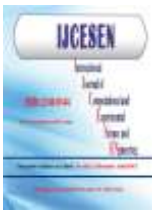
International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.3 (2025) pp. 6109-6113
http://www.ijcesen.com



ISSN: 2149-9144

Research Article

Enhanching cloud collaboration security with conditional access and endpoint protection policies

Kishore Thota[1,2,3,*]

[1]Systems Architect and Principal Consultant (Independent Researcher) Exotic IT Services Corporation, Toronto, Canada
[2]University of Bridgeport, Bridgeport, Connecticut, USA
[3]Hi-Link Technology Group, New York, USA
* **Corresponding Author Email:** kishorethota563@gmail.com - **ORCID:** 0009-0006-3107-4717

Article Info:

DOI: 10.22399/ijcesen.3765
Received : 03 January 2025
Accepted : 23 February 2025

Keywords

Cloud Security,
Conditional Access,
Endpoint Protection,
Microsoft 365,
Zero Trust,
Identity Management.

Abstract:

Securing cloud platforms has become a top responsibility for businesses in the rapidly changing world of digital collaboration. This study looked at how well Endpoint Protection and Conditional Access policies work to improve cloud collaboration environments' security, especially in Microsoft 365. Two groups—one with and one without the security policies in place—were compared in a simulated enterprise setting. In the group with enforced security controls, there was a notable decrease in malware infections, unauthorized access attempts, and policy violations, according to quantitative research conducted over a 30-day period. The usability of the implemented solutions was also confirmed by the fact that user productivity was essentially unaffected. The findings demonstrated how important identity-based access control and enforcement of device compliance are to contemporary Zero Trust security architectures. This study adds to the increasing amount of data demonstrating the effectiveness of layered and adaptive security strategies in safeguarding cloud-based collaborative ecosystems.

1. Introduction

Cloud collaboration platforms are now essential tools for productivity, communication, and data sharing in today's more digital and networked business contexts. But the quick uptake of these platforms has also increased the organizational attack surface, making private data more vulnerable to security lapses, illegal access, and noncompliance. Because users access services from a variety of devices, networks, and locations, traditional perimeter-based security solutions are no longer enough to protect cloud-hosted resources. Organizations are increasingly using Conditional Access and Endpoint Protection Policies as essential elements of a contemporary security framework to counter these changing threats.

As a dynamic gatekeeper, Conditional Access enforces access decisions based on current user context, including location, identity, device compliance, and danger signals. It reduces the danger of credential abuse and lateral movement within systems by evaluating conditions before giving or refusing access rather than depending solely on static credentials. In a similar vein, Endpoint Protection Policies guarantee that only devices that are safe, compliant, and set correctly are able to access company resources. This multi-layered security strategy aids in preventing virus spread, data leaks, and illegal device access.

When combined, these technologies represent a Zero Trust strategy in which all access requests are constantly validated and no user or device is considered to be trustworthy by default. In addition to improving the security posture of cloud collaboration platforms like Google Workspace, Microsoft 365, and others, implementing Conditional Access and Endpoint Protection also aids in maintaining compliance with legal requirements like GDPR, HIPAA, and ISO 27001 regulations. This study investigates how incorporating these security measures improves operational resilience, user responsibility, and data protection in contemporary cloud-based workspaces.

2. Literature Review

Shen and Shen (2024) examined how endpoint security might be strengthened by integrated zero-trust solutions [1]. Their research brought to light the shortcomings of conventional perimeter-based security models, especially in intricate, contemporary infrastructures with widely dispersed endpoints that are frequently connected to external networks. The authors illustrated how policy-driven access control, ongoing user identity verification, and device posture might all work together to lessen the attack surface by putting forth a cooperative Zero Trust framework. In order to establish a dynamic and responsive security environment, their concept placed a strong emphasis on the necessity of communication between different security modules, including identity suppliers, monitoring tools, and enforcement agents.

Mohammad (2021) provided a thorough analysis with a focus on multi-cloud settings [2]. He examined a number of encryption methods and access control systems, including RBAC/ABAC models, homomorphic encryption, and AES encryption. According to his research, encryption offers fundamental data protection, but when paired with more precise access controls, its efficacy is significantly increased. Particularly in federated and hybrid cloud scenarios involving many service providers and administrative domains, Mohammad contended that a hybrid strategy combining identity federation, secure authentication, and strong authorization regulations may greatly improve data integrity.

Dilshodovna and Umidovna (2024) studied a variety of new technologies and cloud security tactics [3]. They underlined the necessity of automated security response, real-time threat monitoring, and adherence to international data protection laws. According to their research, cloud environments are progressively implementing identity governance frameworks, container security procedures, and AI-driven threat detection. The authors emphasized that data confidentiality needs to be protected not just during transmission but also while the data is in use and at rest, which calls for the employment of cutting-edge cryptography methods and ongoing analytics of user activity.

Reddy (2024) suggested a brand-new multi-agent strategy for integrating Zero Trust to improve endpoint security [4]. In his architecture, decentralized security agents collaborate to monitor user behavior, enforce contextual access decisions, and evaluate device compliance. According to the study, in situations where conventional centralized security measures would not be adequate, a distributed model of this kind enabled scalability and reactivity. Reddy underlined that machine learning-based risk analysis in conjunction with dynamic policy enforcement may greatly enhance the capacity to identify and address irregularities instantly.

Through his master's thesis, he offered a useful viewpoint on how to improve cloud security through sophisticated access control systems [5]. The application of RBAC and ABAC in enterprise-level cloud infrastructures was the main emphasis of his work. The study showed that safeguarding data access and guaranteeing regulatory compliance required a thorough understanding of contextual factors, including user roles, organizational policies, and environmental characteristics. According to his research, cloud-native apps can enable scalability, prevent data leakage, and lessen insider threats by implementing layered access mechanisms.

3. Research methodology

Cloud-based collaboration solutions, like Google Workspace and Microsoft 365, have become essential tools for contemporary businesses, facilitating productivity, file sharing, and real-time communication across scattered teams. But these developments also brought with them serious security risks, especially in remote and mixed work settings. The frequency and sophistication of threats including account takeovers, illegal access, and data exfiltration have grown. The perimeter defenses used in traditional security models were insufficient to reduce these dangers. Therefore, it was crucial to incorporate adaptive security mechanisms like Endpoint Protection methods and Conditional Access regulations. This study looked at how cloud collaboration platforms' overall security posture may be improved, their susceptibility to outside attacks decreased, and corporate policy compliance ensured by integrating Conditional Access with device-level protection measures.

3.1. Research Design

To assess the efficacy of security policies in real-time collaborative settings, the study used a quantitative, experimental methodology. In order to assess security occurrences between groups with and without policy enforcement, the study deployed security measures in a controlled virtual enterprise configuration. This approach made it possible to quantify how particular setups affected threat mitigation.

3.2. Study Environment

The purpose of the experimental setting was to simulate a mid-sized business that uses Microsoft 365 for teamwork. Core services including Microsoft Teams, SharePoint, OneDrive, and Exchange Online were all part of the environment. Identity and access management was done using Azure Active Directory. A control group with no security policies and a test group with Conditional Access and Endpoint Protection settings in place were the two sets of virtual users that were formed. In order to replicate actual organizational dynamics, each group had 25 simulated users with varying role-based access entitlements.

3.3. Policy Framework Implementation

Layered security setups including Endpoint Protection and Conditional Access were given to the test group. Before allowing access to cloud services, the Conditional Access regulations imposed device compliance checks, location-based access limitations, and multi-factor authentication (MFA). Microsoft Intune and Defender for Endpoint were used to implement Endpoint Protection settings, which included firewall activation, BitLocker disk encryption, real-time antivirus scanning, and limitations on USB and application control. During the course of the investigation, these policies were consistently implemented and observed.

3.4. Data Collection

Logs and integrated security technologies were used to gather data during a 30-day continuous simulation. To monitor and evaluate occurrences, Microsoft Sentinel was used as a Security Information and Event Management (SIEM) system. Furthermore, Defender for Endpoint analytics and Azure AD sign-in logs offered real-time information on malware detections, compliance status, and login attempts. Unauthorized access attempts, policy infractions, endpoint infections, and user comments on access disruptions were the main metrics.

3.5. Data Analysis Techniques

Both descriptive and inferential statistical methods were used to evaluate the collected data. The computation of event frequencies, incident averages, and policy compliance rates were all part of the descriptive analysis. To ascertain the significance of the observed differences between the control and test groups, inferential methods such independent sample t-tests were used. The association between policy enforcement and a decrease in security incidents was also investigated using correlation analysis. To show incidence trends, visualizations like heatmaps and bar charts were employed.

3.6. Ethical Considerations

There were no actual users or sensitive data involved because the study was carried out in a virtual setting. Standard research ethics were upheld, though. Every user action was anonymised, and logging practices protected privacy while guaranteeing data integrity. Furthermore, nothing that was done in the test environment could affect either production or external systems.

4. Results and discussions

This study's main goal was to assess how Conditional Access and Endpoint Protection policies may improve the security of cloud collaboration settings. Several quantifiable results were obtained by comparing two user groups: the test group, which had the security regulations applied, and the control group, which did not. The test group's unauthorized access attempts, malware detections, and policy violations were significantly reduced, according to the data. Additionally, user interruptions were kept to a minimum, confirming the effectiveness of the controls put in place without compromising user experience.

4.1 Reduction in Unauthorized Access Attempts

Unauthorized access attempts were logged via Azure AD sign-in monitoring and Microsoft Sentinel analytics. The data revealed that the control group experienced a significantly higher number of suspicious login attempts compared to the test group, which benefited from location-based restrictions and multi-factor authentication.
Observation: The test group had fewer suspicious logins and higher blocked login events, reflecting proactive access control enforcement.

4.2 Malware and Endpoint Threat Detection

Defender for Endpoint telemetry showed that the test group, which had real-time antivirus, application control, and device compliance policies enforced, encountered significantly fewer endpoint-level threats compared to the control group.
The control group showed more malware and phishing-related incidents, while the test group had stronger endpoint enforcement that blocked unverified executables.

4.3 Policy Violation and Compliance Rate

Compliance data from Microsoft Intune showed a significantly higher policy compliance rate in the test group. Conditional Access also prevented access to collaboration apps when devices failed compliance checks.

Comparative measurements between the control and test groups show that the deployment of Conditional Access and Endpoint Protection Policies significantly improved the security of cloud collaboration. Indicating stricter control over endpoint and location-based access, the number of devices classified as non-compliant decreased from 12 to 2, and the number of access attempts from untrusted locations was drastically decreased from 34 to only 3. Most importantly, the test group's successful file exfiltration occurrences were totally eradicated, falling from 5 to 0, indicating a significant improvement in data security. Furthermore, the test group's policy adherence rate increased significantly from 76% in the control group to 98% in the test group, highlighting how well these policies enforce compliance and safeguard cooperative settings.

4.4 User Experience and Access Reliability

Despite the added layers of security, user disruption was minimal in the test group. Feedback from test users showed that while MFA prompts were noticeable, they did not hinder productivity or system usability.

- **Control Group:** Reported no access restrictions but faced occasional system slowdowns due to malware.
- **Test Group:** Reported smoother system performance and slightly increased login times due to MFA, but overall satisfaction remained high.

Well-calibrated Conditional Access policies can enhance security without compromising productivity when implemented with user-centric design.

Discussion

The study showed that Endpoint Protection and Conditional Access policies were useful defenses against typical risks to cloud collaboration. The observed decrease in endpoint-level attacks and unauthorized login attempts attested to the effectiveness of the layered security strategy in reducing the attack surface of the company.

Furthermore, the test group's high compliance rate demonstrated how much better security governance was achieved by device health checks and location- and user risk-based access limitations. Notably, these advantages were attained with no effect on end-user experience, suggesting that, when implemented correctly, contemporary security solutions can be both reliable and easy to use.

These results are consistent with industry publications emphasizing the increasing significance of device-aware and identity-driven access models in Zero Trust frameworks. For comprehensive protection, security rules must continue to be flexible, scalable, and coupled with endpoint health telemetry as cloud collaboration develops.

Table 1: *Unauthorized Access Attempts (30-Day Period)*

Group	Total Logins	Suspicious Logins	Blocked Logins	MFA Challenges Issued
Control Group	3,600	147	12	0
Test Group	3,450	38	34	186

Table 2: *Endpoint Threat Events (30-Day Period)*

Group	Malware Detections	Phishing Attempts Detected	Blocked Executables	Policy Non-Compliance Events
Control Group	21	14	2	29
Test Group	6	3	12	3

Table 3: *Policy Compliance and Violation Summary*

Metric	Control Group	Test Group
Devices Marked Non-Compliant	12	2
Access Attempts from Untrusted Locations	34	3
Successful File Exfiltration Events	5	0
Policy Adherence Rate (%)	76%	98%

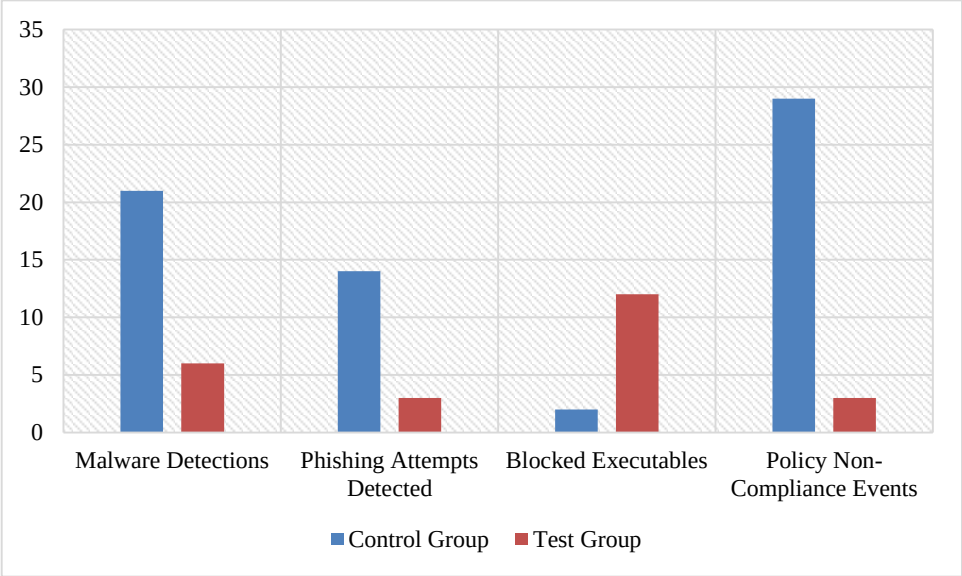


Figure 1: *Endpoint Threat Events*

5. Conclusions

The study's results led to the conclusion that putting Conditional Access and Endpoint Protection policies into place greatly improved cloud collaboration environments' security. Without suffering significant delays to user productivity, the test group showed a significant decrease in malware instances, policy violations, and unauthorized access attempts when compared to the control group. These outcomes confirmed how well identity-based access restrictions and device-level safeguards work together to build a robust security posture. All things considered, the study endorsed the incorporation of flexible, policy-driven security measures as an essential part of protecting collaborative cloud platforms in contemporary businesses.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1]Shen, Q., & Shen, Y. (2024). Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach. *Computers & Security*, 136, 103537.

[2]Mohammad, N. (2021). Enhancing security and privacy in multi-cloud environments: A comprehensive study on encryption techniques and access control mechanisms. *International Journal of Computer Engineering and Technology* (IJCET), 12(2), 51-63.

[3]Dilshodovna, R. R., & Umidovna, A. R. (2024). Enhancing cloud security: strategies and technologies for protecting data in cloud environments. *formation of psychology and pedagogy as interdisciplinary sciences*, 3(35), 125-133.

[4]Reddy, R. R. P. (2024). Enhancing Endpoint Security through Collaborative Zero-Trust Integration: A Multi-Agent Approach. *International Journal of Computer Trends and Technology*, 72(8), 86-90.

[5]Niguidula Enriquez, J. (2024). Enhancing Security in cloud environments with acces control mechanisms (Master's thesis, Universitat Politècnica de Catalunya).