INFORMATION WEEK

WHITE PAPER

Who's Watching The Machines? An Effective Strategy for Managing Machine Identities

Today, most organizations have more non-humans than humans accessing their digital resources. If you aren't taking appropriate steps to authenticate, manage, and secure those machine accounts, you are opening yourself up to risk from cyberthreats and non-compliance.

Sponsored by

Table of Contents

The Rise of the Machine

If your organization is like most, you have a robust identity and access management (IAM) solution in place to monitor the activity of the people on your network. Your IT and cybersecurity teams work hard to ensure that all the humans accessing your digital resources don't gain access to data or applications they shouldn't access.

But what about the machines on your network?

72% **said the machine identities are more difficult to manage than human identities.**

These days, nonliving entities on networks often outnumber the living ones. Actually, a 2024 Dimensional Research study sponsored by SailPoint found that "**69% of companies have more machine identities than human identities, and 47% have 10 times or more.**" These machine identities fit into a lot of different categories, like application service accounts, database service accounts, cloud service accounts, SaaS integrations, application programming interfaces (APIs), and bots created for robotic process automation (RPA).

And the number of machine identities is rising fast. Trends like cloud computing, microservices architecture, artificial intelligence (AI), and RPA are feeding extremely rapid growth. As organizations look for new ways to increase efficiency and productivity, they create increasingly interconnected computing systems that rely heavily on machine accounts.

This evolution has led to a number of challenges for organizations.

The Machine Identity Crisis

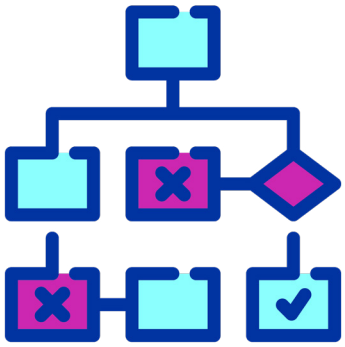
At most organizations, the IT teams don't know how many machine accounts exist or who owns them. The Dimensional Research study revealed that only 38% of organizations had the ability to create an accurate list of active machine identities.

Even if you do have visibility into machine identities, you might lack an effective way to manage them. Among study respondents, 72% said that machine identities are more difficult to manage than human identities. They pointed to three key reasons why this task is so challenging:

1. Manual processes

It's a little counterintuitive, but creating and managing machine identities often requires more manual work than managing humans. In fact, 69% of those surveyed by Dimensional Research confirmed that this was the case for their organizations.

Many of the existing IAM solutions in use were designed solely for humans. It isn't always possible to convert existing processes and tools to support machines. For example, while a centralized systems administration team usually creates the accounts for new employees during an onboarding process, machine accounts might be created by developers or integrators from any number of different teams, or they might even be created programmatically as they are needed for different tasks. And machine accounts often expire or disappear from the network relatively quickly, making monitoring even more difficult.



In many cases, existing solutions don't provide visibility into the machine identities on a network. Even if they can identify the machine accounts, administrators often can't tell who created or currently owns a machine account. As a result, teams default to tracking them with spreadsheets that quickly become outdated.

2. Ownership challenges

Those manually updated spreadsheets provide a good segue into the second key reason managing machine identities is difficult: ownership challenges.

The sheer volume of machine accounts makes it difficult to figure out who owns a particular identity. In many cases, machine accounts have such a short lifespan that

they might be created and expire before anyone can update the ownership records.

For machine accounts that last a while, identifying an owner isn't much easier. In fact, the survey revealed that "75% of companies have machine identities without a dedicated employee responsible for them." This can happen because the machine identity was created programmatically or because the person who created the identity is no longer in the same role. And all too often, no documentation exists to explain when, why, and by whom machine identities were created.

60% **of identity, access, and security personnel**

stated that machines identities pose greater risk to the business than human identities

This lack of ownership information makes it really difficult to determine if a machine identity has the appropriate level of access to data and systems. It also makes it hard to decide when a machine account can or should be deleted. As a result, 72% of organizations keep old machine identities active. That can be a serious mistake because it increases cybersecurity risk, as well as the likelihood that an organization will fail its compliance audits.

3. Security and compliance risk

The general lack of visibility and awareness around machine accounts poses a real threat to organizations. According to the survey report, "60% of identity, access, and security personnel stated that machines identities pose greater risk to the business than human identities."

In many cases, respondents came to this conclusion based on their personal experience. More than half (57%) said that their organizations had given a machine identity access it should not have had, and another 16% said they were unsure if this had happened.

Given these responses, it's not surprising that 60% of those surveyed said that their organizations had experienced compliance challenges related to machine identities.

Data breaches and a lack of compliance can have serious financial consequences for organizations. Globally, the average cost of a data breach is US$4.88 million, and in the United States, the average is even higher — $9.36 million. Researchers say that a single minute of downtime at a large organization costs around $9,000 for most companies, and in some industries, it can be more than $5 million per hour.

In addition, non-compliance can lead to huge fines. At the time of writing, the EU had issued fines totaling more than €4.9 trillion (US$ 5.37 trillion) related to just one law — GDPR. Those fines are just the tip of the iceberg because organizations that receive them suffer additional financial consequences from the damage to their brand's reputation.

Machine Identity Security

To address these challenges, many organizations are seeking solutions tailored to the unique complexities of managing machine identities. According to Gartner's latest Market Guide for Identity Governance and Administration, machine identity management ranks as one of the top three in-demand capabilities due to its growing volume and rapid market innovation. As organizations mature their identity security programs, they seek to extend governance to their service accounts, bots/RPAs, and other non-human accounts.

A machine identity solution allows organizations to see at a glance which machine identities are accessing which systems and data. It provides the proactive risk management capabilities that organizations need to reduce their cybersecurity risk and maintain compliance.

If your organization is considering deploying an machine identity solution, experts recommend looking for products with the following features:

- **Comprehensive discovery capabilities** — Visibility into the machine identities accessing your system is foundational to all other machine identity solution capabilities. Make sure any solution you consider has the ability to find machine accounts and to work across all the platforms and applications in your environment.

- **A unified platform** — As previously mentioned, machine identity solutions share a lot of common features with IAM solutions. If you can standardize one solution that can manage both human and non-human accounts, it improves efficiency and effectiveness for your IT teams.

- **The ability to assign and transfer ownership** — In addition to knowing which accounts are on your network, you also need to know who has created and is responsible for those accounts. And when someone leaves the company or changes roles, you need to be able to transfer ownership to a new person. This makes it easier to shut down zombie identities that remain active on your systems long after they have outlived their purposes.

- **The ability to group multiple machine accounts under one machine identity** — It seems obvious that each person in your organization usually has multiple accounts for the many different systems and applications they access. The same is true for machines. Being able to group accounts together under a machine identity makes it easier to manage those accounts, make sure they have the appropriate levels of access, and shut them down when necessary.

- **An automated certification experience** — Many organizations rely on tedious manual processes to make sure that machine account ownership and access levels are accurate. Look for a machine identity solution that replaces those labor-intensive processes with a purpose-built certification experience that increases efficiency while improving accuracy.

- **Scalability across an entire organization** — Because employees in many different roles create machine accounts, you need a solution that can span the entire breadth of your organization. And because the number of machine accounts continues to grow, you need to make sure that the machine identity solution you choose will continue to keep pace.

For many organizations, the concept of using a tool to manage and secure machine identities is a relatively new one. If your needs are beginning to outgrow the manual processes you have been using to track machine identities, SailPoint has resources that can help you learn more about machine identity security. Visit https://www.sailpoint.com/products/identity-security-cloud/atlas/add-ons/machine-identity-security for more information about how the right identity solution can help protect your organization against evolving cyberthreats.

About SailPoint

SailPoint equips the modern enterprise to effortlessly manage and secure access to applications and data through the lens of identity — at speed and scale. As the category creator, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyberthreats while enhancing productivity and efficiency. SailPoint helps the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.

Key Machine Identity Terms

- Machine — any non-human user (such as a service account, API, or bot) that accesses digital resources
- Machine account — the authentication credentials that allow a non-human user to access digital resources
- Machine identity — a collection of machine accounts all related to the same non-human user
- Machine identity security — the processes and tools that allow an organization to identify, authenticate, and manage machine accounts and identities