УДК 004.056.5

THREATS AND STRATEGIES OF SECURING THE SAAS ECOSYSTEM

Chaimae Michich, Kadatska Olha
e-mail: olha.kadatska@nure.ua
Kharkiv National University of Radio Electronics,
V.V. Popowskyy dep. ICE,
Kharkiv, Ukraine

The widespread adoption of Software-as-a-Service (SaaS) platforms has transformed global collaboration, enabling seamless workflows in academia, healthcare, and enterprises. However, this shift introduces complex security challenges, ranging from inadvertent human errors to sophisticated cyberattacks. This paper explores the evolving threat landscape, analyzes systemic vulnerabilities through real-world incidents, and proposes actionable strategies to balance productivity with robust security.

SaaS platforms such as Microsoft Teams, Salesforce, and AWS have become critical infrastructure, supporting real-time collaboration and cloud-based operations. These platforms offer unparalleled flexibility, scalability, and cost-efficiency, making them indispensable for modern organizations. However, their widespread adoption has also introduced significant security risks. According to Gartner, 78% of organizations reported SaaS-related security incidents in 2023, with human error accounting for over half of these breaches [1]. Traditional perimeter-based security models, designed for on-premises environments, are ill-equipped to address SaaS-specific risks like shadow IT, API misconfigurations, and unauthorized third-party integrations. We study integrates behavioral research, technical safeguards, and policy frameworks to propose actionable mitigation strategies that balance security and usability.

APIs are the backbone of SaaS integrations, facilitating over 80% of data exchanges between platforms. However, they are also prime targets for attackers due to weak authentication, deprecated endpoints, or insufficient encryption. The breach of Mindful Health, a teletherapy platform, exemplifies this risk, attackers exploited an unauthenticated API endpoint, exposing millions patient session notes [2]. To mitigate such risks, organizations are adopting zero-trust API gateways, which validate tokens and encrypt payloads to prevent unauthorized access. Regular audits using tools like Postman’s API Network Scanner are equally critical to identify vulnerabilities such as outdated OAuth scopes or deprecated endpoints.

Phishing campaigns increasingly target SaaS credentials, with attackers mimicking login pages to hijack accounts. Once inside, attackers can deploy ransomware, exfiltrate data, or exploit connected apps, there in Microsoft credential theft attempts, underscoring the growing sophistication of these attacks [3]. Geo-

fencing and multi-factor authentication (MFA) have proven effective in blocking unauthorized access, with one trial showing an 89% reduction in breaches. AI-driven anomaly detection systems, such as Darktrace's Antigena, can neutralize threats within seconds by isolating suspicious activities.

Our research focused on implementing and testing a secure SaaS framework using Next.js, NextAuth.js, and Prisma ORM. Vulnerability analysis was conducted through comprehensive security testing, targeting common attack vectors in multi-tenant SaaS environments.

We highlight the importance of proactive governance and the risks posed by unvetted third-party integrations. A holistic defense strategy requires integrating governance, encryption, and incident response protocols:

Unified SaaS governance tools like Zylo map SaaS usage via SSO logs, while platforms like Vanta automate compliance audits.

The solutions that help organizations maintain visibility and control over their SaaS ecosystems.

- Encryption: client-side encryption (e.g.,Virtru) ensures data protection even if SaaS providers are compromised. This approach is particularly critical for sensitive industries like healthcare and finance.

- Incident preparedness: regular backup testing and breach simulations using frameworks like MITRE ATT&CK improve response efficacy. Automated tools like Own Backup validate restored weekly, ensuring data recoverability.

- Emerging technologies like AI-driven threat hunting and post-quantum cryptography (e.g., NIST's CRYSTALS-Kyber) will redefine SaaS security. AI models can correlate login anomalies with endpoint data to detect lateral movement, while quantum-resistant algorithms preempt decryption risks [4].

These advancements will enable organizations to stay ahead of evolving threats.

In conclusion, SaaS security demands a multidisciplinary approach combining technical controls, continuous training, and proactive governance. By adopting frameworks like CISA's SCuBA and learning from past incidents, organizations can mitigate risks while maintaining innovation. The integration of behavioral science, advanced technologies, and robust policies will be critical to securing the SaaS ecosystem in an increasingly interconnected world.

References:

1. Gartner. (2023). Market Guide for Enterprise Low-Code Application Platforms. URL: https://www.gartner.com (accessed 01/12/2025).

2. OWASP. (2023). Low-Code Security Top 10. URL: https://owasp.org (accessed 01/12/2025).

3. HIPAA Journal. (2023). Microsoft Power Apps Data Breach.URL: https://www.hipaajournal.com (accessed 01/12/2025).
4. Darktrace. (2024). Low-Code Cryptojacking Incident Report.URL: https://darktrace.com (accessed 01/10/2025).