# Machine identities outnumber humans in Australian organisations, raising security concerns



A new report by CyberArk has revealed a marked increase in machine identities within Australian organisations, exposing significant vulnerabilities due to inadequate security measures for these accounts. The findings come from CyberArk’s 2025 Identity Security Landscape report, which surveyed 2,600 cybersecurity decision makers worldwide, including a substantial cohort from Australia.

The report highlights a profound shift whereby machine-generated identities now considerably outnumber human identities in Australian businesses, with 79 machine identities per human identity. These machine identities have proliferated in part due to heightened cloud adoption and the expanding use of artificial intelligence (AI) technologies. Despite this growth, 92% of Australian organisations still define a ‘privileged user’ solely as a human, leaving many machine identities with sensitive or privileged access insufficiently protected.

Thomas Fikentscher, Area Vice President for ANZ at CyberArk, commented on the findings in an interview with SecurityBrief Australia. He noted, “As GenAI and LLMs become a key driver of cybersecurity investment in Australian organisations, there is an urgent need to rethink how identity security is approached. While most security strategies remain focused on human identities, the rapid growth of machine identities – especially those linked to GenAI and cloud environments – is creating a new and often ungoverned layer of risk.” Fikentscher added that intensifying compliance demands and fragmented identity systems are further challenging organisations’ ability to maintain visibility and control over access to critical assets.

The report reveals that almost one-third (32%) of machine identities in Australia have privileged or sensitive access, many of which lie beyond the scope of traditional identity security frameworks. Security professionals rated unknown and unmanaged machine identities as the leading risk to cloud infrastructure, with 36% identifying this as their principal concern. Moreover, 41% anticipate cloud environments will be the main source of new privileged or sensitive identities in the near future.

Identity-related breaches remain a persistent concern in Australia. Over the past year, 35% of respondents reported experiencing phishing or vishing attacks, including those involving deepfake technology, while 27% had at least two incidents involving compromised privileged access during the same period.

The increasing integration of AI and large language models (LLMs) within organisations further complicates the security landscape. Both sanctioned and unsanctioned AI tool adoption is accelerating, with AI poised to drive the creation of the largest number of new privileged identities in 2025. Yet, 69% of organisations lack specialised identity security controls for AI, and 38% report an inability to secure shadow AI use within their networks. Common barriers to securing AI agents include fears about external manipulation and the risk of sensitive access being compromised.

Fragmentation in identity security programmes adds another dimension of organisational risk. The report states that 60% of Australian respondents attribute cybersecurity vulnerabilities to siloed identity systems, while 73% acknowledge that inadequate visibility into privileged accounts exacerbates cyber risk. Additionally, 65% cite poor integration between identity and security tools as a critical weakness that undermines overall resilience.

Compliance pressures are mounting as well. Ninety-three percent of Australian organisations report increasing demands from insurers to enforce stricter privilege controls. Wider compliance requirements related to identity and access management also weigh heavily on security teams.

Australian organisations recognise these systemic gaps. More than two-thirds (68%) believe implementing compliance frameworks tailored to their most business-critical assets could foster better self-regulation and ensure alignment with government cybersecurity and critical infrastructure standards.

Despite these persistent threats and compliance challenges, there remains a notable misalignment in priorities. Three in four Australian organisations (75%) admit to placing greater importance on business efficiency over robust cybersecurity, even as identity-related security incidents continue to rise.

The CyberArk report captures a broad panorama of cybersecurity perspectives from large organisations across multiple sectors and countries, including Australia, the UK, Brazil, Canada, and several regions in Europe, Asia, and the Middle East. It underscores the evolving threat landscape driven by machine identities and AI proliferation, and it highlights the urgent need for updated security strategies in Australian organisations to effectively manage the complex identity security risks of the future.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://kbi.media/press-release/new-cyberark-research-rapid-growth-of-machine-identities-ai-adoption-and-cloud-native-innovations-leave-organisations-more-vulnerable-to-attacks/> - This article discusses CyberArk's 2025 State of Machine Identity Security Report, highlighting the rapid growth of machine identities in Australian organizations and the associated security vulnerabilities.
2. <https://itbrief.com.au/story/cyberark-report-reveals-rise-in-machine-identity-breaches> - This piece reports on CyberArk's findings that nearly half of Australian security leaders have experienced incidents or breaches due to compromised machine identities, emphasizing the need for improved security measures.
3. <https://securitybrief.com.au/story/cyberark-report-reveals-rise-in-machine-identity-breaches> - This article highlights the significant increase in machine identities within Australian organizations and the resulting security challenges, as reported by CyberArk's 2025 study.
4. <https://www.intelligentcio.com/apac/2025/03/27/cyberark-asia-pacific-research-78-of-security-leaders-reported-security-incidents-or-breaches-linked-to-compromised-machine-identities/> - This report presents CyberArk's research indicating that 78% of Asia Pacific security leaders have encountered security incidents or breaches linked to compromised machine identities, underscoring the urgency for enhanced security strategies.
5. <https://www.cyberark.com/state-of-machine-identity-security-report/> - CyberArk's official report detailing the state of machine identity security, including statistics on the prevalence of machine identities and the associated security risks.
6. <https://www.itnews.com.au/feature/machine-identity-a-key-priority-for-organisations-security-strategies-cyberark-615920> - This article discusses the importance of machine identity security in organizational strategies, referencing CyberArk's insights on the challenges posed by the proliferation of machine identities.
7. <https://news.google.com/rss/articles/CBMinwFBVV95cUxPQnpIRko4cnl4dk9XYWZTSUpvMFdVZkhWV3ZMOVgwdG8yT19rNXBJVzlKdjk3SWRnV2ZNMGY0dTF0X3dKNUo5NHZURFBwOGx4ZVdZajdaR1U2dzVJcUFZYUQtYU5VNDgwa3JjRW1LVWczS3lSeEVQajdoOFZMS2JXLTJrODB0U3JKcWZPUGE0aU1VME5lNGJwSHcyWGdKU1k?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data