EBOOK

Enabling Business With Modern Identity Security

Saviynt™

Contents

Designing a Modern Identity Security Initiative 4
- Assemble the right team 4
- Identify organizational needs 5
- Define the value and purpose 7

Mastering Your Approach 8
- Start (and stay) stakeholder-centered 8
- Remain Agile 8
- Learn from and lean on the community 9
- Don’t copy and paste 10
- Have a post-migration strategy 10

What’s Required of Modern Identity Security? 11
- Converged, but extensible 11
- Cloud-native 11
- Intelligent 12
- Customer-first 12

Take the First Step 12

About Us 13

Confident. Secure. Future-ready. Three things that something all enterprises want to be. Confident enough to go after the really big goals. Invent a new product. Expand globally. Achieve even your most aggressive targets.

Secure enough to feel empowered by your processes rather than hindered by them. Secure in the knowledge that you're protected from outside (or inside) threats. After all, sixty percent of data breaches are related to humans — a number that remains consistent year-over-year, according to Verizon's **2025 Data Breach Investigation Report.**

Future-ready and able to handle anything that comes your way. New government regulations? No sweat. Traditional, generative and agentic AI? Handled. No process or software is ever truly future-proof, but with the right support structure — including your people, processes and technology — you can be ready for whatever the future throws at you.

The problem we've found in talking with enterprises all over the world is that so many are held back from being confident, secure and future-ready. The question is why?

Sometimes it's from fear. The unknown always holds a certain amount of mystery, but it's often tinged with fear. It's easy to be afraid of uncertainty and not knowing what will happen next. Plus, change in and of itself is scary. The more you amp up how much change you enact, the scarier it becomes. All the "what if"s start creeping in, even when you don't want them to.

Or maybe it's from the perceived cost. Your organization has spent months or years building your programs and systems to the point they are now. Why replace something when you could patch it up? Again. Realizing that the foundation is cracked, unsteady and moments from collapse is more difficult than it seems. However, at the end of the day, the cost of doing nothing is often far higher than the cost of change. Unfortunately, many organizations fall victim to the sunk cost fallacy.

Sunk cost fallacy. noun

The cognitive bias where an entity is reluctant to abandon something because they've heavily invested in it, even when it's clear abandonment is the right course of action.

There's always the question of prioritization, too. It sometimes feels like the "top priority" changes every day simply because there's so much that needs to be done. Truly understanding what is and isn't a top business priority — and what's holding you back from getting there — takes a lot of work. It's so easy to chase after the loudest voices or sharpest pains rather than take a step back and solve the underlying issues versus merely the symptoms.

When your organization quells its qualms, however, and promotes confidence, security and being future-ready, it can take on that future without hesitation. Embrace the changing nature that is business and deliver on your highest enterprise goals. Empower your identities to be agile, efficient and productive no matter who, where or what they are (e.g., internal, external, or non-human).

All this requires a platform that isn't stuck in the stone age. Instead, you want one able to use the latest technologies (such as AI) to streamline, augment your team's processes and handle the way business works today.

Stop being held back by outdated tech and unnecessarily complex processes designed to work around a system you may not even use anymore. With a modern identity security platform, your workforce can easily do what's right in terms of security. Lower risk, achieve continuous compliance and get full visibility while lowering the total cost for your identity security program.

Modern identity security helps you go from where you are to where you want to be. You've already done great things. Now let's find out what your organization is really capable of.

Designing a Modern Identity Security Initiative

No matter the current state of your current identity security program, it's time to take a step back and evaluate it as objectively as you can. To ensure you don't encounter the same pitfalls and find yourself in the same situation in the future, we've collected expert advice and real-world examples from practitioners on the other side of successful transitions—leaders just like you.

Assemble the right team

Additionally, to understand what you need, you have to have the right people in the room to answer the questions that come next. Identity security requires both a top-down and bottoms-up approach so you can ensure you're aligned to top business priorities as well as solving the needs and pain points of the ones using the platform.

Simeio Vice President, Batool Aliakbar, suggests leaders start by taking inventory of impacted roles. "Be transparent with everyone: auditors, risk managers, application owners and end users."

Acknowledge all the different stakeholders that you must bring to the table and understand what makes them tick — and determine what category they fit themselves within. Get insight from those that use new technology as well as those still holding onto their old-fashioned ways to fully understand what's happening in the enterprise.

From there, Campbell's Soup Co. Senior Information Security Architect, Anne Gorman, recommends building a story about life being easier — not just different. "Stakeholders often hold processes too closely, like a baby with a binky. The fastest way to break down a silo is a story about how [identity security] makes lives easier."

Start building the team by designating project leads. They're the ones who will help get things done (e.g., deployment, implementation, maintenance). Then, identify your champions. Who will help others see the value of your collective efforts? Finally, don't be afraid to include those who will challenge you. Even designating someone as a "devil's advocate" to help poke holes in your plan can help you build a stronger program.

> "It's OK to have naysayers and take criticism. Always welcome feedback and you'll improve your program.
>
> – Batool Aliakbar, Vice President at Simeio

At the end of the day, vibrant discourse is good. The more issues and potential problems you find now, the fewer you'll find once you're past your go-live date or if (really, when) something unexpected happens.

Building a **RACI matrix or chart** (i.e., identifying who is responsible, accountable, consulted and informed about each part of the program) will help immensely. A favorite project management framework for many, RACI charts help clearly lay out roles and ensure you have the right people for each part of the program.

Identify organizational needs

Once you have your team together, it's time to sit down and have some real conversations. What are the business's goals for the next one, three and five years? What's keeping you from achieving those goals? Ask the team these questions:

- What challenges has the business faced in trying to achieve your previous goals?
- As business needs evolve, what are you doing to bridge the gap?
- How are you managing and governing new technologies, such as AI?
- How would you want to use AI as part of your identity security efforts to empower your teams?
- Where is your current identity program insufficient for compliance efforts, especially as they increase year after year?
- What worked well the last time you implemented a large-scale program such as identity security? What didn't work well?
- What is the ideal end result of the program? How will you measure it?

Any KPIs you identify must connect to — and prove — the improvement story that your program promises. Campbell's Gorman often finds that companies don't "establish that a program can do what they say it will do."

Of course, these aren't the only questions that you'll need to answer during discovery. During the initial conversations with your team, determine the required answers you want to get from the team, but let the conversation flow naturally. Putting things in terms of real-world examples can sometimes help make the team think about things in a grounded way versus simply theoretical.

Take the goal of an acquisition for example. If that is one of your main business goals over the next few years, how would it progress with your current systems? Would you be able to quickly and completely integrate the acquired company's identities into your ecosystem? What about their applications? How would access to those apps be managed? If they have external identities, such as contractors and suppliers, would (and how would) they be governed?

Could you ensure the AI bots they use only have access to the information they should? Verizon's Data Breach Investigations Report revealed that 89% of employees using generative AI on corporate devices do so outside corporate purview. The access isn't necessarily the problem; it's the data users share over which the organization has no oversight.

Finally, consider what a completed acquisition would cost you. Not in terms of the capital spent, but instead the time and cost associated with integrating the organization itself and everything that comes with it.

When identifying what the business needs, be truthful above everything else. Sugarcoating the situation only hides potential issues that will almost certainly pop back up later and be much more difficult to solve then.

When determining goals...

Don't get lost in the "art of the possible" — instead, pick metrics or targets that add momentum via early wins. Consider organizing goals by complexity and project stage. For example, you may start with day-one app access and then move to a reduction in ad-hoc access requests.

Ultimately, any goal or metric must connect with executive leaders' priorities; understanding those priorities must be your first task. We've seen goals range from quantifiable cost savings to "squishier" targets like continuous compliance or no standing privilege.

Target improvements and identify metrics that matter to leadership. These metrics might be business outcomes (audit/compliance performance, reduced costs, increased productivity, data-driven decision-making, etc.) or operational changes (fewer deficiencies, faster access review cycles and remediations, increased percentage of identities and systems managed by your identity security platform, etc.). As you designate metrics, make sure to identify ways to easily report on them (ideally without the need for additional, expensive tools).

Sample metrics & goals

Access is provisioned on day one for new hires (including contractors)

X% increased revocations in the next re-certification campaign

Take 10 minutes off the time it takes users to review an access request

X% reduced cyberinsurance cost

Self-service is enabled for low-risk access requests

X% increase in identity and asset coverage in platform

Need a little help identifying goals? Saviynt Experts can help guide you throughout the discovery process to uncover what your business needs and how to solve for them.

Get Demo

Define the value and purpose

With the right team on board and goal posts clearly marked, you're ready to do perhaps the most important part of the whole program: explaining what the program will do for your organization — and the individuals within it.

During the discovery phase, part of the reason why it's so important to answer all those questions about where you as a business is today and where you want to be in the future is to assign values. And we're not only speaking monetarily. Just as you identified both hard and soft goals (and as we'll discuss in a bit), it's important to show both the financial and non-financial value of modern identity security.

> **The 30,000-foot view:** For the board and executives, perhaps you'll lower the total cost of ownership (TCO) of your identity security program. Or, maybe you'll have complete coverage of the identities, systems and apps, assets and resources in the organization. When everyone uses the new, modern solution (or, at least, identity security adoption improves), productivity and operational efficiency will increase.
>
> Break down what this means for them. For instance, a lower TCO could mean fewer (or no) on-premises servers to maintain, freeing up not only upgrade costs and physical office space, but also employee time and resources. Part of your calculations for TCO could also entail new benefits you couldn't even consider before, such as integrating the platform with the rest of your tech stack. What else, then, does this lead to?
>
> Maybe it's complete visibility of identities' access to organizational resources. When you know what your identities are doing and can ensure least privilege for more of the enterprise, business risk dramatically decreases. This lowers cybersecurity insurance costs. Audit failures and fines reduce in severity and number — or disappear entirely. Consider both the obvious and try to uncover the not-so-obvious benefits and effects from making such a foundational change and clearly communicate those benefits to leadership.
>
> **The 30-foot view:** Just as you painted a picture for those at the top, do the same for your end users. After all, if they don't adopt the processes and technology you put in place, your identity security program will fail. As you do so, remember that it's far easier to get buy-in and user adoption if you talk about what identity security means for them in their terms.
>
> To put it bluntly, your end users don't particularly care when the company fails an audit — unless it affects them directly. What they do care about is how long it takes to complete their portion of a certification campaign. Or, how long it takes them to get access to necessary systems and info when they need it.
>
> To "sell" your identity security initiative, figure out your users' pain points and then describe how you will either fix them or, at least, make them more tolerable. For instance, by offering self-service access requests, they no longer have to submit IT tickets and can get what they need within minutes. This frees them up to work on their tasks as they need to rather than waiting around for access to crucial systems or data.

As you're delving into benefits and understanding the cost of your initiative, pin down what the cost of waiting will be. There are countless projects constantly fighting for budget. As critical as it is, identity security is not a small program, and it's easy for executives to focus on the cost without recognizing all the benefits brought about by it.

Put things in real terms for your stakeholders. Money talks, sure, but often the threat of potential catastrophe (e.g., data breaches, audit failures and fines) is more compelling. Use everything at your disposal to help the ones who will sign the dotted line understand what's at risk.

Mastering Your Approach

Now that you have a clear path forward, it's tempting to dive in head-first. But before you set off on your exciting, new identity security initiative, there are a few extra things to keep in mind to better ensure your success.

Start (and stay) stakeholder-centered

Building a team is the first step for a reason. Identity security revolves around — surprise — people. Your identity program must seek to solve the organization's needs and address its priorities, but at the end of the day, the people in your organization are who will drive it forward.

Starting stakeholder-centered means the right people are always involved in the process. Use their knowledge and opinions to identify the business's needs and inform the program's goals. Make them champions of the program, and they'll foster acceptance and rally others to your cause.

Staying stakeholder-centered means ensuring the program you're building is followed and whatever processes and technology come out of it are used. As such, user experience must be a priority and one of your main goals must be to minimize friction and alleviate users' pain points.

At each stage of your rollout plan, remember to set up training for both your workforce and your external identities (contractors, suppliers, etc.) so they know what's new, what's changing and what's staying the same. Make sure to add this training to your onboarding programs so both existing and new identities are informed.

Remain Agile

Modernizing an organization requires change. Scaling a business requires change. At the end of the day, the nature of all things is change.

Put another way, you can't put together a plan to initiate change without expecting some change to the plan itself along the way. Build flexibility into your plans and anticipate that you'll need to adapt when something new crops up (e.g., include buffer times before a particular milestone to allow for a few more review cycles). However, don't be so flexible that you never get anything done. Having firm cut-off dates — as if you were committing code — will help to keep slippages in check.

Promoting agility and flexibility can also mean adopting **Agile**, a popular project management framework. While we won't get into all the details here, the framework focuses on breaking an initiative into phases and smaller projects. Rather than build a plan from start to finish and have a monumental launch at the end of a years-long process, Agile batches tasks into "Sprints" (that then

roll up into “Epics”). Sprints are often only a couple of weeks in length, with several Sprints in each Epic.

By approaching your identity security program in this fashion, you hit milestones early and often, allowing the organization to celebrate wins throughout the process. Plan minimum-viable-projects (MVPs) and a staged rollout over time. This phased approach helps ease your change management efforts.

Large, sweeping change that radically alters how the business functions is incredibly difficult to pull off. The classic all-or-nothing cutover approach takes time, prolongs costs and migration pains, and increases the likelihood of needs changing before you realize any benefits. But if that large, sweeping change happens over time, bit-by-bit, it’s a far easier pill for the organization to swallow.

By breaking the initiative into smaller phases, it’s important to understand that you’ll have two identity programs running concurrently in your organization. But, this is a good thing. Not only will this approach let you turn on specific features and processes as they’re ready, it’ll let you use the pain your users have with your current systems to keep informing your efforts and help encourage adoption.

Learn from and lean on the community

Up to this point, the organization has done a lot of work hiring the best people for their respective roles: identity, IT, finance, etc. But as good as they are, you can’t expect your team to know everything. Many different identity-focused communities exist, each with have hundreds (or thousands) of years of collective experience in them.

As you’re building out the program, find, learn from and then lean on these communities to make your identity security program the best it can be. Test out your theories for what’s possible. Get a second (or third or fourth) pair of eyes on your timelines. Have them find what’s potentially missing. There are lots of other leaders just like you that have undertaken this process before; learn from their successes (and missteps).

In addition to designated communities, analysts such as Gartner, KuppingerCole and Forrester all have dedicated experts that live and breathe identity. Their analyst reports have valuable insights and analysis that you can use to build a more robust identity security program — and know which vendors are delivering the best solutions.

Finally, take advantage of package offerings from partnered service and implementation providers. As you're evaluating potential identity security vendors, see who they work with. Having a partner to help you through the entire process and take some of the weight off your team's shoulders — while also providing valuable expertise and insight — and can make the entire program more efficient.

Don't copy and paste

If there's ever a time to abandon the saying, "If it ain't broke, don't fix it," now is it. Remember, your legacy identity governance platform brought you to this point because something is broken. Take advantage of the situation to understand your entire identity program and design your ideal state.

Remember to include people, process and technology changes while revamping the program, and keep in mind that your organization may follow a particular protocol as a workaround for a system you may not even have anymore. It's tempting to make this process a quick as possible. And while expediting migration and implementation is admirable, don't just transfer "as is" legacy processes to your new platform. You'll end up disappointed and fall short of what's possible with modern identity security.

For instance, many companies have a habit of running access certifications quarterly or half-yearly. Instead of mimicking this in a new environment, be aware of optimization opportunities like triggering immediate access certifications, or "microcertifications" around critical identity or joiners-movers-leavers events.

Have a post-migration strategy

Once you finally switch off your legacy identity governance platform and pack it all up, your identity security program isn't over. As organizational needs evolve and the world around the business changes, you will need to revisit the program to ensure it's achieving the goals you set. At the same time, start diving into what else you can do with your newfound capabilities.

It may be helpful to schedule standing review cycles or regular retrospectives (another beneficial aspect of Agile) to review the program's success. You will almost certainly identify necessary changes — and that's a good thing! While you shouldn't aim to change program aspects "just because," you shouldn't keep them the way they are for the same reason.

Remember, the key to success will be to refine processes and workflows as time goes on rather than switch everything out in one go.

What's Required of Modern Identity Security?

For your identity security program to succeed, you must build it on the right foundation. As you evaluate potential identity security platforms, it's crucial to identify your organization's required capabilities based on your program and business goals. That said, the more successful identity security deployments have platforms with the following capabilities.

Converged, but extensible

One of the main issues with traditional identity tools is they require an entire tech stack to be built around them. With every deployment, new holes in the perimeter open, with new tools following suit to patch them. Your modern identity security platform must be a converged platform that can streamline identity governance, application access governance and privileged access management.

It should centralize your identity efforts across every environment you use: on-premises, public and private clouds, and hybrid environments. By converging identity security into a single platform, you get one control plane that manages all identities (including workforce, external and non-human identities), applications and systems across your entire tech stack.

But the platform you choose mustn't be a "jack of all trades." It should be focused on identity security while allowing you to extend its capabilities to enable governance for every part of your organization. With converged identity security, you reduce the complexity of your tech stack while improving your overall security posture.

Cloud-native

As organizations continue in their digital transformation journey, one thing has been made abundantly clear: the future of business is in the cloud. There are any number of reasons why enterprises may hold onto their on-premises solutions, but the fact is: traditional environments' time is limited, and this includes legacy identity governance tools.

As you look to the future, you need something that is resilient, scalable and flexible. A platform that doesn't rely on your office's space or power and is always up-to-date. And it shouldn't be a "solution" that was merely ported from its elder on-prem sibling with a tenth of its capability.

Instead, make sure you look for a platform that was built in and for the cloud. With all the features and functionality you require — including all the necessary industry certifications — while being flexible enough to adapt to changing needs.

Intelligent

Sometimes artificial intelligence may feel like a buzzword, but ensuring AI is used productively in your identity security platform will only help you. With an intelligent platform, you can be sure your teams are making more data-driven, informed decisions. The more advanced identity security platforms even provide recommendations for actions to take in regular functions such as certification campaigns.

Intelligent identity is all about augmenting your team to be more secure throughout their interactions with the platform and eliminating the slow, manual and risky processes that so often open your enterprise to threats. It's making the right decision the easy one, while giving your identity team complete visibility and AI-powered data analysis to create and enforce consistent and efficient policies at scale.

With AI and as it continues to evolve, it will learn from your data, proactively alerting you to risky behavior or combinations of access (e.g., segregation-of-duty risks). An AI-powered identity security platform can create dynamic peer groups based on key identifiers such as location, role or department to make access governance simpler. Intelligent identity makes your organization smarter, safer and grow past what you previously thought possible.

Customer-first

Pretty much every vendor will label themselves as customer-first, so this aspect will be a little tougher to accurately judge. Of course you want a solution that will be with you for the long haul; one that prioritizes innovation in conjunction with its customers and places great importance on fostering collaboration in a large ecosystem of partners and advisors.

In your search, look for a platform that is loved by its users. Your first stop will likely be review sites. As you peruse, remember to get full context: star ratings, reviews, and most importantly, awards. Feel free to tap into the identity communities we mentioned earlier, too, so you can get opinions from others who have undergone similar migrations.

When you reach conversations with a potential vendor, ask to hear what successes their customers have experienced. These proof points are invaluable for weeding out the platforms with great marketing, but a not-so-good product. Then, learn what they offer in terms of support. Top-tier identity security vendors will have expert guidance and services available so you can be sure you're maximizing your investment.

Take the First Step

Change isn't easy — but anything that delivers an impact never is. Transformation demands agility, scalability and improvement, and you shouldn't let outdated, traditional platforms and mindsets limit your pursuit.

To help you on your path to modernization and guide in your search for a platform and partner, check out our **Buyer's Guide to Identity Security.**

Saviynt™

Saviynt's AI-powered identity platform manages and governs human and non-human access to all of an organization's applications, data, and business processes. Customers trust Saviynt to safeguard their digital assets, drive operational efficiency, and reduce compliance costs. Built for the AI age, Saviynt is today helping organizations safely accelerate their deployment and usage of AI. Saviynt is recognized as the leader in identity security, with solutions that protect and empower the world's leading brands, Fortune 500 companies and government institutions. For more information, please visit www.saviynt.com.

Saviynt™

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

310.641.1664
info@saviynt.com
www.saviynt.com