

ASPECTS OF CLOUD ENVIRONMENT PROTECTION IN HIGHER EDUCATION. MICROSOFT TECHNOLOGIES

Elitsa Pavlova¹

e-mail: epavlova@unwe.bg

Abstract

The transition to cloud infrastructure presents significant cybersecurity challenges for higher education institutions. This report examines the role of three leading Microsoft solutions – Microsoft Defender, Microsoft Sentinel, and Azure Security Centre – in providing comprehensive IT protection. It analyses their application, benefits, and opportunities for integration into academic environments. The study highlights the need for a unified cloud cybersecurity strategy, security policy enforcement, and IT team training to ensure data integrity and privacy in the higher education sector.

Keywords: cloud environment, cybersecurity, higher education institutions, Microsoft Defender, Microsoft Sentinel, Azure Security Centre

JEL: O10, O14

Introduction

In the face of growing cyber threats and regulatory compliance requirements, ensuring reliable protection of cloud infrastructure is becoming a key task for higher education institutions, raising several issues related to security breaches and unauthorized access, privacy and data protection issues, malware and social engineering attacks, and shared responsibility model (SRM). Universities and academic institutions are increasingly moving to hybrid or fully cloud-based solutions for data storage, academic resource management, virtual learning, and collaboration. Generative artificial intelligence, third-party risks, continuous threat exposure, communication gaps, and security approaches are the driving forces behind the leading cybersecurity trends for 2024, according to Gartner, Inc. (Gartner, 2024).

¹ Eng., PhD, Department of National and Regional Security, Faculty of Economics of Infrastructure, University of National and World Economy, Bulgaria

Security leaders recognize that shifting focus from increasing awareness to fostering behavioural change will help reduce cybersecurity risks. By 2027, 50% of large enterprise CISOs (Chief Information Security Officer) will have adopted human-centric security design practices to minimize cybersecurity-induced friction and maximize control adoption. Cybersecurity culture programs encapsulate an enterprise-wide approach to minimizing cybersecurity incidents associated with employee behaviour. The report also states that as more organizations move to an identity-first approach to security, the focus is shifting from network security and other traditional controls to IAM (Identity and Access Management), making it critical to cybersecurity and business outcomes. While Gartner sees an increased role for IAM in security programs, practices must evolve to focus more on fundamental hygiene and hardening systems to improve resilience. This research employs a qualitative methodology, drawing on a comprehensive review of current literature, industry reports, and best practices related to cloud security in higher education. By analyzing case studies and synthesizing expert opinions, the study aims to identify key challenges and effective strategies for protecting cloud environments using Microsoft technologies. This approach ensures a well-rounded understanding of both the technical and organizational aspects influencing cybersecurity outcomes in academic institutions.

Activities and measures to protect the cloud environment

Universities and scientific institutions are increasingly moving to hybrid or fully cloud solutions for data storage, academic resource management, virtual learning and collaboration. They are required to comply with national and international regulations on personal data protection, such as GDPR, to ensure the security of sensitive information – personal data of students and teachers, academic achievements, research information and official documentation (SSARM, 2020). The main activities and measures to ensure the security of the cloud environment can be divided into technical, administrative and training.

Technical measures include data encryption, which is a key tool for protection against unauthorized access. Cloud providers offer built-in encryption mechanisms that universities must activate and manage properly. Another effective measure against unauthorized access is the introduction of multi-factor authentication for access to cloud services, which, through the combination of a password and an additional code (SMS, mobile application or biometric data), significantly increases security. The implementation of virtual networks, firewalls and access policies to certain resources also reduces the risk of internal attacks and lateral intrusions. Constant monitoring of system logs, user activity and traffic anomalies allows for early detection of incidents and real-time response.

The administrative measures that universities support are the creation of cybersecurity policies and procedures (e.g. password policy, access rules), management of user rights and roles by applying the principle of “least privilege”, creation of backups and disaster recovery plans. The report *Cybersecurity in Higher Education: Problems and Solutions* states that they all aim to limit the possibility of abuse of administrative access to ensure the resilience of systems to attacks or data loss (Toptal Insights, 2022).

Training and awareness. Conducting regular training and labs in a secure environment will remind you of building practical skills and increase responsiveness to real-world threats. The article “A Cybersecurity Workforce Training Guide” states that according to a study by Stanford University, more than 90% of data breaches involve human error, which is why it is important for employees to be aware of the dangers of cyberattacks, what they look like in the real world, and what role they play in preventing them (Cybintsolutions, 2021).

Daily cloud security activities are related to incoming alerts and incidents that need to be reviewed, triaged, and prioritized. Table 1 shows sample daily, and monthly cloud security activities based on the Top 25 Cloud Security Best Practices (SentinelOne, 2025).

Table 1: Daily and monthly cloud security activities

Daily Activities	Monthly Activities
Review system logs	Audit user accounts and roles
Check alarms from SIEM/IDS/IPS systems	Check cloud compliance policies
Review user access and rights policies	Update security rules and firewall policies
Check for suspicious activity and IP addresses	Conduct backup recovery tests
Confirmation of successfully created backups	Evaluation of all IAM policies and key rotation
Scan for vulnerabilities	Review settings for data encryption at rest and in transit
Check cloud resource configurations	Analyse trends in incidents for the last month
Monitor automated security tools, security testing through penetration tests	Security testing through penetration tests
Internal communication in case of detected incidents	Conduct a comprehensive audit of the cloud infrastructure

Source: SentinelOne (2025).

Daily monitoring of logs, alarms and user activity allows for timely detection of suspicious actions, such as unauthorized access, privilege changes or unusual network behaviour. This creates the opportunity for proactive response before a threat escalates into a serious incident. On the other hand, monthly activities such as access audits, configuration assessments, compliance policy reviews and disaster recovery testing contribute to long-term security and maintaining regulatory compliance with international standards such as ISO/IEC 27001 (ISO/IEC 27001, 2024) and GDPR. By systematically automating and performing these routine tasks, universities can minimize human errors, improve transparency in the management of cloud resources and ensure the continuity of their digital services in a dynamic and often decentralized environment.

Security Tools

Using integrated solutions such as Microsoft Defender, Microsoft Sentinel, and Microsoft Defender for Cloud to protect cloud infrastructure in universities provides a comprehensive platform for detecting, preventing, and responding to cyberthreats in real time (Yelevin, 2025). Microsoft Defender provides protection for endpoints, cloud applications, and identities, enabling advanced investigation and automated incident response (Diannegali, 2025). Sentinel is a cloud-based SIEM/SOAR platform that offers intelligent signal analysis and incident correlation using artificial intelligence. Through it, university security teams can effectively track threats, manage incidents, and automate responses using playbooks. Additionally, Azure Security Centre enables centralized control over the configuration and compliance of resources in the Azure environment, identifying vulnerabilities and non-compliance with best practices and regulatory requirements. The synergy between these tools enables universities to build a strong and adaptable security strategy that not only ensures the continuity of the educational process, but also protects scientific research and the personal information of students and employees in an increasingly complex cyber environment.

Microsoft Defender is a comprehensive security platform that includes Microsoft Defender for Endpoint, Defender for Office 365 – email and document protection, Defender for Identity – analysis of suspicious account behaviour, Defender for Cloud Apps – detection and control of SaaS (Software as a Service) applications, Microsoft Defender for Cloud – protection for cloud and hybrid environments.

Managing the security of SaaS applications requires modern and automated approaches that allow proactive identification and remediation of misconfigurations. In this context, the use of tools such as the Microsoft Secure Score dashboard provides a comprehensive view of organizational security and

supports the process of its improvement. For system alerts to work effectively, it is essential to ensure that components such as application connectors, conditional access policies, API tokens, SIEM agents, and automatic log uploads are properly configured. The Message Centre provides timely information about upcoming changes, new features, and support that may impact the Microsoft Defender for Apps environment. Logging and analysing activity through the management log and activity logs provides critical information about the status of completed tasks and is an integral part of the threat investigation process. Special attention should be paid to repetitive actions such as multiple failed logins or suspicious requests, and new policies for enhanced monitoring can be created based on them.

Effective incident management includes a systematic review of the dashboard, classification by priority and source, and proper assignment of responsibilities and status of incidents. Implementing best practices such as using the Streaming API to send data to EventHub, as well as creating custom analysis rules, requires highly skilled experts with in-depth knowledge of cybersecurity.

The article “Common mistakes during Microsoft Defender for Endpoint deployments” describes common administration errors related to non-enabled modules (e.g. Defender for Endpoint), lack of integration with Azure AD Conditional Access, and poorly configured security settings, which can lead to loss of control over access to critical resources and missed attacks (Jeffrey, 2025).

File policies and alerts in Defender for Cloud Apps provide the ability to enable a wide range of automated processes aimed at protecting information. They can be used to implement electronic discovery measures, as well as data loss prevention policies when sensitive content has been shared publicly. Security teams can perform regular checks to see how many files are shared publicly, as well as whether there are files with content or names that suggest sensitive information. Based on these analyses, existing policies can be adapted, and if necessary, new ones can be created for more precise control.

Microsoft Sentinel is a cloud-based SIEM/SOAR platform that works with data from Azure, Microsoft 365, AWS, Google Cloud, and other sources, could create automatic “playbooks” through Logic Apps, centralized security management and analysis, and automated incident response, making it convenient for working in a university environment. Effective administration of Microsoft Sentinel requires the application of best practices that cover all aspects from deployment and maintenance to threat analysis and resource optimization. At the implementation stage, it is recommended to carefully plan the architecture of the workspaces and activate appropriate Data Connectors to provide comprehensive visibility into the information infrastructure through logs from Microsoft 365 Defender, Azure AD, firewalls and other sources. Using the built-in analytical rules for threat detection should be an initial step, followed by developing customized rules based on the

specific context of the organization. Incident management should be carried out through categorization and prioritization, automation of responses with Logic Apps playbooks, as well as integration with Defender XDR for better grouping and tracking of signals. It is a good practice to implement policies to filter out irrelevant logs through Data Collection Rules, optimize the retention period, and use Basic or Archived Logs for less important data. Constantly monitoring the environment through visual workbooks and sending automatic notifications for incidents is a key element of proactive security. Access management should be implemented through role-based control models, providing different levels of access depending on the user's role. Common mistakes made in administering Microsoft Sentinel are related to overly broad alarm rules, which leads to "alert fatigue", without priority and a lack of automated playbooks. To achieve a sustainable and adaptable security management system in a cloud environment, cooperation between security, infrastructure, and support teams, as well as regular auditing of Sentinel configuration, is important.

Microsoft Defender for Cloud, formerly known as Azure Security Centre, provides a security assessment of Azure resources; recommendations for improving security; detection of vulnerabilities and configuration errors; and protection of hybrid environments (on-premises and cloud) such as those often used by universities. Many universities use the platform for courses in artificial intelligence, data, and networking.

Cloud Discovery is a key component of Microsoft Defender for Cloud that analyses network traffic logs and provides detailed visibility into the use of cloud applications in the organization. With support for a catalogue of over 31,000 cloud applications, the system classifies and scores them based on over 90 different risk factors, enabling the identification of Shadow IT and assessment of potential threats. Although anomaly detection rules in Cloud Discovery are disabled by default, administrators can manually create policies to detect new applications using criteria such as risk score, categories, traffic volume, and more. Practice shows that many university institutions lack policies for managing Shadow IT, which emphasizes the need to set up Cloud Discovery and its active use. The report "Microsoft 365 security practices complete guide" presents several good practices, such as integration with Microsoft Defender for Endpoint and Microsoft Defender for Apps, which facilitate the detection and management of unregulated applications (Acronis, 2024). The daily review of the discovery dashboard provides consolidated information about the used applications, users, source IP addresses and distribution method, as well as a risk assessment and alert status. After assessing the discovered applications, they should take actions to approve or ban, including applying tags and creating policies for automated management. Mistakes made when administering Azure Security Centre include ignoring se-

cure score recommendations, gaps in roles and rights, and not using Azure Policy to enforce security. Other vulnerabilities arise from the fact that universities often have hybrid environments, and not all components are monitored.

Challenges and recommendations

The main challenges facing higher education institutions in securing their cloud environments are data protection and GDPR compliance, budget and resource constraints, lack of centralized management, identity management, cloud misconfigurations, their impact and possible solutions. European higher education institutions are data controllers under the GDPR and are responsible for ensuring that data is stored or processed in the cloud lawfully and securely. The challenges stem from difficulties in verifying data residency, Microsoft 365 or Google Workspace, uncertainty around data transfers to third countries and enforcing data classification policies. Another challenge is that public universities often operate with limited budgets and rely only on default cloud settings or free security tools. This affects their ability to purchase security tools, hire qualified staff and leaves them vulnerable to evolving cloud threats. There is a lack of centralized IT decision-making, which leads to inconsistent cloud policies across organizational units: faculties, departments, research centres, etc. Institutions often lack a unified cloud strategy, which leads to unmanaged risks. An example of this is faculty using unapproved platforms to share files with student data, and security teams lack visibility into the risks associated with them. Identity and access management for thousands of students, faculty, staff, researchers, and external collaborators is extremely difficult. It is a bad practice to open student accounts for access to services after graduation. Some universities use outdated authentication systems, incompatible with single sign-on or conditional access, and do not integrate with cloud platforms out of the box. This contributes to increased complexity in securing hybrid environments. Misconfigured settings and incorrect cloud configurations, open databases, and a lack of a unified access control strategy are the main causes of cloud breaches. Regular cloud health assessments are needed with tools like Microsoft Defender for Cloud or AWS Config, but universities lack qualified cloud security professionals.

Conclusion and directions for future development

In the context of the increased need for security in cloud environments, building an effective cloud security strategy requires an integrated and multi-faceted approach. First, it is necessary to adopt a cloud security framework, such as the ENISA Cloud Guidelines (ENISA, 2024) or NIST SP 800-53 (NIST, 2018), to serve as a basis for risk management. This is followed by the implementation of

appropriate technological solutions, including the implementation of Zero Trust principles across all cloud services and the use of tools like Cloud Access Security Brokers to monitor shadow IT. It is also important to work together with cloud service providers that are compliant with European standards and regulations, such as GAIA-X or those with data centres located in the EU.

This paper contributes to systematizing the challenges and best practices in protecting cloud environments in higher education, focusing on the application of Microsoft technologies and modern concepts such as Zero Trust and IAM. The novelty lies in the unification of the academic and practical context through the integration of solutions such as Microsoft Defender, Sentinel and Defender for Cloud with EU regulatory requirements and the specific characteristics of universities. The practical value for higher education institutions in Bulgaria and Europe lies in the fact that the proposed approach provides a clear model for building a sustainable and centralized cloud security strategy that simultaneously protects scientific research, administrative data and the educational process. In addition, the emphasis on training and security culture creates prerequisites for long-term sustainability and reduction of human errors, a key factor for the cyber resilience of university environments. Training IT staff and end users on cloud-specific threats is a key element, which should be complemented by the implementation of automated policies and response scenarios. Particular attention should be paid to the inclusion of cybersecurity in curricula, as well as the development of training programs for students and administrative staff. In this context, it is advisable to closely integrate Microsoft solutions within a unified cloud strategy, to optimize security and resource management.

Focusing primarily on the Microsoft ecosystem, while practical for universities already using these solutions, limits the analysis in terms of alternative platforms and multi-cloud strategies. Such an approach may leave out of the scope of the study important practices applicable in environments built on Google Cloud, AWS (Amazon Web Services) or open solutions, which are also used in higher education in the EU (European Union). To achieve a more complete picture, future research should conduct a comparative analysis of different cloud providers and security tools, including their integration capabilities, compliance with European regulations and cost-effectiveness for public universities with limited budgets. This will outline a more balanced and adaptable cloud security framework that meets the diverse needs of universities in Bulgaria and the EU.

References

- Acronis. (2024). Microsoft 365 security practices complete guide, available at: <https://www.acronis.com/en-sg/blog/posts/microsoft-365-security-practices-complete-guide/>
- ENISA. (2024). Cloud Security Guide for SMEs, available at: <https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes>
- Cybintsolutions. (2021). Cybersecurity Training for Employees, Cybintsolutions, available at: <https://www.cybintsolutions.com/cybersecurity-training-for-employees-what-you-need-to-know/>
- Diannegali. (2025). Microsoft Defender XDR, learn.microsoft.com, available at: <https://learn.microsoft.com/en-us/defender-xdr/microsoft-365-defender>
- Gartner. (2024). Gartner Identifies the Top Cybersecurity Trends for 2024, available at: <https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024>
- ISO/IEC 27001 (2024) ISO/IEC 27001:2013 Information technology, ISO, available at: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html>
- Jeffrey, (2025). Common mistakes during Microsoft Defender for Endpoint deployments, available at: <https://jeffreyappel.nl/common-mistakes-during-microsoft-defender-for-endpoint-deployments>
- NIST. (2018). Uses and Benefits of the Framework, available at: <https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework> (accessed 4 August 2021)
- SentinelOne. (2025). Top 25 Cloud Security Best Practices, available at: <https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-best-practices/> (accessed 22 April 2025)
- SSARM. (2020). Data security challenges in cloud services, available at: <https://ssarm.bg/453/>
- Toptal Insights. (2022). Cybersecurity in Higher Education: Problems and Solutions, Toptal Insights Blog, available at: <https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education>
- Yelevin. (2025). Microsoft Defender XDR integration with Microsoft Sentinel, available at: <https://learn.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration>