Solution Scorecard for Saviynt Security Manager

ARCHIVED Published 10 February 2021 - ID G00739934 - 18 min read

By Homan Farahmand, Katiuska Alvarado Ilarraza

Security and risk management technical professionals evaluating identity governance and administration platforms want to know whether Saviynt Security Manager can meet their enterprise IGA needs. This assessment scores Saviynt Security Manager against Gartner's 317-point Solution Criteria for IGA.

Overview

Key Findings

Saviynt Security Manager (SSM) meets 97% of Gartner's Required criteria, 96% of Gartner's Preferred criteria and 89% of Gartner's Optional criteria for IGA platforms. Its overall weighted score on the Solution Scorecard is a 96 out of 100.

SSM met 100% of required IGA capabilities in the categories of identity life cycle, entitlement management, access request, workflow, policy and role management, and auditing. In other categories like access certification, fulfillment and connectors, identity analytics and reporting, and ease of deployment and availability, SSM lacked some minor features.

SSM is a full-featured, cloud-delivered IGA solution, which can also be deployed on-premises using the same code as a virtual appliance. However, most Saviynt customers leverage the solution via public cloud deployment. SSM offers microservices-based architecture along with Kubernetes-based containerization for cloud customers.

SSM extends the core IGA capabilities in some categories like providing robotic process automation (RPA) functionality to support fulfillment and connector operations, data access governance (DAG) to gain visibility into access for unstructured data, segregation of duties (SOD) control monitoring to eliminate toxic combination of access, and some privileged access management (PAM) functionality to support cloud infrastructure entitlement management (CIEM) use cases.

Recommendations

Security and risk management technical professionals interested in SSM for IGA should:

Assess SSM as a full-featured IGA provider when cloud-delivered or hybrid (cloud-delivered and on-premises) IGA capabilities are required or preferred. This is particularly important when ease of

use, lower infrastructure maintenance, and quick deployment and enrollment of target systems are a priority.

Use SSM as an option when your enterprise has complex IGA requirements that require both core and advanced features and functionalities. This includes the use of advanced connectors for popular enterprise applications such as SAP and Epic, identity analytics to enhance core capabilities such as access request and access certification, and the use of RPA as part of core capabilities.

Leverage SSM identity risk exchange, continuous controls framework, flexible entitlement management, role workbench and other policy templates to accelerate deployment. This is particularly useful for new IGA deployments or simplifying existing identity life cycle processes.

Evaluate SSM add-on capabilities to address SOD control monitoring, some PAM use cases, and DAG data classification and prebuilt as opposed to acquiring separate third-party tools.

What's New in This Update

This document was revised on 27 April 2021. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Note: *We have a new format for our Solution Scorecards. A complete version of the current criteria and scoring is available at Gartner CloudScores. You can also access the data in the downloadable Excel file. Note, however, that the CloudScores data may not be available until several days after this document's publication.*

Solution Scorecards are meant to be read alongside Gartner's Solution Criteria for Identity Governance and Administration. This is the first version of the Solution Scorecard for Saviynt Security Manager.

Bottom-Line Assessment

The IGA capabilities within Saviynt Security Manager (SSM) were assessed considering that SSM extends the scope of IGA to include functionality usually associated with PAM, DAG and SOD control monitoring products. Thus, the scope of this evaluation is limited to IGA context.

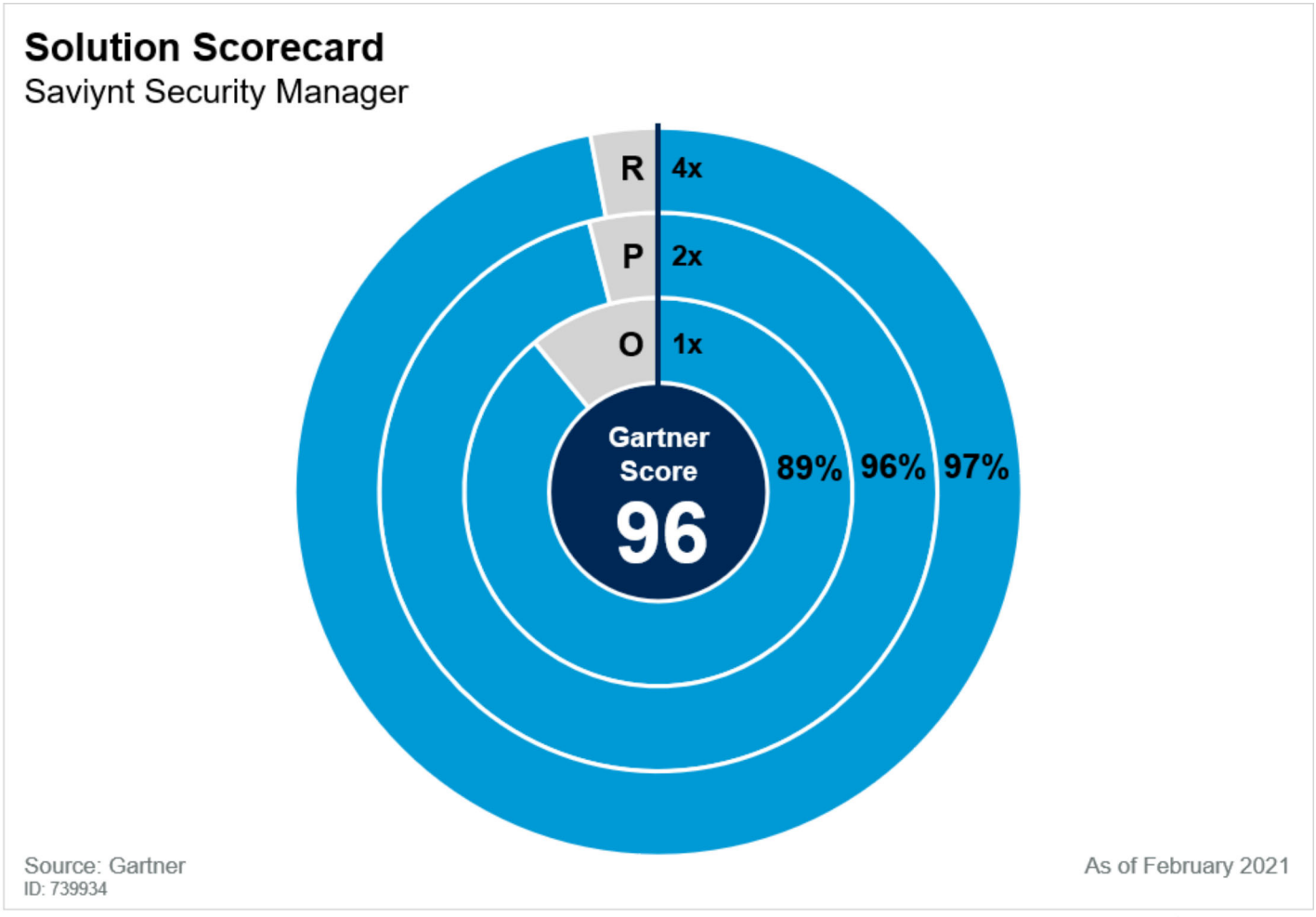
This assessment benchmarks SSM against Gartner's Solution Criteria for identity governance and administration published in December 2019. For IGA platforms, SSM satisfies 97% of Required criteria, 96% of Preferred criteria and 89% of Optional criteria, resulting in an overall weighted score of 96 out of 100. This score reflects a mature, cloud-delivered IGA platform with a breadth and depth of features suitable for deployment at enterprise scale.

We strive to continuously improve the quality and relevance of our research. If you would like to provide feedback on this document, please visit Gartner GTP Content Feedback to fill out a short survey. Your valuable input will help us deliver better content and service in the future.

Solution Scorecard and Feature Snapshot

Figure 1 shows that SSM has an overall solution score of 96 out of 100. It also shows that SSM meets 97% of Gartner's Required criteria, 96% of Gartner's Preferred criteria and 89% of Gartner's Optional criteria.

Figure 1: SSM Solution Scorecard Summary



Note: *The above scores are accurate as of the published date, but they will be periodically updated. A complete version of the current criteria and scoring is available in the downloadable Excel file. In addition, the data will also be available on Gartner CloudScores, where it will periodically be updated.*

Note, however, that the CloudScores data may not be available until several days after this document's publication.

Solution Scorecard Calculation

Gartner uses a weighted system to calculate the overall Gartner score:

Required criteria are assigned a weight multiplier of 4.

Preferred criteria are assigned a weight multiplier of 2.

Optional criteria are assigned a weight multiplier of 1.

Clients can customize the weight values to meet their needs in the companion Excel spreadsheet. To omit weighting, clients should assign a multiplier value of 1 to all criteria.

Solution Criteria Framework

Gartner developed the Solution Criteria framework to address the current and future needs of our clients. This framework categorizes market features as:

Required: Capabilities essential to developing, deploying and managing mission-critical, secure and compliant production applications. Missing Required capabilities may be "showstoppers" that necessitate specific risk mitigation or that make the provider unsuitable for your use case.

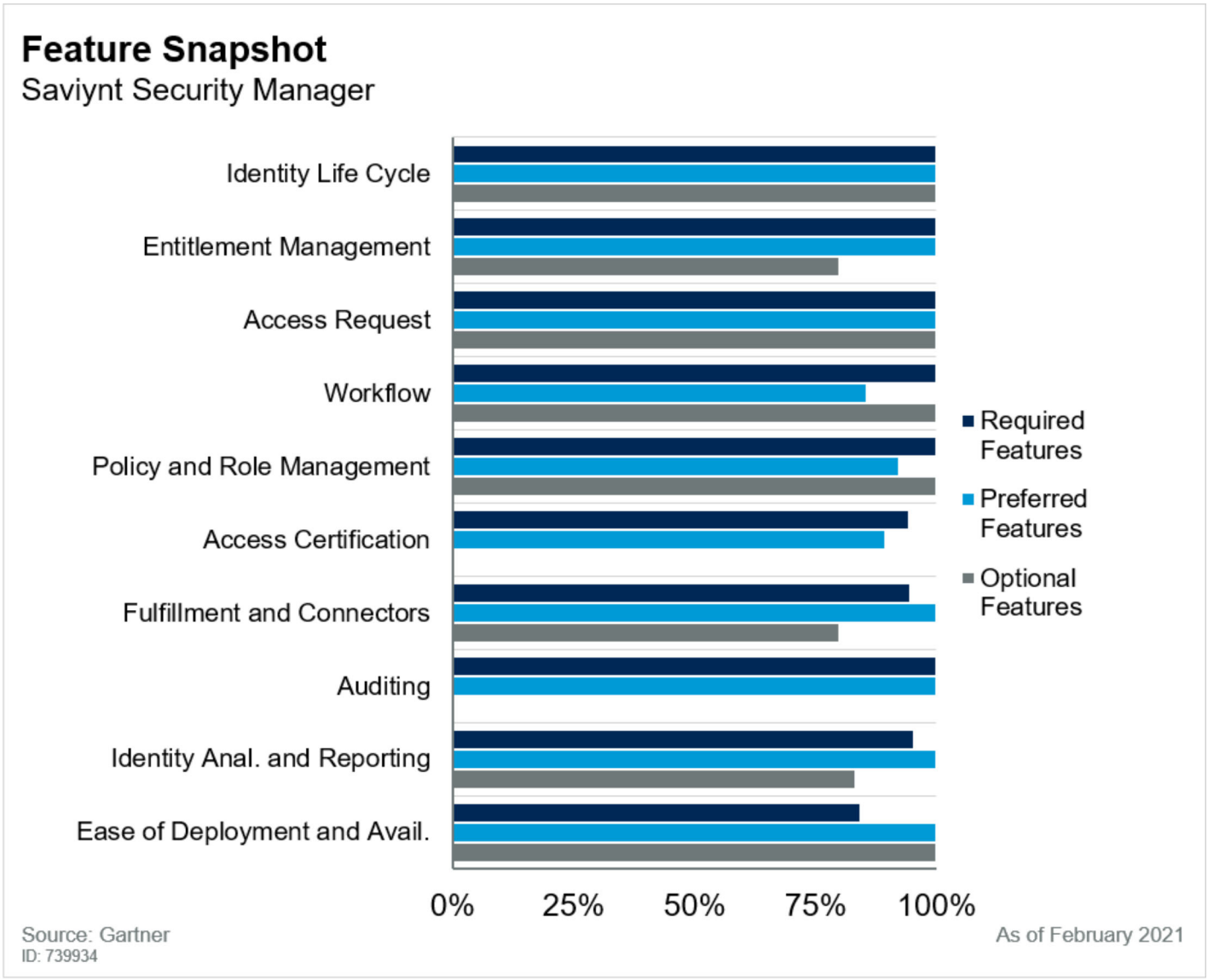
Preferred: Capabilities that are necessary, but not vital, to a broad range of use cases. Missing Preferred capabilities will often need to be replaced by other solutions. Most customers will have at least one application that requires these capabilities.

Optional: Capabilities that are beneficial for specific use cases, but which many customers will not need. In many cases, these capabilities represent emerging technologies.

A companion Microsoft Excel spreadsheet accompanies this document. Clients should modify and customize this spreadsheet to create a comprehensive list of criteria that takes their specific needs into account. For assistance with using and modifying the spreadsheet, clients should refer to the How To tab within the spreadsheet.

Figure 2 shows the SSM feature snapshot. Overall, Saviynt scores highest in the categories of identity life cycle and access request followed by policy and role management, and then entitlement management. Its lowest overall scores were in the categories of ease of deployment and availability.

Figure 2: SSM Feature Snapshot



Note: *The above scores are accurate as of the published date, but they will be periodically updated. A complete version of the current criteria and scoring is available in the downloadable Excel file. In addition, the data will also be available on Gartner CloudScores, where it will periodically be updated. Note, however, that the CloudScores data may not be available until several days after this document's publication.*

Strengths

The primary strengths of Saviynt are:

SSM has strong capabilities in the identity life cycle, access request and auditing categories, where it meets all Optional, Preferred and Required criteria. Saviynt's identity life

cycle management supports multiple personas with complex relationships and underlying data models. SSM access request includes a mobile application that can be used for initiating requests, managing approvals, viewing dashboards and managing certifications. SSM provides out-of-the-box controls to detect policy violations and create custom controls/audit policies (e.g., for SOD) and scan to detect actionable policy violations.

SSM meets all Required criteria for entitlement management, workflow, and policy and role management. SSM provides a set of out-of-the-box attributes to manage entitlement catalog metadata. Customers can also add and manage custom attributes to map to any entitlement catalog attribute. Saviynt workflow provides serial and parallel processing as well as static and dynamic routing. Customers can also specify that a quorum of approvers need to approve. The workflow definition process includes a node called Action Event. This node is used to invoke external applications/API within a workflow process. This node can be included at any point of the workflow process. SSM supports key identity analytics functionality including role mining, policy mining and access recommendations using ML.

SSM meets all the core requirements of access certification, connectors and fulfillment, and identity analytics and reporting. SSM provides filters for retrieving certification data in user manager campaigns and service account campaigns. For all the connectors, SSM supports the generic capabilities such as reconciliation, provisioning, password management, etc. In addition, depending on the target system's capabilities, SSM supports advanced capabilities such as usage analytics, license management, data classification, user activity monitoring and entitlement management. SSM identity analytics and reporting provide 65 generic reports that are predefined and around 37 predefined dashboards. Additionally, depending on the managed systems, administrators can create their own dashboard metrics. Also, the Control Center module creates a persona-based interface and prioritized KPIs.

Weaknesses

The primary weaknesses of Saviynt are:

SSM access certification does not provide any built-in functionality for an offline-mode certification review and a remediation challenge period. The IGA solution should provide an option for the reviewer to download the certification file as a spreadsheet and complete it offline. The completed spreadsheet is then uploaded to the certification tool. Also, the solution should support a challenge period that gives end users a chance to contest a pending remediation resulting from an access certification.

SSM identity analytics and reporting via third-party tools requires additional coding and access to data via API functions. Mature IGA suites should allow third-party reporting tools to access identity-related data for purposes of reporting. The reporting tool should easily integrate with the IGA solution at the data level. Also, SSM does not provide functionality for dashboard tagging.

Mature IGA suites should have the ability for users to identify things in the dashboard that are important to them.

SSM ease-of-deployment and availability categories currently provide dispersed and limited functionality for change management and extension management. Mature IGA suites should have a robust change management process for policies, system configuration, role definition, workflow definition such as documentation, workflow approvals, email notifications or other safeguards. Also, mature IGA suites should have an easy-to-use customization and extension management. While Gartner recommends that clients minimize customizations, there may be times when changes and extensions are necessary. These customizations and extensions (e.g., user interfaces, workflows, forms, policies, reports and connectors) must be isolated and easily upgradable without excessive professional services effort.

Reasons to Deploy

Gartner recommends SSM as an IGA platform for the following situations:

The organization desires robust, scalable and flexible core and/or advanced IGA capabilities. Saviynt implements scalability by combining Kubernetes-based containerization, best practices for data modeling and processing, and the modularity of the product itself through microservices-based architecture. Most of the modules within Saviynt can be deployed as stand-alone applications or instances that can interact with other modules deployed elsewhere. This provides the flexibility to deploy resource-intensive modules (e.g., role mining, usage analytics, etc.) in a separate container. Finally, Saviynt has architected autoscaling deployment for its SaaS offering that automatically increases/decreases the resources based on the demand.

The organization is primarily deploying a cloud-delivered or a hybrid IGA solution. In case of a hybrid model, the IGA solution has a cloud-delivered component as the primary instance that works in conjunction with an on-premises component as the secondary instance for target systems in data centers. The SSM on-premises solution (the same code as the cloud version but deployed in a virtual appliance) can expand support for on-premises systems. SSM can provide a practical path for gradual migration of all IGA capabilities to the cloud.

The organization would like to consume entitlements from systems with complex, multilevel authorization models. This includes the ability to consume and understand entitlements from applications with complex authorization models such as Epic, Oracle E-Business Suite (EBS) or SAP. Saviynt provides a fairly flexible entitlement model, including a hierarchical entitlement model. Organizations can create various entitlement types that are relevant for each application and bring in and map entitlements with those types. For each target application, organizations can define the corresponding entitlement types, set up hierarchy, set up corresponding approval workflow, and define how the entitlements of these types appear while requesting them in access requests.

The organization would like to complement IGA suite capabilities with adjacent solutions in the same platform. For example, SSM platform provides its own privileged access management solution that is unified with the IGA suite as well as integrates with external PAM solutions such as CyberArk, BeyondTrust and Thycotic. Also, Saviynt offers DAG data classification and policy management that can be applied to some cloud and on-premises applications, services, and platforms. The examples are file systems, Box, Dropbox, Microsoft SharePoint, O365, Google Drive, Apache Hadoop, NetApp, Microsoft SQL Server and Oracle.

Reasons to Not Deploy

Gartner recommends refraining from deploying SSM in the following situations:

The organization prefers to adopt a full-featured IGA system that is delivered as on-premises software that can be installed directly on a server. SSM is packaged as a virtual appliance called Saviynt in a Box for on-premises scenarios. This model may not be suitable for clients that would like to have full control over the software.

The organization IGA requirements are simple and less complex to the degree that the organization will not leverage the full extent of Saviynt capabilities and features. SSM is a full-featured IGA suite that is typically deployed by organizations that require advanced and complex requirements.

The organization expects substantial customization; however, it lacks Java development skills and doesn’t want to establish Java development competencies. Saviynt customizations use standard languages such as Apache Groovy, JSON-based settings and Java for advanced cases.

Analysis

Saviynt was founded in 2010 to offer an IGA solution, which is called Saviynt Security Manager (SSM). This included advanced identity analytics capabilities and a cloud-delivered, cloud-architected IGA platform in 2015. In 2018, Saviynt introduced a cloud PAM solution to secure privileged access in a dynamic, multicloud ecosystem.

SSM in its current release is a full-featured IGA solution that extends the scope of IGA to include functionality usually associated with PAM, DAG and SOD control monitoring products. This is offered as a cloud-delivered, cloud-architected and usually single-tenant service. Alternatively, Saviynt offers the same solution as a virtual appliance that can be hosted in clients’ data centers, using the same codebase and capabilities of the cloud-delivered service.

The identity life cycle capability covers all key use cases, including RPA software robots, with built-in functionality. Entitlement management capability provides a deep and flexible entitlement data model that supports multilevel hierarchical entitlements. It also provides a full-featured UI for maintaining application inventory that supports assigning and tracking activities related to application onboarding.

A graphical dashboard provides various risks and comparators to aid decision making. The access request capability user interface is based on a limited shopping cart model.

Workflow provides features such as preventive SOD checks, including digital signatures support. Policy and role management capabilities support the two-level role model to bridge the gap between business and application role management. Policies for role assignment (and detachment) are handled separately via provisioning rules. The access certification capability offers support for targeted campaigns that include a specific scope such as exceptional access, changes within a certain period or specific types of accounts. Risk-based recommendations are available throughout the product. Microcertifications can be automatically triggered based on events.

The fulfillment capability offers a wide range of direct provisioning connectors, some with full functionality such as LDAP, AD, UNIX, RACF, database, SCIM and scripted REST, and some with basic functionality. The product combines support for user-developed and OpenICF connectors, with extensibility through custom REST web services and Apache Camel middleware integration framework. Optional connectors can be acquired separately, some as premium editions of the basic connectors. These premium connectors are necessary for performing more advanced governance of accesses in these platforms such as SOD monitoring. There is a capability for indirect fulfillment via the access request interface or via ITSM tool integration.

The auditing capability provides a continuous controls framework, including several out-of-the-box controls. In addition, customers can create their own controls/audit policies and scan to detect actionable policy violations. In addition, SSM provides functionality for SOD policy definition, detection and remediation. The audit capability also provides a case management interface that can assign follow-up for the full range of audit events. The identity analytics and reporting supports risk scoring at both user and application levels as well as outlier detection. Role mining and related affinity analytics provided by the Role Workbench assist with role management for applications with complex authorization models. SSM also provides mapping to various regulations and compliance frameworks that can significantly expedite compliance reporting. As part of Saviynt Identity Risk Exchange capability, SSM integrates with various external security solutions such as SIEM, UEBA, CASB, vulnerability management, and identity proofing to determine risk-score.

Gartner conducted the technical assessment of Saviynt from June through December 2020. Capabilities had to be generally available by December 2020 to count for scoring purposes. Links to the vendor’s supporting technical documentation are included where available.

Required Features for Production

Saviynt meets 97% of Gartner’s Required IGA criteria. Note that criteria require all features in order to get a “Yes,” and partial fulfillment is a “No.”

Some missing criteria that typical organizations require include:

Access certification supporting data attachment: The solution must allow users to attach supporting documents or data to the access review. This feature is particularly important when exceptions are made to out-of-compliance access and the approver needs to document the reason for the exception. In SSM, certifiers can provide necessary justification and/or comments along with their review decisions through comments option; however, attachments are not supported.

Fulfillment and connector retention period: Some organizations chose to disable an account for a defined period and then delete the account on a future date. The IGA solution must allow organizations to define a retention period. SSM does not provide a built-in functionality to set up a retention period for an account. This could be achieved by defining a control that checks for accounts that were disabled “n” number of days ago and deprovisions them.

Ease of deployment and availability directory software support for common platforms: The IGA solution should run on common Windows, Linux and UNIX operating system platforms, including Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, IBM AIX and Oracle Solaris.

Ease of deployment and availability change management process: Changes to policies, system configuration, role definition, workflow definition and so on could have a significant impact on users and the IGA system. The IGA solution must include robust change management processes, including documentation, workflow approvals, email notifications or other safeguards. SSM provides audit logs for changes and test-to-production management but not a change management process for configuration items with approval workflow and notification.

Ease of deployment and availability extensions management: While Gartner recommends that clients minimize customizations, there may be times when changes and extensions are necessary. IGA vendors should, at a minimum, provide extensions for user interfaces, workflows, forms, policies, reports and connectors. Customizations must be isolated and easily upgradable. SSM lacks a central console to manage isolation and tracking of extensions for future upgrades.

Preferred Features for Production

Saviynt meets 96% of Gartner’s Preferred IGA criteria. Note that criteria require all features in order to get a “Yes,” and partial fulfillment is a “No.”

Some missing criteria that typical organizations prefer include:

Workflow return for additional input: An approver may need additional information before an approval decision can be made. The IGA solution should allow an approver to reroute the workflow task back to the originator or a previous approver for additional input. SSM is introducing an in-line consultation option as part of approval workflow. When more information is required to process a workflow task item, an approver can initiate a consultation directly from the access

approval interface and get feedback from other users, including the requester, an expert or another approver. This feature is currently in the early access stage.

Policy and role management approval workflows for role assignment changes: When a permission is changed or removed from a role, all users associated with that role are affected.
The IGA solution should allow organizations to define a workflow approval process that allows business owners or delegated administrators to accept or reject the proposed change on an individual user basis.

Access certification challenge period: The solution should support a challenge period that gives end users a chance to contest a pending remediation resulting from an access certification.

Access certification offline review mode: The IGA solution should allow the reviewer to download the certification file as a spreadsheet and complete it offline. The completed spreadsheet is then uploaded to the certification tool.

Optional Features for Production

Saviynt meets 89% of Gartner's Optional IGA criteria. Note that criteria require all features in order to get a "Yes," and partial fulfillment is a "No."

Some missing criteria that typical organizations consider optional include:

Entitlement management language support: The ability to render entitlement names and descriptions in multiple languages so that they appear correctly for users with different languages specified.

Fulfillment and connector unified endpoint management (UEM) support: Organizations may wish to govern data and mobile applications consistent with their software and SaaS-delivered applications. In this case, the IGA solution must support integration with common UEM systems in order to provision and deprovision mobile applications, gather identity analytics data, and trigger events based on risk (e.g., wiping a device).

Identity analytics and reporting dashboard tagging: The solution should have the ability for users to identify things in the dashboard by tagging them with an attribute such as a critical item.

Evidence

All ratings for this Solution Scorecard are based on vendor surveys or briefings, publicly available sources, and interactions with Gartner clients that have used Saviynt SSM.