Gartner

G00299338

Critical Capabilities for Identity and Access Management as a Service, Worldwide

Published: 29 September 2016

Analyst(s): Neil Wynne, Gregg Kreizman

To assist IAM leaders with their IDaaS vendor selection process, Gartner evaluated 18 vendors' services in this research using 11 critical capabilities and three common use cases: workforce to SaaS, business-to-consumer and traditional/legacy workforce.

Key Findings

- Gartner estimates that 90% of client interactions on the topic of IDaaS indicate a need for either workforce to SaaS or business-to-consumer (B2C) use cases. Ten percent of interactions focus on on-premises application support with more in-depth IGA requirements.
- IDaaS functionality is evolving and improving, with some vendors proving that they can deliver from the cloud functionality that has traditionally been provided by full-featured, on-premises IAM stacks.
- While IDaaS is expected to offer ease of deployment, implementations are more complex, time-consuming and costly when organizations have requirements for IGA functional depth and when they have legacy on-premises application targets.

Recommendations

Identity and access management (IAM) leaders developing IDaaS requirements should:

- Identify IAM business drivers and constraints as well as the use cases and depth of IAM functionality that must be supported to determine if the IDaaS delivery model is a good fit for your organization.
- Figure out how much your organization spends on IAM internally before making a decision to use IDaaS, and when evaluating transition and subscription fees for these services.
- Use this document alongside the companion Magic Quadrant to aid IDaaS selection decisions and identify key differentiators among services.

Strategic Planning Assumption

By 2020, 40% of identity and access management (IAM) purchases will use the identity and access management as a service (IDaaS) delivery model — up from less than 20% in 2016.

What You Need to Know

This research complements Gartner's "Magic Quadrant for Identity and Access Management as a Service, Worldwide." The vendors reviewed in this research include some covered in the Magic Quadrant as well as others that did not qualify based on market presence or functional breadth, but which can address specific use cases. These vendors do not represent an exhaustive list.

This Critical Capabilities research helps IAM leaders understand the most important functionality needed to meet the most popular use cases expressed by Gartner clients. It rates IDaaS services based on 11 areas of differentiation, or "critical capabilities," and weighs the importance of these capabilities in the three most common use cases in which Gartner clients are interested (see the Use Cases section below for additional details):

- Workforce to SaaS
- Business-to-consumer (B2C)
- Traditional/legacy workforce

The result shows the relative strengths of the IDaaS offerings against those popular use cases.

The Critical Capabilities Definition section sets out the criteria used for the evaluation. Table 1 explains the weightings of product functionality used for the three use cases. Critical capabilities ratings (without weightings) can be found in Table 2. Individual product scores can be found in Table 3.

Analysis

Critical Capabilities Use-Case Graphics

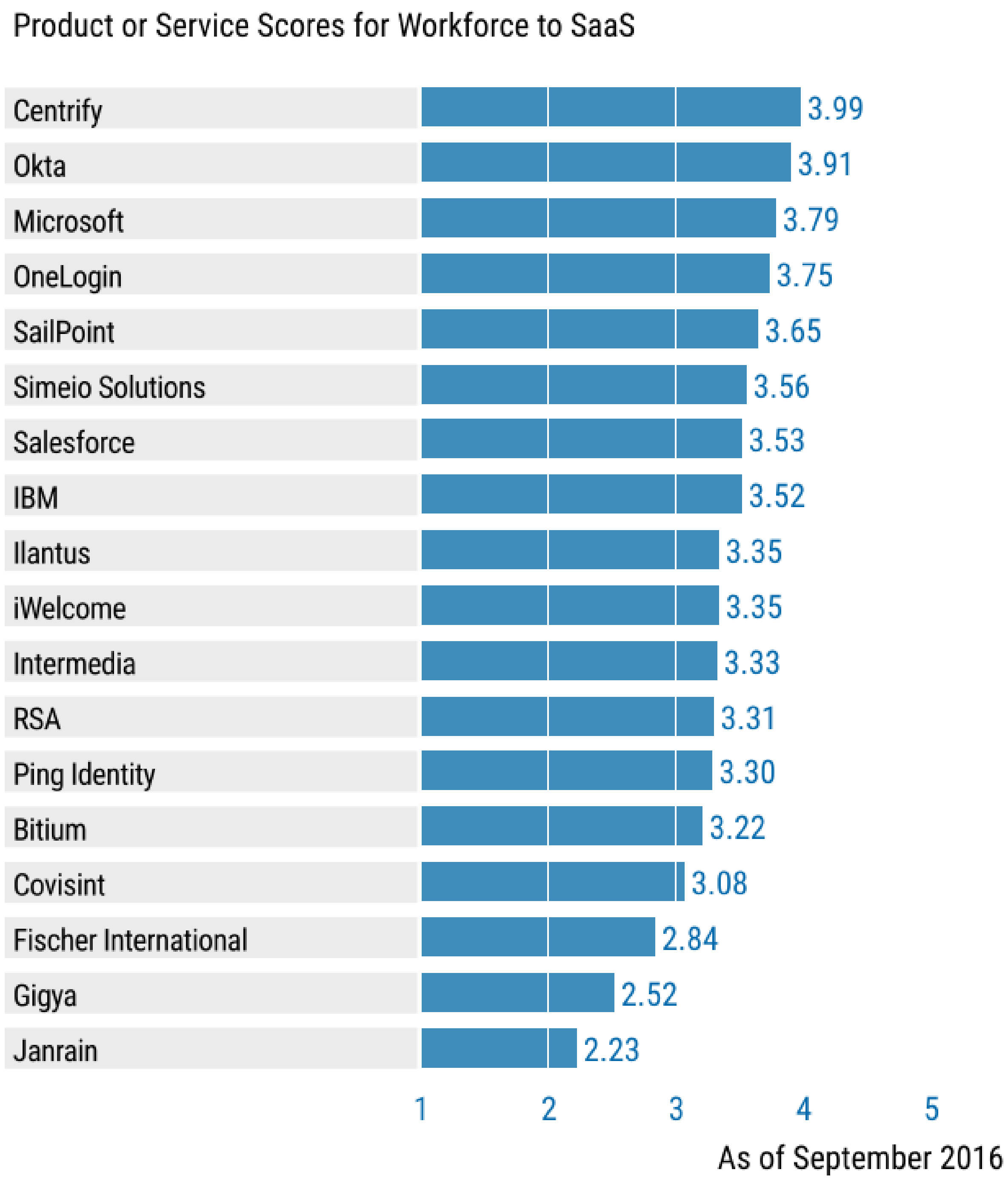
Figures 1 through 3 show aggregate product service across the 11 critical capabilities that have been weighted for each use case. Each of the services has been evaluated on the critical capabilities using a scale of 1 to 5:

- 1 = Poor or Absent: Most or all defined requirements for a capability are not achieved.
- 2 = Fair: Some requirements are not achieved.
- 3 = Good: Meets requirements.
- 4 = Excellent: Meets or exceeds some requirements.

- 5 = Outstanding: Significantly exceeds requirements.

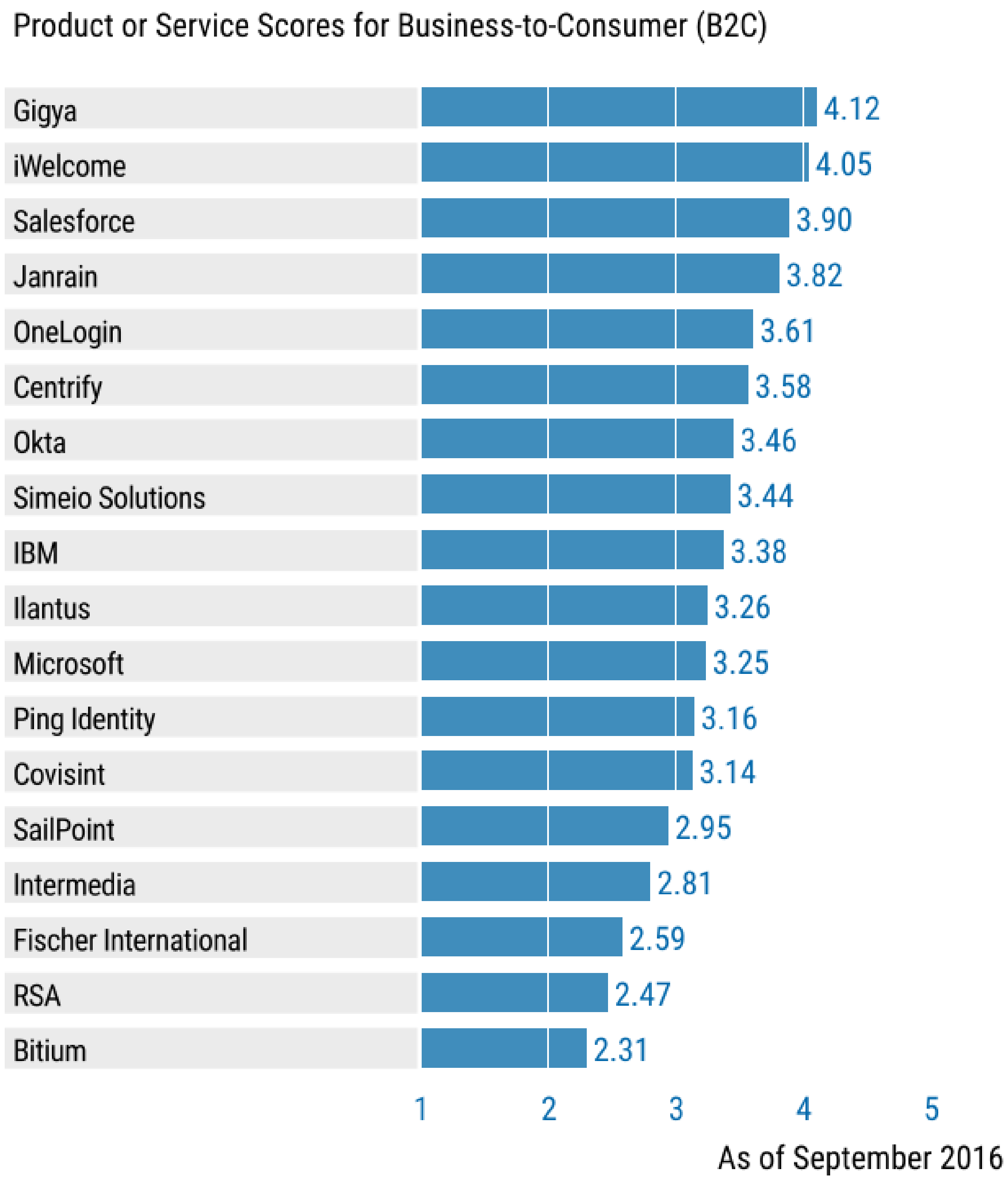
The critical capabilities are described in the Critical Capabilities Definition and Use Cases sections. Capability weightings and scores by use case by vendor are shown in Tables 1 and 2. Although Gartner has provided recommended weightings for each critical capability and use case, individual client requirements vary greatly. Clients are advised to use the web-based interactive version of this Critical Capabilities research to set weightings that better reflect their own needs.

Figure 1. Vendors' Service Scores for Workforce to SaaS Use Case



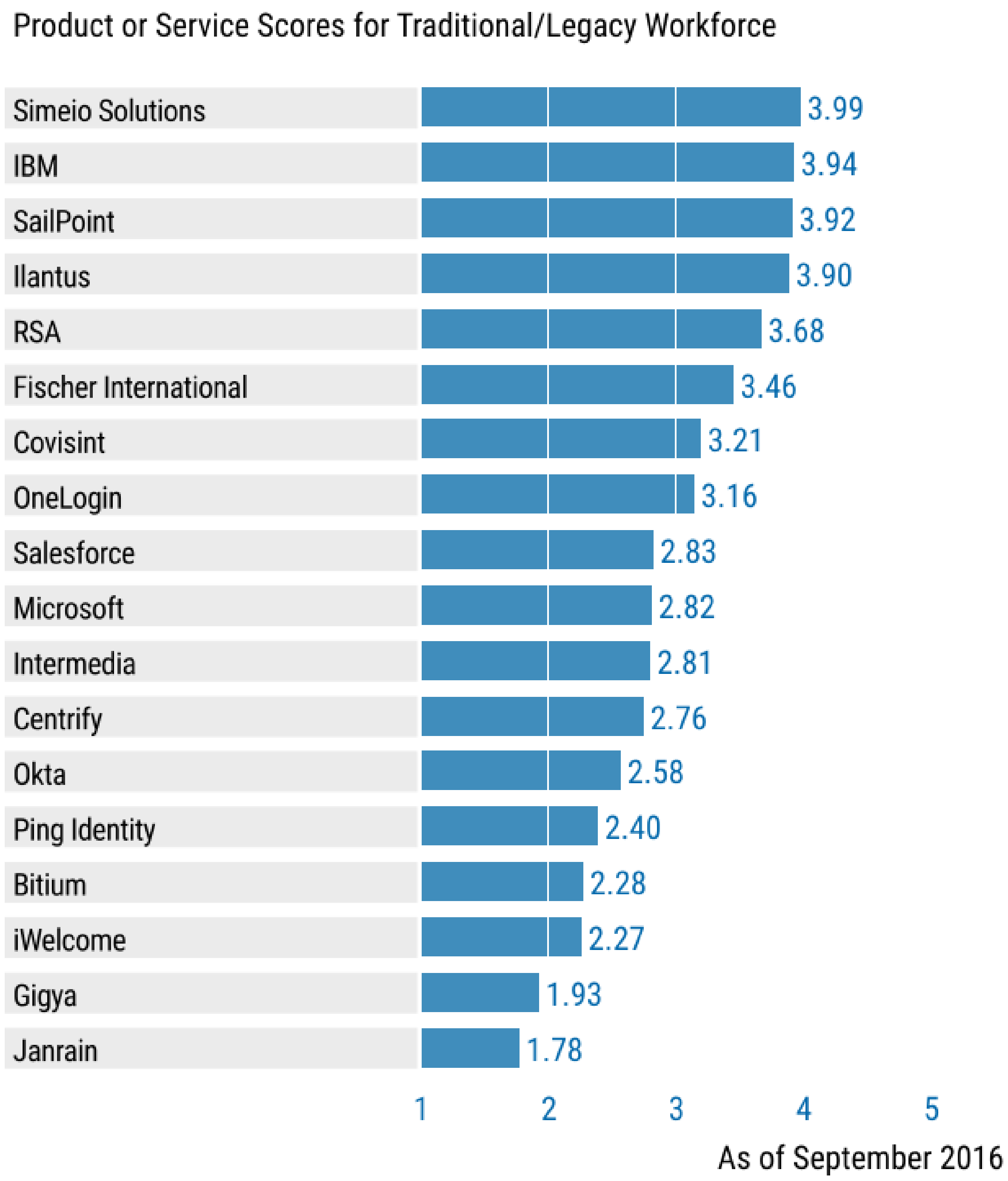
Source: Gartner (September 2016)

Figure 2. Vendors' Service Scores for Business-to-Consumer (B2C) Use Case



Source: Gartner (September 2016)

Figure 3. Vendors' Service Scores for Traditional/Legacy Workforce Use Case



Source: Gartner (September 2016)

Vendors

Bitium

Bitium offers a cloud-based service to integrate SaaS applications that includes single sign-on (SSO) and user provisioning. Bitium also offers a type of application sharing feature that allows users to give secure, delegated access to an application or website that they have access to, without sharing any usernames or passwords. This could be useful for the marketing team sharing a corporate social media account, for example. Bitium is able to integrate several SaaS applications enabling them to exchange data with each other by providing a brokering service for OAuth tokens.

Bitium has solid capabilities in support of the workforce to SaaS use case. However, the lack of social identity integration and poor on-premises application integration limit its consideration for the other two use cases.

Centrify

The IDaaS portion of Centrify's Identity Service offering provides web application SSO using federation standards or password vaulting and forwarding, user provisioning and reporting. In addition to web-centric IDaaS, Centrify's Identity Service also includes EMM and privileged access management (PAM). The integrated mobility management capabilities provide many of the features of stand-alone EMM vendors. Notable features include security configuration and enforcement, device X.509 credential issuance and renewal, derived credentials, remote device location and wiping, and application containerization. Centrify also supports mobile fingerprint biometric authentication options as well as SSO support without requiring use of a specialized mobile SSO application.

Centrify's Identity Service received high scores for both the workforce to SaaS and B2C use cases but the lack of access certification and legacy application support make it a poor fit for the traditional/legacy workforce use case.

Covisint

Covisint is the longest-standing IDaaS vendor in the market. Covisint got its start in the automotive industry and provided integration broker, portal and identity services to support supply chain connectivity. Its work in the automotive industry and in supporting vehicle identities has also helped it build foundation services that can be used in other Internet of Things (IoT) applications.

Covisint Identity Manager's strong user administration workflow, administrative delegation and access certification features can support complex business-to-business and business-to-consumer relationships. While it can also support the workforce to SaaS use case, Covisint's focus on large customers with enterprise B2B and B2C use cases will make it an unlikely choice for SMBs.

Fischer International

Fischer International, a pure-play IAM provider with a user provisioning focus, was one of the first vendors to deliver IDaaS. Fischer's capabilities are available in IDaaS, dedicated hosted, managed or on-premises software delivery models. The vendor provides functionally deep user administration and fulfillment capabilities along with good governance functionality, privileged access management and federated SSO. Its services have been particularly appealing to the higher education vertical.

Despite its lack of an access control engine for authorization enforcement, Fischer International's deep administration functionality, robust workflow, provisioning engine and good integration with both SaaS and legacy on-premises applications can address pure authentication and SSO needs within the workforce to SaaS and traditional/legacy workforce use cases. Its embryonic social identity integration significantly impacts its suitability for the B2C use case.

Gigya

Gigya provides an IDaaS service specifically designed to meet the majority of functional requirements for consumer IAM. The service includes an extensible directory, progressive profile and preference management, traditional registration and login, along with feature-rich and flexible social registration, login and social sync functions. The service also provides SSO using SAML and OpenID Connect federation, multifactor authentication using out of band (OOB) SMS, in-depth customer analytics, and integration with common third-party sales and marketing systems.

Gigya's excellent social identity integration and profile and password management capabilities make it well suited for the B2C use case. This is the only use case Gigya supports by design, which accounts for the absence of critical capabilities required to properly address the other two use cases.

IBM

IBM Cloud Identity Service (CIS) is provided in a multitenant model. However, components of the service can be delivered in a dedicated model. CIS is underpinned by IBM's SoftLayer infrastructure as a service (IaaS), and IBM's IAM software that delivers identity administration, approval workflow, user provisioning and access certification, along with authentication and access enforcement functionality. IBM has integrated CIS with Fiberlink's MaaS360 EMM capabilities to provide access enforcement that can use device registration and security posture to render access decisions.

IBM has a long track record as an enterprise IAM suite vendor with its strong federation, provisioning and governance features reflected through high Critical Capabilities scores overall and good alignment with the workforce to SaaS and traditional/legacy workforce use cases. CIS can address the B2C use case reasonably well and has customers leveraging it on a large scale for this purpose.

Ilantus

Ilantus provides IDaaS in a dedicated hosted tenant model. Ilantus began as an IAM system integrator, and has experience with traditional large-vendor IAM stacks. It offers four functional services: Xpress Access for identity administration, Xpress Governance for access governance, Xpress Sign On for SSO and Xpress Password for password management. Xpress Access and Xpress Governance are underpinned by RSA and IBM products. Ilantus also provides a cloud-based access certification offering called Access Review as a Service.

Ilantus particularly excels at addressing workforce to SaaS and traditional/legacy workforce use cases that require identity governance, provisioning and SSO to legacy application targets. It can support the B2C use case as well.

Intermedia

Intermedia offers a broad suite of cloud services, combining Microsoft products, proprietary products and third-party products. Intermedia's IDaaS offering, AppID, provides a strong set of capabilities for integrating with web applications, whether cloud-based or on-premises. This aligns AppID nicely with the workforce to SaaS use case, but organizations with traditional/legacy workforce requirements will likely find the lack of governance and on-premises legacy application support an issue. AppID does not have any social identity integration capabilities and is an unsuitable fit for the B2C use case.

iWelcome

iWelcome provides its IDaaS in a dedicated single-tenant delivery model to allow for customization and customer branding. Its offerings include authentication, SSO, federation, self-service registration and user provisioning support for on-premises and SaaS applications.

iWelcome is particularly strong in the area of access management with solid authentication, federation protocol and identity repository support. However, it lacks access request and workflow capabilities as well as support for legacy on-premises applications. iWelcome offers excellent support for the B2C use case, owing to its consumer-oriented features such as social registration and login, consent management, service desk automation, and configurability of the UX and European Union General Data Protection Regulation (EU GDPR) compliance.

Janrain

Janrain provides an IDaaS service specifically designed to meet the majority of the functional requirements for consumer IAM. The service includes an extensible directory, profile and preference management, delegated administration, flexible social registration and login functions, configurable SSO using federation, in-depth customer analytics, integration with fraud detection vendors, and integration with common third-party sales and marketing systems. The service supports OOB SMS authentication, in addition to passwords.

Janrain's strong social identity integration and profile and password capabilities make it well-suited for the B2C use case. This is the only use case it supports, however, given the absence of Critical Capabilities required to properly address the other two use cases.

Microsoft

Microsoft's Azure Active Directory (AD) Premium offering provides features that are in line with other web-centric IDaaS providers, and includes licenses for Azure Multi-Factor Authentication (MFA). It also includes licenses for Microsoft Identity Manager (MIM) that can be used with customers' on-premises web applications and for PAM. Microsoft offers Azure Active Directory Premium as part of its Enterprise Mobility Suite (EMS), along with Microsoft Intune EMM and Azure Rights Management, and the on-premises Advanced Threat Analytics tool.

Azure AD Premium aligns well with the workforce to SaaS use case. Its weak governance features and lack of support for legacy on-premises applications affect its suitability for the workforce to SaaS use case.

Microsoft recently expanded its IDaaS service to cover the B2C use case with Azure Active Directory B2C. Although it has some capabilities gaps, it can meet basic B2C needs for application developers.

Okta

Okta's IDaaS offering is delivered multitenant, with lightweight on-premises components for repository and target system connectors. IDaaS is Okta's core business. The vendor delivers basic identity administration and provisioning capabilities, access management for web-architected applications using federation or password vaulting and forwarding, and reporting. Okta also provides multifactor and adaptive authentication capabilities, including its own phone-as-a-token solution. The vendor added an integrated EMM product in 2014.

Okta excels at the workforce to SaaS use case and can satisfactorily support the B2C use case. Okta does not align well with the traditional/legacy workforce use case due to its nascent governance and legacy on-premises application support.

OneLogin

OneLogin's service architecture is multitenant, and lightweight integration components are used for on-premises connections. IDaaS is OneLogin's core business. The vendor delivers basic identity administration and provisioning capabilities, access management for web-architected applications using federation or password vaulting and forwarding, and reporting.

OneLogin does a good job meeting the workforce to SaaS and B2C use cases, and its acquisition of Cafésoft in late 2015 has allowed it to deliver improved support for on-premises web applications. However, OneLogin's weak identity governance functionally impacts its suitability for the traditional/legacy workforce use case.

Ping Identity

The PingOne cloud service is a multitenant web-centric IDaaS offering that Ping Identity targets toward large enterprises. Ping Identity provides a lightweight self-service bridge component to integrate a customer's Active Directory to the service, and also uses the well-established PingFederate product as the on-premises bridge component for customers when broad protocol and directory support are needed. In addition, PingAccess can be deployed to support proxy access to internal web applications and APIs. PingOne cloud includes PingID, a multifactor phone-as-a-token authentication solution that can utilize contextual data.

PingOne cloud does a good job of supporting workforce to SaaS and B2C use cases. However, the lack of user self-service access request, provisioning workflow and most identity governance features impact its scoring and make it an unlikely choice to be used alone for the traditional/legacy workforce use case.

RSA

RSA, a Dell Technologies business (acquired in September 2016), offers the RSA SecurID Suite of which IDaaS is a component. The RSA SecurID Suite has coalesced from the acquisitions of Aveksa and its IGA toolset and the acquisition of Symplified's intellectual property and some of its key staff. RSA SecurID Access is the service that provides web access management (WAM) functions, single sign-on and identity assurance. RSA Identity Governance and Lifecycle is the overarching name for a set of IGA functional offerings. The RSA SecurID Access and RSA Identity Governance and Lifecycle services, despite being marketed under one umbrella, are still technically very distinct services with their own administration and user interfaces joined by a portal. RSA SecurID Access' components are offered in a hybrid architecture with administrative components and multifactor authentication services mostly delivered from the cloud. The Access policy decision and enforcement points are implemented via an identity router that can be implemented in the cloud or on-premises.

RSA's mix of full IGA functionality and integrations with both SaaS and legacy on-premises applications make it a good fit for both the workforce to SaaS and traditional/legacy workforce use cases. Despite its strong heritage, RSA's cloud-delivered authentication capability lacks parity with the breadth of on-premises options. The absence of social identity integration make RSA a poor fit for the B2C use case.

SailPoint

SailPoint IdentityNow features access request and provisioning, access certification, password management, authentication and SSO service elements. The architecture is multitenant and can deliver services completely in the cloud, and it can be bridged to enterprise environments to support on-premises applications.

SailPoint has a full complement of provisioning connectors that enable integration with a wide variety of SaaS and on-premises applications, allowing it to align with both the workforce to SaaS and traditional/legacy workforce use cases. In contrast to its excellent access certification capability, the access request and workflow capability are particularly weak. IdentityNow does not support social identity integration, and is not a strategic fit for organizations seeking to address the B2C use case.

Salesforce

Salesforce provides Salesforce Identity as part of its Salesforce App Cloud PaaS. It sells Salesforce Identity as an independent service offering, but also includes it for established Salesforce customers. Identity Connect is Salesforce's on-premises bridge component that is sold separately. The Salesforce Identity service includes the baseline functionality required for inclusion, as well as social registration and login, federation gateway functionality, and deep access request and user provisioning workflow functionality.

Salesforce Identity's combination of excellent access request and workflow, strong social media integration and location-aware OOB push authentication (from the acquisition of Toopher in 2015) make it a suitable fit for the B2C and workforce to SaaS uses cases. However, Salesforce Identity does not support password vaulting and forwarding for applications that are not federation-enabled. Salesforce Identity does not align with the traditional/legacy workforce use case due to the absence of access certification capabilities and proxy-based access to on-premises web applications.

Simeio Solutions

Simeio Solutions provides a mixture of dedicated hosted and on-premises managed service offerings. Its services are underpinned by products from other well-established IAM software vendors, which allows the vendor to provide WAM; identity administration; access request; role and compliance; privileged access management; risk intelligence; IT governance, risk and compliance services; and directory services. The vendor provides its own overarching administration components and identity bridge that integrate with underlying products from other vendors.

Simeio's use of major IAM stack vendors' technologies provides it with an arsenal of products that are leveraged to provide highly rated capabilities across all three use cases, with notably excellent support for the traditional/legacy workforce use case. However, Simeio's use of OEM software from third-party vendors can add additional cost and complexity to a proposed solution.

Context

Vendors evaluated in this Critical Capabilities research come from distinctly different backgrounds. Their pedigrees vary greatly, as do their abilities to provide IAM functional depth and support for different use cases.

The IDaaS market was originally fueled by SMBs that used SaaS as their predominant application delivery model. Most of their applications already were in the cloud, and they preferred to buy rather than build infrastructure. In turn, SaaS applications became new identity silos, each with their own administration, access, authentication and event-logging capabilities.

IDaaS vendors create integrations with SaaS vendors for the purposes of authentication, SSO and account management (when SaaS vendors provide APIs to enable account management). In doing so, this allows IDaaS customers to enjoy seamless integration with a wide variety of SaaS applications. IDaaS vendors also can bridge customers' on-premises identity and authentication services, and use data held or copied from there (such as directory group or organizational unit membership) to provision and deprovision accounts on SaaS targets. This automation saves customers the effort of manually provisioning and deprovisioning accounts, and also can help to avoid orphaned active accounts on SaaS that can leave organizations vulnerable and paying for unused accounts.

Vendors with the ability to broker all the functions between users and SaaS have become increasingly appealing to organizations of all sizes over the past few years. During this time, web-centric IDaaS vendors have made solid gains at the lower end of the market, supporting the workforce to SaaS use case. As these vendors have moved upmarket, they found that larger organizations tend to have IAM products in place. These larger organizations also have deeper IGA functionality needs than web-centric vendors can provide, as represented by the traditional/legacy workforce use case. In addition, prospects with deeper IGA functionality needs typically require integration into legacy systems. This is forcing shallow-function, web-centric IDaaS vendors to add deeper functionality and integration capabilities to their roadmaps.

Conversely, IDaaS vendors with deeper IAM functionality and integration capabilities tend to be deployed in larger, complex implementations, and do not have competitively priced offerings for rapid handling of the workforce to SaaS use case. These vendors will need to provide a streamlined, rapidly deployable offering for this use case if they wish to make gains in the SMB market. Indeed, these bidirectional moves are starting to happen. By the end of 2017, Gartner anticipates the fuzzy line between web-centric and full-featured offerings will get even fuzzier. Overall, by 2020, 40% of IAM purchases will use the IDaaS delivery model — up from less than 20% in 2016. Of those IDaaS implementations, Gartner believes that 40% will replace on-premises IAM implementations (rather than simply augment those implementations) — up from 10% in 2016.

The workforce to SaaS use case drove growth in the early IDaaS market, and it still predominates. The B2C use case has grown in importance as organizations look to provide consumer access to their online applications or replace a mixture of custom-developed IAM products and traditional on-premises IAM products. Some larger organizations also are augmenting part of their IAM needs by IDaaS in a hybrid approach, even when they may own IGA and access tools that could be extended to the cloud. In these instances, IDaaS is being viewed as a quick win, and sometimes as a way to standardize a solution for one part of the organization's IAM problem space. However, IDaaS is not for every organization, and the IDaaS delivery model continues to represent a minority share of the overall IAM market (see "Magic Quadrant for Identity and Access Management as a Service, Worldwide"). IAM leaders should analyze the business and technology drivers and blocking factors, as well as the total cost of ownership, to make an appropriate choice (see "How to Choose Between On-Premises and IDaaS Delivery Models for Identity and Access Management").

Product/Service Class Definition

An IDaaS vendor is expected to deliver a predominantly cloud-based service in a multitenant or dedicated and hosted delivery model. The service brokers a set of functionality across multiple IAM functions — specifically, identity and governance administration (IGA), access enforcement, and analytics functions — to target systems on customers' premises and in the cloud.

Critical Capabilities Definition

Access Certification

Access certification is the process of requiring people such as managers and resource owners to certify the access that users have to resources on a periodic basis to ensure that access is still reasonable. Access certification helps with cleaning up accumulated access and regulatory compliance.

Many regulations, such as the Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA) and others require organizations to regularly validate the appropriateness of users' access.

To receive a "Good" rating for this capability, a service must include automated processes that utilize workflow and business-friendly interfaces for resource owners (or approvers) to review all users who possess certain entitlements.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also include support for an organization chart certification process that enables managers to review the access assigned to their subordinates as well as support for special-purpose certification campaigns, including organizational hierarchy certification, role certification, contractor certification and certification of a single user after moving between business units.

Access Request and Workflow

Access request and workflow provides a user-friendly access request experience that offers users access to a broad range of resources along with the workflow to support IDaaS components that enlist people to help make decisions in support of policy.

The user interface that allows users to request access to resources like applications and accounts has a significant impact on UX. This capability also includes the associated workflows that orchestrate a logical sequence of steps to enable critical provisioning functions such as access approvals, notifications, escalations and integration with other business processes. Workflows also allow business stakeholders, application owners and other authorities to validate and approve proposed changes before they are applied to target applications.

To receive a "Good" rating for this capability, a service must offer a business-friendly access request experience that enables end users to request access for themselves and for managers to request access for subordinates. Workflows for approval processes must support an approver delegating certain authority to others and the forwarding of requests to another approver if there is no response within a given time limit.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also include support for the creation of templates for frequent access requests; the ability for a requester and recipient to view request status and change or cancel in-flight requests; and the ability for end users to inspect their own access and view history of requests made on their behalf. Workflows for approval processes must support the ability to include multiple levels, applications or resource owner approval, and policy analysis (such as segregation of duties policy exceptions) with additional approval steps for unresolved policy violations by a control or policy owner.

Authentication

Authentication evaluates the range and variety of methods offered, as well as the incorporation of contextual/analytic and adaptive techniques. Particularly for consumers, for whom UX is critical, adaptive features and identity proofing are often required to achieve a sufficient level of trust.

To receive a "Good" rating for this capability, a service must offer native multifactor authentication options via an OTP app or out-of-band (OOB) methods along with integration support for third-party user authentication products.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also include OOB push modes and leverage broad contextual and/or adaptive authentication techniques as well as identity proofing natively or through integration with third-party providers.

Authorization Enforcement

Authorization enforcement primarily focuses on runtime authorization decisions made during a user's attempt to access specific applications or perform actions within applications, and the granularity to which policies can be enforced.

To receive a "Good" rating for this capability, a service must offer coarse-grained authorization enforcement to target systems.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also provide more granular authorization enforcement to target systems, for example, by allowing or limiting access to the subfunctions of a target application.

Cloud Directory

Cloud directory includes the flexibility to scale to support millions of users' profile data and associated identity attributes while enabling an organization to offload utilization, performance, failover and other availability concerns by leveraging this delivery model.

A cloud directory can be a practical place to store end-user records for partners, customers or contractors that an organization might want to keep separate from its on-premises employee user directories and related IAM infrastructure.

To receive a "Good" rating for this capability, a service must offer a cloud directory that includes support for connectivity to other sources and targets of identity.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also support extensibility for customers to alter and manage their own schemas, including the ability to add, change or delete attributes and their relationships.

Mobility Management

As mobility and identity are closely linked and further converging, IDaaS is extending its value into related markets for mobile devices by offering enterprise mobility management (EMM) capabilities as well as the ability to overcome native mobile application SSO and provisioning challenges.

To receive a "Good" rating for this capability, a service must support native mobile application integration and baseline mobile device management (MDM) functionality such as device registration, certificate management and certificate-based SSO.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also provide broader EMM functionality, including integrated device and identity service registration, native mobile app provisioning, and the use of mobile device security posture and contextual data to support access enforcement actions at runtime.

On-Premises Application Integration

On-premises application integration includes single sign-on (SSO) as well as user provisioning and deprovisioning for those applications that are still within an organization's domain, which may be web- or legacy-architected.

SSO enables access to multiple systems without requiring the user to log on to each system separately. A proxy approach can be used as an efficient alternative to federation to enable SSO. User provisioning and deprovisioning is the process of fulfilling changes on target resources based on identity life cycle events (such as join, leave and move). User accounts and their associated profiles can be created, modified, disabled and deleted according to policy across on-premises IT infrastructure and business applications.

To receive a "Good" rating for this capability, a service must support proxy or agent-based access to on-premises web, legacy and thick-client applications, and handle provisioning and deprovisioning for on-premises web applications.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also handle provisioning and deprovisioning for on-premises legacy (non-web-architected) and thick-client applications. The breadth and depth of built-in connectors and methods for configuring them are also considered.

Profile and Password Management

Profile and password management includes the ability for end users (and in the case of employees, their managers) to manage their data in a direct and transparent fashion, including their user profile and privacy settings. This also includes self-service registration and self-service password reset.

To receive a "Good" rating for this capability, end users must be able to access all self-service and delegated administration tasks from a common web interface. The user interface should be highly usable regardless of PC, mobile browser or app used. More specifically, a service must offer the following baseline functionality for profile and password management:

- Profile management — Provide self-service management capabilities that allow users and delegated administrators to create, update and delete the account information stored in the user profile such as identity attributes, username and password, user preference and privacy settings.
- Password management — Support the ability to set and maintain passwords for user accounts according to policy with enforcement of password constraints.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also include support for additional profile management features such as self-service registration and progressive profiling. Additional password management features must be included to aid with enrollment of users for self-service password reset (SSPR) as well as support for multiple password policies, authentication methods and control over accounts to which passwords are propagated for password synchronization.

Reporting and Analytics

Reporting and analytics provides a detailed audit trail of identity-related transactions and a set of predefined, out-of-the-box reports and dashboards as well as the ability to mine identity and activity data to enable actionable, context-specific insight.

To receive a "Good" rating for this capability, a service must log all administrative and access events, and make the log data available to customers for their own analysis through built-in reports, dashboards and export options.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also support custom reports as well as the analysis of identity and activity data using multiple perspectives and statistical methods. This information should enable insights to be obtained, such as role mining, advanced risk analysis and scoring, peer group analysis, anomaly detection, privileged access monitoring, proactive analytics and fine-grained separation of duties (SoD) analysis.

SaaS Application Integration

SaaS application integration includes single sign-on (SSO) as well as user provisioning and deprovisioning for a variety of SaaS applications.

SSO enables access to multiple systems without requiring the user to log on to each system separately. Federation technology is the best and most common way to achieve SSO to SaaS applications because it provides a secure, standards-based approach to providing cross-domain SSO. Finally, because many SaaS applications still do not support federation, organizations choose to resort to password vaulting to provide an SSO experience for users even though it is not as secure as federation. User provisioning and deprovisioning is the process of fulfilling changes on target resources based on identity life cycle events (such as join, leave and move). User accounts and their associated profiles can be created, modified, disabled and deleted according to policy across cloud-based IT infrastructure and business applications.

To receive a "Good" rating for this capability, a service must support SaaS application SSO using federation standards or password vaulting and forwarding, as well as user provisioning.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also have an extensive catalog of out-of-the-box integrations with SaaS applications as well as a good UX for end users and easy configuration for administrators.

Social Identity Integration

Social identity integration includes support for social registration, social login and social identity linking with organization-managed identities for common social networks such as Facebook, Twitter, Google, VK, QQ, Weibo, LinkedIn and others.

In a typical B2C use case, permission-based user data is automatically captured as part of a social login, an identity provider's authentication process or a registration process.

To receive a "Good" rating for this capability, a service must support social login for the most common social networks as well as the retrieval of attributes to support identity provisioning, and link these social identities with the service's or enterprise customer's established identities.

To receive a rating in the "Excellent" or "Outstanding" range, a service must also include significant malleability and depth of functionality for integrating social identities, support a broad range of social identity providers, and support advanced integration features such as social sharing and data aggregation.

Use Cases

Gartner has identified three use cases for IDaaS, each with its own requirements, to capture the most important functionality expressed by Gartner clients. However, there are other use cases for IDaaS (such as B2B) that may be relevant to some organizations yet have not reached a level of client interest to warrant inclusion in this document. Use cases are not mutually exclusive, so more than one may apply to a particular organization.

Workforce to SaaS

The workforce to SaaS use case focuses on IAM to predominantly SaaS applications for employees.

This use case is primarily driven by the need to extend basic IAM functions and serve employees accessing SaaS applications. This need is often viewed as lower hanging fruit than replacing an established on-premises software suite implementation that supports legacy applications. IDaaS vendor authentication, provisioning and reporting capabilities prove compelling for organizations with significant or increasing SaaS adoption, particularly if it is having difficulty maintaining staff IAM expertise.

Given this context, the SaaS application integration critical capability is weighted most heavily for the workforce to SaaS use case followed by authentication, profile password management, access request, and workflow and mobility management.

Business-to-Consumer (B2C)

The business-to-consumer use case focuses on IAM to on-premises and cloud-based web applications for consumers.

Social identity integration can significantly enhance a consumer's user experience by reducing login and account creation friction, and also by providing attributes that enable a website to provide a richer, more personalized experience, in turn deepening customer intimacy. Accordingly, this critical capability is weighted most heavily for the business to consumer use case.

The authentication critical capability is also weighted heavily because many organizations will need additional assurance that the end user is a real person (not a bot) or is a specific individual. This is particularly important in situations where the end user will have access to sensitive information that will require some level of step-up authentication or adaptive access processing.

Finally, profile and password management is weighted heavily for the B2C use case since this capability is essential to rounding out a secure, unified and compelling customer experience.

Traditional/Legacy Workforce

The traditional/legacy workforce use case focuses on requirements for more functional depth in IGA and includes legacy (non-web-architected) on-premises application targets.

IDaaS functionality continues to evolve and improve. Some IDaaS vendors have proven that they can deliver the functionality from the cloud that traditionally has been provided by full-featured IAM stacks managed within the enterprise (see "Magic Quadrant for Identity Governance and Administration"), such as multilevel provisioning approval workflows, as well as identity governance features like access certification, segregation of duties policy enforcement, and role lifecycle management.

Based on these requirements, the on-premises application integration capability is weighted most heavily for the traditional/legacy workforce use case followed by access certification.

Inclusion Criteria

A vendor must have a service that meets the following criteria:

- Must be a predominantly cloud-based service, delivered via a multitenant or dedicated and hosted model.
- Must be manufactured and operated by the vendor or must be a significantly modified version obtained through an OEM relationship. Service offerings that have merely been obtained without significant functional modification through a licensing agreement from another vendor (that is, as part of a reseller/partner or service-provider agreement) do not meet this criterion.
- Must have been in general availability and deployed in customer environments as of 31 December 2015.

- Must have a presence in at least two locations worldwide and be industry-independent.
- Must have a significant market presence in at least one of the use cases and at least four of the critical capabilities listed below. Market presence can be demonstrated in one of two ways — by significant market share or by differentiating innovation.

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Workforce to SaaS	Business-to-Consumer (B2C)	Traditional/Legacy Workforce
Access Request and Workflow	10%	0%	10%
Access Certification	4%	0%	19%
Authentication	16%	15%	5%
Authorization Enforcement	4%	0%	6%
Cloud Directory	4%	8%	1%
Mobility Management	10%	1%	8%
On-Premises Application Integration	0%	4%	30%
Profile and Password Management	14%	25%	14%
Reporting and Analytics	7%	5%	7%
SaaS Application Integration	30%	7%	0%
Social Identity Integration	1%	35%	0%
Total	**100%**	**100%**	**100%**
			As of September 2016

Source: Gartner (September 2016)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases

Critical Capabilities Rating

Each of the services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 2. Service Rating on Critical Capabilities

Critical Capabilities	Bitium	Centrify	Covisint	RSA	Fischer International	Gigya	IBM	Ilantus	Intermedia	iWelcome	Janrain	Microsoft	Okta	OneLogin	Ping Identity	SailPoint	Salesforce	Simeio Solutions
Access Request and Workflow	3.0	3.0	4.5	4.5	4.5	1.0	4.3	4.2	2.8	1.0	1.0	3.0	3.5	3.0	2.0	2.4	4.8	4.5
Access Certification	1.0	1.0	3.3	3.7	3.0	1.0	4.4	3.8	1.0	1.0	1.0	2.0	1.0	2.0	1.0	4.7	1.0	4.4
Authentication	3.0	4.3	3.2	3.5	3.0	3.0	3.5	3.0	4.0	4.1	2.5	4.5	4.0	4.0	4.0	4.0	4.0	3.0
Authorization Enforcement	3.0	3.0	3.0	3.0	1.0	1.0	3.5	3.0	4.5	2.0	1.0	3.0	3.0	3.0	3.0	3.0	3.0	4.5
Cloud Directory	2.5	3.0	4.0	3.0	2.5	4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.5	4.5	4.0
Mobility Management	2.5	5.0	1.0	3.0	2.0	1.0	3.5	2.5	2.0	3.0	1.0	4.5	4.0	3.0	2.0	3.0	3.0	2.5
On-Premises Application Integration	2.0	2.0	3.0	4.0	4.0	1.2	4.0	4.5	3.0	2.0	1.0	2.0	2.0	3.5	3.0	4.5	2.0	4.0
Profile and Password Management	3.0	4.0	4.0	3.0	4.0	4.8	3.5	4.0	4.0	4.0	4.6	3.0	3.5	4.0	2.3	4.0	4.4	4.0
Reporting and Analytics	3.0	4.0	3.0	4.0	4.0	4.0	4.0	4.0	3.0	3.0	3.5	4.5	3.0	3.0	3.0	3.0	4.0	4.0
SaaS Application Integration	4.3	4.5	2.7	3.0	2.0	2.0	3.0	3.0	3.5	4.0	1.5	4.0	4.9	4.5	4.6	4.0	2.8	3.3
Social Identity Integration	1.0	3.0	2.5	1.0	1.2	5.0	3.0	2.5	1.0	4.5	4.7	2.5	3.0	3.0	3.0	1.0	3.8	3.0
As of September 2016																		

Source: Gartner (September 2016)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case

Table 3. Service Score in Use Cases

Use Cases	Bitium	Centrify	Covisint	RSA	Fischer International	Gigya	IBM	Ilantus	Intermedia	iWelcome	Janrain	Microsoft	Okta	OneLogin	Ping Identity	SailPoint	Salesforce	Simeio Solutions
Workforce to SaaS	3.22	3.99	3.08	3.31	2.84	2.52	3.52	3.35	3.33	3.35	2.23	3.79	3.91	3.75	3.30	3.65	3.53	3.56
Business to Consumer	2.31	3.58	3.14	2.47	2.59	4.12	3.38	3.26	2.81	4.05	3.82	3.25	3.46	3.61	3.16	2.95	3.90	3.44
Traditional/Legacy Workforce	2.28	2.76	3.21	3.68	3.46	1.93	3.94	3.90	2.81	2.27	1.78	2.82	2.58	3.16	2.40	3.92	2.83	3.99
As of September 2016																		

Source: Gartner (September 2016)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrant for Identity and Access Management as a Service, Worldwide"

"How to Choose Between On-Premises and IDaaS Delivery Models for Identity and Access Management"

"How Products and Services Are Evaluated in Gartner Critical Capabilities"

Evidence

The following sources were used in the creation of this research:

- Gartner client interactions
- Phone interviews and online surveys for vendor-provided references
- A comprehensive vendor survey and video demonstration that aligned with the critical capabilities

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp