converge360 TECH TALK PAPER

Redmond MAGAZINE

Cover: HTGanzo / Adobe Stock

SECURING THE RISE OF MACHINE IDENTITIES

How automation, AI, and bots are changing cybersecurity

SailPoint

www.sailpoint.com

Although organizations work diligently to secure and manage user accounts and other user-related identities, machine identities are often overlooked. These identities tend to be more privileged than user identities, yet organizations frequently lack basic oversight over them.

In a recent Redmondmag webcast, Steve Toole, Principal Solutions Consultant at SailPoint, explained, "Human identities are things like employees and contractors. Machine identities include service accounts and bots, which are the most common types. However, machine identities can also encompass API keys, secrets, certificates, tokens, and more."

Although machine identities have existed in some form for decades, their proliferation accelerated during the digital transformation era. Toole noted, "As organizations embraced digital transformation, the need for machine identities surged. These identities are essential for enabling applications to communicate and operate seamlessly with one another."

WHY CYBERCRIMINALS TARGET MACHINE IDENTITIES

Unfortunately, machine identities have become a favorite target for cybercriminals. One reason is their sheer number—most networks contain far more machine identities than human identities. In some environments, machine identities may outnumber human identities by as much as 50 to 1.

However, it's not just their abundance that makes machine identities attractive targets. They also tend to have more privileges than the average user account. Compounding the issue, machine identities are often less governed and less protected than human identities. Although organizations implement robust security measures for human identities—such as password or conditional access policies and multifactor authentication—these same protections are rarely extended to machine identities.

As Toole explained, "The problem with machine identities is that there are a very large number of them, they have more access than their human counterparts, and, lastly, they're less governed or controlled. So, if you were a cybercriminal, it would just make sense to focus on machine identities because they would probably give you a better success rate."

THE VULNERABILITIES OF AGING MACHINE IDENTITIES

Machine identities are vulnerable to compromise for several reasons. One common issue is the lack of ongoing security maintenance associated with these identities. For example, consider an organization that deploys a new application intended for long-term use. Ten years later, the application may still be using the same service accounts, even if the application itself has undergone multiple updates over the years.

In many cases, the service accounts' passwords likely haven't been updated since the application was deployed. Even if the passwords are periodically changed, the age of the accounts and associated security settings can eventually render the machine identity insecure. For example, there was a time when eight-character passwords were considered secure. If an application were designed to restrict its associated machine identities to eight-character passwords, those identities might have been secure when the application was initially deployed. However, by modern security standards, such passwords would now be considered inadequate.

OVERCOMING THE CHALLENGES

Managing machine identities is inherently challenging. These identities take on various forms and are distributed across different systems and workloads. Historically, organizations have lacked effective tools to discover all the machine identities in use, let alone consolidate them into a centralized portal for easier management.

Although the discovery process is critical, it's only the beginning. As Toole explained, "You need a process for onboarding new machine identities. These identities are not all the same, and they don't have the same risks, so it's important to classify identities to understand which ones are doing what."

Tracking ownership of machine identities has also been a persistent challenge. It's essential to identify who or what workload owns a particular identity, as this information helps determine whether the identity is still in use or has become obsolete.

Another significant challenge is access certification. Organizations need a robust process for regularly reviewing machine account access and revoking privileges when necessary. Without such a process, machine identities can easily become overprivileged or fall into misuse, increasing security risks.

These challenges highlight the need for visibility into the machine identities within an organization—how they are being used, who owns them, and whether they are appropriately secured. Toole underscored this by citing a common security adage: "You can't manage what you can't see."

HARNESSING AUTOMATION

The key to effective machine identity management lies in leveraging automation. Ideally, organizations should implement automated processes for creating and deploying new machine identities. Additionally, automation should support a discovery process to detect identities that may have been created outside of established policies, ensuring comprehensive oversight.

Automation is also invaluable for identity lifecycle management. For example, automated systems can periodically contact identity owners to confirm whether the identities they manage are still in use. Automation can also address situations like when an owner leaves the organization, resulting in an ownerless identity. Finally, automated processes can be employed to decommission identities that are no longer needed, reducing the risk of unused or forgotten identities becoming security vulnerabilities.

LAYING THE FOUNDATION FOR MACHINE IDENTITY SECURITY

The first step in securing machine identities is to conduct research to identify the identities in use across your organization and their associated owners.

Toole recommends a proactive approach: "Begin identifying your machine identities. Assess the applications within your organization and correlate machine accounts to these applications. Determine potential ownership—whether of the accounts themselves or the associated applications. These are steps you can take today."

Once you have a clearer understanding of the machine identities within your organization, the next step is to invest in technology to streamline and automate their management.

SailPoint offers a comprehensive suite of products designed to enhance security by reducing identity-related risks. Their Identity Security Cloud provides complete visibility into your entire identity landscape, including machine identities, through the Machine Identity Security solution. This enables a consistent and unified approach to identity governance across the organization.

Learn more about SailPoint Machine Identity Security and walk through your use cases.