



User Identity Access Management

Market Segment Report



May 2019
Cyber Source Data
Wellington Research

Updated July 2019

User Identity Access Management

Market Segment Report

Table of Contents

Market Spotlight for User Identity Access Management	3
Introduction	4
The What and Why of User Identity Access Management	4
UIAM and the Market Spotlight	5
Profiles of Market Segment Supply and Demand	6
UIAM Vendors - Segment Specialists	7
UIAM Vendors - Market Innovators	8
UIAM Vendors - Technology Innovators	9
UIAM Vendors - Market Leaders	10
Relative Vendor Value	11
Market Spotlight Value	12
Market Cycle for UIAM	13
Market Size and Growth Forecast	14
Futures Forecast for UIAM	15
Finding "Best-Fit" Market Offers	16
Summary Observations	17
Cyber Standards and Reference Frameworks	17
Vendor Inclusion and Assessment Criteria	18

List of Figures

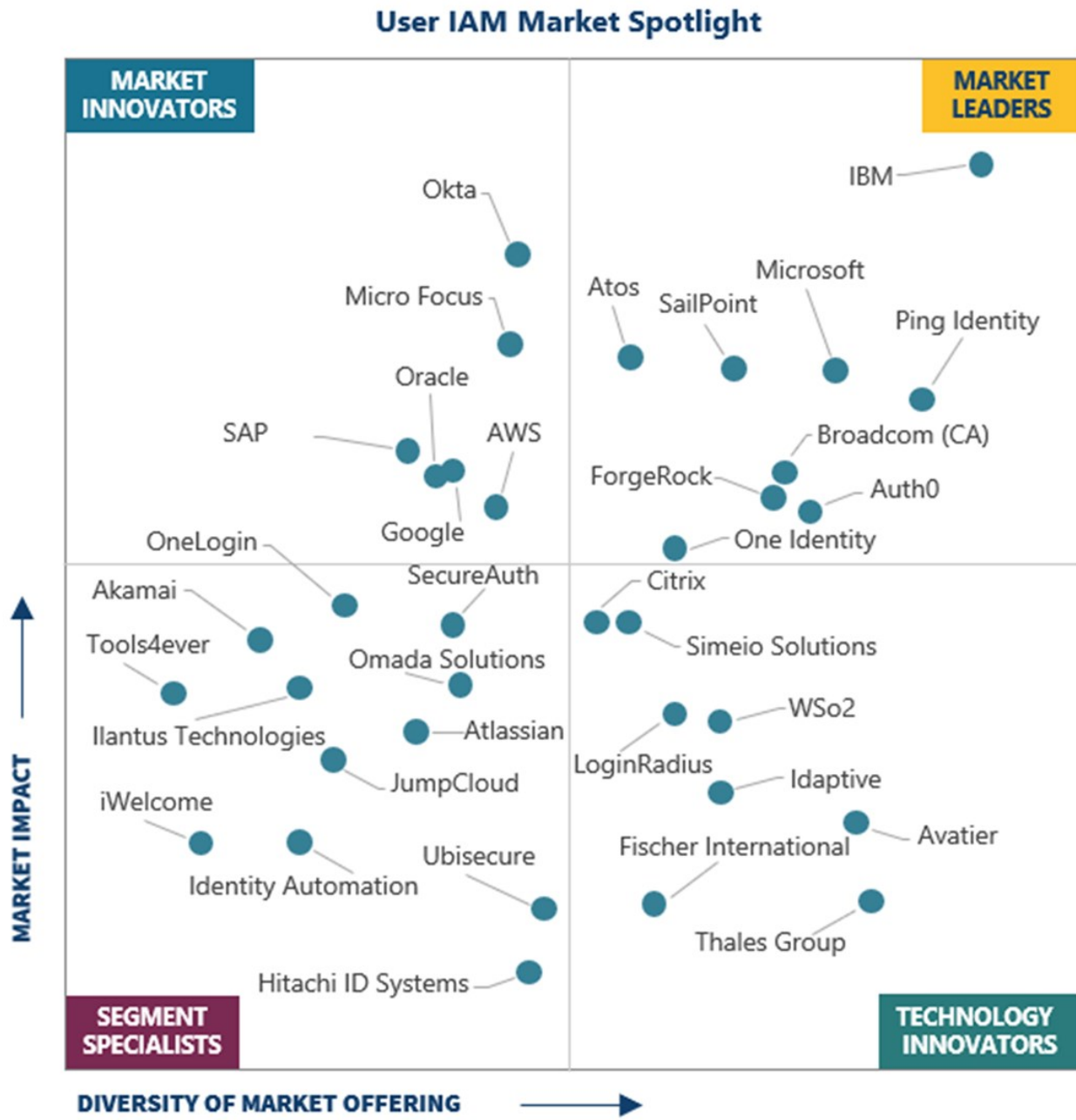
Figure 1: Market Spotlight for User Identity Access Management	3
Figure 2: Scope of User Identity Access Management	4
Figure 3: Segment Specialists	7
Figure 4: Market Innovators	8
Figure 5: Technology Innovators	9
Figure 6: Market Leaders	10
Figure 7: Relative Vendor Value for UIAM	11
Figure 8: Market Spotlight Value for UIAM	12
Figure 9: Market Cycle for UIAM	13

This report is updated effective July 2019

Market Spotlight - User Identity Access Management

The Market Spotlight for User Identity Access Management (UIAM) covers the market positions of thirty-five (35) vendors delivering products and services for UIAM along the Market impact x Cyber diversity axis. Another equally valid perspective on vendors identifies the relative differences in value being delivered for the money being spent on UIAM. This Market Segment Research Reports covers both and asks readers to make "best-fit" selection of vendors to meet their needs.

Figure 1: Market Spotlight for UIAM



Introduction

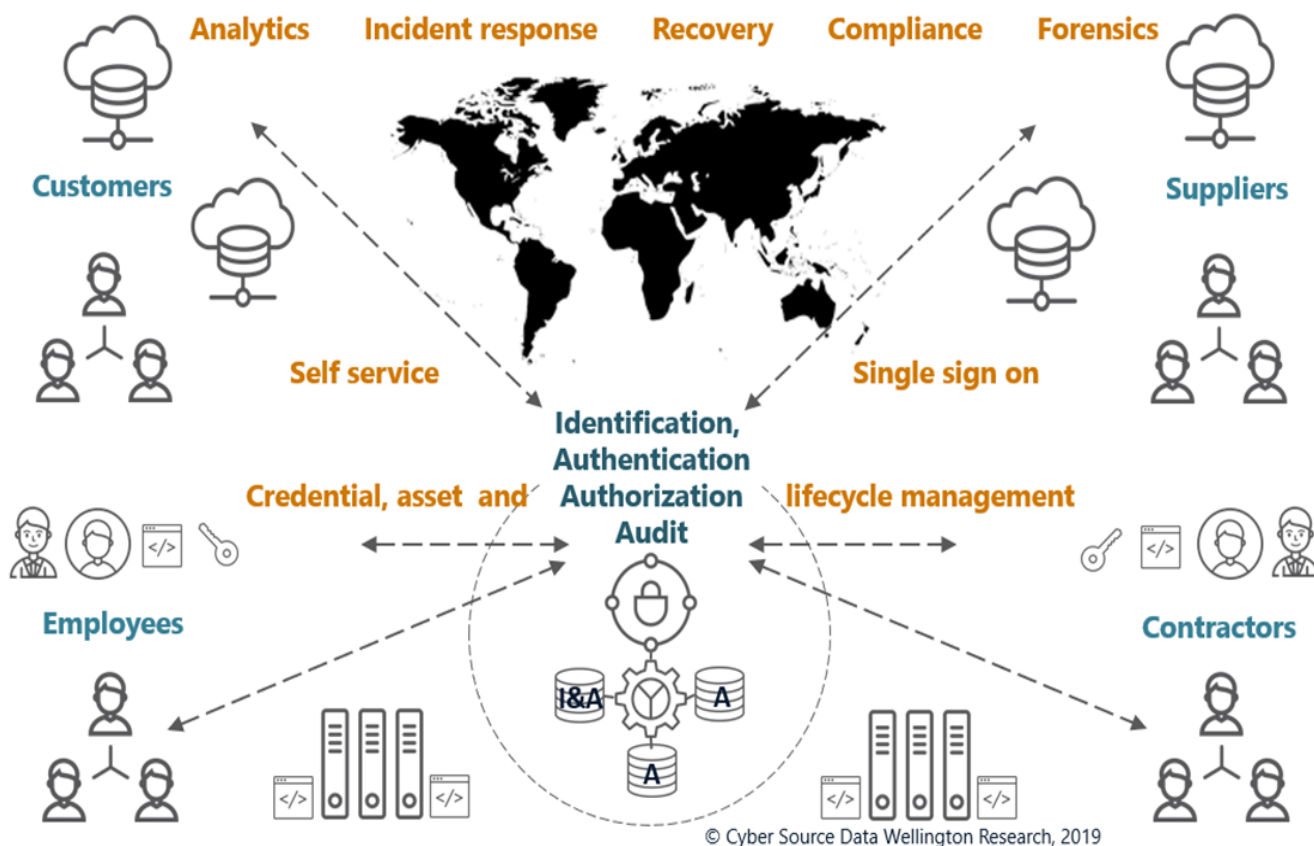
This Market Segment Report covers User Identity Access Management (UIAM) and the market positions of 35 vendors delivering products and services for UIAM. The Report includes the Relative Vendor Value and Value Spotlight charts, Market Size and Forecast and Segment Futures for UIAM. Of the 35 vendors profiled by this report:

- Twelve are operating as segment specialists
- Six are market innovators
- Eight are currently technology innovators
- Nine are market leaders

The What and Why of User Identity Access Management

At its core, UIAM is about providing users with access to digital resources, assets, applications, data, and business procedures. The users may be customers, suppliers, contractors, or employees of an organization. UIAM identifies users, authenticates users, audits what users access and do, and provides a record of access requests and actions taken by users and software applications acting on behalf of users. In addition, many UIAM deployments must deliver access to authorized digital assets used in business operations, including enabling users to register and create their own accounts, allowing users to manage their own accounts and credentials, logon users once to access authorized applications and data, analyze logon patterns for fraud and Cyber attacks, provide evidence for incident response, be instantaneously recoverable, ensure compliance with local laws and regulations, not cause disruptions and remain always-on, 24 x 7 x 365, year-in and year-out.

Figure 2: Scope of User Identity Access Management



The holy grail of UIAM is validating digital identities to provide authorized access while *remaining a frictionless experience and not being noticed*: in short UIAM must be as invisible as a ghost yet be as vigilant as a relentless guard dog at all times.

Why UIAM is important to organizations varies by industry and entity, generally depending on several factors, including: (a) the importance of using digital and the user experience to expand and grow market share, revenues and earnings, (b) the complexity of the digital value chain of the organization, (c) the legal and regulatory mandates buffeting the organization, and (d) the cost of labor for provisioning and managing logon systems and accounts, credentials, digital assets, and maintenance of such accounts to provide users with authorized access to digital assets.

As a recent development, some vendors are claiming a new category of User IAM exists being called "Customer Identity Access Management (CIAM). This Market Segment Research Report does segregate a CIAM sub-category, and instead includes all User Identity Access Management, whether people are citizens, consumers, business customers, suppliers, contractors or employees. The result is that most vendors of UIAM offerings, including those with and without so-called CIAM offers - subject to constraints listed in the Vendor Inclusion and Assessment Criteria found on page 14 - are included herein.

UIAM and the Market Spotlight

The following sections provide comparative insight into some of the differences in the market for UIAM offerings, from market specialists, technology innovators, market innovators, and market leading vendors. Market Spotlights and this Market Segment Report cover the following:

- Market Spotlight Charts formulate a market offering segment by the impact of vendors (on the Y-axis) and diversity of Cyber offerings of vendors (on the X-axis)
- Vendors with larger market impacts - larger revenue, geographic sales and service, and partnerships - are located in the upper-half of Market Spotlight charts while vendors with smaller market impacts - smaller revenue, geographic sales and service, and partnerships - are located in the lower-half of Market Spotlight Charts
- Vendors with more expansive Cyber offerings - more digital ecosystem, cyber activity, market offer and partner coverage - are found on the right-hand side of Market Spotlight Charts while those with less diverse Cyber offerings - fewer digital ecosystem, cyber activity, market offer and partner coverage - are on the left hand side of Market Spotlight Charts
- The four corners of a Market Spotlight chart are denoted as *Segment specialists* in the lower left, *Market innovators* in the upper left, *Technology innovators* in the lower right portion of the chart, and *Market leaders* in the upper right part of the chart

Each of the market segment categories – and the vendors in each category – offer something unique for UIAM and each vendor is considered a "best-fit" by their customers. We encourage readers to assesses their own needs and accomplish this using the sourcing and selection framework listed in the section entitled "Finding The Best Fit Market Offer" of this report.

The criteria used for inclusion of vendors, and the assessment and formulation criteria for Market Spotlights is found on the last page of the Market Segment Research report. Acquisitions or spinouts of UIAM related vendors are denoted within parenthesis next to the active going concern vendors for each of the categories that follow.

Profiles of Market Segment Supply and Demand

Segment Specialists

Segment specialists meet customer requirements other suppliers are unable or unwilling to satisfy, whether these be tangible needs such as functions, terms and prices or intangibles such as services, value and supply chain extensions among others. Segment specialists are sought out for highly specialized or customizable digital products and services and can become trapped by a cycle of one-off customization and less standardization. The segment specialists never disappear although the suppliers populating the category may change over time due to mergers and acquisitions, financial difficulties, or changes in market strategy. The segment specialists are dominated by private firms and smaller businesses. Buyers tend to be dominant by industry and size and all have some unusual size shoes to fit.

Market Innovators

Market innovators are especially attractive to late adopters seeking to use the market transforms of stable vendors that can assist with aspirational business objectives of buyers. Market innovation tends to occur later in market cycles between market consolidation and decline and is more typically provided by larger established vendors rather than new startups and less mature sources of supply. A few Cyber segments are populated by market innovators and these tend to be focused on longer-lived Cyber market segments. Market innovating vendors tend to have deeper pockets from which to pursue larger deals with buyers that tend to be skittish of new technology. Buyers are from all industries, all size organizations and all stages of market development.

Technology Innovators

Technology innovators are on the leading edge, seeking technology leadership as market differentiators. The products and services of these suppliers are eagerly purchased by early adopters and organizations seeking to employ digital technologies for their own market differentiation efforts. What was once novel eventually becomes commonplace, generating the need to reinvent using technology again. Technology innovation is replete with short product life cycles and is more common in select industries, tends to be populated by start-ups and smaller private firms on the supply side. Buyer's tend to hail from all industries with a few notable industries by size dominating early-stage technology buys. As the new technology becomes common, it makes its way to mainstream buyers.

Market Leaders

Market leaders are sought by most mainstream buyers worried about selecting technologies and suppliers too soon or too late. Heavily swayed by peer pressure, these buyers tend to move in packs, resulting in onrushes of orders and markets that can define winner-take-all vendors and markets in five years or less. Focused obsessively on operational "ability" characteristics, these buyers dominate technology orders and markets. Over time the choices of these buyers can force some vendors to reposition their value propositions, products and services to attract market orders and remain relevant.

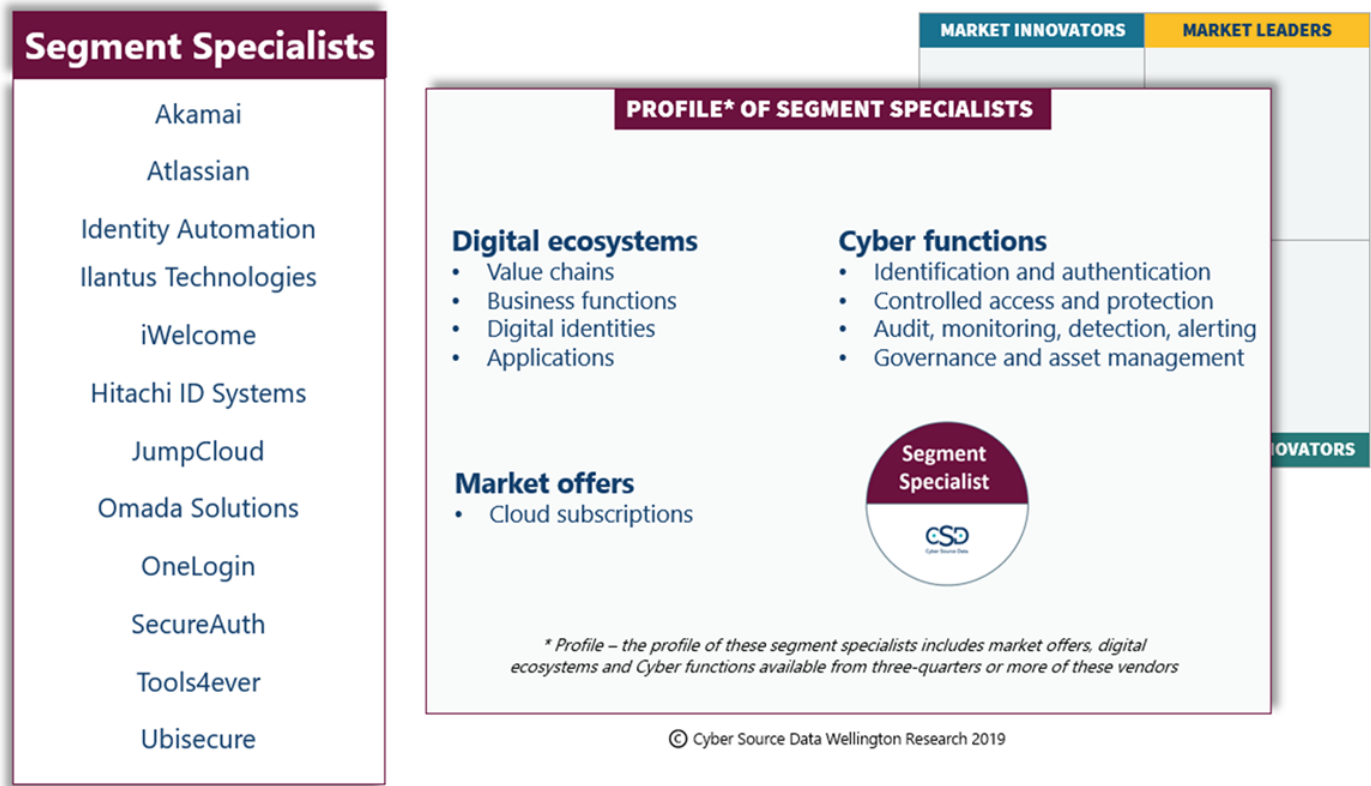
UIAM and Market Segments

The following pages provide an overview of the vendors occupying each of the market segments, the pros and cons of each segment, and the broad product and service coverage - by three fourths or more vendors - for digital ecosystems, Cyber activities and market offers of the vendors in each of the segments.

UIAM Vendors - Segment Specialists

Among the 35 vendors covered by this Market Segment Report, twelve (12) are operating as Segment Specialists. The segment specialists for UIAM include: Akamai (*Janrain*), Atlassian, Identity Automation (*2FA, HealthCast*), Ilantus Technologies, iWelcome, Hitachi ID Systems, JumpCloud, Omada Solutions, OneLogin (*CafeSoft, Portadi, Sphere Secure, ThisData*), SecureAuth, Tools4ever, and Ubisecure. These vendors currently share more than 10 percent of total market spend on UIAM while delivering about five percent of its aggregate cyber diversity.

Figure 3: Segment Specialists



All of the segment specialists are delivering core requirements for UIAM while specializing in one or more things for UIAM and doing it exceedingly well. Some of these vendors may focus on more specialized implementations of UIAM and/or customizing UIAM products and services when compared with other vendors.

Segment Specialist Pros

Most of these vendors are uniquely focused on delivering UIAM for the value chain, be that with consumers, business customers, or among business supply chain providers, and most are focused on delivering UIAM as a Cloud service. More of the vendors in this category are expanding their UIAM offerings through organic growth rather than acquisitions.

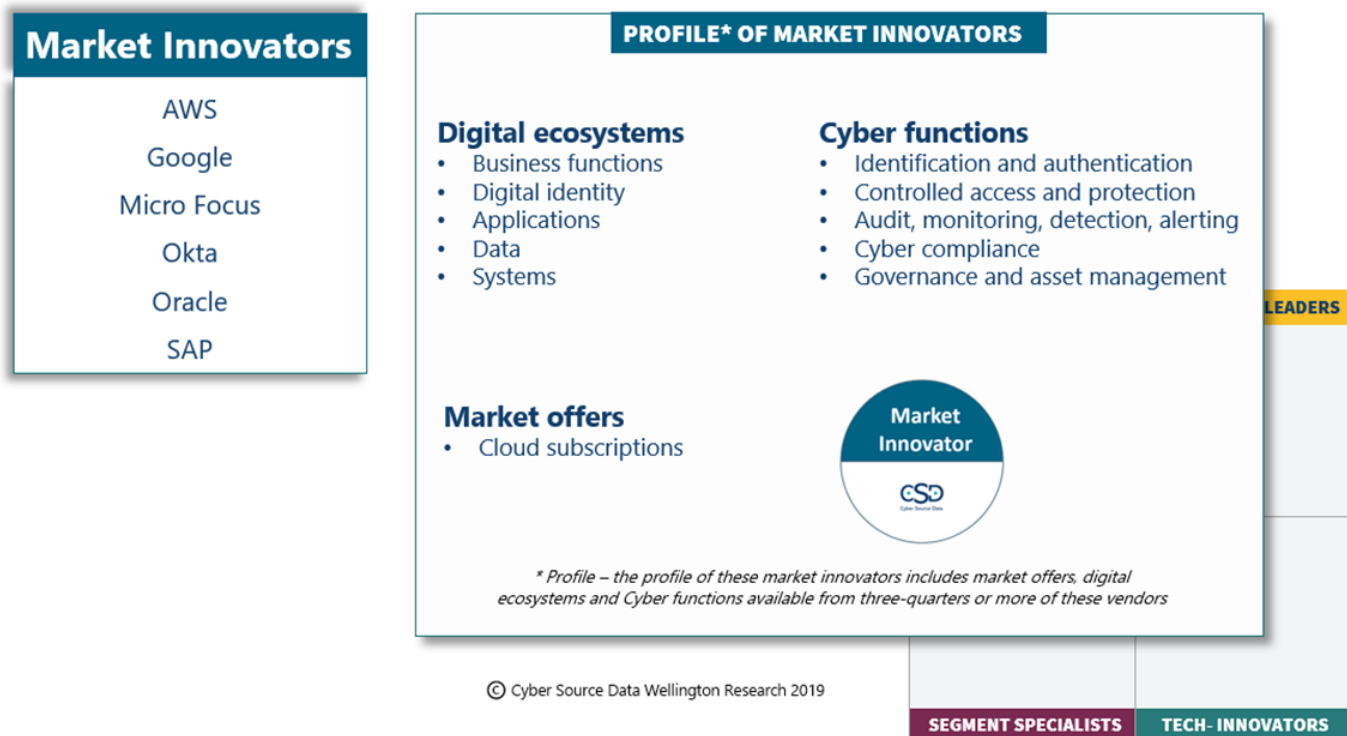
Segment Specialist Cons

Buyers seeking on-premises products for UIAM may be disappointed by the relative lack of support for this among most - but not all - segment specialists: most of which are focused on Cloud subscription services for UIAM.

UIAM Vendors - Market Innovators

Among the 35 vendors covered by this Market Segment Report, six (6) are operating as Market innovators. The market innovators for UIAM include: Amazon Web Services (listed as AWS), Google (*Bitium*), Micro Focus (*NetIQ*), Okta (*Azukua*), Oracle (*many acquisitions*), and SAP (*Gigya*). These vendors share more than 30 percent of the total spend on UIAM while delivering just four percent of its aggregate cyber diversity.

Figure 4: Market Innovators



All of the segment specialists deliver core requirements for UIAM while specializing in innovative market integration and delivery of UIAM services using Cloud services. Most of these vendors focus on implementations of UIAM unique to the environments in which the vendor specializes, whereas a few focus on cross-platform and cross-environment specialization.

Market Innovator Pros

Most of these vendors are uniquely focused on delivering UIAM for day-to-day business functions, be that with business customers, or among business supply chain providers, and most are focused on delivering UIAM as a Cloud service.

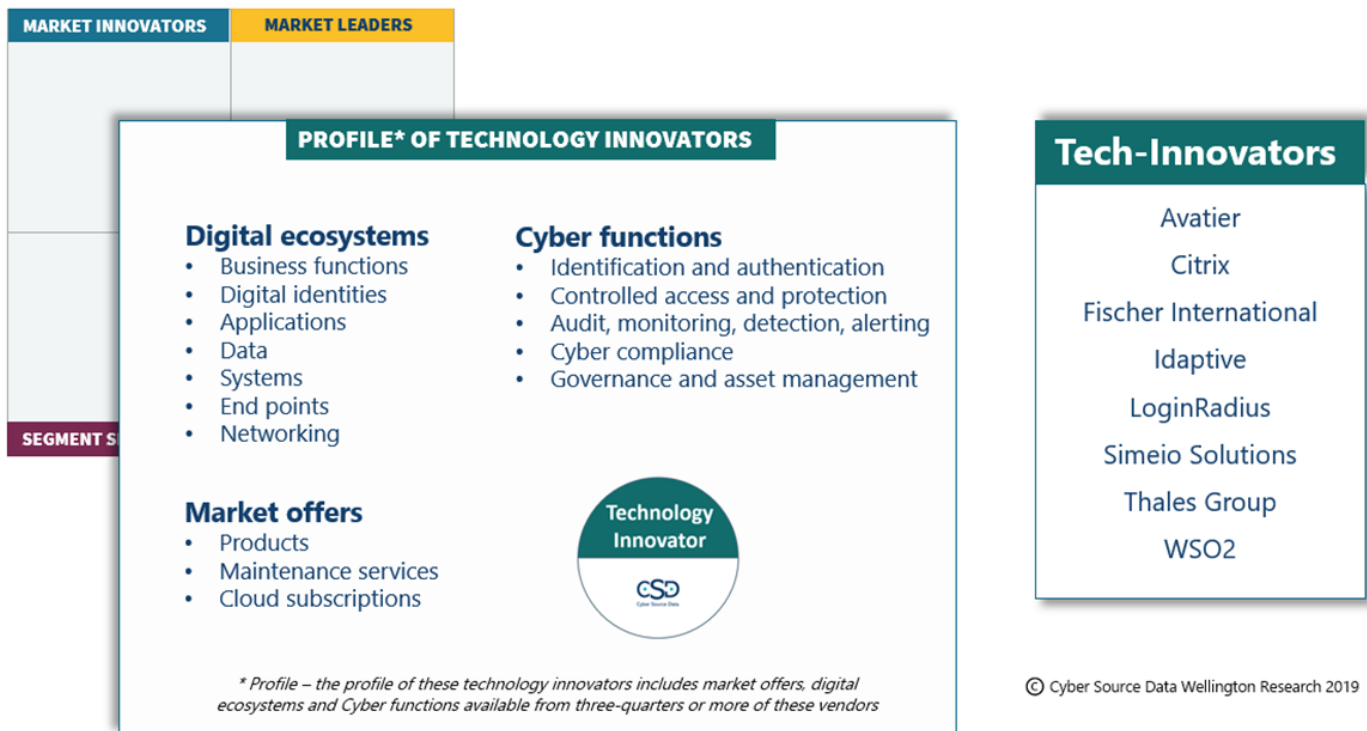
Market Innovator Cons

Buyers seeking on-premises products for UIAM may be disappointed by the sparse lack of support for this option among most - but not all - market innovators, most of which are focused on Cloud subscription services for UIAM. All of the vendors in this category are expanding their UIAM offerings by pursuing acquisitions.

UIAM Vendors - Technology Innovators

Among the 35 vendors covered by this report, eight (8) are operating as a technology innovators for UIAM, including Avatier, Citrix, Fischer International, Idaptive (a Centrify spinout), LoginRadius, Simeio Solutions, Thales Group (*Thales, Gemalto, SafeNet*), and WSO2. These vendor are delivering capabilities for UIAM that approach and in some cases exceed what market leaders are delivering. These vendors share about seven percent of total spend on UIAM while delivering more than 30 percent of its aggregate cyber diversity.

Figure 5: Technology Innovators



Technology Innovator Pros

Some of these vendors are delivering support for cyber activities, digital ecosystems, market offers and partnerships that approach that of market leaders, but generally at lower price points. These providers offer a choice of products and Cloud services for UIAM, and surround core UAIM functions with innovative applications for compliance, asset management and governance. The vast majority of these vendors are expanding their UIAM offerings via organic growth rather than through acquisitions.

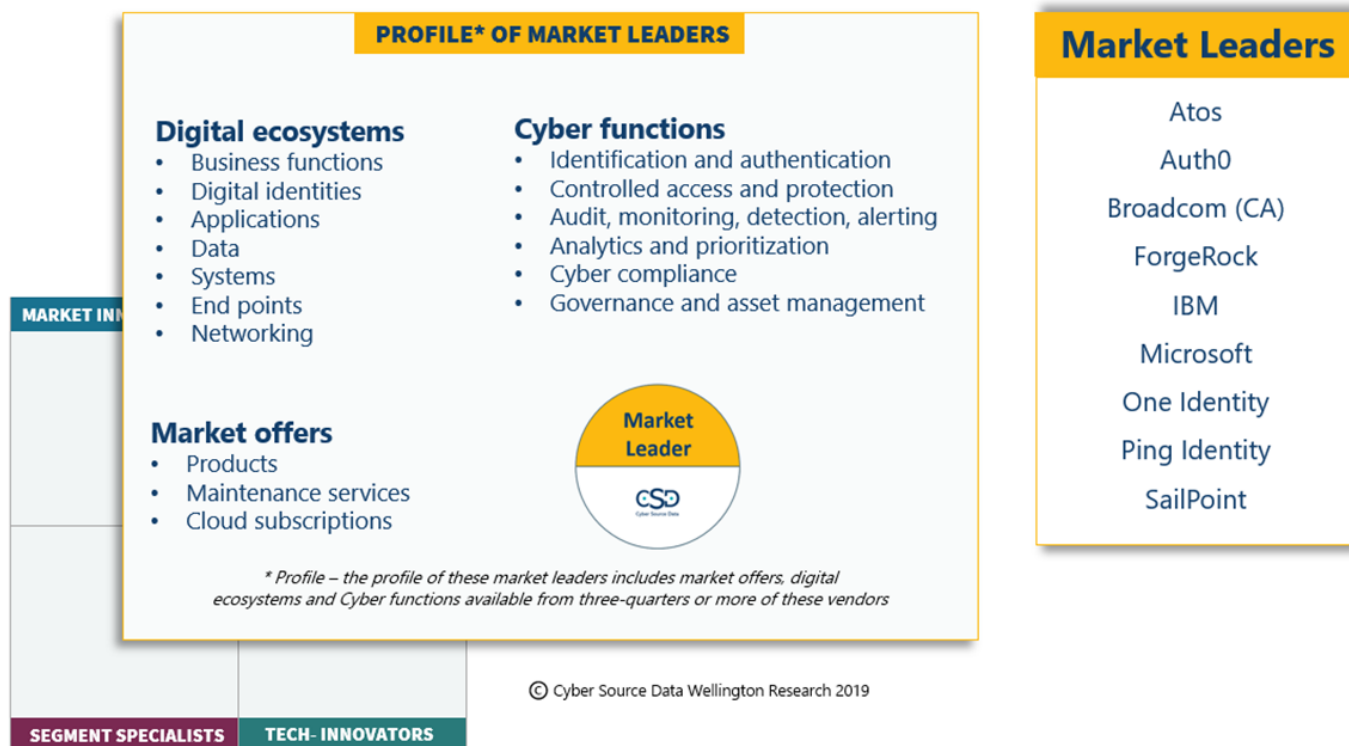
Technology Innovator Cons

Some of these vendors - but not all - are delivering first generation robotics and analytics that may have to be retrofitted at a later date. What some of these vendor may lack in customer service, training and integration services may - or may not - be counterbalanced by more attractive pricing or terms than market leaders.

UIAM Vendors - Market Leaders

Among the 35 vendors covered by this Market Segment, nine (9) are operating as market leaders for UIAM. These vendors include: Atos (*many acquisitions*), Auth0, Broadcom (CA, *many acquisitions*), ForgeRock, IBM (*many acquisitions*), Microsoft (*many acquisitions*), One Identity (*Balabit*), Ping Identity (owned by Vista Equity partners), and SailPoint (*Whitebox Security*). These vendors are receiving about 52 percent of total market spend on UIAM while delivering about 60 percent of its aggregate cyber diversity.

Figure 6: Market Leaders



Market Leader Pros

These vendors are generally delivering the most expansive capabilities and feature sets for UIAM and reaching the needs of more customers than any other segment. In addition this category of vendors is - mostly - uniquely delivering advanced analytics and prioritization services for UIAM that make the holy grail of UIAM more achievable.

Market Leader Cons

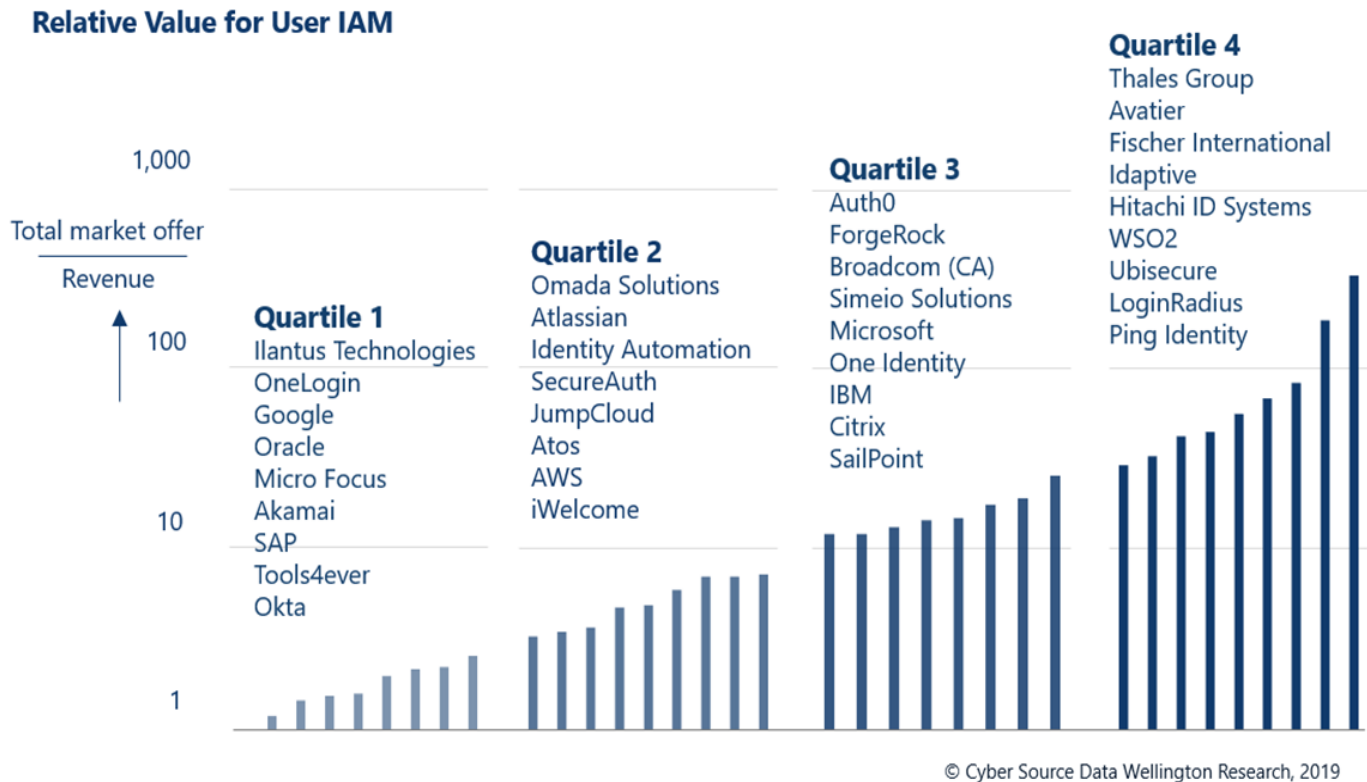
The advantages offered by these vendors comes at generally higher prices for goods and services and there may be some risks for smaller customers of these vendors, whose revenue contributions are less likely to be noticed than that of larger customers. The majority of these vendors have expanded their UIAM offerings via acquisitions rather than through organic growth.

Relative Vendor Value for UIAM

The relative vendor value chart (Figure 7) displays overall Cyber capabilities being delivered by vendors for the money spent by the market. Relative Vendor Value employs observable measures of market impact (such as revenue) and Cyber diversity (such as market offers, technology partners, and coverage of cyber activities and digital ecosystems) to display the relative differences of Cyber diversity by market impact of the UIAM vendors covered by this report.

For the same market impact (approximate to revenue), vendors with higher Relative Vendor Value deliver more diverse UIAM offerings to customers while those with lower Relative Vendor Value are delivering less diverse UIAM products and services. A different way to interpret the chart is that for the same level of Cyber diversity, vendors of lower Relative Vendor Value may be charging more than others (~ revenue) while those delivering more Relative Vendor Value may be charging less than others.

Figure 7: Relative Vendor Value for UIAM



Of course the Relative Vendor Value charts are just that: it is a relative comparison of Cyber diversity divided by market impact of a cohort of vendors. Its shortfalls include: 1) no insights into whether Cyber diversity delivered by a vendor meet the needs of a buyer, 2) whether the vendors offerings require an inordinate amount of money and time for integration, or 3) whether the scalability and other *ility requirements can be achieved.

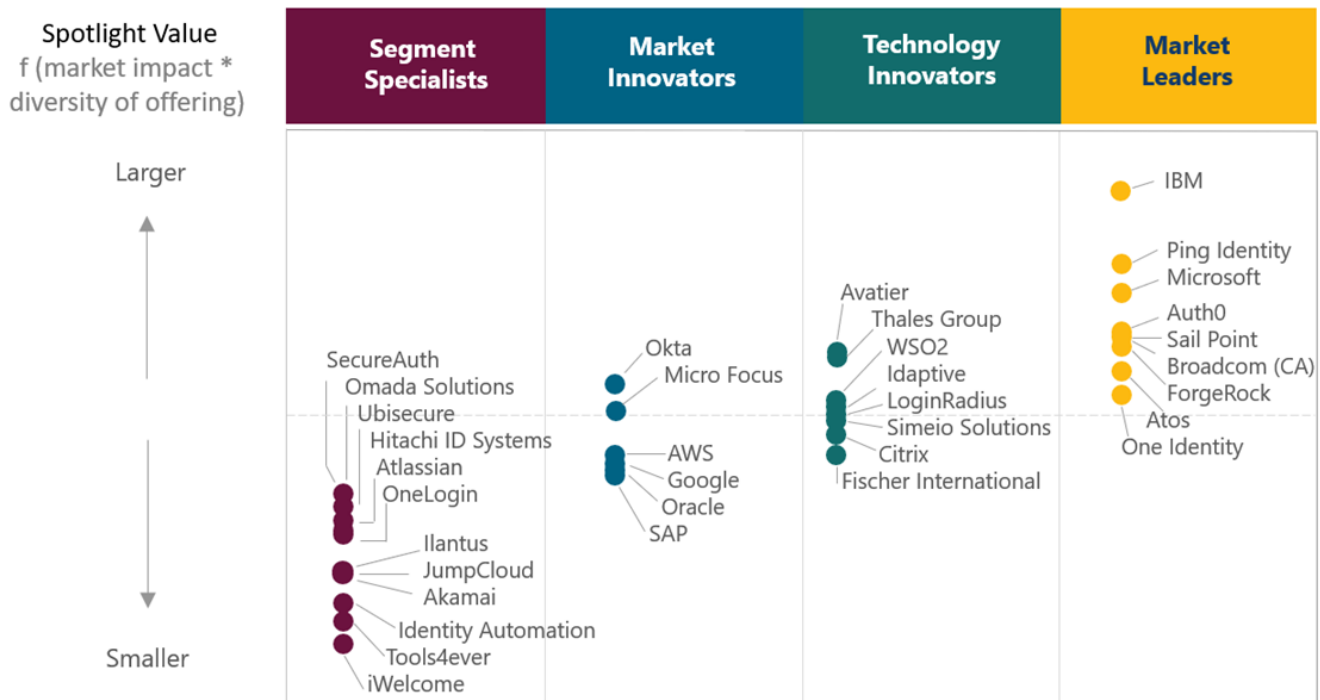
For these reasons – and more - we recommend the Relative Vendor Value chart be used not as an absolute comparison but rather as an indicator and input for seeking “best-fit” market offers. Further insight into value can be found in the Market Spotlight Value chart (Figure 8) that is a summation of overall Cyber diversity and market impact of by the market segments - segment specialists, market innovators, technology innovators, market leaders - currently occupied by vendors.

Market Spotlight Value

The Market Spotlight Value for UIAM depicts the overall value within each Spotlight segment as a sum of the market impact and cyber of each vendor.

As the combination of market impact and cyber diversity increase, vendors deliver more expansive offerings that are more attractive to the market, and where it declines, vendors tend to focus on market innovations and specialist offerings for specific markets.

Figure 8: Market Spotlight Value for UIAM



© Cyber Source Data Wellington Research, 2019

The narrowest range of Spotlight Value for UIAM occurs among the market innovators, with value increasing along a path from segment specialists to market innovators, and then again from technology innovators to market leaders.

Based on these results it appears little overlap exists between the firms operating as market specialists and all other vendors. After this there is a common overlap between the market and technology innovators, and then again between the market leaders and some of the technology innovators.

Mainstream buyers motivated by value may elect to confine their search in ways that make most sense for them. This might include sourcing from the market leaders, a combination of market leaders and technology innovators, or across the three segments of market leaders, technology and market innovators.

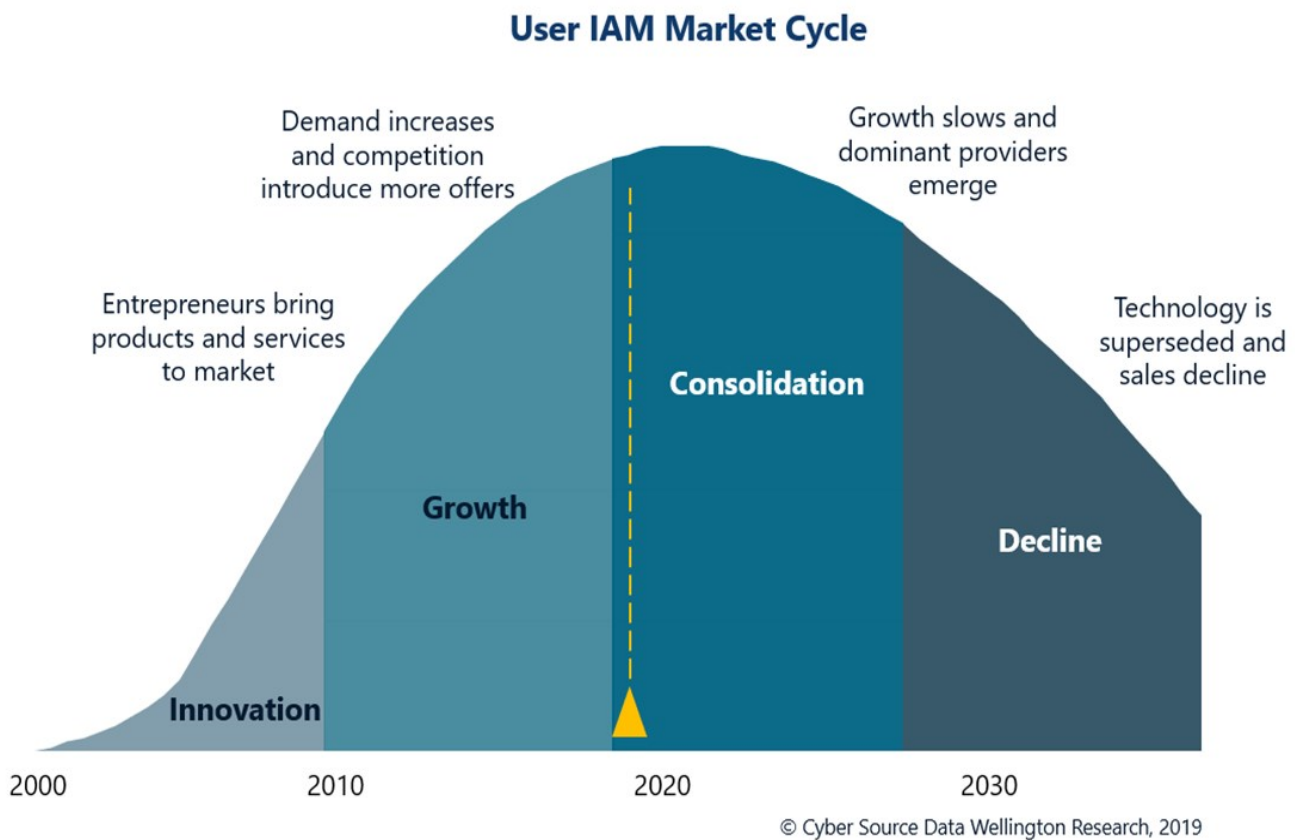
The Market Spotlight, Relative Vendor Value and Spotlight Value charts provide insight for the comparison of UIAM providers covered in this report. We recommend buyers use these charts for their relative guidance - not as absolutes - when seeking "best fit" market offers because what fits one buyer may not fit another, because Cyber capability requirements of buyers change, and the market impact and cyber diversity positions of vendors change in time.

Market Cycle for UIAM

The market cycle for UIAM commenced between 1997 and 2000 when early entrepreneurs tested the idea of what became identity management and federated identity services and brought these to early market adopters. The demand for UIAM has since led to an increasingly crowded field of vendors and market offerings competing for buyer allegiance and business.

As the market for UIAM approaches its peak growth is expected to remain robust over the coming few years and then start leveling off and then consolidating. The emergence of slower growth later in the coming decade will be augmented by changes in market offerings among what will later become ever more dominant providers of UIAM services.

Figure 9: Market Cycle for UIAM



Now is the time for all buyers and providers to assess where they want to be as the market for UIAM travels through its peak and commences a longer consolidation phase between now and 2028, and before it goes into a decline phase and is augmented or replaced by the next big mega-trend.

Early adopters may want to evaluate the gap between early UIAM portfolios and current offerings and future needs. Market growth buyers may want to assess where they are today and where they want to be in five-to-ten years as the market for UIAM peaks and then commences its consolidation phase.

Later stage buyers of UIAM may be less subject to turmoil and cost associated with upgrades or change-outs of early-stage technologies but will have lost benefits of not using UIAM while waiting for market maturity. And therein lies another tale about the companies that lose market-share as the digital on-ramps for customer interactions change around them.

Market Size and Growth Forecast

The market for UIAM is currently valued at \$4.1 billion from the sale of all products and services and is forecast to grow to \$6.5 billion by 2023, at a compound annual growth rate of nine point six (9.6) percent over this period.

The market is currently not dominated by any one vendor, nor is it dominated by any one category. Rather the market is being shaped by vendors along the top-half of the Market Spotlight (Market impact) and the right-hand side (Cyber diversity) of the Market Spotlight. These conditions are flags of intense rivalry along the axis of technology and market innovation, and denoting the market is in flux, as buyers seek to expand uses beyond traditional employee access to include supply and value chains, and as more business application workloads and data are dispersed between Cloud and mobile devices.

The heady growth rate of nearly 10 percent is likely to be uneven across the spectrum of vendors as buyers consolidate one or more UIAM platforms that may be in production, and potential displacement remains one way of expanding addressable market.

Leaders by Market Impact x Offer Diversity

1. IBM
2. Atos
3. SailPoint
4. Microsoft
5. Ping Identity
6. Broadcom (CA)
7. ForgeRock
8. Auth0
9. One Identity

Leaders by Relative Vendor Value

1. Thales Group
2. Avatier
3. Fischer International
4. Idaptive
5. Hitachi ID Systems
6. WSO2
7. Ubisecure
8. LoginRadius
9. Ping Identity

The market for UIAM is driven by responses to simplify the complexity of user access to assets and resources for increasingly complex digital ecosystem environments, using complex series of software libraries for authentication, authorization and federation. Consisting of three separate activities, UIAM includes: (a) accepting input streams of digital identity credentials, (b) authenticating or validation of the presented digital identity credentials, and (c) provisioning and federating access to digital resources for validated and authenticated digital identity credentials. Many contemporary UIAM systems use one or more dominant code bases that include Security Assertion Markup Language (SAML), Open Authorization (OAuth), Active Directory, Light Weight Directory Access Protocol (LDAP), and OpenID. Variations on these may also include FOAF, MPA, Shibboleth, WebID and XACML among others.

The market for UIAM includes: (a) commercial products and services from vendors covered in this report, and (b) organizations that previously went with roll-your-own UIAM systems. Increasingly, roll-your-own approaches are being replaced by commercial off-the-shelf software (COTS) as organizations include user constituencies beyond their own employees, as virtualized and micro-service directories enable agile federation, and as organizations focus their efforts on providing access to digital applications and data acting as market differentiators for customer experiences.

Futures Forecast for UIAM

The drivers for UIAM are business imperatives, including: (a) accelerated digitization of business processes, and (b) cost reductions made possible by just-in-time and the optimal digital integration of suppliers and contractors to meet customer requests and orders.

Business imperatives. Vendors with UIAM offerings that accelerate the realization of both value (more customers, more revenue, more orders) and earnings (reduced costs, more efficient operations) will be greatly favored as UIAM transitions from a former role-your-own on-premises stand-alone computing world to one involving the integration of constituents and digital resources everywhere.

Digital simplicity. While business imperatives are UIAM's motive drivers, the complexity of the digital environment acts as friction retarding forward momentum. Eliminating - or significantly reducing - the impact of the complexity of access to resources across digital ecosystems will reward vendors featured in this report, but only if the vendors are delivering against the business imperatives of UIAM.

Change agents. While business imperatives pull UIAM and digital simplicity push it, vendors and buyers of UIAM will be buffeted by five market change agents, as follows:

- Autonomous self-service for disconnected people and entities
- Digitized robotics, analytics and self-service for user accounts, credentials, access entitlements
- Virtualized plug-n-play interoperable directory services
- Common UIAM API integration services
- Automated functional testing, Cyber testing and recoverability services

Autonomous Self-service. The market imperative for UIAM is focused on ubiquitous access to digital resources for anyone, at anytime, from anywhere and for anything. Autonomous self-service for disconnected people and entities will play a key role in making it easier for anyone and anything to participate in the digital conversations occurring between customers and suppliers, citizens and governments, patients and caregivers, and any digitally-enabled relationships.

Robotics and Automation. Digitized robotics, self-service and analytics will take over the drudgery of credential, asset, lifecycle and access management workflows of UIAM over the coming five years, freeing up resources for more productive pursuits. Virtualized directory services for today's directories and tomorrow's micro-services will introduce new forms of federation between digitally-enabled ecosystems, thereby reducing friction and introducing greater ease of access. Common UIAM API services will provide simple hooks for DevOps to more readily use and reuse services across many UIAM products and service offerings. Automated functional and Cyber testing and recoverability services will be essential for greater assurance, compliance and audit among other uses.

Plug-n-play and Common API services. Vendor lock-ins will become increasingly taboo as business imperatives push the boundary of UIAM outwards through value chains and away from the confines of employee-only access systems. Vendor lock-ins will not disappear completely though and may evolve using other means such as common API services and interoperable virtualized directory services.

A peek into the future helps when considering the options for UIAM that currently exist today and should be a part of every assessment of the "best-fit" market offer.

Finding “Best-Fit” Market Offers

There is not one vendor for UIAM that is “best-fit” for all buyers. Rather, there are multiple vendors meeting the unique needs of different buyers and buying segments. The Market Spotlight, Relative Vendor Value and Value Spotlight charts should be treated as guides to the five steps for finding the best-fit market offers, which include:

1. Capability assessments
2. Form, fit and function assessments
3. Risk-cost” tradeoffs
4. Vendor short-list bake-offs and try-buys
5. Sourcing “best-fit” vendors

Capabilities assessments

Capability assessments are a blue-sky open-ended discovery process resulting in rank orderings of all possible needs. These do not preclude nor pre-judge best-fit requirements. Rather these are attempts to discover and then prioritize all possible requirements to meet objectives. The most successful companies treat these assessments as “everything is free” with “no constraints.”

Form, fit and function assessments

- *Form* assessments evaluate external characteristics of Cyber systems and are most evident in the look and feel and User eXperience (UX) of Cyber systems. Evaluation of form for UIAM must include interactions between the fit and function of market offers, the business processes and people that will be using these systems.
- *Fit* assessments evaluate the ability of Cyber systems to mate with and join existing Cyber controls, procedures, data and analytics. The vendors with larger Cyber diversity offerings will more likely - but are not guaranteed - provide smoother integrations and fits with existing systems, Cyber and otherwise. Fit is an important consideration to adoption within the enterprise.
- *Function* assessments determine whether a Cyber system performs its state purpose effectively and reliably. For example, a UIAM system for internal employee uses may be inappropriate for one targeted for use as a business-to-business network and these may rate very differently when considering the needs for business-to-consumer applications.

Risk-cost tradeoffs

The business case for UAM takes into account the operating value the organization can accomplish the UIAM system in place, without it in place, and the risks associated with it deployed and not available.

Vendor short-list bake-offs and try-buys

This is where the so-called rubber meets the road, when vendors are invited in to demonstrate and provide proofs of concepts. Amazingly our research suggests that not enough buyers are availing themselves of the opportunity to conduct vendor bake-offs due to a number of factors including (1) inexperience, (2) lack of staffing and resources, (3) lack of a clear Cyber strategy, and (4) inefficiencies borne by organizational fragmentation. Full-scale bake-offs are rare for smaller orders and due to this we encourage the use of “try-buys” to deliver proof-of-concept” results prior to sourcing best market offers and vendors.

Summary Observations

User identity access is the root all things Cyber and UIAM is the cornerstone of digital access anywhere, at anytime, by anything and for anyone, and becomes more important - not less - as a core business operations and financial transformation tool.

It is what defines what and who has entitlements, privileges and access to resources, applications, data, transactions, and all-things-digital. It is essential to the integrity, reliability and inviolability of business, agency and non-governmental operations and functions.

User Identity Access Management establishes - and maintains - the orderliness of swim lanes and interactions for business procedures that are increasingly dependent on digital interactions, entitlements and proof. It is at once the arbiter of digital access and the recorder of digital access, the alpha and the omega of digital events, for the interactions and overlays between people, organizations, business processes and transactions.

Selections of UIAM are perhaps one of the more influential Cyber sourcing decisions organizations will make. The Market Segment Report for UIAM - including the Market Spotlight, Relative Vendor Value and Value Spotlight charts - provides the necessary background and inputs to achieve wiser and more informed decisions for the pivotal Cyber function of user identity access management.

Cyber Standards and References

UIAM is covered by many frameworks, including the following:

- [IETF LDAP RFC2251](#)
- [ISO/IEC Frameworks](#)
- [ITU ASN.1](#)
- [NIST Frameworks](#)
- [OAuth](#)
- [OASIS](#)
- [OpenID](#)
- [Open Identity Exchange \(OIX\)](#)
- [SAML](#)

Updated - July 2019

Vendor Inclusion and Assessment Criteria

Normally, all relevant vendors are covered by Market Spotlights. If this results in too many vendors, segments are narrowed to smaller subsets while maintaining and promoting apples-to-apples comparisons of relevant vendors. In the case of this UIAM Market Segment Research Report and the Market Spotlight accompanying it, guidelines were employed to focus the list of included vendors. The guidelines include: (a) vendors must be delivering a Cloud subscription service for UIAM, (b) products/services must accept many forms of digital identity credentials, (c) products/services must deliver core feature-sets and complimentary lifecycle management capabilities for managing authorized user accesses, and (d) products and services must be sold and serviced for a broad cross section of industries and not focused on just one industry. Within the constraints of these selection criteria the UIAM products and services covered by this report generally represent the currently available universe of commercial UIAM options, although some exceptions may exist.

Market impact of vendor market offers (the Y-Axis)

The market impact of vendors is driven by revenue, the number of direct geographic sales locations by geographies, and third-party partnerships. These factors are direct indicators of commercial market acceptance of vendor market offers and are the primary factors used to formulate the market impact of vendors through their offers.

Diversity of vendor market offers (the X-axis)

Diversity of Cyber market offering consists of factors that include: value chain use, business function use, digital identities, applications, data, systems, end-points, networking, identification and authentication, controlled access and protection, audit, monitoring, detection and alerting, analytics and prioritization, incident response, cyber recovery, cyber compliance, governance and asset management, forensics, professional services, managed services, Cloud subscription services, product purchases, product installation and maintenance services, and technology integration partnerships. Combined these factors are direct indicators of the expansiveness and coverage of vendor market offers and are the primary factors used to formulate the Cyber diversity of vendor market offerings.

Cyber Source Data

Wellington Research

Market Spotlights and Market Segment Reports deliver relevant information – market impact and diversity of market offers - not available from other sources. Cyber Source Data does not recommend vendors, has no ownership interest in vendors covered, has no financial interest in vendors covered, does not charge fees for Market Spotlights, and encourages the free distribution of Market Spotlights.

The research presented in this report is based upon information then available at the time of publishing and represents the opinion of Cyber Source Data. Vendors highlighted in Market Spotlights and Market Segment Reports are provided the opportunity to provide input to the research but not the ability to review or otherwise influence what is published by Cyber Source Data.

All Market Spotlights, Market Segment Reports, Market Insight Reports, Benchmarks, Infograms and Market Data are the intellectual property and copyright of Cyber Source Data and Wellington Research. Any similarity with any other Industry research is purely coincidental. Users of this Research Report use it at their own risk. Cyber Source Data and Wellington Research make no warranties, express or implied, including without limitations those of merchantability and fitness for any purpose. Users of this report assume all responsibility for the uses to which the information is made. Cyber Source Data and Wellington Research are not liable for damages of any kind, including without limit, direct, incidental or consequential damages, any claim attributed to errors and omissions or other inaccuracies contained in this report. This Research Report is subject the **Terms of Use found on the Cyber Source Data website.**