IDC MarketScape

IDC MarketScape: Worldwide Governance Administration for Identity Security 2022 Vendor Assessment

Jay Bretzmann

THIS IDC MARKETSCAPE EXCERPT FEATURES SAILPOINT

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Governance Administration for Identity Security Vendor Assessment

Source: IDC, 2022

November 2022, IDC #US47254121e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Governance Administration for Identity Security 2022 Vendor Assessment (Doc # US47254121). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

The focus on identity governance administration (IGA) is steadily growing within larger organizations as artificial intelligence and machine learning (AI/ML) capabilities surface within popular vendor offerings. A few years back, IGA was more of an administrative solution, sometimes called the passive side of governance, where organizations would implement largely on premises to improve their regulatory compliance positions, working to refine role definitions and improve least privileged access (LPA) to sensitive and private data. It was an activity-only larger organizations — typically in financial and government verticals — and had the resources to perform.

Today, IDC believes this element of the identity solutions stack is finding new acceptance across the broader market due in part to the emergence of cloud-based alternatives but also an availability of resource after more organizations have moved from in-house to commercial identity solutions and tackled the basics of access (single sign-on [SSO]) and authentication (MFA). Regulatory compliance (SOX) continues to be a driver, but a new focus on zero trust environments, call this the active side of governance, seems only possible by taking a proactive approach to role- and attribute-based access controls using AI/ML intelligence and higher levels of automation for provisioning and deprovisioning. Getting humans out of the process for recognized requests and approvals is so essential.

Zero trust doesn't happen without tighter LPA and better separation of duties (SoD) assignments, but there's a natural resistance to just handing over the keys to a machine. PAM and IGA solutions have been on-premises resources due to a reluctance of trust. It's something that time can heal, but it takes time and perhaps wasted energy toward the end of that comfort period; nevertheless, security teams sleep at night when they're more sure.

IDC expects to see a considerable increase in IGA solution investment by public solution providers and private equity companies as they prepare for this next round of identity market competition. After years of start-ups and point product, best-in-class solutions, IGA capabilities will grow within platform offerings similar in the way privileged access management (PAM) recently started its journey. The IGA/PAM needs are intertwined but defining and developing a perfect solution is next to impossible (as with all things related to identity security).

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied 13 organizations that offer identity governance security software across the globe and surveyed more than 18 of their customers using these technologies in 2021. Evaluated vendors typically provide global capabilities, and while there are more total vendors in the broader market, the following specific offering criteria must've been met to have qualified for this assessment:

- **Revenue.** Each vendor was required to have greater than $5 million in 2020 worldwide security governance software product revenue — as determined by IDC.
- **Technology.** Solutions must support discovery and monitoring of user identities, the aim being to help security teams better understand and adjust who's doing what with the rights they've been granted.
- **Portfolio considerations.** Solutions can be either focused, single-point offerings or a component of a larger platform approach (but will be so identified).

For these reasons, identity management solutions more associated with the onboarding and initial access provisioning capabilities were excluded from the study.

ADVICE FOR TECHNOLOGY BUYERS

Data cleanup and importation was widely cited as the most difficult step in implementing a new or different identity governance system among the customer references we were given. Even those fortunate enough to benefit from standards-based interfaces (versus a unique API connection), organizations typically have to align multiple systems and extend a governance database schema in order to get the full benefit from the investment. The availability of trained professional services personnel is a factor to consider when choosing a specific vendor's offering.

With your recently completed identity risk analysis report in-hand, your next step is to narrow the list of potential IGA suppliers down to three. Nothing terribly deep there, but it puts an emphasis on developing and implementing a "desired" state of application and data access and a milepost for calculating any drift away to an "actual" or current state of privileges, policies, and controls. Expecting and planning for change is a primary reason for adding IGA to your identity security platform stack.

Look for automation. This is the bottom-line value of IGA; it's automating the management of people (mostly workforce and partner identities) that are in a constant state of change. As for what should be automated, it's both the review of access activities across an organization seeking outliers and the anomalies worthy of human review and adjustment. The need to govern "things" is not yet materially relevant for most organizations. Though the need may exist, it's not yet high enough on most priority lists.

Software entitlements management is another important feature that's gaining in importance. Some of the solutions provide this today but the view can be limited to a single-tenant environment or split across on-premises and cloud resources. Enterprises would prefer something more wholistic that helps them manage access and reduce costs associated with unused resources.

Watch for convergence of IGA with identity management and privileged access management solutions. Unique and hard requirements still exist within certain industries, but product differences are diminishing — as they should be — while the market for identity solutions continues to mature. Also, the existence of low-code/no-code workflow orchestration capabilities is a significant game changer. Solutions that support it allow IT or security teams to develop and revise onboarding activities, access requests, access reviews, and so forth in minutes, without the need to involve software developers who can often take weeks.

During almost every client reference interview, IDC asked what percentage of the IGA code base they thought they were using. The typically answer was "40% or less." Literal interpretation: half the capabilities are marketed but not currently implemented. IDC believes this speaks to a latent need for advanced technology — in the current offering or on the near-term road map — that organizations will eventually utilize, before deals for a simpler solution get cut today. IGA is another sticky technology choice, and customers want to hear about the possible.

What's missing here is some general agreement on what a governance portal should include. Security teams could be more productive if they knew what was coming at them. Vendors should line it up; it's all about access or not. There's a lot of material that describes skills shortages in the industry. Maybe it's time for a specialized identity governance class (SANS take notice).

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges. Some vendors declined to participate in the full process, so IDC has given best efforts to represent their solutions.

SailPoint

SailPoint is positioned in the Leaders category in the 2022 IDC MarketScape for worldwide governance administration for identity security.

SailPoint's identity governance solution was introduced in 2005 helping develop IGA into the discipline it is today. Recognizing the growing strategic significance of identity governance, the company is now repositioning itself as an identity security leader. Its recent reacquisition by Thoma Bravo foreshadows a broadening of the platform as the AI/ML capabilities SailPoint has developed are applicable across numerous identity security technologies.

The company has two offerings separately addressing the on-premises needs of its original client base and the cloud-based needs of new customers. The on-premises version is called IdentityIQ and has been highly customized to meet clients' needs over the past 17 years. While cloud migrations are currently inflight, in some cases, it will take years for customers to make the switch. The cloud-based version is called IdentityNow offering the active governance features supporting zero trust environments; the majority of new customers seek to help them automate their emerging identity governance practices and get humans out of manual processes where "outlier" conditions don't exist.

SailPoint also has "manager" offerings for Cloud Access Management pulling data from AWS, Azure, and GCP clouds; SaaS Management for discovering shadow IT usage and examining what's happening with large SaaS applications; File Access Management for data discovery and PII searches; and Access Risk Management for discovering SoD and other GRC violations. These products provide wide visibility across on-premises and leading cloud services platforms.

Strong industry partnerships, out-of-the-box integrations, extensive reporting capabilities, and the ready availability of third-party trained professional services are among the best in the identity security industry.

Strengths

Role definitions, access modeling, and access reviews are very mature within IdentityIQ helping on-premises customers initially define better roles (rather than subsequent reviews) than are typically found within an IGA solution.

AI/ML capabilities (mostly associated with IdentityNow) include advanced features and capabilities grouped into three components names — Access Insights, Access Modeling, and Recommendation Engine — able to represent behaviors and relationships within very graphical dashboards and models.

The Recommendation Engine is designed to eliminate the bulk of normal certifications or attestation work that so many passive identity governance solutions were purchased to perform. Through an iterative process, the AI engine and the human administrators are educating each other about what people and machines not only do but could possibly do.

Challenges

There is a feature/function gap between IdentityIQ and IdentityNow and always will be. Some capabilities of a cloud solution have to be more standardized than one would find in an on-premises solution customized to meet unique needs. The challenge is managing the expectations of both prospects or customer sets and applying the right level of investment to both offerings.

Consider SailPoint When

Consider SailPoint if you have an environment large enough that it's obvious humanly managed identity tasks are either currently — or soon will be — simply impossible. Governance will grow in importance for the next 10 years — until one day, when most of the activities become transparent. SailPoint with IdentityNow IDaaS has the lead on AI/ML capabilities that most organizations will be able to implement.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

This identity security technology submarket includes software developed for the better management of complete identity life cycles. Governance generally applies after a user is onboarded through an identity management solution and recorded within a directory (LDAP, others) system. Identity governance solutions deliver user life-cycle management, password management, compliance controls, and application, and data access governance capabilities. As a standalone offering, this is primarily a workforce (B2E) identity solution. B2C identity management solutions embed similar features but are focused more on individuals than user groups.

Some solutions are identity discovery capabilities that can help security teams understand any related identities for the same user and different roles one identity may possess. More advanced IGA solutions also include AI/ML analysis capabilities to develop peer-level insights. Assessed activities for people with similar roles may suggest refinements for some, and thus reducing unnecessary access. As a bonus, IGA solutions simplify and automate access approval requests for IT admins, security teams, and LOB managers.

LEARN MORE

Related Research

- *Worldwide Analysis Perspective: Worldwide Identity and Access Management, 2022* (IDC #US48670422, August 2022)
- *Worldwide Identity and Access Management Forecast, 2022-2026: Lead, Follow, or Get Out of the Way* (IDC #US48670522, July 2022)
- *Will SailPoint Broaden the Platform Beyond Identity Governance?* (IDC #lcUS49055222, April 2022)
- *IDC's Worldwide Software Taxonomy, 2022* (IDC #US48990921, April 2022)
- *OMB Delivers a Federal Zero Trust Architecture Mandate* (IDC #lcUS48859922, February 2022)
- *Identity Governance Spending in 2021 — Is It Riding Identity Coattails or Satisfying New Requirements?* (IDC #US48127421, August 2021)
- *IDC TechScape: Worldwide Identity Governance, 2020 — Pennies Saved and Compliance Earned* (IDC #US46159719, April 2020)

Synopsis

This IDC study presents a vendor assessment of the 2022 governance administration for identity security market using the IDC MarketScape model. Perhaps more than other identity security technologies, IGA is a solution where users never get to the top of the mountain and claim the job's done because the management of identities is in a constant state of flux. The older IGA installations are typically found within financial and government verticals where access reviews and certifications were a hard requirement and least privilege (LPA) was a dreaded, manual task. Credit the federal Sarbanes-Oxley Act (SOX) act passed in 2002 aimed at improving auditing and public disclosures as the tip of the identity governance requirements spear.

Fast-forward 20 years and organizations today understand the growing importance of IGA as identities (for people and things) have exploded in numbers. One retail organization serving as a reference said, even as recently as three years ago, there were 45 IAM tools within the company and more than 2,500 separate directory instances across three on-premises and cloud solutions managing 550,000 identities. Then consider that most employees likely have multiple assigned roles and the enormity of the problem becomes obvious. Automation, intelligence, and simplified orchestration capabilities are essential.

"The identity governance administration market is another fragmented opportunity for security vendors," said Jay Bretzmann, research vice president, Cybersecurity research, IDC. "Today's solutions are split across two main camps: passive on-premises solutions largely implemented for compliance purposes and active cloud-based solutions serving a more modern need for out-of-control access management situations with a focus on limiting the need for human involvement."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com