SailPoint

ADDENDUM

The ultimate guide to unified identity security checklist

Table of contents

Evaluate core requirements

Once you have the "big picture" of what it will take to accomplish your goals for improving identity security, you'll want to look at the individual capabilities of various identity security solutions to determine whether they can provide the functionality required.

The following pages provide checklists for evaluating solutions. Each section includes a set of qualifying questions which can be used to evaluate solutions across a set of criteria required.

Building the business case

Providing a compelling business case for acquiring and deploying an identity security solution is a critical step in any project. Ask the following questions to understand how the solution under consideration can help you to solve your current business problems related to securing user access within the enterprise.

- What real-world examples of cost savings or cost elimination can the vendor provide associated with:
  - Managing and securing ever-changing access to resources
  - Proving compliance and eliminating audit deficiencies that can lead to fines and penalties
  - Migrating from aging identity access management systems
  - Eliminating ad hoc access management processes
- What capabilities does the vendor provide to build a strong, upgrade free identity security solution in a SaaS-based all-in-one package?
- Is the vendor able to explain if and how much downtime is required for updates, upgrades, or regular maintenance?
- How quickly can the vendor deliver and prove return on investment across identity security, compliance, and provisioning?
- Do the pre-defined workflows for 3rd party identity management provide pre-configured processes to allow delegation of validation and management tasks to multiple "owners" such as project managers, vendor managers, and supplier managers to re-confirm identities are still performing tasks for the company?
- Is the solution architected in a way that allows you to start quickly and expand based on future needs without requiring major rework, customizations, or upgrades?
- How does the solution scale as your business needs change? For example, is the solution able to instantly scale up in the case of a major M&A without prior notification to the vendor?
- Will the solution help you strengthen your security and compliance posture with end-to-end identity and access strategy?

Access requests and approvals

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

- In what ways does the solution reduce the strain on IT by eliminating manual repetitive processes?
- Is the solution able to suggest to the requester any access that is likely to be required, actively helping the requester to navigate the hundreds of thousands of access rights?
- Can the solution automatically grant or deny access to corporate applications and resources — both on premises and in the cloud?
- How does the solution incorporate usage data to drive efficiency and security within the access request and approval processes?
- How does the solution leverage risk data to drive efficiency and security within the access request and approval processes?
- Does the solution integrate with traditional ITSM systems to tie into existing business processes?
- How does the system dynamically adjust access based on identity changes — e.g., new role, change in job title, new project assignment?

Automated provisioning

Give workers access wherever they are – automatically and securely – helping reduce risk while improving your compliance and productivity.

- How does the solution deploy best practices to expedite the onboarding and configuration of new users?
- Does the solution prevent excess permissions by automatically adjusting and removing user access as changes happen?
- Will the solution enable you to save time by automating low-risk IT tasks to accelerate delivery of access to users?
- Does the solution provide visibility to access changes initiated through automated change events — e.g., new hire, promotion, termination?
- Does the solution offer easily configurable access request workflows to ensure access is approved by the correct entity prior to provisioning?

Access certifications

Prevent the risk of over-entitlement by easily identifying and revoking unneeded user access.

- How does the solution enable you to focus reviewer attention on the most anomalous and risky access?
- How does the solution emphasize efficiency and effectiveness of compliance controls while reducing compliance fatigue?
- How does the solution drive end-to-end remediation of inappropriate access, even if on a disconnected system?
- How does the solution inform reviewers about new, or special access?

Separation-of-duties

Detect and prevent conflicts of interest and potential fraud across all applications.

- How quickly is it possible to create a suite of comprehensive SoD policies that enforce critical controls?
- Does the solution easily apply and enforce policies across multiple systems and applications?
- Can the system both detect and prevent policy violations?
- What integration use cases does the solution support with common GRC solutions like SAP GRC and Oracle EBS?

Password management

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

- Does the solution give your users an easy and intuitive way to change or reset passwords themselves while still enforcing strong password policies across all applications and systems?
- Does the solution support both on-network and off-network self-service password resets?
- Does the solution reduce help desk calls with self-service password resets?
- Does the solution allow for password management of both cloud and on-premises applications?
- How does the solution enable consistent password policy enforcement across applications?

Access insights

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

- Does the solution enable discovery of identity access outliers automatically giving visibility into excessive access privileges (e.g., through AI)?
- Does it proactively give you visibility into access privileges that are anomalous or pose a risk to the organization such as abnormal entitlements and dormant or orphaned accounts?
- How does the vendor allow you to determine what access an identity should have versus what access an identity does have?
- How does the solution allow you to identify outlier access and then bring that access back into governance?
- Does the solution provide a single source of truth, collecting all access-related activity and events, including any changes in access and entitlements?
- Fom a single dashboard, can you flag outlier identities, review, and recommend actions to remediate and reduce — or better yet eliminate — the number of outliers in your organization?

Recommendations

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

- How does the solution allow you to decide what access should be requested, approved, or removed with recommendations based on peer group analysis, identity attributes, and access activity?
- How does the solution leverage technology like AI and ML for insights that enable you to make more educated access requests and decisions?
- How does the solution identify outliers (e.g., by comparing user access) to help you determine whether someone should have access or not?
- Will the system help you maintain continuous compliance and prevent audit issues by enabling business managers to make more accurate access certification decisions rather than rubber-stamping?
- How does the solution help increase your trust in your decisions by helping you understand the reasons behind each recommendation decision (whether it is based on similar identities, location, role, and department)?

Access modeling and role management

Define new roles to be adopted and continually monitor for updates to existing roles.

- How does the solution give you the insights you need to model and adapt access to the ever-changing patterns typical in your enterprise?
- How does the solution eliminate manual processes so you can create and adapt roles that align with the evolving needs of your business?
- Does the solution use advanced technology like machine learning to suggest roles based on similar access between users?
- Can the solution accelerate the implementation of roles by identifying potential roles that will have the greatest impact?
- How does the solution continuously maintain roles to prevent role decay and ensure the effectiveness of your access model?
- How does the solution optimize your role program to drive greater security?
- Does the solution automatically create the most common access roles such as “Joiner” for faster onboarding and quicker access to key applications?
- How are business users enabled to review, refine, and maintain roles, taking the burden off of IT teams?

Cloud Infrastructure Entitlement Management (CIEM)

Make faster and more informed access decisions and detect potential risks for your IaaS cloud platforms and workloads.

- Can you view cloud entitlements from your identity certification process?
- Does the solution enable you to view a user’s cloud infrastructure activites and privileges from their cloud entitlements?
- What level of visibility do you have to all access paths from a user to a cloud resource in your identity solution?
- What level of visibility do you have to view federated cloud access in AWS, Google Cloud Platform, and Azure?
- Can you view AWS IAM Identity Center users and permission sets in your identity solution?

SaaS management

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

- Does the solution give you complete visibility into your entire SaaS footprint, including SaaS applications purchased or expensed without the involvement of IT and procurement?
- Does the solution help uncover SaaS sprawl, letting you discover your entire SaaS footprint and any unauthorized or hidden applications?
- Does the solution integrate with your current SaaS applications so you can unlock full visibility into your SaaS security, usage, and spend, letting you discover every purchase in real-time?

Data access governance

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

- Does the solution give you a complete picture of where data lives, what sensitive information it contains, and how access to the data is granted?
- How does the solution automate compliance certifications for data privacy and access governance?
- Does the solution automate Data Subject Access Request (DSAR) campaign workflows to address right-of-access and right-to-be-forgotten use cases?
- Does the solution leverage advanced technologies (like an AI-powered Natural Language Processing data privacy engine) to provide advanced classification capabilities to easily identify PII data?
- Does the solution support an enhanced connector for AWS, integration with Microsoft Azure files and support for Google G-Suite shared drives and external accounts?
- Does it offer an extensive array of preset and custom policies for PII, Personal Health Information, and Payment Card Industry (PCI) data to comply with such regulatory standards as GDPR, CCPA, and others?

Connectivity and integrations

Extend, connect, and integrate core identity security capabilities with the key applications and systems that you use to run your business.

- Does the solution feature integrations with all your critical business applications?
- Is the solution extensible to meet your needs to govern your SaaS, On-prem, and custom developed applications?
- What features does the solution provide to ensure scalability and performance of connectors and integrations?
- Are the solution's connectors and integrations backed by strategic alliances and collaborations with application vendors?
- What capabilities does the solution offer for customers who need to quickly configure custom connectivity via standards-based protocols?
- How well does the solution meet industry-specific connectivity and integration requirements for healthcare, financial services, government, and other key industries?

Resources

For further information on the topic of identity security, visit these links to experts, industry associations, and publications.

SailPoint
www.sailpoint.com
www.sailpoint.com/blog/

Analysts

Forrester
Identifies and analyzes emerging trends in technology and their impact on business.
www.forrester.com

Gartner
Provides research and analysis of the computer hardware, software, communications, and related information technology industries.
www.gartner.com

IDC
Provides data, analysis, and advisory services on information technology (IT) markets, trends, products, vendors, and geographies.
www.idc.com

KuppingerCole
Provides research and analysis, focused on information security, both in classical and in cloud environments.
www.kuppingercole.com

Membership organizations

Cloud Security Alliance
The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations, and other key stakeholders.
www.cloudsecurityalliance.org

Identity Defined Security Alliance (IDSA)
The IDSA is a group of identity and security vendors, solution providers, and practitioners that acts as an independent source of thought leadership, expertise, and practical guidance on identity-centric approaches to security for technology professionals. The IDSA is a nonprofit that facilitates community collaboration to help organizations reduce risk by providing education, best practices, and resources.
www.idsalliance.org

Internet Engineering Taskforce (IETF)
IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The organization now has adopted a working group dedicated to the development of SCIM.
www.ietf.org

(ISC)²
The global leader in educating and certifying information security professionals throughout their careers. A network of certified information security professionals. Members have access to current industry information, networking opportunities, discounts on industry conferences, and valuable career tools.
www.isc2.org/#

National Institute of Standards Technology (NIST)
NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
www.nist.gov

OASIS
OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium that drives the development, convergence, and adoption of open standards for the global information society. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.
www.oasis-open.org

Publications

The below list features identity, cybersecurity, and technology publications that provide the latest news, insights, and trends in the industry and could prove to be a helpful resource along your buying journey.

CIO
www.cio.com

ComputerWeekly.com
www.computerweekly.com

ComputerWorld
www.computerworld.com

CSO Magazine
www.csoonline.com

Dark Reading
www.darkreading.com

eWEEK
www.eweek.com

InformationWeek
www.informationweek.com

InfoWorld
www.infoworld.com

ISMG News Network
www.Ismg.io

Information Age
www.information-age.com

SC Magazine
www.scmagazine.com

SDxCentral
www.sdxcentral.com

Security Boulevard
www.securityboulevard.com

Security Magazine
www.securitymagazine.com

Security Today
www.securitytoday.com

SecurityWeek
www.securityweek.com

TechTarget
www.techtarget.com

TechRepublic
www.techrepublic.com

ZDNet
www.zdnet.com

SailPoint

About SailPoint
SailPoint is a leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.

sailpoint.com

SP2261-2304