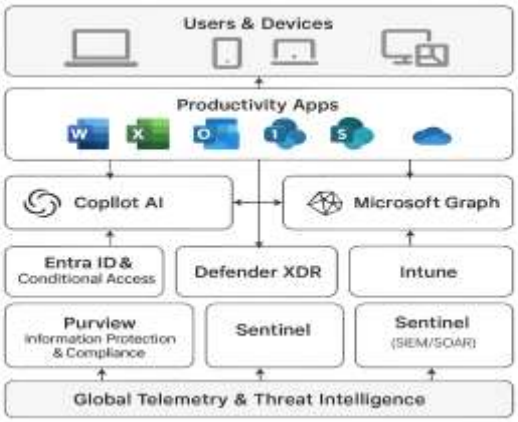

Fig 1 - System Architecture of Microsoft 365 Premium with Copilot AI

3.2. AI Integration Strategy

A strategy for integrating Copilot AI with Microsoft 365 Premium should be both data-driven and secure. The key element to the first is a strong data inflow via the Microsoft Graph API, which acts as a central hub for all the data within an organization. The Graph receives signals from users, devices, applications, identities, and workloads, thus providing Copilot with the necessary context to deliver valuable insights.

Next in line is the layer of user prompt flows for Copilot AI. These flows determine the handling of user prompts by the system, i.e., the system's enrichment, validation, and interpretation of the prompt before the response generation. It is the prompt flow that interacts with the language model, Graph signals, and the underlying M365 controls to perform the requested task if a user tells Copilot to summarize a document or find a security breach. Prompt flows confirm that the output is free of

ISSN: 3071-5636
PP: 138-150.

content leakage and is in compliance with the organization's policies by incorporating content filtering, sensibility validation, and tenant-specific rules. Hence, output safety is guaranteed, and the system mitigates its own potential issues, such as data leakage or hallucinations.

4. CASE STUDY

4.1. Deployment in a Mid-Size Financial Services Company

A mid-sized financial institution consisting of around 1200 employees took a step towards the digital transformation to enhance operational efficiency & cyber resilience. The firm provided services such as wealth management, corporate lending, and insurance advisory. Most of the employees were working in a hybrid mode at the regional offices, and there was a frequent movement of sensitive financial data between the branches, customer portals, and internal systems. Even though the company has already implemented Microsoft 365 for collaboration, it has not yet utilized the full capacity of M365 Premium or Copilot AI.

The management was looking for a smarter, more integrated solution that could consolidate security controls, document workflow automation, and reduce regulatory compliance process manual overhead. The organization, with the escalating security incidents in the financial sector, especially around identity theft, malware infiltration, and fraudulent email activity, understood that its current security model was missing the AI-driven visibility and predictive capability necessary to address modern threats.

4.2. Challenges

The organization dealt with a complex array of problems that were closely related to its regulatory, operational, and security environment. The company, as a provider of financial services, had to comply with industry regulations that were very strict like PCI-DSS, ISO 27001, local banking regulations and also data-retention regulations. These requirements called for continuous monitoring, very strict access control, encryption, and audit trails that were transparent. They were reaching the point at which audit fatigue and compliance gaps were the results of their efforts to fulfill these demands through manual processes and the use of disconnected tools.

The firm had its share of problems with the increasing ransomware threats as well. The incurring agents were able to lure financial institutions to open the door to them through the use of sophisticated email phishing campaigns, malicious attachments, and social engineering tactics aimed at account executives and customer service teams. In the meantime, the traditional anti-malware tools are least effective against this fully-fledged threat activity, which results in the creation of blind spots in identity behavior, Teams messages, and use of data across different platforms.

The uncontrolled use of cloud storage became a major challenge for them as well. The employees were often found to be storing sensitive spreadsheets, client contracts, investment summaries, and risk assessment documents in OneDrive, SharePoint sites, Teams channels, and email threads. The lack of centralized visibility and automated classification led to situations in which the

ISSN: 3071-5636
PP: 138-150.

confidential financial information was at times even being misplaced, mislabeled, or shared without the correct retention and DLP policies applied.

4.3. Implementation Steps

To overcome such difficulties, the company rolled out Microsoft 365 Premium in stages with a well-organized plan. Initially, Entra ID was set up as the main identity layer. Conditional Access policies were implemented depending on user roles, device compliance, location, and risk scores for the moment. Multifactor authentication was required for, for example, portfolio managers and finance officers, i.e., those who were in high-risk roles.

After that, Microsoft Defender for Office 365, Defender for Endpoint, and Defender for Cloud Apps were turned on and integrated with each other to give the service of email scanning, endpoint monitoring, attack surface reduction rules, and SaaS threat detection. The security team, by using Microsoft Sentinel, collected the logs and prepared the automated playbooks for handling incidents.

Lastly, Copilot AI was switched on and linked to the organization's sensitivity labels, DLP policies, and compliance frameworks. Prompts were prepared for legal, document, and SOC tasks. The company also set up feedback systems so Copilot's suggestions and results could get better gradually.

5. RESULTS AND DISCUSSION

5.1. Productivity Outcomes

The implementation of Microsoft 365 Premium combined with Copilot AI led to substantial gains in organization-wide productivity. Among other outcomes, the most visible effect was the cut of the very tedious manual jobs that employees used to execute for a good portion of their work hours. Not only that, but Copilot's ability to summarize, draft, and offer contextually relevant suggestions pretty much did the heavy lifting in the areas of client communications, meeting note collections, regulatory document preparations, and email thread answering. What was once a regular and time-consuming chore in the employees' work was now done more quickly and more reliably, and that is why employees could no longer complain about it.

The speed of document creation went through the roof. To gather the necessary contextual, frequently referenced, and template-based information, Copilot used Microsoft Graph. Consequently, the staff could write detailed financial summaries, operational reports, and client-facing documents in mere minutes rather than hours. As a result of this, the first draft of a document was reported to have been cut down by 30–40%, and the teams could now use the remaining time for content refinement and analysis delivery. It also saved time and made the AI more efficient in its work because human editors did not have to assist the AI in double-checking or redoing the parts of the work where formatting or the correct sensitivity labels had already been used.

Collaborative work was another aspect that saw a marked improvement as a result of employee engagement across Teams, Word, and Outlook becoming more natural. The summarization of existing

ISSN: 3071-5636
PP: 138-150.

threads by Copilot was the reason why there were fewer meetings and the follow-up task suggestions resulting from the underlying thread enhanced accountability and clarity. Besides that, Microsoft Graph insights enabled Copilot to offer quite a few targeted recommendations, such as the right datasets to be used or the people to be consulted who are based on the same ongoing projects. This led to a work environment that was more connected and informed.

To begin with, such results fast-tracked daily workloads and on top of that gave great support to collaborative decision-making processes. By significantly lessening the mental burden and granting employees more time for strategic activities, M365 Premium, and Copilot AI have made a noticeable positive impact on the company's operational culture, which has become more agile and efficient as a result.

Table 2: Before vs After Deployment Metrics in the Financial Services Case Study

Metric	Before M365 Premium + Copilot	After M365 Premium + Copilot	Improvement
Microsoft Secure Score	54%	87% (after 4 months)	+33 percentage points
Misclassified / mishandled sensitive data incidents	Baseline (100%)	~40% of baseline	~60% reduction
High-risk phishing emails detected beyond standard filters	0 (not systematically identified)	37 in first 2 months	New detection capability
SOC analyst workload (time spent on triage)	100% baseline	~75% of baseline	~25% reduction
Audit preparation effort	100% baseline	~60% of baseline	~40% reduction

5.2. Security Enhancements

The integration of M365 Premium and Copilot AI from a security perspective led to very few instances of attacks and also made it easier to manage them. The major improvement was the reduction of successful phishing attempts, and in fact, it was quite significant. Employees received clear warnings, risk explanations, and contextual insights about suspicious emails, as Defender for Office 365 and Copilot-assisted email analysis made them obvious. So, rather than just automated filters, Copilot was educating users and drastically lowering the percentage of users who clicked on a malicious link. At the same time, the chance of compromising credentials was also reduced.

Incident response times were drastically enhanced. A situation was at hand when work on incidents involved many hours spent on manually going through the logs and at the same time trying to connect the dots between several different tools, a process that was quite difficult. On the other hand, after deployment, Copilot for Security was not only a bright idea but also a real effective helper for the SOC, which helped in importing and summarizing the data promptly in reality and at the same time, it suggested the next moves to be taken. The analysts were able to promptly know the level and breadth

ISSN: 3071-5636
PP: 138-150.

of occurrences, which made them deliver their actions quicker and more efficiently. Automated workflows in Microsoft Sentinel played a great further role in enabling uniformity during triage and at the same time reducing human faults as well.

6. CONCLUSION AND FUTURE SCOPE

6.1. Conclusion

The combination of Copilot AI with Microsoft 365 Premium is a major step forward in how enterprises of today can increase their productivity and improve their security at the same time. By understanding the corporate environment, automating the repetitive tasks, and bringing up the important insights, Copilot AI is empowering the employees to work more efficiently and effectively. Thus, the teams get a chance to simplify their document creation, have more efficient communication, and enhance collaboration, whereas the IT and security wings can experience benefits in the form of automated threat detection, intelligent triage, and easy policy enforcement. The twofold effect of this platform, i.e., on one hand increasing the work output and on the other hand lessening the security risks, is what makes it a potential revolutionary agent in digital operations.

The integrated AI-security framework that comes with Microsoft 365 Premium is the answer to the question that most concerns the modern enterprise environment, namely, how to be secure and yet maintain agility. The days when separate sets of tools, manual workflows and reactive security strategies were good enough are over in a world full of identity-based threats, cloud data sprawl, AI-generated content and ever more stiff compliance requirements. By unifying Entra ID, Defender XDR, Intune, Microsoft Graph and Copilot AI in a single well-designed architecture, enterprises get a panorama of the security situation and have a more stable and manageable security posture.

6.2. Future Scope

In the future, the development of Copilot AI and Microsoft 365 Premium can be a source of a wide range of sophisticated, independent, and context-aware security and productivity features. Basically, one of the major goals can be the creation of more powerful Retrieval-Augmented Generation (RAG) models within Copilot. With AI-generated outputs based on enterprise-specific data, organizations can gain the most accurate, reliable, and domain-aware responses by using data, knowledge bases, and regulatory frameworks. The application of such information to less sensitive industries is also promising, for example, finance, healthcare, and legal services.

Another important part of the future of deep integration with Microsoft Sentinel is synchronized growth between Copilot's investigative capabilities and the SOC analyst's graphical toolkit. The use of the copilot as a tool for querying, summarizing, and correlating SIEM and SOAR data will be expanded to the SOC analyst; thus, the thorough investigation of the incident and the wider visibility are accomplished consistently in this cross-platform interaction. The progression to such autonomous operations can be gradual. At first, AI may only be handling tasks of lower severity, such as executing automated playbooks and escalating only high-risk events. Besides, the latter

ISSN: 3071-5636
PP: 138-150.

scenario will help human teams to achieve long-term resilience planning and conduct strategic threat hunting, in addition to reducing the risk of analyst fatigue.

Generative AI aware of policies is another new field of possibilities. One way to do it is to include not only the rules of compliance, retention policies, regulatory guidelines, and sector-specific limitations, but also AI reasoning in the form of Copilot that models the data for proactive prevention of policy violations. In a hypothetical example, the technology can alert users before sharing sensitive client data externally or serve as an automatic redactor of the regulated information in the documents that have been generated. This particular level of understanding of policies reduces the risk factor, thus embracing the use of AI in the enterprise setting and increasing users' trust in it.

REFERENCES

[1] Brinkhoff, Christiaan, Sandeep Patnaik, and Morten Pedholt. *Mastering Windows 365: Deploy and Manage Cloud PCs and Windows 365 Link Devices, Copilot with Intune, and Intune Suite*. Packt Publishing Ltd, 2024.

[2] Zbořil, Martin. "Security risks associated with deployment of AI solutions into organizations." *IDIMT-2024: Changes to ICT, Management, and Business Processes through AI* (2024).

[3] Shargorodsky, Dmitry. *Microsoft Dynamics 365 AI for Business Insights: Transform your business processes with the practical implementation of Dynamics 365 AI modules*. Packt Publishing Ltd, 2024.

[4] Homoliak, Ivan, et al. "Enhancing security of AI-based code synthesis with GitHub copilot via cheap and efficient prompt-engineering." *arXiv preprint arXiv:2403.12671* (2024).

[5] Akbar, Nur Arifin, Ardian Webi Krida, and Akbar Setiawan. "Reverse Engineering GitHub CoPilot: Creating an OpenAI-Compatible Endpoint for Enhanced Developer Integration." *Intechno Journal: Information Technology Journal* 6.2 (2024): 95-107.

[6] Asare, Owura, Meiyappan Nagappan, and N. Asokan. "A user-centered security evaluation of copilot." *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. 2024.

[7] Horne, Dwight. "Pwnpilot: Reflections on trusting trust in the age of large language models and ai code assistants." *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*. IEEE, 2023.

[8] Arsal, Muhammad, et al. "Emerging cybersecurity and privacy threats of chatgpt, gemini, and copilot: Current trends, challenges, and future directions." (2024).

[9] Sheggam, Harshith, and Xiaowen Zhang. "Exploring Security Risks and Mitigation Strategies in AI Code Helpers." *2024 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, 2024.

[10] Alhur, Anas. "Redefining healthcare with artificial intelligence (AI): the contributions of ChatGPT, Gemini, and Co-pilot." *Cureus* 16.4 (2024).

[11] Emily, Thompson, Gupta Rajesh, and Fernandes Lucas. "Enterprise-Scale AI-Augmented Data Engineering: Accelerating the Software Development Lifecycle with GitHub Copilot, Automated Testing Pipelines, and Intelligent Code Review Systems." *Innovative: International Multi-disciplinaryJournal of Applied Technology* 1.1 (2023): 112-128.

[12] Dincă, Ana-Maria, et al. "AI Tools introduced in Software Development. Analysis of Code quality, Security and Productivity Implications." *2024 IEEE 30th International Symposium for Design and Technology in Electronic Packaging (SIITME)*. IEEE, 2024.

[13] Sai, Siva, et al. "Generative AI for cyber security: Analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space." *IEEE access* 12 (2024): 53497-53516.

[14] Sheggam, Harshith, and Xiaowen Zhang. "Exploring Security Risks and Mitigation Strategies in AI Code Helpers." *2024 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, 2024.