Nasdaq

The Growing Importance of Machine Identity Security in the Digital Age

July 2025

Ilaria Sangalli, Index Research Lead

In today's rapidly evolving digital landscape, identity is no longer confined to humans alone. The focus has expanded beyond just managing people to include the oversight of numerous machines. Machine identity security is becoming increasingly critical in the cybersecurity space. But what exactly are machine identities? They refer to digital entities that verify, authenticate, and authorize machines - such as devices, servers, applications - within a network. Just as human identities use usernames, passwords or other biometric identifications, machine identities rely on digital credentials and cryptographic keys to manage and secure interactions and data transfer between machines.[1]

The number of machine identities is growing exponentially and it has now vastly surpassed the number of human identities. According to CyberArk, there are as many as 40 machine identities for every person in certain organizations.[2] This proliferation necessitates a robust security framework. As businesses depend more and more on a network of connected devices, services, and applications, their digital presence has significantly grown. Each of these devices necessitates authentication. If left unchecked, these identities can be exploited by malicious actors, leading to severe security breaches.

Machine identities have become a prime target for cybercriminals as they are typically granted with higher levels of privileges compared to standard user accounts. Additionally, machine identities often receive less oversight and protection than human identities. This suggests that, while organizations are becoming more skilled at identifying the risks associated with human identities, many still have significant progress to make in safeguarding machine identities. Nearly 42% of the 1,200 security leaders surveyed by CyberArk[3] admit their organizations lack a cohesive machine identity security strategy. In addition, half of those organizations have experienced security breaches due to compromised machine identities over the past year.[4]

Machine identities aren’t going anywhere. With AI solutions becoming more common, the number of machine identities in use will only rise. As organizations continue to integrate AI and machine learning into their operations, and start embracing Agentic AI, the need for robust security controls for machine identities and AI systems becomes increasingly critical. By prioritizing these security measures, enterprises can better protect their sensitive data and mitigate the risks associated with unauthorized AI usage.

[1] https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/machine-identity-management/
[2] https://www.cyberark.com/resources/machine-identity-security/ai-surge-drives-a-40-1-ratio-of-machine-to-human-identities
[3] Across the U.S., U.K., Australia, France, Germany, and Singapore
[4] https://www.cyberark.com/CyberArk-2025-state-of-machine-identity-security-report.pdf

Sources: Nasdaq Index Research, Bloomberg, FactSet.

Disclaimer: