SailPoint

Sixth edition

The ultimate guide to unified identity security

How to elevate your security posture with strong identity security - no matter your starting point

Table of contents

Identity security—the core of your business operations

Business leaders across industries are recognizing that managing digital identities and their access across the organization today is essential to securing the business and providing the agility the business needs to unlock its full potential. Effectively managing identities is critical to enabling seamless collaboration with business partners, streamlining operational efficiency, complying with rising cybersecurity and privacy regulations, reducing risks, and recovering from cyberattacks.

Identity security (also known as identity governance and identity management) protects organizations by discovering, managing, and securing technology access for a diverse workforce of digital identities. Digital identities include humans—employees, contingent workers, customers, business partners, etc.—along with machines such as RPAs (Robotic Process Automation aka bots) or OT/IoT devices.

These identities connect to upwards of billions of technology access points, all with varying levels of access requirements that evolve as the needs of the business change. Identity security ensures that each identity has the access needed to do their job – no more, no less. With the right access, the identity can continue its digital journey with permission to access data, applications, systems, cloud platforms, and other resources.

Identity security puts an emphasis on enablement, security, and compliance, which means not only providing access but also properly controlling that access.

This guide is designed to help you understand what to look for in a solution that can move your organization towards a more mature identity security program. You'll find help defining the specific business goals you most need to achieve, understand the right questions to ask, and identify the pathways that will help you achieve quick wins in strengthening your identity security program.

You'll discover what it takes today for a solution to achieve the goals you set, as well as what to look for in a vendor that will maximize your success. Finally, we wrap up with a quick introduction to SailPoint's identity security solutions.

We hope you find reading this guide, and the associated **The ultimate guide to unified identity security addendum**, a useful step on your journey to a future-proof and successful identity security program. Give us a call or visit **www.sailpoint.com** when you're ready to move ahead.

The need for developing a long-term, sustainable identity security program

Having a mature, modern identity security program has a real impact on almost every threat vector in your business because it weaves through all of your business applications, infrastructure and critical data, which makes it relevant to all the stakeholders you need to approach to get buy-in.

The changes impacting an organizations security are all around us. The boundaries of a globally connected enterprise today extend well beyond the datacenter. The shift to work from anywhere and cloud-based services means more critical business operations are being conducted outside the corporate network. The proliferation of mobile devices enables anytime/anywhere access, and business partners and customers expect on-demand access to corporate applications and data. As the enterprise security perimeter evolves, identities are the new corporate firewall.

Additionally, organizations face greater risk as cybercriminals have more opportunities than ever to infiltrate their business. We've seen an explosion both in cyber threats—including software supply chain attacks, ransomware, advanced persistent threats—and ever-changing international, federal, state, local and industry-specific regulations.

An identity security program must address the immediate, tactical needs of the organization; at the same time, it must be sustainable, part of a strategy for long-term business improvement. Identity security is essential for managing user access to applications, systems, data and cloud environments, without compromising business agility, inhibiting worker productivity, or violating compliance regulations.

Here are some of the questions that will help everyone responsible for identity security — from the senior leadership team to those working directly in security or in IT supporting security — determine how well your current identity security program is meeting the challenges faced by your business including around the **4 identity maturity vectors** of strategy, operating model, technology/tools, and talent.

- **Does our identity security program align to the overall business strategy**, so that it is understood and utilized across the organization?
- **Do we have a dedicated team** to centrally manage our identity infrastructure and operations?
- **Does our model allow us to centrally manage access** for our identities or is management done in siloes, or maybe not at all?
- **Are we confident we have a comprehensive view of all identity access** (employees, non-employees, and machines) across all applications, systems, cloud, and data?
- **Have we eliminated time lags and unnecessary cost** from the way we now manage the security of identities and access rights by using automation to adjust access as users join, change roles, take on new projects, or leave the organization?
- **Do we have the right technology needed** to help decrease risk posed by human actions such as phishing, malware, employee access to sensitive information, and insider data leaks?
- **Are we satisfied with our current capabilities** in connecting and integrating our growing set of cloud and SaaS solutions for maximum security?
- **Are we certain we have minimized the error and risk in the way we manage identities** and access rights—things that can expose the organization to business, brand, and financial risk?
- **Have we achieved the right balance** between giving workers access that maximizes their productivity and minimizes risks like overprivileged, conflicting or compromised access?
- **Are we enforcing a proper least privileged access model,** so that people have only the access they need to perform their job at the time they need it, reducing the exposure of sensitive data and the impact of a cyberattack?
- **Are we confident we are complying with all regulatory requirements** and providing proof-of-compliance?
- **Are we able to satisfy requirements in our cyber security insurance policy** and are we confident we will be covered in case of breach?

Identify business priorities and establish clear business goals

As you've discovered by now, identity security is a strategic imperative for organizations of all sizes. Companies ranging from large, multi-national enterprises to mid-sized enterprises and smaller, fast-growing businesses must address requirements to protect and govern access to critical applications, systems and data whether in the cloud or on-premises.

Identity security plays a critical role in enabling organizations to inventory, analyze and understand the access privileges granted to all of the identities associated with employees, contractors, vendors, service accounts and even software bots in order to answer the critical question: "Who has access to what data?"

At the same time, today's agile enterprise demands faster and higher levels of service delivery across an increasingly diverse and dynamic environment:

- New users come on board daily, requiring immediate access to enterprise resources.
- Users' roles and responsibilities change, or their relationships with the enterprise end, and access must quickly be modified or revoked.
- Some applications and users represent a higher level of risk to the organization than others and require more focus.

The challenge becomes how to meet service-level demands while identifying and managing high-risk activities, enforcing policy and security, maintaining stringent controls, and addressing compliance requirements.

Because there are many different business drivers for identity security, you may wonder how and when to put the different components of a solution in place. How do you identify outcomes worthy of investment? The answer depends on your business priorities and the immediate challenges facing your organization.

To get started, step back and assess your most urgent issues. Do you understand what you want your solution to help you achieve?

Here are some common business goals that can help you determine your own unique priorities:

1. Speed up delivery of access to business users while freeing up IT staff
2. Increase user productivity – no matter who, what, or where they are
3. Reduce cost, complexity, and human error by automating identity processes
4. Centralize access controls and policies across the organization
5. Manage fine-grained access across on-premises and cloud applications
6. Eliminate audit deficiencies and improve audit performance
7. Lower the cost of compliance
8. Replace an existing provisioning system

Let's look in more detail at each of these business drivers for identity security — the goals organizations most frequently hope to achieve with their implementation.

1 Speed delivery of access to business users while freeing up IT staff

In the average enterprise, the process of providing people with the right access to perform their job is still one that requires a lot of manual steps and IT involvement. Given the fast-paced and dynamic environment of business today, enterprises are handing out more access than people need, which compromises their security and hinders compliance efforts. Business users cannot wait days or weeks for access to systems required to perform their job duties. Onboarding new users needs to happen Day 1. Similarly, organizations cannot tolerate huge gaps in deprovisioning access when a user changes positions or leaves the organization.

Changes to user access must be performed in near-real time, with minimal IT intervention, while remaining a controlled and auditable process that is visible to the business. The current state of identity security in most organizations makes it almost impossible to provide consistent and effective service levels to the business due to the following challenges:

- Heavy use of disparate manual access request and change processes
- Lack of end-user participation and visibility into identity management processes
- Ad hoc methods for dealing with external identities and their access rights
- The growing number of cloud-based applications that are managed outside of IT
- Help desk staff that is over-burdened with access request and password resets

What organizations need is an easier, more cost-effective way to deliver the right access to the right users and, at the same time, deliver a strong identity security posture to the business. With the right self-service tools, business users can manage their own access, from requesting new access or roles to recovering forgotten passwords, using intuitive, business-friendly interfaces. In addition, today's user provisioning solutions offer easy-to-configure options for automating the entire access lifecycle of a user based on information from authoritative sources such as your Human Resources systems and changes in roles. Minimizing the need for manual changes frees up IT staff for more strategic work.

By providing an integrated approach that leverages business-friendly, self-service access request tools and automated lifecycle changes, identity security solutions with intelligence and automation at the core can streamline the delivery of user access across your organization while continuously enforcing least privilege, governance rules, and compliance policies. Business users become active participants in the process, managing their own access and passwords, monitoring the status of their requests, and modeling their access as required in an agile business environment. All without slowing IT down or otherwise frustrating these processes, resulting in a significantly lower workload of help desk and IT operations teams.

2 Increase user productivity – no matter who, what or where they are

Whether you're managing the identities of internal users (employees, contractors, and bots) or external users (supply chain partners, agents, volunteers), you want to implement technologies that reduce the burden of granting the right access to the right data for all types of users. Having the right identity security strategy will reduce internal costs and improve productivity, but it can also contribute to revenue growth and profitability.

Today's workers want access anytime, anywhere, via any device. Every minute that a user has to spend waiting for access to be granted or changed, retrieving a lost password, or having the help desk reset a password is an unproductive minute — and when you multiply the growing number of applications by the amount of time wasted, the high price of inconvenience becomes pretty clear.

Here are some questions you should consider as you plan your strategy to ensure your identity security solution delivers convenience and improves user adoption and productivity:

- **Do you make it as simple as possible for new users** to get access to your business systems — even if they have no prior relationship with your organization?
- **Are you able to give fast, secure access** to the full range of applications, systems and data that each individual needs in their specific job function?
- **Are you providing your users with rich self-service capabilities** that provides the business the flexibility and security they require?

3 Reduce cost, complexity, and human-error by automating identity processes

Managing the complex relationships between thousands of users and millions of access privileges continues to be a daunting and expensive task for most organizations. For many, changes to user access are initiated, approved, and implemented using fragmented, disjointed processes. Coupled with the fact that in most organizations, the processes and tools used to request or change user access are highly manual. The result is an inefficient, error-prone, and costly execution of access requests and changes. The reality is that this has moved well beyond human capacity and is consuming a lot of IT staff.

Does your organization wrestle with the following problems when fulfilling access changes across enterprise IT systems?

- **Multiple front-end processes** are used by the business to request new or change existing access privileges
- **Manual processes** are required to facilitate changes to user access
- **Heavy reliance on help desk or IT admins** to assess and implement access changes
- **Different provisioning/deprovisioning** processes are used for different applications

If these situations sound familiar, it's time to take a new approach. You need to centralize the delivery of access across disparate IT resources spanning both the datacenter and the cloud and reduce the costs associated with managing the initiation and fulfillment of access requests and changes. The right identity security solution automates identity lifecycle events, such as onboarding new hires and managing job transfers, by directly assigning or changing roles and entitlements to match a user's current job function. It also automates the offboarding process to remove access privileges upon termination. By automating these events, organizations can effectively discover, manage, and secure user access at scale; and reduce the number of self-service requests initiated by business users, the number of approvals required to grant access, and the number of calls to the help desk to fulfill these changes. Automation not only frees up IT staff but can also help significantly minimize risk that comes from overprovisioned user access and manual, error-prone provisioning processes.

4 Centralize access controls and policies across the organization

The modern enterprise is a digital ecosystem with workflows driven by diverse applications and data stores used by employees and third parties with different access rights.

You want this rich ecosystem to promote greater productivity with smooth connectivity between all of these elements—but not at the risk of compromising the security of business-critical applications and sensitive data. When identity security management is highly fragmented, the risk of error and abuse increases.

Decisions about who has what level of access across different applications used by the organization become complicated when tied to roles that can change frequently and require context to get right. For some organizations, providing that context requires time-consuming, costly custom integrations and development whenever new applications are onboarded. And then retesting every time applications are updated.

Here are some questions you should consider as you plan your strategy to ensure your identity security solution reduces the effort and cost of controlling access across your organization:

- **How does the solution enable you to better centrally manage and control all access and identity types** across the organization according to your policies?
- **Can it incorporate new access rights** into the existing role model to keep roles current?
- To what degree does it allow you to **centralize access controls and policies?**
- **How does it make it easier to incorporate identity functionality into applications** users rely on every day, even as they change roles?
- **How does it reduce the effort required to ensure new applications give the right access** to the right people so that you begin to realize the value-add of those applications as soon as possible?

At the heart of a mature program is an identity security solution with centralized policies and controls providing 360-degree visibility to “who has access to what” for all resources — across your entire digital ecosystem. This helps secure the extended enterprise by placing the responsibility and control where it belongs.

5 Manage access across on-premises and cloud applications

While many companies no longer have local data centers, they typically do have legacy applications they have simply moved into the cloud, replacing one virtualization environment for another. Hosting a legacy system in the cloud doesn't make it a modern application; the same requirements still apply when it comes to managing access and governance.

Adding to the complexity of this environment, business units are gaining more autonomy to buy and deploy applications — which can often house sensitive, corporate data — without consulting or involving the IT organization.

Here are some of the signs that your organization may be struggling to manage new cloud applications:

- **IT is not fully aware of the mission-critical cloud applications** in production across various departments and business units.
- **Business units are performing their own user administration** via spreadsheets and manual updates.
- **Business units are requesting that IT integrate cloud applications** with directories for periodic synchronization.
- **Business units are purchasing their own identity and access management solutions** — without consulting IT or considering what identity security infrastructure is already in place.
- IT audit processes, such as access certifications, **have not been extended to cover cloud applications.**

A mature, modern identity security solution should help enterprises embrace the cloud while at the same time allowing the IT organization to effectively apply centralized identity security policies, detect violations, and demonstrate full regulatory compliance. Successful identity security solutions will allow you to automate compliance and provisioning processes for cloud applications in the same manner as on-premises applications.

6 Eliminate audit deficiencies and improve audit performance

Identity security is a focal point for IT audits and one of the areas most commonly flagged for ineffective controls. During many audits, weak identity controls often receive negative audit findings in the form of control deficiencies or material weaknesses. And audits are more abundant with more regulations affecting companies than ever before. Sarbanes-Oxley (SOX), GDPR, HIPAA, and CCPA are just a few of the many regulatory frameworks out there.

Here are some of the most common identity risks which flag the attention of auditors:

- **Orphan accounts:** Access that remains active for employees or contractors after termination due to failure to remove privileges.
- **Entitlement creep:** The accrual of privileges over time through transfers, promotions or other changes in roles resulting in employees with access beyond their job requirements.
- **Separation-of-duty (SoD) violations**: Inappropriate access resulting in excessive control over business transactions or the ability to perform conflicting duties (like accounts payable and accounts receivable).
- **Poorly managed privileged user accounts:** Shared accounts that are typically the domain of privileged users are managed using manual processes and are very difficult to audit.
- **Lack of visibility into access by job function:** Business users struggle to interpret technical IT data to make business decisions about what access is required to perform a specific job function.

There is another common identity risk that arises a number of times during the year. Business managers get a list of entitlements to review and certify for his/her team. Without context, and to speed the process, many of them are rubber stamping and approving everything, fearing that they may accidentally revoke the needed access for their employees. As a result, over-provisioning occurs, increasing the potential attack surface. Risk of non-compliance increases as well.

If you've failed an audit due to weakness around any of these identity risks, we have good news. The right identity security solution will improve your visibility into risky or non-compliant areas and automate your processes for managing these risks. An enterprise-wide view of your identity data and AI-enabled access recommendations can help you to effectively analyze risk, make more informed access decisions, and implement the appropriate controls in an automated and more sustainable fashion.

Further, aligning user access with job functions through role modeling strengthens user access controls by providing valuable business context around how specific sets of access map to the underlying business function being performed by an individual. Roles significantly reduce the number of individual access rights to be reviewed and highlight additional access granted outside of the role model (exceptions). This leads to greater accuracy and better decisions, resulting in less chances of negative audit findings or failing another audit. It is also an important requirement and enabler for realizing the benefits of automation.

7 Lower the cost of compliance

Compliance can be complex and difficult — and as a result, costly. Meeting industry and regulatory mandates requires organizations to regularly review and certify user access privileges. This leaves many companies constantly battling with error-prone and inefficient processes such as manually generating access reports and manually remediating inappropriate user access privileges.

Signs that show you need to simplify compliance processes and reduce compliance costs include:

- **Building or leveraging multiple**, homegrown solutions to handle audit and compliance needs
- **Hiring full-time staff or consultants** to handle compliance projects like access certifications and SoD policy enforcement
- **Requiring application owners to manually export** and then format data for the next audit
- **Using inefficient tools like spreadsheets and email** to drive manual compliance processes
- **Treating high-risk and low-risk users** the same, where insufficient attention is given to high-risk users, or spending too much time and effort on low-risk users

To gain better control of your identity data, you need to replace expensive paper-based and manual processes with centrally defined policies and automated access certification processes. By doing so, not only can you significantly reduce the cost of compliance, but you can also establish repeatable practices for a more consistent, auditable, reliable, efficient, and easier-to-manage access certification effort.

If you struggle to effectively implement compliance processes and integrate them into your systems and infrastructure, a modern identity security solution is the launching pad you need to improve your effectiveness and reduce the costs of sustainable, continuous compliance.

8 Replace an existing provisioning system

Many organizations have one or more legacy user provisioning solutions that no longer meet their needs, doesn't do what the vendor promised it would, or more importantly, is already, or will no longer be supported in the future.

Do you find yourself facing any of the following issues with your existing provisioning solution?

- Your project is behind schedule and over budget.
- You lack the necessary coverage for applications.
- You spend a lot of time and effort creating and then maintaining "custom" connectors.
- You spend more time on managing and maintaining the environment then on actually using the solution.
- Updates and upgrades are expensive and time consuming, especially when the solution has been customized.
- Your provisioning product is being "retired" and must be replaced.
- You have compliance weaknesses related to ineffective off-boarding processes, entitlement creep, SoD violations, and more.

Now is the time to address those issues and migrate away from your legacy provisioning platform. Invest in a technology that will address your current and future provisioning challenges, improve your overall identity security strategy, integrate with all the systems you need to integrate with, and never requires you to perform another upgrade. Look for a solution that will provide your organization with a smooth transition and allow you to take a non-disruptive, stepped approach while making the most of your existing investment as you transition to a next-generation solution.

The new solution must also be able to balance core user provisioning requirements — add, change, delete user accounts and password management — with user-friendly interfaces and processes that empower business users to request and manage access on their terms. A solution that leverages AI to automate these processes is ideal for not only improving IT efficiency but also significantly minimizing risk.

Finally, and most importantly, it must offer an integrated approach to identity security. Governance and compliance should be handled as an integrated activity within your identity infrastructure, not as separate processes.

Choose an identity security path with the strongest returns

Now that you've identified your business goals for improving identity security, you'll want to consider the steps you need to take to achieve them. You have several pathways to choose from, and you can prioritize them based on the unique business requirements and goals of your organization. In this section, we outline how to maximize your success in the shortest amount of time to achieve quick wins while laying a strong foundation for a future-proof identity security program.

Find your starting point

Once you've agreed upon your top priorities and goals, you will have a better understanding of what you must achieve first. By focusing on a few "quick win" opportunities, you can help accelerate and build momentum for future phases of your projects.

An incremental approach to project implementation helps you focus, ensuring you tackle high priority applications and user populations that are most affected by your stated objectives. By demonstrating small, quick wins up front, you will build confidence in the solution, help ensure ongoing adoption, and make it easier to secure funding for additional projects.

Starting point: User access

If your organization struggles with inefficient and/or non-compliant processes for granting new access privileges or making changes to existing access privileges for employees and non-employees including contingent workers, contractors, and partners, then it may make sense to focus on automating on-boarding, off-boarding and changes in-between.

Here's how to get started:

1 Enable self-service access request

One of the best ways to get started with improving user access is to focus on the business users first. Empowering business users to find and request access without assistance from the help desk or IT admins can save headaches and money at the same time.

2 Automate access fulfillment

Another quick win is to automate the fulfillment of access requests with AI-powered recommendations. You can maximize the cost savings generated by initially focusing on a few high-churn applications where user accounts are created, updated, or deleted on a regular basis then extend to all apps from there.

3 Automate access assignment

The largest return on investment is realized by automating assignment of access. This process can leverage identity data from your HR systems or other authoritative sources to completely automate the assignment of access for both human and non-human identities.

4 Streamline password management

Password management provides a quick path to the success of your identity security project by allowing end users to reset forgotten passwords and bypass the help desk. Using the same business-friendly user interface, users can change or reset passwords across target systems.

Starting point: Compliance

If audit deficiencies and the high cost of compliance are top of mind issues in your organization, then you may want to focus on compliance automation initially. You may already be in the process of establishing a "least privileged access model" as required by many regulatory frameworks as well as being a key element of enforcing a Zero Trust approach to identity security. With least privilege, you ensure that people only have the access they need to perform their job function so that if an identity or an account is breached, the exposure of such a breach is limited to the access that person was supposed to have, rather than over-privileged access users frequently have, which could lead to higher fines and more exposure.

Here's how to get started:

1 Gain centralized visibility

The starting point for any compliance project should be to understand the current state of users by getting a central view of identity access across the organization. This stage involves creating a single repository for user and access information by integrating with and aggregating data from your authoritative sources, such as HR systems and contractor databases, and target resources.

2 Identify and close all orphan accounts

Finding and eliminating orphan accounts is one of the most effective risk mitigation steps you can take in your compliance project. Once you've identified these high-risk accounts, you can launch remediation actions for all unowned accounts — remove, mark as service, or, where possible, correlate to known identities.

3 Detect and remediate outliers

The next step in the data clean-up process is to identify outliers: users that have significantly different access from what can be expected. As you build the business case for your identity security program, look for a solution with AI which can spot risky users and access outliers and significantly strengthen security by helping to detect and remediate vulnerabilities.

4 Automate access certifications

Next, generate a certification campaign that can help automate access reviews for all users. Today, your team can be assisted by recommendations fueled by AI which simplify and shorten the certification review cycle. Your team will easily know whether or not it is safe to approve or deny access. Initial certifications should be used to establish a reliable baseline of data.

Starting point: Mitigating cyber risk

As work environments get more complex and continue shifting to the cloud, attackers are increasingly targeting identity as a vector. Data breaches pose a serious risk to the enterprise, with consequences ranging from financial loss to reputational damage and downtime. If you have recently suffered a breach, you know first-hand it takes just one compromised identity to potentially cost an enterprise tens (to even hundreds) of millions of dollars in lost revenue and regulatory fines.

Taking a siloed, manual approach to managing and governing access is the greatest threat to your company's hybrid, multiple-application business systems. Not unifying identity security controls and SoD monitoring across SAP ERP, S/4HANA, and other apps in your business ecosystem can result in costly and damaging fraud, data breaches, and audit deficiencies. This is why organizations must put proper cyber risk mitigation strategies in place to protect against such an event.

Here's how to get started:

1. **Stay ahead of risk** by identifying SoD violations and sensitive access risks across ERP systems. Look for on-going risks by user, role, and business processes. Automated and AI-informed identity security solutions can give you the visibility and actionable information you need to gain deep visibility and analysis of a user's access history.

2. **Leverage AI** to help you detect and prevent toxic access combinations that could lead to fraud or data theft. AI makes it easier to identify risks at scale and monitor behaviors helping you to build a more resilient organization.

3. **AI can also help you identify and prevent access risk** before provisioning and have the intelligence needed to run "What If" scenarios. Put in place a process to elevate or grant emergency access with automated controls and streamlined reviews.

4. **Automate workstreams for administrators and reviewers** to ensure periodic access review cycles. Keep your entire team — IT, audit, compliance, security business owners, and board members — continuously informed of threats with reports.

5. Longer term, **make cyber risk mitigation a part of security design**, implementations, and remediation activities.

Starting point: Data governance

Most corporate data stored in cloud-based file-sharing services like Box, SharePoint, and Google Drive, is subject now more than ever to increasing attacks, including insider threats. If your organization struggles to understand what sensitive data and PII data is stored in files across your file systems (for example, inside Microsoft Teams or Box folders and SharePoint sites), then it makes sense to start with Data Governance.

Here's how to get started:

1. **Make sure you know where your sensitive files are stored,** including reports out of your finance system and intellectual property. If your marketing department has ever exported significant amounts of customer contact details for a campaign, do you know whether they have been properly handled afterwards?

2. **Update your knowledge on who has access rights** to unstructured, regulated, and sensitive data. You should be able to monitor, control, and certify who has access to this data and understand why this is the case.

3. As mentioned under compliance, **tighten access controls:** Remove over-privileged or unused access, monitor for malicious activity, and automatically take corrective action in real-time. Certify data access to meet compliance and audit requirements.

The big picture: What does it take to reach your goals for improved identity security?

Before starting to evaluate the details of individual identity security solutions, you can make your buying journey a little smoother by understanding the "big picture" of what's required to meet your strategic business goals. There are three key areas of capability that are table stakes for leading identity security solutions today.

First, they must help you achieve a much deeper level of visibility and intelligence into the access rights that are available, giving you the insight needed to ensure that you can remediate unneeded access and ensure the security of every identity:

- Collect the right data on each identity (human and machine) to better assess what they currently have access to, how access is being used, and what they should have access to – driving smarter, more context-aware identity decisions.
- Easily understand, report on, and dynamically manage critical identity security policies across today's ever-evolving enterprise environment.
- Gain a 360-degree view across all identities and their access, leveraging this intelligence to detect and address access anomalies, prevent toxic access combinations, and reduce access risk while securely enabling the business at speed and scale.

Second, to successfully streamline identity processes to better discover, manage, and secure user access and free your workers to focus on innovation, collaboration, and productivity, an identity security solution must enable you to:

- Replace manual processes with automated, intelligent workflows to ensure timely, optimal access to essential business resources and data.
- Apply technologies like AI and machine learning to monitor your organization as it evolves – enabling you to autonomously adapt access models and policies so your security stays up to date and compliant with company and regulatory requirements.
- Simplify the administration of identity security programs by automating important identity decisions like access requests, role modeling, and access certifications, saving time and freeing up IT teams to focus elsewhere.

Third, the solution must extend your ability to embed identity context across your hybrid environment and centrally manage and control access to all data, applications, systems, and cloud infrastructure:

- Seamlessly integrate with existing business and security systems to infuse identity context and decisions into the everyday workflow of the business, creating a frictionless, user-centric experience that improves time to value.
- Build a strong security fabric by embedding identity data across your enterprise for holistic visibility into technology access and usage.
- Centrally manage and control all access and identity types across all applications with a robust policy engine to enable a holistic security and compliance strategy.

Combined, these three areas of capability enable an enterprise to:

- Secure and support the next generation of business tech transformation and innovation programs, as well as mergers and divestitures, with "built in" flexible, scalable enterprise identity controls.
- Dramatically improve operational efficiency and reduce costs associated with security operations.
- Mitigate the risk of crippling fines, disruption to business operations, and public loss of reputation due to regulatory non-compliance.

Framing the big picture: Ensuring your identity security program succeeds

As your experience with identity security solutions has probably shown, technology is only part of any solution you implement. When you partner with a vendor for products and services that have value, look for a customer success management function that can support you every step of the way.

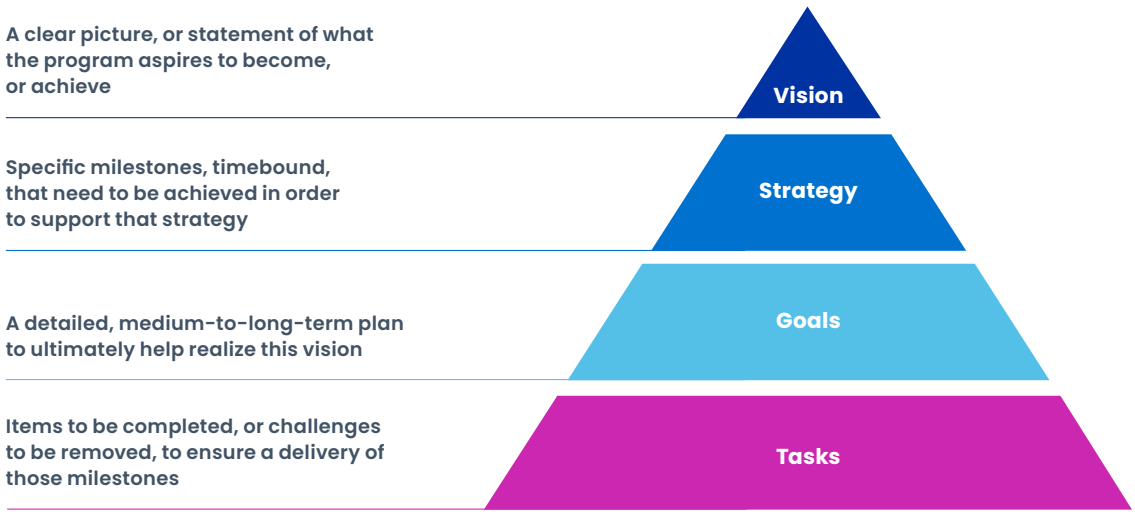
How does your vendor define customer success?

- As your partner, they should offer a bespoke engagement structure to ensure you stay on track in achieving your desired business outcomes in a holistic business case for identity security.
- You should expect them to act as an advisor, understanding and supporting your identity security business case, developing an effective engagement model that fits.
- Key elements you should look for in a customer success management program are threefold:

1 A Customer Success Manager, with an option to pick from shared pool or named CSM, who can leverage the vendor's:

- **Learning programs**
- **Technical advisors**
- **Consulting teams**
- **Product insights**
- **Value assesments**
- **Peer-to-peer events**

Customer success plan: Making the connection between vision and tasks



2 A personalized customer success plan (CSP) that:

- Clarifies your vision and value picture for identity security, reflecting goals of key stakeholders (e.g., Cybersecurity, IT leadership, Auditors, Regulators, Finance)
- Establishes tangible measures and milestones
- Documents an agreed-upon engagement structure to ensure progress, for example:

  Digital: Web-based engagements, best practice sharing, scheduled outreach, virtual event invitations with options for additional services, and problem triage.

  Medium-to-High touch: Detailed customer success plan, CSP reviews, forward planning and risk mitigation, problem triage, and get-well planning.

  High-touch: More frequent CSP reviews, strategic planning, monthly check-ins, exposure to vendor roadmap, customer advisory board facilitation (CAB), executive sponsorship.

3 Verified outcomes that help you show the return on your company's investment in terms of:

- Improved compliance and reduced effort that is expended on internal audits
- Improved productivity through faster provisioning of new user access
- Faster ability to detect and respond to cyber-attacks
- Significantly reduced access risks by eliminating lag in deprovisioning worker accounts
- Reduced help desk costs through automating previously manually processed helpdesk tickets such as self-service access requests and password resets

Where are you in your identity security journey?

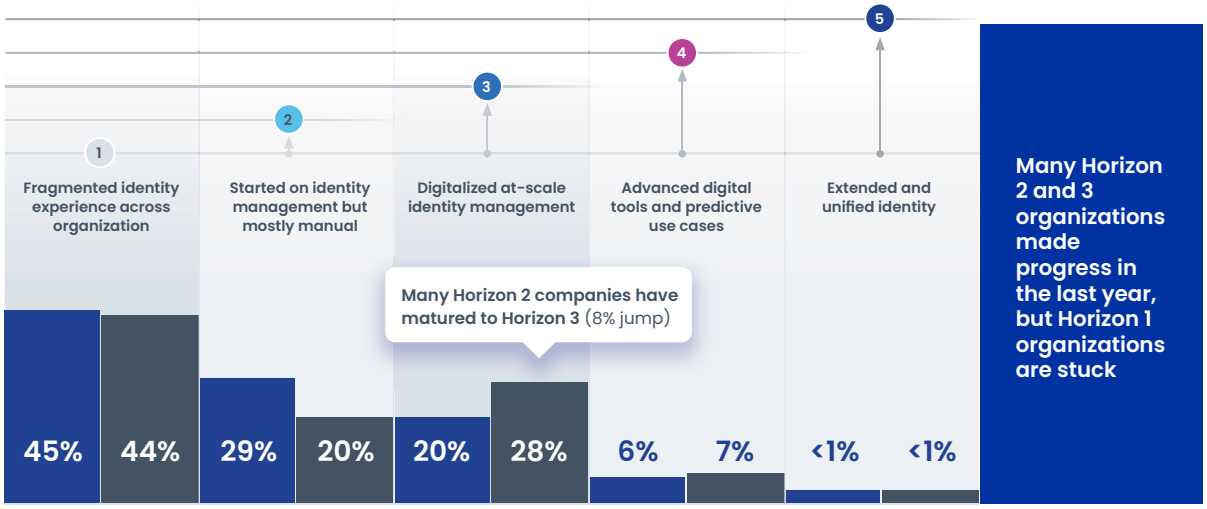
The 2023-2024 Horizons of Identity Security Report gathered insights from identity security decision-makers, including CIOs, CISOs and Directors of Identity, from more than 375 companies across the globe.

Organizations were grouped into five horizons based on their strategy, talent, operating model, and technology capabilities:

- At Horizon 1, the lowest maturity, companies lack the strategy and technology to enable digital identities
- Those at Horizon 2 have adopted some identity technology but still rely heavily on manual processes
- Organizations at Horizon 3 have adopted identity capabilities at scale
- Those at Horizon 4 have automated at scale and use artificial intelligence (AI) to enable digital identities
- Horizon 5 is closest to the future of identity - serving as a critical control point in reducing cybersecurity risk and supporting business in next-gen technology innovation

44% of organizations are still at the beginning of their identity journeys

Comparing the identity landscape between now and 12 months ago, we found that nearly half of the companies we surveyed still have immature identity programs and are struggling to move beyond Horizon 1.



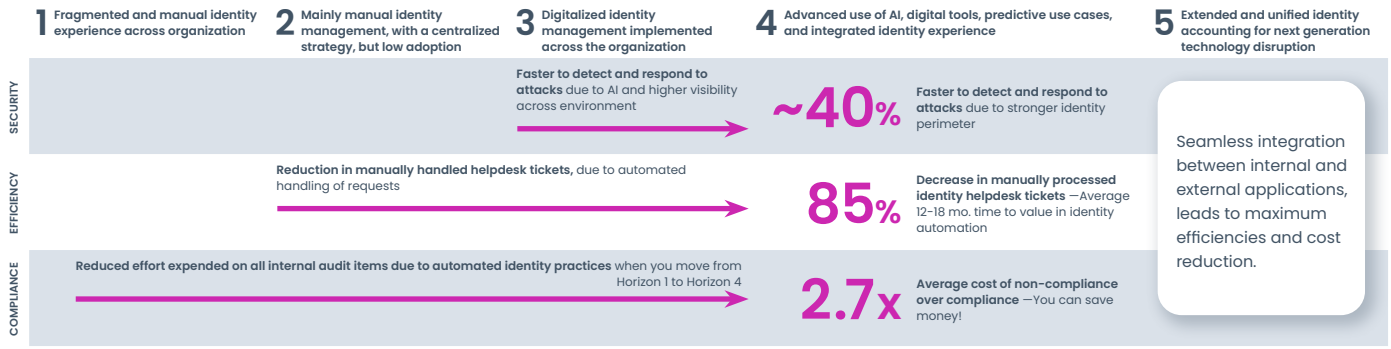
Most companies are stuck in Horizon 1 (44%), indicating that barriers at the beginning of the identity journey are hardest to overcome

Source: **The horizons of identity security**, 2023 - 24, SailPoint in collaboration with Accenture.

Given rising cyberthreats and accelerating digital innovation, companies need to do more to build capabilities in digital user identity.

Those further along in their journeys already consider identity security a strategic enabler to business innovation and security – and recognize the benefits of an advanced identity security program.

Customers improve their security posture and resilience as they advance through their journey



Top 10% **Most secure companies that have realized significant security benefits and increased resilience are the ones who invested in their identity security.**

Source: **Horizons of Identity Security**, SailPoint, 2022.

SailPoint is the core of identity security for the modern enterprise

SailPoint is the leading provider of identity security for the modern enterprise, enabling complex organizations worldwide to build a security foundation capable of defending against today's most pressing threats.

At the core of SailPoint Identity Security is artificial intelligence and machine learning. A foundation that protects organizations by automating the discovery, management, and control of ALL user access.

With SailPoint, you can ensure that each identity, human or nonhuman, has the right access needed to do their job – no more, no less. SailPoint provides, on average, a 345% ROI over 5 years. Successful outcomes from actual customer case studies include:

IT efficiency

90%

identity tasks automated and improved

Access certification

1 year › **1** month

New user access

14 hours to **2.5** minutes

Deprovisioning terminated accounts

30+

days to minutes

Self-service access requests

62K requests fulfilled automatically

0 help desk calls

Password resets

5.5K automatically preformed

0 help desk calls

Choose from our intelligent, autonomous, and integrated identity security solutions that best fit where you are in your identity security journey, matching the scale, velocity, and environmental needs of your business.

Looking for the market-leading SaaS technology that allows you to mature your identity security program at your own pace?

SailPoint Identity Security Cloud

With AI and machine learning at its core, SailPoint's Identity Security Cloud is a bundle of SaaS capabilities that deliver unmatched intelligence, frictionless automation, and comprehensive integration that allows enterprises to manage access across the most complex cloud environments.

Our experience working with leading global brands has provided insight into exactly what is needed today: targeted, organized SaaS-based products that work together as a single solution.

Choose the bundle that best fits where you are in your identity security journey.

Looking to start or reset an identity security program?

SailPoint Identity Security Cloud Business bundles all the core identity security capabilities that organizations need when starting or resetting an identity security program.

Access Requests & Approvals

Empower users and approvers with easy-to-use request tools.

Automated Provisioning

Give workers access wherever they are – automatically and securely.

Access Certifications

Prevent the risk of over-provisioning by revoking unneeded user access.

Separation-of-Duties

Detect and prevent conflicts of interest and potential fraud.

Access Insights

Get a complete view of access history, identify access outliers, and generate detailed access reports.

Recommendations

Use AI-driven insights to make better-informed access requests and decisions.

Take advantage of over 100+ out-of-the box connectors, a full set of APIs, event triggers, and additional capabilities to extend identity security across a hybrid environment.

Looking for more advanced identity security capabilities in a single SaaS solution?

SailPoint Identity Security Cloud Business Plus includes all core identity security capabilities offerings in the Business bundle, adding advanced SaaS-based components designed for deeper management, control, and security of access.

Access Modeling

Define new roles to be adopted and continually monitor for updates to existing roles including suggesting optimizations to those roles.

Cloud Infrastructure Entitlement Management

Make faster and more informed IaaS access decisions and detect potential risks.

SailPoint SaaS Management

Uncover and mitigate hidden access risks due to shadow IT by bringing all SaaS apps under control.

Additional SailPoint identity security solutions

Access Risk Management

Automate real-time access risk analysis, simplify GRC processes, and identify potential risks before access is granted to users.

Non-Employee Risk Management

Execute risk-based identity access and lifecycle management strategies for non-employees.

File Access Manager

Gain visibility and control over unstructured data, discover exactly where your data lives and what sensitive information it contains.

Password Management

Minimize calls to the helpdesk by providing users with self-service access.

Get started

With this buyer's guide in hand, you now have:

- Help to identify the most important business goals you want to achieve in improving identity security outcomes worthy of investment
- Capabilities you should look for in a solution to help realize those goals
- Knowledge on how SailPoint identity security solutions, along with its vast ecosystem of partners, delivers those capabilities to help you succeed

As your first step in developing the plan for improving your identity security program, try our online adoption assessment tool at **www.sailpoint.com/identity-security-adoption** to understand which identity security horizon your company has reached and understand how you can move forward confidently.

Bring the whole organization along on the journey rather than just the IT or IAM team by building a business case and establishing clear ownership and needs.

SailPoint can help you build your business case. SailPoint's Business Value Assessment process (available at no charge) will enable you to build a detailed business case based on your specific challenges and opportunities:

- Understand the specific identity security business challenges and functionality gaps that exist in the current environment and how SailPoint solutions can address them.
- Quantify the tangible and intangible benefits that could accrue, including productivity and effectiveness benefits, using industry benchmarks, best practices, and specifics of your processes.
- Deliver a business case unique to your project and company: ROI, NPV, and payback analyses delivering results in a format that is needed for your internal cost justification / CapEX review and approval process.

An additional resource available to you is the **The ultimate guide to unified identity security addendum** that includes key questions to ask when evaluating different identity security capabilities.

We are always available and happy to answer any additional questions you may have. To help fine-tune your business goals and create a transformation roadmap, reach out to us.

www.sailpoint.com

About SailPoint

SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity – at speed and scale. As a category leader, 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 cyber threats while enhancing productivity and efficiency. SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.

sailpoint.com

SP2258-2406