EBOOK

Fixing Organizations' Identity Security Posture

Saviynt

Contents

It's about time we finally recognize that, despite enterprises' best efforts, data breaches will most likely be a problem we never completely solve. But that doesn't mean organizations should throw in the proverbial towel and give up.

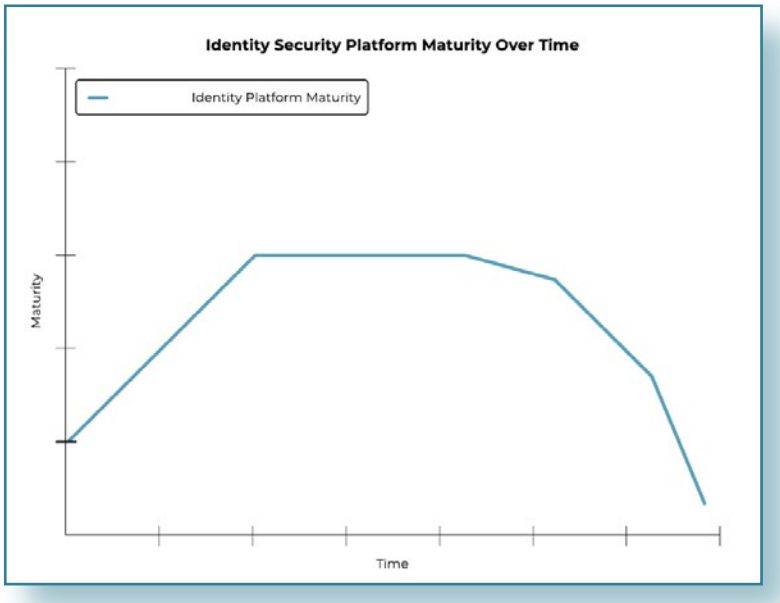
One constant over the years, however, is the weakest link causing most breaches: identities.

To combat this, many enterprises have adopted an identity security platform. But identity security isn't simply a switch you can flip on. Properly implementing an identity security program is difficult in and of itself due to its foundational nature.

It's a combination of people, processes and technology, and must be part of every area of the enterprise for it to function properly. Unfortunately, this need for widespread integration and adoption drastically raises the barrier to entry.

Once an organization does implement an identity security platform, it experiences rapid and rampant success. Incidents that would have slipped through before are stopped in their tracks, and many events are prevented before they can get off the ground.

Last year, 90% of breaches[1] were related to identity. And 83% of organizations[2] reported that they experienced some kind of insider attack.



However, the world around the organization keeps evolving. Enterprises change their environments and adopt new technologies, while they must also comply with new regulations as they continue to increase in size. Meanwhile, their identity security platform often stays stagnant.

[1] 2024 Trends in Securing Digital Identities, IDS Alliance
[2] 2024 Insider Threat Report, Cybersecurity Insiders

Evaluating your identity security posture

The more enterprises fail to bolster their efforts and address new challenges, the riskier organizations become. Even if it seems like your organization implemented identity security recently, how quickly you adopt new technology and update your program could mean your identity security posture isn't where it should be. Here are four key signs your organization needs a change:

Inferior identity data quality

Look at all the data your identity security platform uses. Do you have ownership data for every application and system? How robust (and accurate) are your role and entitlement descriptions? Look at your access classifications, tags, and glossary terms. Are they up to date?

Incomplete platform coverage of apps and identities

As you bring on new tech, including new types of identities such as external or non-human identities (e.g., NHIs, AI agents), you must onboard those into your identity security platform. Due to integration challenges, often, these are left on the outside, and over time, it means the majority of apps and identities are ungoverned by your identity security practices.

Non-continuous compliance and lack of audit readiness

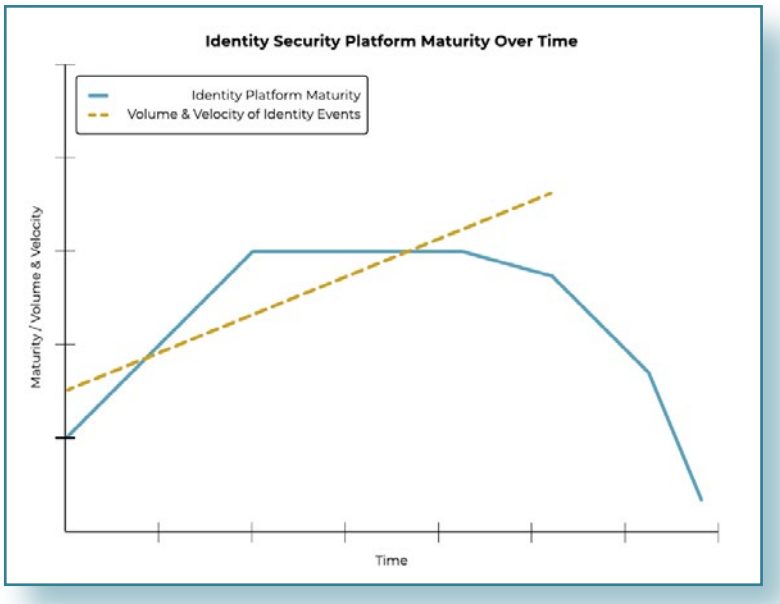
As global regulations continue to increase in number and stringency, the work your organization must do to get ready for audits drastically increases. If audit time feels like a mad rush to get everything in order, it's time to look at your tools and processes.

Manual governance processes

We're officially in the age of automation. When your access approvers must manually approve and certify access thousands of times, your identity security program suffers. When they don't easily know the right decision to make regarding access, your program suffers. As more identities and apps are added, these issues only compound, rippling out to the rest of the organization and slowing down work.

The consequences of lagging behind

Whether you identify with one or all these areas, it's important to understand that all of them affect the maturity level of your identity security program. After the initial success of implementing an identity security platform and as your enterprise fails to advance and evolve the program, it degrades and opens the business to more risk.



Decisions made in the dark

Access approvers often have a mountain of work ahead of them come re-certification time. When they're able to sit down and try to understand who should keep access, however, they find supporting information severely lacking. And when approvers don't understand what an entitlement is and cannot easily find who would know, your program suffers.

Unfortunately, this situation isn't an outlier. After analyzing data from hundreds of companies, we found that more than 60% of entitlements[3] in an average identity platform implementation have poor descriptions or no description at all. And up to 90% of entitlements either have the incorrect owner or are missing a defined owner.

The lack of data and poor data hygiene practices makes every part of your organization's identity security program that much more difficult. After all, poor data quality begets poor data analysis. By using dirty data, your team makes incorrect decisions on a much larger scale: inaccurate decision-making, incomplete understanding of the state of the business, etc. This leads to a severe erosion of security and maturity of the state of identity.

And, of course, as the organization continues to grow and adds more applications, identities and events to the platform, the problem only compounds.

[3] Sourced from conversations Saviynt has had with enterprises

Agile, but unprotected

Organizations cannot afford to be the once-lumbering behemoths that take months or years to complete tasks and projects. The speed at which innovation is made, products are launched and "the new" is adopted can be the difference between success and failure.

For many enterprises, this means opting for quick solutions to problems, buying cloud applications and using stopgaps whenever needed. But, each new app opens a potential hole in their security, and unfortunately, onboarding them into traditional identity security programs is often prohibitive.

In fact, our conversations with enterprises found that shifting priorities, budget constraints and integration challenges resulted in more than 80% of ungoverned applications[3] in an enterprise ecosystem. Meanwhile, all the machine identities the organization brings on quickly outnumber their human ones, up to 100 to 1[4]. This AI agent growth isn't a surprise. In 2025, 85% of enterprises[5] are planning to adopt AI agents in their business operations.

Unfortunately, today many of these machine identities are undiscovered. So, as enterprise environments continue to grow but coverage levels aren't maintained or improved, identity security posture rapidly deteriorates.

Compliant, but at a glacial pace

Sometimes the original impetus for the identity security program, compliance and audit processes are often where inefficiency most often rears its ugly head. It's incredibly common for organizations to spend untold resources on being audit-ready, feverishly collecting evidence and working with internal and external auditors to get tasks done on time.

But most identity security platforms aren't prepared to handle those requests, forcing manual processes onto those in the campaign, slowing them down and making the entire process take far longer than it should. The dirty data in your identity security platform causes even more problems during audits, as does the lack of intelligent analytics, slowing down findings and leading compliance officers on wild goose chases.

[4] **Rise of the Machines**, KuppingerCole
[5] **2024 GenerativeAI Survey**, Gartner

When compliance is manual, and your team can't completely trust the data you have, everything slows to a crawl. Rather than improve your posture and readiness, your platform now only serves as a distraction and deterrent.

Growth becomes an impediment

Underpinning every aspect of the challenges that face you and your identity security program is the nature of business itself: growth. As your organization develops, it adds more (and more types of) apps, identities and events. While the enterprise enjoys its progress, the increase in data and complexity only complicates the problems you face in your identity security program.

To best represent this, consider how many entities an average identity security platform has[3]:

- **500,000+** certification items that must be regularly certified
- **225+** applications strewn across on-premises, cloud and hybrid environments
- **220,000+** roles, including human and non-human, both in and outside the business

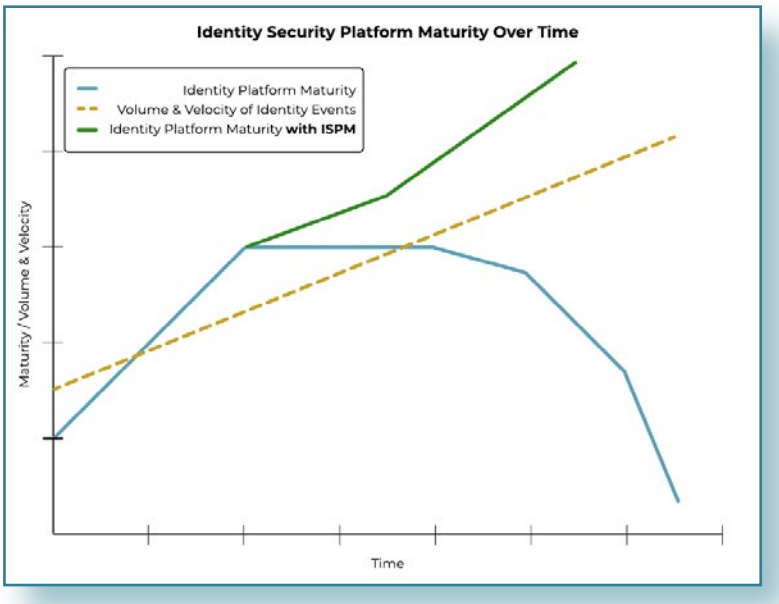
Of course, the ever-increasing numbers, combined with the intense pressure approvers face to get tasks done as quickly as possible, lead to issues such as rubberstamping. As a result, the organization hugely increases its risk and opens itself up to potential disaster.

A revolutionary approach

Until now, when organizations have realized they're in dire straits and must address these issues, they've been met with a decided lack of options. Traditional identity security posture management (ISPM) tools have drastically fallen short of organizations' needs.

Too often, ISPMs have only scratched the surface of what enterprises need, glossing over important information and providing only basic visibility. As such, organizations can't see what's really going on and issues aren't found, much less addressed.

Today's enterprises need a modern ISPM solution that does more. One that automatically discovers all identities, access and assets to provide holistic visibility and helps the organization see what's hidden in the shadows. Then it pulls in data from all over the organization, ensuring proper hygiene along the way and providing invaluable insights.



With centralized visibility based on clean, comprehensive identity data, the business and its users are empowered to see and do more faster and easier, **something no ISPM has done to date.** The business is now more efficient and can recover costs — from licensing and unnecessary tools, in addition to simply from being more productive as a whole. Modern ISPM lessens the burden on your technical resources and streamlines your entire identity program.

Above all, the solution itself must be able to keep up with the times. It should use the latest technology, such as AI, to help the business now and as it grows. With modern ISPM, organizations can understand their risk across all entities — including the ones the enterprise adds after implementation — with accurate, timely recommendations for remediation as it finds issues.

Make ISPM the cornerstone of your identity security program

When your organization implements ISPM, you strengthen your foundation across your entire identity security program, including identity governance, privileged access management, external identity management, machine identity management and more. It serves as the orchestrator to start your strategy correctly.

Whatever the state of your identity security program — even if you're still experiencing initial success — ISPM helps your enterprise confidently drive business growth and be ready for whatever comes your way.

Learn more about how Saviynt's ISPM can help your organization.
Visit Saviynt.com/ISPM.

Learn More

Saviynt

Saviynt empowers enterprises to secure their digital transformation, safeguard critical assets, and meet regulatory compliance. With a vision to provide a secure and compliant future for all enterprises, Saviynt is recognized as an industry leader in identity security whose cutting-edge solutions protect the world's leading brands, Fortune 500 companies and government organizations.
For more information, please visit **www.saviynt.com**.

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com