PLAY IT SAFE

Jim Lippie *reveals the hidden dangers of SaaS applications*

SaaS adoption is skyrocketing. The average company now uses 112 SaaS applications, but with half of all SaaS accounts being largely unmanaged guest users this trend is leaving organisations vulnerable to cyber threats they may not even see coming. To uncover the hidden security risks in SaaS environments, Kaseya recently published its SaaS Application Security Insights (SASI) Report 2025. Based on a comprehensive analysis of anonymised SaaS security data from over 43,000 SMBs and nearly six-million end-user accounts, the report reveals some of the most critical security risks related to SaaS applications, from token hijacking and lax authentication practices to risky file sharing.

The report highlights how traditional brute-force attacks are taking a backseat as attackers embrace more efficient and dangerous techniques like token harvesting (intercepting authentication tokens) and Generative AI-powered threats. Meanwhile, phishing is more sophisticated than ever as platforms like Phishing-as-a-Service (PhaaS) are making it easier for even novice hackers to execute credential theft schemes – fuelling a growing ecosystem of cyber crime.

61 percent of SaaS end-user accounts had been disabled or were not using multifactor authentication

Jim Lippie is the chief product officer at Kaseya.

Many of the attempted cyber attacks detected by Kaseya's SaaS Alerts platform originated from just a handful of countries. In 2024, five geographical locations – China, South Korea, India, Russia and Australia – accounted for over half of all unauthorised login attempts, with cyber criminals trying to gain access to SaaS applications using valid user credentials.

HIGHLY SENSITIVE DATA

With highly sensitive data and workflows held in popular SaaS applications such as Microsoft 365, Google Workspace and Salesforce, it is no wonder that these platforms represent attractive targets for hackers. However, while Microsoft 365 and Google Workspace registered a significant amount of potentially suspicious activity – largely due to the fact that they are the most widely used applications – the highest percentage of critical security events was seen in Slack. Of the 31-million alerts detected in Slack, over one in ten (12 percent) were classified as critical, marking a considerable jump from 3.8 percent in 2022. Less widely used applications posed significant threats too and overlooking them could prove costly for organisations.

Kaseya's report also analysed how the most common threat vectors create major security gaps in organisations' SaaS environments. One concerning finding was the rise in guest user accounts, which can become a serious security liability when left unmonitored or inactive. Businesses typically create guest accounts for quick, temporary access – for instance, to share files with contractors, allow suppliers to use company SaaS apps or to collaborate externally. However, what starts as a short-term necessity all too often turns into long-term exposure.

The data showed that currently, more than half (55 percent) of all SaaS accounts are guest user accounts rather than licenced users, with many mistakenly granted the same permissions as internal staff, including privileged access. Guest credentials that linger for months or years become an open invitation for cyber criminals who can turn these accounts into unseen entry points to sensitive company data.

RISKY BEHAVIOUR

Another often overlooked threat vector is risky file-sharing behaviour. While SaaS applications make it easy for employees to collaborate on files both internally and externally, this convenience comes with a risk of unintentionally leaking unauthorised data outside the organisation. Businesses may not be aware of the extent to which this happens, either. The SASI report showed that in 2024, more than one third (37 percent) of all file-sharing activity involved external users, potentially exposing sensitive data. The risk is even higher when file-sharing links that were only meant for temporary access aren't subsequently revoked or disabled.

As the number of SaaS applications used by organisations rises, so does the likelihood of a cyber attack – especially when users create shortcuts around security measures for their convenience. Password fatigue is a growing problem, with many employees bypassing traditional logins and instead signing into apps with their Microsoft or Google credentials via OAuth. While this reduces the hassle of managing multiple passwords, it introduces a major risk: If a hacker successfully compromises a Google or Microsoft account, they can then gain access to all connected SaaS apps.

Similarly, while multifactor authentication (MFA) is the single most effective defence against identity compromise and account takeovers, the report found that 61 percent of SaaS end-user accounts had been disabled or were not using MFA, making it easier for intruders to gain access.

Most leading SaaS applications provide security tools to help protect accounts, but these aren't foolproof. Misconfigurations, weak enforcement and poor end-user habits can create vulnerabilities that lead to intrusion and data exfiltration. Training employees on security best practices to avoid phishing and prevent accidental leaks must therefore be a priority.

CYBER ATTACKERS ARE STARTING TO EMBRACE MORE EFFICIENT AND DANGEROUS TECHNIQUES

To strengthen their SaaS security, organisations should enforce MFA across applications and ensure that only authorised users in approved locations can access critical apps. Monitoring must include all third-party apps connected to Microsoft 365 or Google Workspace via OAuth. In addition, administrators should track file-sharing activity and terminate old file-sharing links. It is also important to actively manage guest users by regularly reviewing and deleting unused accounts. As a rule, guest accounts should only be granted minimal permissions and have automatic expiration dates as standard.

Without proper monitoring, malicious activity can go undetected for a long time so businesses should keep a close eye on what is happening in their SaaS applications. For example, excessive file downloads can signal a data exfiltration attempt, while excessive file uploads may indicate unauthorised data transfers. Prompt investigation of login or file access attempts from unapproved locations or IP address ranges are also key, as these can indicate a critical security breach.

Finally, businesses can implement automated threat responses to suspicious events – such as blocking access or expiring logins. With automation tools, threats can be stopped early before they lead to serious security breaches.

The transition from legacy on-premises systems to SaaS applications is in full swing. While enjoying the boost in efficiency and convenience, businesses must not forget that this shift also introduces new cyber security risks. By actively monitoring their SaaS environments and responding fast when risky behaviour is found, IT providers, administrators and security professionals can stay ahead of evolving threats. ●