

The Future of Identity Management (2018-2023)

Abstract

Identity Management is at the epicenter of digital transformation and the next generation of enterprise IT. The corresponding changes in identity systems and services over the next five years are expected to be as disruptive as the new business models, applications and ecosystems they are supporting.

This highly actionable report is designed to support enterprise technology infrastructure and business transformation plans. We believe that a critical element of an enterprise technology strategy and business transformation program is getting Identity and Access Management (IAM) right. And given the accelerating changes in business, technology and IAM we are looking to provide guidance to our enterprise clients as to where the puck is going; as it is traveling really fast with many disruptive forces in play.

We make specific projections as to where we believe Identity Management will be going over the next five years and we describe a model for identity abstraction that provides an extensible services oriented architecture. We include newer disruptive models such as DevOps/microservices in identity systems, cloud-based IAM, self-sovereign identity leveraging blockchain, IoT support, evolving privacy regulations, and new governance and provisioning models.

To provide our clients with the most comprehensive view of Identity Management, we augment our own expertise with the insights a few of the top thought leaders and industry experts to deliver a comprehensive perspective on the Future of Identity Management.

Authors:

Gary Rowe
CEO, Principal Consulting Analyst
Gary@techvisionresearch.com

Nick Nikols
Principal Consulting Analyst
Nick@techvisionresearch.com

Doug Simmons
Principal Consulting Analyst
Dsimmons@techvisionresearch.com

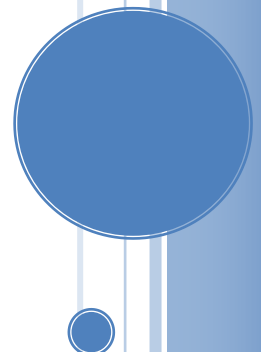


Table of Contents

Abstract	1
Table of Contents	2
Executive Summary & Key Advice	3
Introduction	5
Key Issues and Technology Trends	7
Discussion: The Future of Identity and Access Management	9
The Future of Identity Management; Identity as a Utility	10
The Future of Identity Management by Category	18
The Foundation; Identity Federation, Virtualization and Normalization	19
Blockchain-based Identity Systems and Self-Sovereign Identity	21
Identity Services as Microservices	23
Privileged Access Management	26
Identity and the Internet of Things (IoT)	28
Relationship and Context-based Identity	29
Cloud-based Identity Management	31
Identity and Security Integration	32
Scaling Identity Systems	33
Identity Governance	34
Identity as a Privacy Enabler	35
Identity as a Business Enabler	36
Customer IAM (CIAM)	37
Recommendations	37
Conclusion	38
Industry Expert Perspectives on the Future of Identity Management	41
Nathanael Coffing, Cloudentity	42
Lasse Andresen, ForgeRock	44
Jackson Shaw, One Identity	46
Michel Prompt, Radiant Logic	48
Phil Windley, Sovrin Foundation and Brigham Young University	50
About TechVision	52
About the Authors	53
Related Reports	54

Executive Summary & Key Advice

Identity Management is the foundation for “real” digital transformation; the secure, flexible and adaptive IT infrastructure that every company, government agency and institute of higher education strives to achieve. The establishment of identities and distribution of those identities will be leveraged by virtually every substantive application and process throughout most organizations. Identity should ultimately be a “utility”; it should be easy to identify individuals, applications and things and use them as needed under proper security controls that are privacy-centric. The management of identities is also a critical part of how organizations directly interact with consumers and trading partners.

The value of establishing and managing identities within organizations, across organizations and for individuals globally can’t be overstated. It is one of the most fundamental building blocks in support of any level of communication, collaboration or commerce within an organization or across the Internet. Identity Management is the foundation for enabling innovation with minimal friction.

That said, many organizations face greater identity management challenges today than they did 15 years ago. One of the key reasons for the proliferation of identity systems that don’t interoperate and connected applications that are “hard-coded” to these largely monolithic, on-premise identity systems. This “identity sprawl” continues to accelerate as exemplified by virtually every large organization TechVision has worked with. Our enterprise clients are looking to simplify, consolidate, integrate and better choreograph their identity systems and services.

The sprawl of identities, attributes and non-interoperable IAM functions also create challenges in governance, user-data privacy, and are hindering proper risk management. As discussed in this report, the only way to address this is to refocus the discussion around a cohesive, well-designed architecture strategy that takes into account flexibility, scalability, integrity and cloud readiness.

This report focuses on supporting our clients as they develop five-year technology infrastructure plans that will certainly include how identities are established, maintained, secured, leveraged by applications and distributed within an organization and externally. We start by introducing the basic Identity Management concepts and then look at some overall technology trends that directly impact the future of Identity Management. Major influencers include the overarching movement to the cloud, the impact of the Internet of Things (IoT), the impact of mobility and the increasing exposure to security and privacy risks.

We then make specific projections as to where we believe Identity Management will be going over the next five years and describe how organizations can best leverage this new era. Specific areas of focus include:

- The Foundation; Identity Federation, Virtualization and Normalization
- Blockchain-based Identity Systems and Self-Sovereign Identity

- Identity Services as Microservices
- Privileged Access Management
- Identity and the Internet of Things
- Relationship and Context-based Identity
- Cloud-based IAM
- Identity and Security Integration
- Scaling IAM
- Identity Governance
- Identity as a Privacy Enabler
- Identity as a Business Enabler
- Customer IAM

This list represents the major IAM themes for Identity Management architects and strategists to factor into a five-year planning horizon. We also describe a model for identity abstraction that provides a services oriented architecture with the flexibility and integration needed to provide Identity Management as a utility within and between organizations.

To provide our clients with the most comprehensive view of Identity Management, we augment our own expertise with the insights of what we consider to be the top thought leaders and industry experts and get their perspective on the Future of Identity Management. These are many of the top influences within the major players in Identity Management, cloud computing and the Internet-based infrastructure. We summarize the interviews with each leader and we have incorporated many of their perspectives into our overall assessment of the future of Identity Management.

This report is highly actionable with specific takeaways and next steps for organizations planning for their next generation of Identity Management services.

Introduction

The concept of identity has a lot of different meanings depending on the context it's used in. Politicians, philosophers, psychologists and anthropologists have a very different understanding of the word identity and its implications than does an IT administrator or an application developer. However, in the digital world, identity takes on a very special role – acting as the foundation for all interaction. Identity is the basis for all digital relationships - identifying who or what you are (or who you claim to be), what is known about you, how you relate to other entities and environments, as well as what you are allowed to do in any given environment.

Identity can be a label – I am who I say I am. But it also is the sum of the data available that uniquely describes me – which demonstrates how I or someone else can prove that I am who I say I am. From this context, my relationships within the digital realm can be established.

The digital world is also made up of objects – lots of them – all of which have identities. An object can be physical (a person, a device or a 'thing') or logical (a process, application, or a virtual compute instance) and its identity can be described – it can be identified – by attributes or characteristics of that object, one of which in the digital world has to be unique to that object. An object with an associated identity can be a person, a resource (a conference room), an organization, a thing (a light bulb, a car), a policy, a process or a variety of other physical or logical entities. Identity labels – how an object is presented to the world – can be descriptive, user friendly, or exceedingly complex, depending on the way they are going to be used and who needs to know.

The identifiers – or attributes – that describe an object uniquely are used to also assess access rights, entitlements, classification and a multitude of other services. If an identity is trusted, the attributes associated with that identity are available to multiple applications. Some of the prime motivations for tracking and managing identities come down to gaining an understanding of the identity relationships for the purposes of determining appropriate access and determining better ways to interact and engage with these entities – whether they are employees, customers, partners, citizens, organizations, applications, devices, sensors, or other "things".

Identities can be self-asserted or supported by a third-party. I could simply state that I am Gary Rowe (my identity) or I could present a driver's license, passport or birth certificate to provide some level of verification that I am who I claim to be (my identification). Organizational identity management systems have several levels of verification ranging from self-declaration to very strong proof that the data is accurate and verified. Trustworthiness of the identity is then tightly correlated to the strength of verification available.

The value of establishing and managing identity within organizations, across organizations and for individuals globally cannot be overstated. It is one of the most fundamental building blocks for any level of communication, collaboration or commerce within an organization or across the Internet. And despite identity's necessity as a foundation, it has

fundamental challenges that only get worse as the scale increases– including protecting individuals' privacy and the theft of identity data.

Identity and Access Management (IAM) systems generally provide the tooling and infrastructure necessary to manage these challenges at scale. IAM and its governance and entitlement focused corollary, Identity Governance and Administration (IGA) are a set of processes, policies, technologies and infrastructure for the creation, maintenance, and use of identities. They provide for the persistent storage, lifecycle management and governance of these identities as well as managing how these identities relate to other systems and determining what they are allowed to do as supported by policies. Determining and enforcing appropriate access to enterprise systems and applications can be distilled down into two primary components: authentication and authorization.

Within authentication, systems and applications identify *who you are* by looking at a host of attributes: identifiers, passwords, digital certificates, federation claims, one-time password tokens, etc. Within authorization, we consider roles, groups, entitlements, individual attributes or other affiliations that systems or applications rely upon to decide *what you are allowed to do and see* in that environment.

These systems are supported by a whole host of backend technologies and processes needed to create and maintain the broad spectrum of identity data that is needed by resources and applications to perform the acts of authentication and authorization. This is where the persistent storage and easy look up of identity data through identity repositories and directories comes into play, as well as where integration and management technologies such as cloud identity brokers, provisioning/identity lifecycle management services, virtual directory/identity aggregation services, meta-directory/identity orchestration services, delegated and administrative user interfaces and network topologies (internal, federated, cloud, self-sovereign, hybrid...) enter the fray.

Authenticating someone's identity at a high level of certainty can be more challenging, but is an absolute requirement in many high-risk transactions, such as online banking. The hard part is establishing that level of surety during initial account creation, a process that has to be better addressed by the enterprise in the future. As a result of the value of establishing and leveraging identity across the Internet and within organizations, IAM is still perhaps the hottest topic in the realm of information security. It's also an area in which most enterprises, no matter what market segment or vertical they are in, still struggle tremendously.

Industry efforts to develop identity standards and tools to solve directory challenges go back several decades and many members the TechVision Research Consulting Analyst team have been in the middle of this since the early days. We were also instrumental in the movement towards directory synchronization and meta-directory technologies as tools in the late eighties and early nineties. Of late we have worked on these and other efforts in an attempt to facilitate better, more consistent use of identity technologies, improve the development of secure applications and environments, as well as help organizations gain a better understanding of identity to foster improved customer experiences. Since then,

guess what has happened? We have talked a lot, written a lot and learned a lot, but not much has really changed – yet. While we’ve moved in the right direction, some of the hardest problems haven’t been solved. Sure, we’ve got shinier tools as well as new buzzwords and catchphrases, but the technology and standards have not kept up with the challenges; and our challenges are greater now than ever.

There is growing sense of frustration amongst professionals that this apparent inertia has gone on long enough. Identity data is scattered everywhere with identities generally tied to specific applications or services: but the scale today is dramatically bigger than it was even five years ago and growing exponentially. And there are trust issues on an Internet scale—users, applications and ecosystems are trying to determine if they can trust that the asserted identity is who/what it claims to be. Associated with that, the risk of identity fraud and identity theft is ever present and growing year on year.

It is TechVision’s goal to help bring about those changes and usher in a whole new approach to IAM fit for purpose in the 21st century.

Now that we have provided this brief level-set for both identity and IAM, let’s dive into the future of Identity Management. We start with a broader perspective on technology futures and then assess our vision of the future of identity management. To provide our clients with the most comprehensive view possible we also share results from interviews with several industry leaders in specific areas we believe are important to the future of Identity Management and, finally we make specific recommendations for our enterprise clients.

Key Issues and Technology Trends

To give the future of Identity Management the right context, we must take a quick look at some of the key trends that will drive Internet and information technology over the next five years. Most of these trends are not new; they represent existing trends we expect to continue to be relevant over the next several years. These trends will directly impact the next generation of identity management products and services. Key trends include:

- **Internet of Things (IoT).** The Internet is extending its web to include almost anything one can think of: from light bulbs to cars and refrigerators to traffic lights, to sensors monitoring our movements and medical devices. IoT will be pervasive in business with real time monitoring and sensors coupled with advanced workflow technologies providing greater efficiencies and responsiveness. Almost everything in the physical world can be tagged, accessed, analyzed, connected and, in theory, optimized. These devices can be connected to the Internet and to other individuals and organizations, but there are complex relationships to manage, personal information to protect and a plethora of challenging security concerns. Establishing identities for these items and enabling appropriate access for these identities throughout the connected ecosystem is stretching identity to new limits.
- **Big data and analytics.** IoT, pervasive social media/data brokering and sophisticated predictive analytic engines drive the hunger for and availability of more and better user data. This is further supported by rapid growth of machine

learning to better analyze, correlate and use this data. Big data can also be used to help secure assets and detect anomalies. As more data is collected, it must be correlated in new ways to try to better understand trends and intent. This trend is accelerating with no end in sight.

- **Privacy and regulatory controls.** Both IoT and big data coupled with an increasing thirst to monetize “free” services will continue to push the envelope relative to privacy, which in turn will drive increased push back from individuals and government agencies. Legislative and regulatory controls such as GDPR in the EU are increasing the investment in better privacy and data controls. Major data breaches coupled with increased government regulations will increase the visibility of and enterprise investment in privacy. Areas such as self-sovereign identity can also support better privacy if properly governed.
- **Everything moving to the cloud.** Cloud computing will continue to gain momentum and is the primary means of delivering applications and services to consumers and among businesses. Identities are being stored in the cloud and identity services are increasingly cloud-based. Cloud-based applications will also store identity information and will authenticate users. Cloud-based services are also supporting the movement to DevOps and microservices.
- **Wireless and Mobile.** Wireless access is increasingly an expectation in most parts of the world and is shaping the applications for both businesses and individuals. Access via mobile devices is becoming the first choice as intelligent phones, tablets and appliances proliferate. The advent of mobile has major ramifications for both identity management and security. These trends will accelerate over the next five years with smarter and more powerful mobile devices.
- **Bring Your Own Device (BYOD).** More and more employees are using their own personal devices rather than corporate-delivered systems to access company business and Internet-based applications and services. BYOD, wireless and mobile means that identification based on static location or a corporate device is no longer a given.
- **Artificial Intelligence (AI) and Machine Learning (ML).** From machine learning to natural language processing, artificial intelligence and cognitive computing are elevating beyond speech recognition and rules-based systems to help organizations consume and derive value from big data and drive decision-making through powerful analytics.
- **Security Investment, Visibility and Intelligence.** Given the increasing numbers of breaches, accessibility to personal data, sophistication of cyber-criminals and corporate risk aversion, security and risk programs are given higher and higher priorities in organizations and for individuals. This acceleration has occurred over the past several years and we expect it to continue to accelerate for the foreseeable future. As the perceived importance of security increases, there will be corporate organizational changes with CISOs reporting to CEOs or Boards instead of CIOs.

This is a consequence of the visibility and damage associated with personal data breaches, stolen intellectual property and other security issues. Expect greater visibility, greater funding and increased enterprise investment in security.

- **DevOps and Microservices.** Many organizations are moving from the traditional monolithic approach to application development to more “Netflix” like DevOps and Microservices models in which applications are broken down into the most basic services and developers are responsible for not just the development, but also the operational support. This type of model is highly scalable and drives more continuous integration and delivery than the monolithic application model that has existed for much of the past 40 years. The goal is to provide updates on a daily or weekly basis (as needed) as opposed to waiting for annual (or worse) release cycles.
- **Blockchain.** The underlying technology developed to support Bitcoin has grown like wildfire in the past three years and is continuing to accelerate. At its core, Blockchain provides a transaction record that doesn’t require a central third party to mediate is tremendously disruptive and has inherent security capabilities as part of its foundation.

The trends described above are influencing today’s thinking on the future of identity management. There are increasingly more objects to identify, more data to classify, more connected devices, increasing privacy concerns/regulations and an accelerating blending of personal and employee data that creates challenges/opportunities for the next generation of IAM. There are also new disruptive technologies that will become increasingly important in developing and deploying identity services over the next several years. We expect Blockchain, DevOps, Microservices, the pervasive movement to the cloud coupled with increasing data privacy regulation to be particularly relevant to identity services over the next five years. We also envision innovative combinations of the above technology trends in supporting identity services that can improve personalization, usability and support for both enterprise and customer use cases.

Discussion: The Future of Identity and Access Management

IAM is at the core of the digital transformation and will be at the epicenter of the secure IT infrastructure that every company, government agency and institute of higher education strives to achieve. IAM also has hooks into virtually every substantive application and process throughout most organizations. Identity extends well beyond the firewall as the management of identities is also critical for organizations directly interacting with its consumers. IAM, in fact, represents the new security perimeter as we described in our “Identity is the New Perimeter” report in September of 2107.

Most organizations should be planning for a substantive IAM evolution over the next five years. Identity systems haven’t changed a lot over the past few decades, but the ways businesses operate and how they leverage technology certainly has. Many of the same approaches to addressing identity, authentication, authorization, provisioning, data quality, data ownership, and data protection haven’t changed much in a long time, but are due for a

substantial upgrade.

In addition to solving long-term problems, new challenges are also emerging in managing Bring Your Own Device/Bring Your Own ID (BYOD/BYOID), social login (i.e., cloud) and dealing with the increased scale presented by the Internet of Things. We will take a look at how these problems will be solved as well as new opportunities to leverage Identity Management as a means of better securing our resources.

But before identity systems and services are able to scale to meet enterprise needs in the future, they must have the technology and processes to better organize, manage and serve up the identity data that is already in place. This is what we refer to as the “necessary prerequisite” for the future of Identity Management and a key to the ultimate goal of having identities served up like electricity or water is served up in modern cities. This bridge between legacy systems/processes and newer, more advanced technology must be there to enable the vision we describe.

The Future of Identity Management; Identity as a Utility

Identity Management needs to become an “Identity Utility”. Much like electricity and water in most modern cities; when you need or want it, the service is there...and it is simple, ubiquitous, and safe to use...like turning a faucet or plugging in an appliance. A simple and frictionless experience for the developer, employee, customer or administrator will be critical for the next generation of identity services.

Identity as a Utility (IaaU) starts with a reliable and consistent means of collecting, organizing and disseminating data. Since enterprise data generally lives in a multitude of disparate silos, the sharing of data and the orchestration of the changes to the data across these silos has been the traditional cornerstone of many solutions and its roots can be seen in current IAM challenges such as user account provisioning. Event triggers, such as changes to authoritative sources of data like Human Resource Management Systems (HRMS), result in the automatic creation of user accounts, assignment of access privileges, and the propagation of user attributes for as many downstream target environments as can exist in an organization.

Identity abstraction can be thought of as the ultimate services-oriented IAM architecture. The target is a ubiquitous service that provides identity data to people, applications and network services. The future of Identity Management will be built on a flexible and highly accessible foundation that integrates data from many environments and provides secure access for many identity consumers.

The challenge in getting to the “utility” state is that most enterprises have so many environments and processes to be normalized and integrated in some cohesive way. This is in part due to a lack of standardization of both integration capabilities and of processes and procedures.

All too often application vendors ignore efforts to provide integration standards like the System for Cross-domain Identity Management (SCIM) and instead provide proprietary interfaces, which places the burden of integration with the IAM deployment. And many of

the IAM vendors have typically lacked a sufficient portfolio of usable connectors that can easily integrate the IAM system (normally the provisioning platform) with the large set of potential target applications. These gaps must be filled going forward to provide this cohesive foundation.

While IAM vendors have for years touted their dozens if not hundreds of connectors, in actuality, we find that they generally have only a few deployed in any large number, and the rest are either purely custom one-off integrations or derivatives of toolkits for creating connectors that haven't seen the light of day, much less actually worked according to plan.

Also, the prevailing philosophy amongst many IAM vendors has been that every deployment is completely unique, and as such unique custom policies and processes must be implemented for each. This has led to a proliferation of expensive, highly customized, brittle, and often very difficult to upgrade deployments. Which in turn, has led to a significant amount of recycling of IAM deployments – where older deployments (that may have initially met the needs of the organization) have been ripped out and replaced once they no longer were able to adapt to the organization's changing needs or that expansion and further integration with additional environments proved to be too costly.

The reality is that most organizations, therefore, end up with maybe two or three connected systems that typically include Active Directory, and complex enterprise applications from Oracle, SAP and others. This situation often leaves hundreds of applications beyond the realm of automated provisioning/de-provisioning and proper access governance processes. And, it leaves senior management very dissatisfied at having invested untold millions of dollars on promises made in IAM projects that do not address enough systems to reduce risk or satisfactorily automate administration.

However, this is not to say that the broader goals of IAM are not achievable. It is simply necessary that to achieve these goals, we need to strive to avoid the pitfalls of getting seduced by the expediency of custom one-off engagements – instead seeking out more standardized best practice policy, process, and implementation. IAM requirements from organization to organization are not that dissimilar. IAM capabilities do align along specific knowable patterns. It is to that end that TechVision has developed the following IAM Reference Architecture. We'll provide a brief snapshot here, but our clients are encouraged to work with our team to leverage these templates with support from TechVision's Principal Consulting Analysts to develop the a customized reference architecture for your enterprise.

The **TechVision Research Reference Architecture for IAM** is a master template that identifies the IAM capabilities (rather than technologies) that can be improved or enabled, allowing business stakeholders and technical architects to achieve a common language for IAM functions, which can then be refined over time. This high-level template provides the top-level foundation for TechVision's IAM reference architecture.

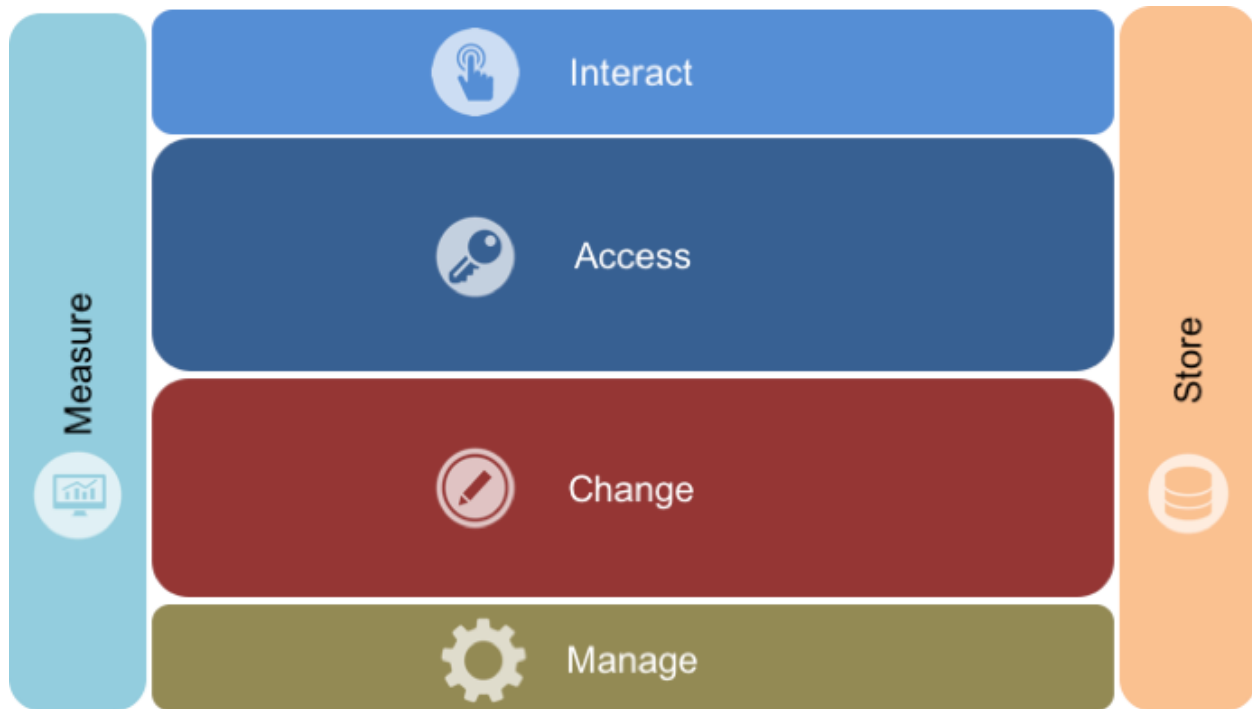


Figure 1: TechVision Research High Level IAM Capabilities

Those capabilities are described at the highest level as:

- **Interact** – how end-users and application developers interact with the IAM platform.
- **Access** – the policies and processes that uniquely identify a given actor and define what that actor is allowed to do based on the assigned roles, rights, entitlements, and obligations
- **Change** – the capability to define and manage the changing nature of the relationships between identities and enterprise resources throughout their lifecycles
- **Manage** – the capabilities required to manage, configure, and upgrade the IAM solution itself.
- **Measure** – the capabilities required to inspect, audit, gain insight, and improve IAM activities.
- **Store** – the capabilities required to persistently store and maintain identity information and their relationships, as well as facilitate easy retrieval of that information.

These capabilities begin to define the basic aspects of identity services, but we can provide more granularity as to their nature. The following diagram provides an additional level of detail:

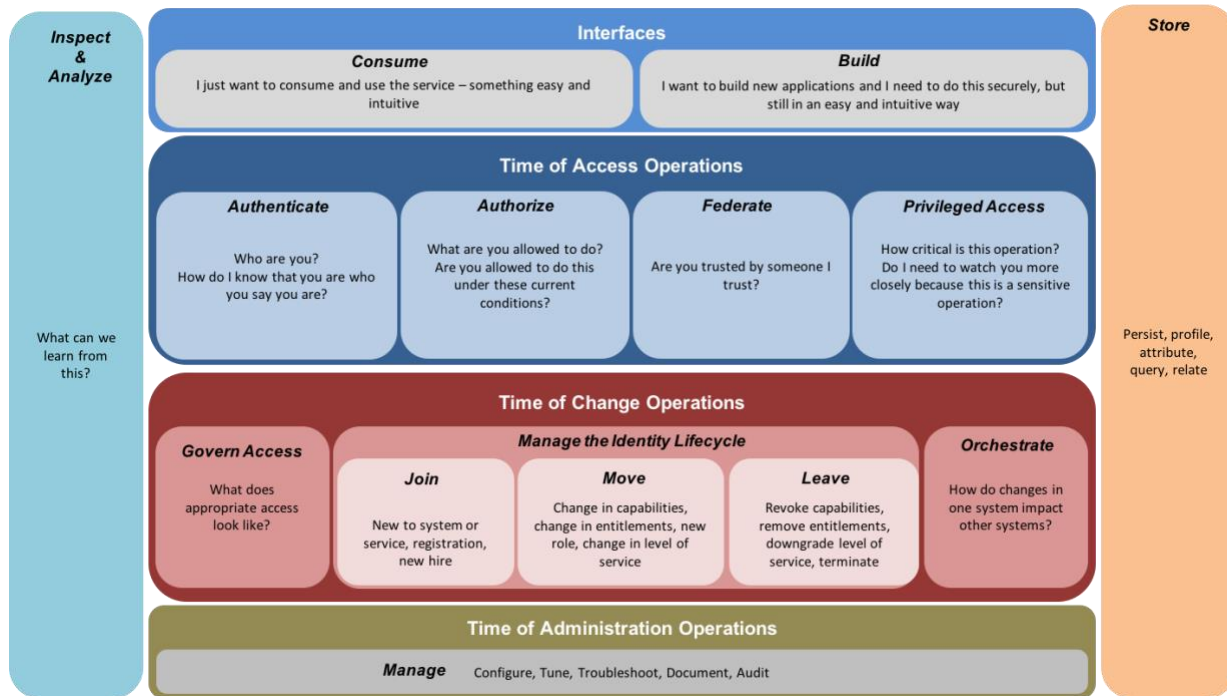


Figure 2: Describing the Capabilities That Define Identity Services

Each element further describes a capability required to effectively deliver IAM, that together provide a comprehensive set of run-time security controls. IAM based controls make it easier to determine the appropriateness of a given activity, operation, or interaction with data because they describe the nature of the relationship between the entity that is requesting/attempting this activity and the resource that is being accessed. The six major groupings of capabilities each contain more detailed capabilities that can themselves be exposed as an identity service.

Interfaces

This is how end users and other services interact with the rest of the identity services. It consists of:

- Portals and Applications that facilitate low-friction interaction with end users
- A set of Identity Services APIs that facilitate developers being able to natively leverage these security controls and services – helping developers with faster development of secure applications and services

Time of Access Operations

These are the operations that happen at the time access is being attempted. It consists of:

- Authentication – Identifying the entity that is attempting access to the resource with the appropriate level of assurance
- Authorization – Making decisions as to whether the authenticated entity is allowed

to access the resource or perform a given activity

- Federation – Is the entity that is attempting access trusted by someone I trust? Can this trusted relationship be leveraged to improve efficiency?
- Privileged Access – Is the operation a privileged or sensitive operation? Often these require additional controls and deeper inspection because of their elevated sensitivity.

Time of Change Operations

These are the operations that happen as the state of the identity attributes and the nature of the identity relationship changes over time. It consists of:

- Access Governance – Helping the right decision makers to be able to inspect and understand the current state of entitlements and permissions, then be able to make better decisions about how access should be granted (what permissions and entitlements should be issued), and attest that the level of access is appropriate
- Identity Lifecycle Management – Helping manage the changing state of identities through the time that an identity joins to participate in the environment (new to system or service, registration, new hire), how it changes and moves over time (changes in capabilities, changes in entitlements, new role, changes in level of service), and how to clean up as the identity's participation ends when it leaves the environment (revocation of capabilities, removing entitlements, downgrading level of service, terminating employment)
- Identity Orchestration – When there are multiple, distributed copies of data across multiple systems, how do changes in one system impact the other systems? How can these changes be orchestrated and managed as a common whole?

Time of Administration Operation

These are the operations that happen as broader environment is being administered. The configuration, tuning, troubleshooting, documentation, and audit of the environment. This consists of:

- Policy Administration
- Delegation
- Self Service
- Audit

Identity Repository

This is the persistent repository for storing the identity information (attributes, relationships, profiles)

Identity Analytics

This provides the inspection of the behavior and operations over time. Allowing for

gaining better insight and learning based on patterns of activity and behavior

Time of Access Operations rely on Time of Change Operations, such as identity lifecycle management (identity registration, provisioning, workflow) and identity orchestration (identity correlation, synchronization, transformation) to provide contextual information about the identities and their current state, permissions, and entitlements. For example, an authorization system may implement the policy that a user with the role or attribute "Employee" can access his or her "password" field in a database. Although the authorization system knows the rules, it cannot function without the identity data that identifies who the employees (or contractors, or customers, etc.) are.

Whereas authorization and other policy enforcement systems control access to resources by actively allowing or prohibiting runtime access attempts; provisioning and orchestration services control the policy settings and the flow of data that those policies rely on by propagating account information and access rights to diverse applications and security domains. These in turn use this information to locally enforce these policies.

Access policy, enforcement infrastructure such as Policy Enforcement Points (PEPs) provides authentication of subjects and may provide authorization and reduced sign-on/single sign-on (SSO) through components such as policy decision points (PDPs) that make authorization decisions on behalf of PEPs. Access gateways, web access managers (WAM), firewalls, proxies, and agents may function as PEPs that contact PDPs such as authorization services or other identity services, or PEPs may be co-located with their own PDP functionality.

Before they can access resources, users coming from within or outside an organization's network may pass through an access gateway (e.g., a portal) and multiple PEPs such as WAMs, firewalls, proxies, and agents. Though they may only have to authenticate once, with their identity propagated securely through the systems.

Access policy enforcement systems usually support reduced sign-on/SSO. In such scenarios, the centralized access services either proxy the access for the user, or generate Kerberos tickets, federation tokens, session cookies, or other session information that the resource can natively recognize. For authorization purposes, centralized policy enforcement services are often applied at the front end while leaving fine-grained or custom authorization to the local resource or resource manager. In such cases, it is important that the centralized policy service's view of identity and the resource view of identity are well correlated.

Many organizations are increasingly implementing identity federation to support access across multiple identity domains. In federated environments, domains exchange just-in-time assertions of identity attributes or events, such as whether a given user has logged into a given site and has a particular set of permissions. Identity federation may be established across internal business units, affiliated enterprises, or public identity networks.

Identity lifecycle management (also referred to as Provisioning) is the process for

automating the creation of accounts and the distribution of user, service account or device attribute information from authoritative sources to the point or points where this information will be used by an authorization process to grant or deny resource access requests. In effect, provisioning services associate an identity with one or more accounts and account privileges on IT systems. Provisioning generally includes:

- Provisioning policies and standards
- Access request methods, including self-service, event-driven and automated workflow
- Approval workflow
- Workflow automation tools
- Provisioning tools to create accounts on target systems
- Reconciliation tools and methods to ensure compliance with provisioning policies
- De-provisioning tools for the revocation of entitlements and clean-up of accounts that are no longer needed
- Audit tools for logging, monitoring and reporting

Another service that we haven't explicitly called out in the above diagram is identity aggregation (sometimes referred to as virtual directory services). Identity aggregation can consolidate data from multiple directories, databases and other sources into a single logical view without the need to copy the data from where it is being persisted. It can dynamically create the desired view of the identity data that best suits the needs of any application, eliminating the need for the application to have an underlying knowledge of how the data is persisted or structured.

Identity services facilitate the persistence, exposure and distribution of identity information—such as names, IDs, credentials, roles, and other attributes—to users, applications, user management, policy enforcement, and other services. Although directory services and other repositories are important components, additional identity services such as aggregation/virtualization, orchestration/synchronization, replication, and identity proxy capabilities are necessary to ensure adequate availability, accessibility, and performance. In particular, federation and virtualization are also important for increasing the utility of identity information for diverse applications and information domains.

From access control to account life cycle management to personal information protection, identity services can be utilized to satisfy several control objectives that IT auditors regularly evaluate. The control of business processes (and the elimination of human error from them) is a core element of many auditing requirements. Therefore, IAM's ability to automate such functions can have a positive effect on internal control and auditing.

To meet legislative, regulatory, and corporate requirements, organizations must implement several controls over identity-related information that:

- Prevent unauthorized access to data or systems, excessive privileges, or other security violations
- Detect non-compliant accounts (such as back door accounts, orphaned accounts or rogue devices) that have circumvented the preventive controls process
- Correct the errors found during the preventive and detective controls processes; this may include removing orphaned accounts, updating a user account to reflect the appropriate access rights based on the user's role, triggering a workflow to notify the appropriate individuals of an incorrect policy, etc.

Once an organization has defined the appropriate IT controls, it must define control activities such as separation of duty (SoD), attestation of user rights, documentation of explicit exceptions, and approval requirements. All events processed through the IAM infrastructure should be audited and logged to an audit log or repository. The audit log may be used for reporting, dashboards, or as a data input source for external systems.

Figure 3 below illustrates how Identity Services may be implemented in an organization in the service of consuming applications.

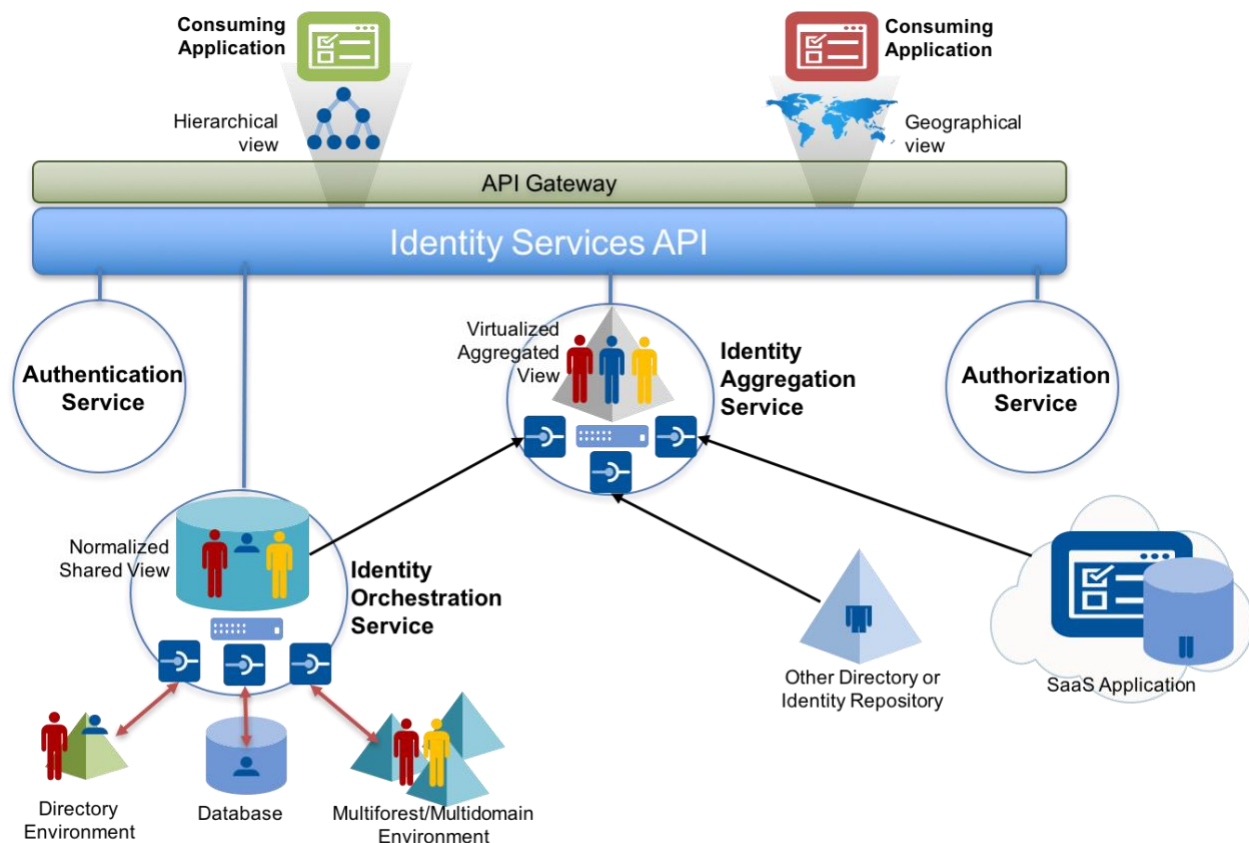


Figure 3 :Example of Using Identity Services

In this diagram, two different applications are consuming the same identity information, but each get the view of this information that best suits their respective needs. They access this data through the identity services API which abstracts the details of the underlying authentication service, authorization service, identity orchestration service and identity aggregation service. The identity orchestration service assembles and normalizes the identity information that is shared amongst the underlying directory, database and multi-forest environments. The identity aggregation service then takes this normalized shared view of the data and aggregates it with data collected from other sources to create a dynamically generated virtualized view for each application in the format that they requested.

An identity services approach focuses on the systemization and consistency of delivering identity information as a utility; where and when needed to applications and people. It starts with a consistent methodology for ensuring the accuracy and maintenance of the data contained in the identity stores. While there may be many moving parts, identity will ultimately be viewed as a utility supporting various applications throughout an organization. While many of the core concepts of identity services (authentication, authorization, virtual directories, federation, provisioning) have been in place for many years, service-oriented architecture and identity abstraction are core concepts that are critical to enabling IAM to support the next generation of identity consumers.

In the following sections, we provide our “stakes in the ground” as to where we believe IAM will and should go over the next five years. The future of Identity Management will leverage, of course, the key technology trends we described earlier...but it will also seek to solve problems that haven’t been adequately addressed from a product, service or process perspective in many enterprises over the past several decades.

So we’ve described the end goal; Identity as a Utility, as well as a how we might get there via cleaning up our existing mess and building a sustainable set of identity services. But this is just the starting point. There are a multitude of new technologies and methodologies that will be a core part of the fabric of identity services over the next five years. We’ll now take a look at the core technologies and approaches we see as critical elements driving successful IAM programs over the next five years.

The Future of Identity Management by Category

We describe the future of IAM within the following categories:

- The Foundation; Identity Federation, Virtualization and Normalization
- Blockchain-based Identity Systems and Self-Sovereign Identity
- Identity Services as Microservices
- Privileged Access Management
- Identity and the Internet of Things
- Relationship and Context-based Identity

- Cloud-based IAM
- Identity and Security Integration
- Scaling IAM
- Identity Governance
- Identity as a Privacy Enabler
- Identity as a Business Enabler
- Customer IAM

Each of these areas is a significant part of the future of IAM. Let's now look at the details of each area.

The Foundation; Identity Federation, Virtualization and Normalization

I know we are all anxious (including TechVision) to jump into the exciting new products and services that will support the next wave of innovation driving real digital transformation. But we'd be remiss not to start by looking at the basic foundation for Identity Management that is the necessary enterprise starting point. There needs to be a consistent, normalized, manageable set of identity services that can be the "launching point" for some of the more advanced and futuristic services we see being introduced within IAM systems over the next several years.

Most enterprises need to simplify and bring together current and expected new identity sources into a cohesive ecosystem. And as these identities continue to scale, we need to start with the solid foundation. These "glue" technologies will help; identity federation, virtualization and other means of bringing disparate environments together. This will be further supported by some of the more futuristic technologies we'll also discuss in this report—like blockchain, verifiable claims and self-sovereign identity we'll talk about later.

There needs to be a consistent, normalized, manageable set of identity services that can be the "launching point" for some of the more advanced and futuristic services we see being introduced within IAM systems over the next several years.

Federation and virtualization starts with the premise that no single company, government agency or organization can generally be the authoritative source for all objects that it needs to interact with—that isn't scalable and generally isn't possible. Identity federation will continue to be a component of the Identity Management in the future as it is means of extending reach with lower friction, particularly as the number of objects to be identified grows exponentially. Federation allows companies to provide access to applications and share resources without the need to adopt the same technologies for authentication, directory services and security. One of the biggest advantages of federation is that it allows

companies to maintain/control their own directories while extending reach beyond local authentication.

The use of identity federation standards can minimize costs by eliminating the need to develop proprietary solutions. Organizations need to identify and authenticate users only once, increasing security and lowering the risks associated with multiple authentications of identity information. Federated identity also improves privacy compliance by effectively controlling user access to information sharing and identity stores. Eliminating the need for new account registration improves the end user experience.

Although there are major advantages to federation, one possible obstacle is the loss of control, as credentials must be accepted from a source outside of the organization. This may be OK if authorization risk is limited to low-value transactions, but high-value, high-risk information may need to be more directly authenticated and managed. This is an issue of trust – that of trusting the federated user identity is truly who they appear to be. Another unfortunate aspect of current federation models is that many organizations use federated authentication as a ‘poor man’s provisioning’ mechanism, by creating local accounts based on a federated connection and thereby reducing the effectiveness of federation.

Thus far we have been focused on business-grade federation, but there is also a lighter weight form of federation commonly used by the major social media services called social log-in. This is when credentials from social media sites such as Facebook, LinkedIn or Twitter are used to log into other sites. This is an emerging area of federated identity that is gaining significant traction on the Internet. It is a double-edged sword for both the party using the service and for the party providing the federated login because there is a trade-off between the ease of integrating social log-ins and the inherent lack of identity verification associated with the typical social log-in. It also generally requires sharing personal information that may challenge escalating privacy regulations. It is also very easy to create a Facebook or Twitter account and masquerade as someone you are not. As a result, the issue of trusting the veracity of the federated identity is further exacerbated by the growth in social logins.

Nevertheless, social log-in has exploded over the past three years and is expected to continue to grow over the next several years. In this light, some protocols have arisen, namely OAuth and OpenID Connect, in addition to the now more widely deployed Secure Assertions Markup Language (SAML). SAML will continue to exist, but we project flattening growth over the next five years.

OAuth (now in version 2.0) provides client applications a secure delegated access to applications on behalf of an application (resource) owner in order to authorize third-party access to their resources without sharing their login credentials. OAuth is commonly used as a way for Internet users to log into third party websites using their Microsoft, Google, Facebook or Twitter accounts without exposing their user credentials (e.g, passwords).

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows web, Java and mobile clients to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile

information about the user in an interoperable and REST-like manner. Furthermore, OpenID Connect allows clients of all types, including Web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users. The specification is extensible, allowing participants to use optional features such as encryption of identity data, discovery of OpenID providers, and session management, as needed.

The Security Assertion Markup Language (SAML) is an XML-based federation technology employed in many cross-domain use cases. However, OpenID Connect can now support many of these same use cases with a simpler, JSON/REST based protocol. Not relying solely on HTTP, OpenID Connect was designed to also support native applications and mobile applications, whereas SAML was designed only for Web-based applications.

It is clear that the industry is making progress in cloud-based identity management and integrating enterprise IT environments with cloud-based application and infrastructure services via federation. To be sure, TechVision Research strongly recommends our customers embrace federated identity management as the means to bridge the migration to cloud-based IT. However, the proverbial elephant in the room is this: federation works very well as long as the federated identity is trusted. As we discussed previously about the weakness of social log-ins, all the federation protocols in the world won't be worth very much if we just don't know for sure that you are who you say you are.

So given some of the risks with social login, is there a better path towards extending IAM services to individuals? We think there is, but it will take some time to be established. We see a path toward this better future model with self-sovereign identity services in which an individual controls his/her identity and presents it to a consumer of this identity. We'll next look into this topic.

Blockchain-based Identity Systems and Self-Sovereign Identity

TechVision has written several reports that cover this topic, so we'll describe this at a high-level here. It is our belief that there will be a new digital foundation that supports a pervasive set of services that supports the sharing of only the necessary and relevant bits of verifiable information necessary to perform specific transactions. These new models can be applied to a diverse set of services ranging from logging on to an employer's network, accessing services from a healthcare provider network or leveraging the services of Amazon, eBay, Bank of America, or eTrade. In accessing any of the services the goal is to develop mechanisms to gain explicit consent to easily share specific information with specific entities.

This future of IAM includes this distributed, self-sovereign identity approach that offers both empowerment for individuals and risk mitigation for the enterprise collecting this information. Think of this as microservices for Identity Management in that an identity can be viewed as an atomic, self-sovereign entity that can be used in multiple ways under the control of the owner. The timing of the Equifax breach further highlights the risks of exposing Personally Identifiable Data (PII) and we describe a model that limits the need for excessive PII to specific data required for authentication, authorization, or data that has been explicitly agreed to by the owner. But it isn't just privacy protection as moving to a

distributed identity model is a more scalable foundation for digital transformation.

The goal is to maintain a digital satchel of non-repudiable and verifiable attributes that can be shared individually with the entity engaged in the transaction or communication; this is where blockchain identity fits in. In fact, some of these attributes can and should be based on reputation – the ongoing establishment of authenticity over time, vouched for by third parties that the service provider recognizes as verifiable and accurate. Let's consider how blockchain and verifiable claims coupled with self-sovereign identity can provide this capability.

The goal is to maintain a digital satchel of non-repudiable and verifiable attributes that can be shared individually with the entity engaged in the transaction or communication.

That said, blockchain can be an important part of this new identity model, but what role does it play and, perhaps more importantly, what role doesn't it play in supporting self-sovereign identity? Blockchain or distributed ledgers can provide greater discoverability of an identity and secure connections to the data needed to support a transaction. Daniel Bucher, the head of distributed identity at Microsoft nicely articulated how blockchain might support IAM at a recent conference. He said "Blockchain-anchored identifiers linked to identity hubs, encoded with semantic data, are the agar upon which apps and services will grow".

So blockchain can provide the identity anchor, allow for discovery and be the immutable unforgeable record to link an identifier to an object. But what it can't do without help is to determine what is needed for a particular transaction to be satisfied: am I old enough to purchase alcohol, am I credit worthy, do I live in the US...for this we need an extension to the blockchain identity anchor; answering these questions requires another element. This new piece in the modern identity puzzle is called a verifiable claim.

In particular, each block in one's blockchain may contain "pointers" to encrypted and signed verifiable claims. A *verifiable claim* is a qualification, achievement, quality, or piece of information about an entity's background such as a name, government ID, payment provider, home address, or university degree. Such a claim describes a quality or qualities, property or properties of an entity that establish its existence and uniqueness. Entities (people, organizations, devices) need to make many kinds of claims as part of their everyday activities.

As organizations progress towards digital transformation, entities need to be able to transmit instantly *verifiable* claims (e.g., about their location, accomplishments, value and so forth) providing electronic proof that the claim is valid. These claims can support the next generation of web applications as they provide the basis for authorizing entities to perform actions based on rich sets of credentials issued by trusted parties. Human- and machine-mediated decisions about job applications, account access, collaboration, and professional development will depend on filtering and analyzing growing amounts of data.

It is essential that data be verifiable. Therefore, standardization of digital claim technologies makes it possible for us to issue, earn, and trust these essential records about their counterparties, without being locked into proprietary platforms.

The cryptocurrency application itself has given us a sketch of new meanings that apply to money and mediums of exchange. The blockchain can house and transact with unlimited amounts of valued assets through its publicly distributed ledger, and among these valuable building blocks is unforgeable data. Blockchain's transparency attributes can support BYOID in a more secure, immutable and non-repudiated identity ecosystem that effectively crosses enterprise and personal identity boundaries. The blockchain has become an important invention and its relevance and scope will accelerate over the next five years.

What would some typical architectures and use cases look like? We'll have to go back to the future. Technologies such as identity federation using OpenID Connect, OAuth and SAML will be necessary in order to broker authentication events centrally and assert user identities to online service/resource providers. This will be (yet another) massive effort, because organizations' existing IT systems will need to be retrofitted to use federation. Any sensitive data (e.g., patient health information) would be stored using data masking and tokenization – or as we have discussed, using a blockchain, such that the theft of these data would be completely worthless.

Last but not least, for a blockchain and verifiable claim-based self-sovereign identity systems to work in the real world there needs to be a governance model and a trust framework that allows for independent identities and claims to be shared with confidence. This is an area we will watch closely over the next several years as its progress will be an indicator as to how quickly this space may mature for large enterprises.

Identity Services as Microservices

DevOps and Microservices are changing the application development world as organizations move from a centralized, monolithic development environment to one that is much more dynamic and adaptive. Microservices represent a way of designing applications as independently deployable services. Microservices start with a focus on business capabilities, not technology. It is an architecture style of developing a single application based on small, self-contained set of services running their own processes and communicating via a lightweight mechanism. There is limited centralized management or governance of these services and they can be written in different languages and use

As organizations progress towards digital transformation, entities need to be able to transmit instantly verifiable claims (e.g., about their location, accomplishments, value and so forth) providing electronic proof that the claim is valid.

different storage approaches.

More traditional monolithic applications incorporate capabilities that are similar to those included in other applications, yet implement them independently. This may make the applications difficult to maintain and doesn't take advantage of lessons learned within the development of other applications. The idea of decomposing common capabilities into microservices is to split an application into set of smaller, interconnected services that facilitate greater reuse and higher reliability by leveraging well established and tested capabilities in new application development. When an application is built as a set of microservices, it is important to decide how the application's clients will interact with these microservices. With a monolithic application there is just one set of (typically replicated, load balanced) endpoints. In a microservices architecture, however, each microservice exposes a set of what are typically fine grained endpoints – each with its own interface.

Microservices enable an 'abstraction layer' that can dramatically simplify application development, integration and operational support. This is similar to the abstraction layer we were describing earlier which may provide a sense for the synergy as identity services are presented via a microservices approach. In this model, IAM services and functions that are enabled in a secure, easy-to-consume manner. As new protocols, techniques and infrastructure approaches emerge (e.g., blockchain, distributed ledgers, verified claims), and old techniques fade away the impact on the IAM infrastructure will remain minimal by following the core principles we describe in this report. Doing so is the surest way to 'future proof' your IAM strategy.



*Microservices enable
an 'abstraction layer'
that can dramatically
simplify application
development,
integration and
operational support.*

Identity and access management typically involves a number of functions regarding the establishment, management and use of identities built into a monolithic application to provide access to information as supported by policies. The enterprise goal is to provide end users (and applications) with appropriate access to enterprise systems and applications. The word "access" has two primary components: authentication and authorization.

- Within authentication, systems and applications identify who someone or something is by looking at a host of attributes: login IDs, passwords, digital certificates, federation, one-time password tokens, etc.
- Within authorization, attributes such as roles, group membership or other attributes or affiliations are used to grant or deny access.

There is also the need to secure access to the microservices themselves. An API Gateway is often employed to help manage and organize access to each of these microservices interfaces. The API Gateway is a server that acts as the single entry point into the system. The API Gateway encapsulates the internal system architecture and provides an API that is

tailored to each client and is responsible for request routing, composition, and protocol translation. All requests from clients first go through the API Gateway. It then routes requests to the appropriate microservice. The API Gateway will often handle a request by invoking multiple microservices and aggregating the results. The following diagram illustrates how a monolithic application can be decomposed into microservices.

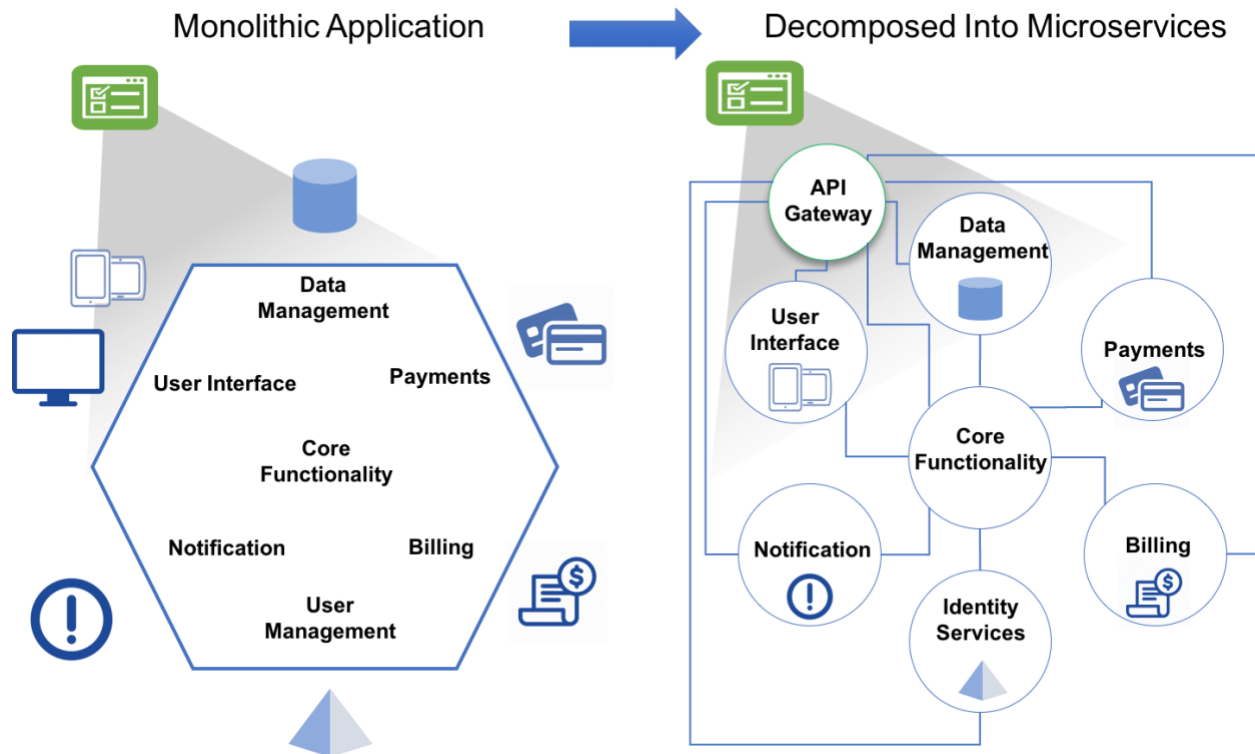


Figure 4: Decomposing Monolithic Applications into Microservices

Over the past decade, an intense transformation of IT has taken place with the widespread adoption of cloud computing, SaaS and PaaS integration, system and infrastructure virtualization, mobility, federation, IoT, IAM and more. Add to this the growth in managed IT services supported by 3rd parties and the typical enterprise IT environment now looks nothing like it did ten years ago.

As part of this transformation, a renewed focus has been levied on the Development and Operations groups responsible for developing, integrating and maintaining IT services - including IAM, for all constituents, whether internal or external to the organization. Traditionally, these two groups operated in a somewhat isolated fashion, with Development working feverishly in its own silo, releasing new "IT products" (whether developed in-house or integrating commercial-off-the-shelf solutions) to the IT Operations staff - who are then challenged with maintaining these products. Such a waterfall model for application development has often lead to severe disconnects between Development and

Operations, because the process is non-iterative and comprises no viable near-real-time feedback loop.

We call these symptoms “DevOps anti-patterns”, which have become prevalent across projects and platforms, typically resulting in infrequent releases with traditional change controls leading to long lead times, and manual, time-consuming, painful, and tedious delivery processes, which act as great inhibitors to digital transformation.

There are two emerging, synergistic approaches to this dilemma:

- Logically combining the Development and Operations groups into a single entity referred to as DevOps, with a primary focus on agile development (the antithesis of the waterfall model) coupled with,
- Microservices architecture and deployment strategies that break down business functions into atomic-level IT functions, or “services”, that can be reused, retrofitted and replaced with minimal disruption to the overall IT infrastructure.

One of the most significant results of such a DevOps model is improved accessibility of IAM services functions, such as user/thing authentication, authorization, lifecycle management and audit readily available to application developers and integrators. Without an effort to move toward a better DevOps paradigm, enterprises will continue to suffer from siloed applications and services that will perpetuate the issues of disconnect that largely exist today.

Privileged Access Management

We stress that many of the most egregious, recent data breaches were ultimately the result of the affected organizations’ administrator accounts being compromised. Without going into detail:

- Target lost over 70 million customer credit card numbers through the breach of an administrative account managing its access control service
- Anthem Health lost over 80 million patient’s personal information when hackers gained administrative privileges to databases where the information was maintained
- Home Depot lost nearly 60 million customers’ credit card details when a vendor’s administrative account was compromised
- JP Morgan Chase lost nearly 80 million customers’ personal data through access to an under-protected server that provided broader administrator access across their network
- Equifax Argentina practically gave hackers access to over 14,000 credit records by ignored basic security practices. Employees were given default passwords that were never changed and administrative accounts were set up with the username being “admin” and the password being “admin”.

- Hackers were able to gain complete access to Deloitte's entire email system, including attachments, IP addresses, and login information by infiltrating an administrative account

Privileged accounts are usually required for system functionality and are created when the system is installed. In the case of privileged accounts within many organizations, there is an enormous need for better forms of authentication and authorization, as administrator accounts are often shared, adequate activity monitoring is often lacking and no one particular administrator can be held accountable. In other words, the majority of these accounts that have access to sensitive information are not associated with any one individual user. Increased auditor sophistication and increased organizational emphasis on compliance combined with the realization of privilege elevation attacks have raised concerns about privileged accounts to the highest levels of the organization.

What is needed in virtually every organization in order to avoid these types of breaches is Privileged Access Management (PAM) that can be defined as “a set of technologies that allow organizations to identify, secure, and monitor accounts that have elevated privileges in order to minimize risks and ensure compliance.”

PAM products can improve the security over sensitive information by restricting access to privileged account passwords. We strongly recommend organizations implement PAM.

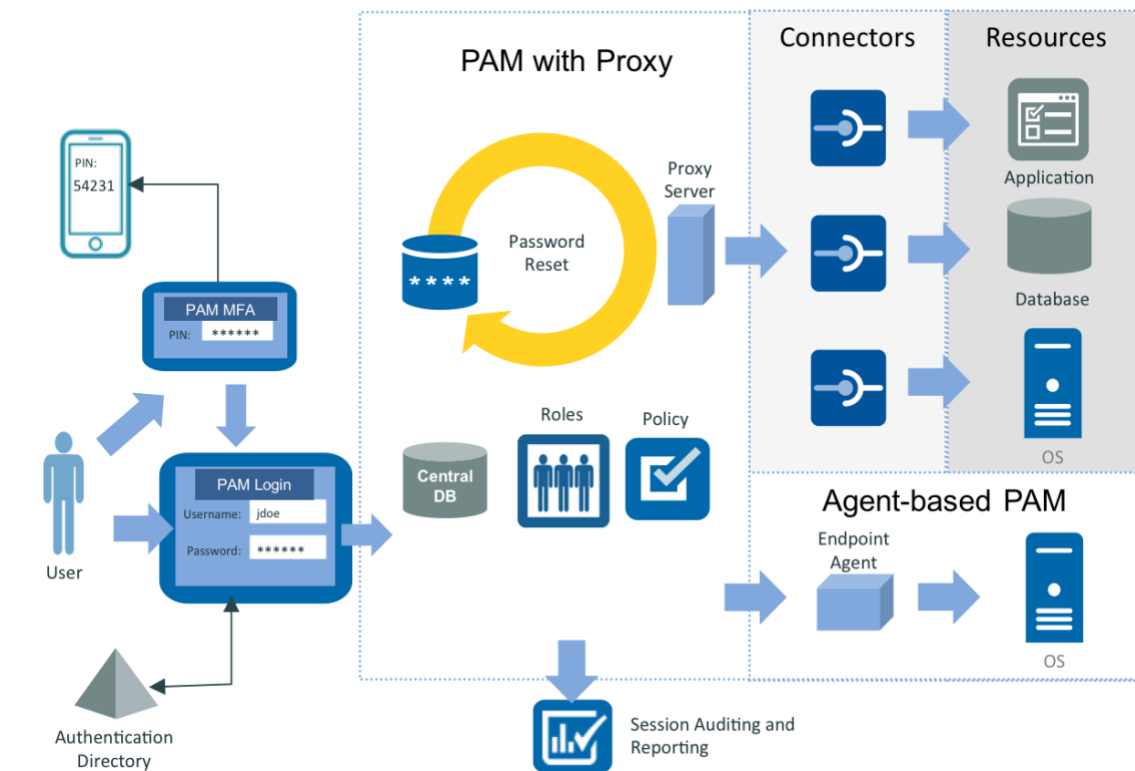


Figure 5: Privileged Access Management

Privileged access management leverages a strong IAM infrastructure and it should be a core part of any organizations security and risk management portfolio. PAM will also be tied into the corporate governance model to help enforce compliance. Organizations should manage PAM to a “least privileged model” where access is only granted when absolutely necessary, revoked upon completion of task, and rigorously monitored. Additional security should be applied to administrators with the highest order keys to the kingdom. PAM will continue to be a foundational infrastructure component for enterprises over the next five years.

Organizations should manage PAM to a “least privileged model” where access is only granted when absolutely necessary, revoked upon completion of task, and rigorously monitored.

Identity and the Internet of Things (IoT)

As Mickey McManus explains in his outstanding book “Trillions”, we are rapidly approaching a world with a trillion plus nodes connected in a global network. This isn’t a trillion isolated devices, but a trillion addressable nodes in an interconnected network. This basic premise has massive consequences on the scale and complexity of the Internet as well as its identity, security and privacy underpinnings. The infrastructure to support IoT scale will include a new or modified registration system for these nodes, new security policies, new privacy policies, revised regulations, new governance models, schema modifications and updated discovery mechanisms at a minimum.

And from an Identity Management perspective it isn’t just the scale, but the relationships many of these devices have; including the manufacturers of the devices, the current owners, the previous owners, major components (like in an automobile), special privacy considerations (like with medical devices), security provisions...so it isn’t just the scale, it is the layers of relationship management that are unique to the IDentity of Things (IDoT)

We will highlight a few early, expected outcomes, but much of how privacy, identity management, data ownership and the Internet as a whole will evolve is a work in progress with many possible paths. What we do know is that while individuals and businesses will gain a lot in terms of productivity and connectivity, the potential for privacy and security issues will increase by orders of magnitude. For example, devices that allow a parent to monitor the location of their child can help protect the child, help inform the parent, but could also potentially enable a child predator. At a business level, a biometric device attached to a senior executive’s wrist can improve health and productivity, but if tapped into, it may leak intelligence about an imminent corporate acquisition. There are many of these scenarios that need to be addressed by the security and identity infrastructure. The problem is that effective technical solutions are limited by many of these endpoints having very low bandwidth, low power consumption as well as other factors

Despite these challenges, how does identity management evolve over the next few years in an environment that includes massive IoT deployment? Identity management systems will need to evolve to recognize the relationships between devices and people / applications / services. This will be important in identifying the connected devices, but also critical in securing them and dealing with the complexities involving device ownership and access. For example, does the individual, the cardiologist or the medical device manufacturer have rights to the data generated by an implanted medical device?

Identity Management systems must be able to handle the sheer volume of connected devices, the complex relationships and the security ramifications. In addition to identifying and managing the connected device, IAM needs to understand the customer connected to the device. Expect IAM for IoT to leverage context data, advanced filtering, artificial intelligence and behavioral analytics. Securing IoT devices that may have little intelligence or security factored in will ultimately need to have device identities baked into the chip.

Connected devices must become part of the IAM infrastructure and leverage and integrate with asset management systems and other device management systems. There will be increasingly sophisticated security and privacy policies to help manage these new resources and limit abuse. Since devices have not traditionally been part of IAM systems in this way, the identity of things (IDoT) must draw upon other existing management systems to aid in developing the single-system view for the IoT. IT asset management (ITAM) and software asset management (SAM) systems have traditionally managed IT and software assets of all types. The IDoT will assume some functional characteristics of ITAM and SAM within or integrated with IAM architecture, or be linked to ITAM as attribute stores.

The ultimate business goal for IoT connected devices will be to leverage relationship data and tie the IoT connected devices to the business systems. For example, IoT data with context will feed CRM systems and affect marketing systems, sales forecasting systems, production systems, and provide customer insights and business data intelligence not available today. While all of these advancements in IoT integration are impressive and realistic, they will place a tremendous load on Identity Management systems. As a result, future identity systems will need better compartmentalization to keep user and thing data and integration logically separate in order to manage service levels and risk appropriately.

Relationship and Context-based Identity

Relationship or context-based identity correlates relevant data with the identity information being stored in the IAM system. Relevant data can include behavior data, location data, usage patterns, preference data, personal data, systems information, group memberships and many other types of data that can be correlated with identity information. As more and more data is stored in the cloud and in enterprise data repositories, linking this data with an identity can provide additional insights that can be used to better serve the individual and the enterprise.

Context-based identity data can also be used to understand relationships, environmental factors, temporal state, roles and be used to assess anomalies. Lastly, context-based identity can help to predict behavior and patterns and detect security threats. Relationship-

based IAM will be a core part of the future of Identity Management and critical to successful digital transformation programs.

The issue for most organizations is not whether to leverage context-based identity information; it is how much is enough. Where do we reach the point of diminishing returns and what line should be drawn in terms of collecting external personal data? Make no mistake; most organizations will need to retain some data about each individual as it pertains to their transaction history (e.g., recent purchases), device identifiers, personalization, proximity, affiliation and so on. This is where a well-defined privacy policy is of considerable value in walking the fine line between the collection/analysis of personal data and organizational risk.

There are the attributes about a person that we store in order to retain context within each user interaction with applications, services and systems. TechVision Research recommends an Identity Data Service as a ready means to assimilate user/transaction data in various repositories in order to allow applications to be more context-aware.

Context-based Identity Management provides valuable data to support security programs. The more data points an organization has to build on, the stronger the intelligence and the ability to discern between normal behavior and anomalies. This is critical to threat detection in a very focused and less invasive way for users. There are massive amounts of data in the cloud that can be used to embellish IAM data in a way that can better protect organizations and individuals.

Context-based Identity Management at cloud-scale and IoT scale will require some changes in underlying database technologies. These changes include a movement towards graph databases, RESTful interfaces and graph APIs to both scale and share valuable relationship information to/from IAM systems. For example, graph models like Neo4J have the potential to efficiently query for authorization and authentication and receive fine-grained access control responses.

So far we've discussed three important enablers for Context-based Identity Management, a larger data pool, the use of graph databases and the migration or extension to the cloud. Another key component for context-based Identity Management to reach its full potential is a meaningful increase in the use of Artificial Intelligence (AI) capabilities to accurately predict which identity proofing and authentication events are to be trusted.

Current use of AI is largely limited to rules-based post-event examination of logs or anomalous behavior detection, looking to uncover recent or in-progress inappropriate activity. There are also a few applications that will provide risk scoring, based on known events, for specific devices or accounts. But by adding machine learning, statistical modeling and predictive analytics to the IdM toolkit, the focus can change from detecting a recent bad event to anticipating or predicting an upcoming bad event. This will allow Identity Management to shift back into preventative mode without the friction that arises from requiring pre-provisioned accounts for every target asset. This has significant implications for securing assets and protecting privacy. AI/ML will be addressed in further detail a bit later.

Cloud-based Identity Management

The combination of applications, computing power, and storage moving to the cloud, pervasive Internet access, the evaporating perimeter, the proliferation of IoT, mobile requirements and the expanding base of consumers of Identity are driving a major shift of IAM to the cloud. Even if an organization elects not to move to cloud-based IAM, identities will be presented from the cloud. This will include employee identities, contractors, suppliers, customers and various trading partners. It is also worth noting that the identities or at least identity attributes established internally will increasingly be consumed by cloud-based services. This may be through federation or simply to verify attributes, but virtually every enterprise will be moving towards cloud-based IAM over the next several years.

Technology and business trends are driving the movement of IAM to the cloud. The combination of enterprise “cloud-first” strategies, a largely disappearing perimeter, the proliferation of IoT devices, and the need to integrate external identities are contributing to an accelerated movement of IAM to the cloud. There is also a massive proliferation of data to be identified and managed; the proliferation of CRM information, the exponential explosion of IoT data being generated, as well as the explosion of social media-based data are supporting businesses that are built on information sharing. The sharing of this information needs to be carefully managed with owners and consumers of data clearly identified. Much of this information is widely distributed and also fits well in a cloud identity service.

We have already discussed at some length how identity data is spread across an organization (as per enterprise use cases) or the Internet (as per consumer use cases). In both of these scenarios we believe that a good deal of this information is already in the cloud in some capacity.

Adding context-based data to identities will also heavily leverage cloud-based services since much of that data is already in the cloud. Furthermore, leveraging the cloud to provide data supporting security and threat assessments will be critical to future security and risk programs.

The next generation of Identity and Access Management (IAM) stretches beyond the traditional enterprise to the broader Internet at large, eliminating borders rather than being constrained by enterprise firewalls. This involves scaling services from supporting thousands or tens of thousands of identities, to supporting hundreds of thousands or potentially millions of personal identities as well as an untold number of objects or ‘things’. These elements support the movement to cloud-based Identity Management.

There are two fundamental approaches to cloud-based IAM as follows:

- **From the bottom up** - where nascent, cloud native IAM vendors have developed from scratch a growing set of cloud-based services, initially entering the market with simple, straightforward point solutions such as authentication, single sign-on (SSO), and federation; and gradually adding on additional functionality such as basic user provisioning, de-provisioning, and access governance. As might be expected,

the focus of these cloud-first offerings have greatly leveraged the multi-tenancy, elasticity, and scalability that cloud-based architectures provide, but often lack the maturity, overall breadth of capabilities, and scope of integration found in many 'more traditional on-premises IAM suite offerings.

- **From the top down** - where more traditional, mature, on-premises IAM suite vendors have begun to transition their products to the cloud, either facilitating hosted deployments of their more monolithic, single tenant architectures, or through managed service providers that will host and manage these deployments on behalf of the customer. The catch here is that while these IAM suite products offer a broader set of capabilities and provide a greater range of integration options, fundamentally they were not designed with the cloud in mind. They tend to be much more complex to deploy and manage, often requiring extensive customization. Hoisting these solutions to the cloud either have required virtualized packaging of the offering to facilitate hosting on IaaS platforms, or the skills of the managed service provider to stand up the necessary instances for each customer.

This leaves organizations in a position at this point in time of having to choose between two less than ideal options – 1) the cloud-native approach that is simple and easy to use and supports future technology trends, but is not as full featured or as capable of addressing the broader set of IAM requirements; or 2) one that is more mature, feature rich with better integration, and can satisfy most IAM requirements, yet remains very complex and unwieldy to manage and is largely on-premise centric. This will change over the next several years as vendors begin to leverage the strengths of both the bottoms up and top down approaches to build what we call a “full-service IDaaS” offering that combines the scalability of an cloud-based service with the governance, provisioning and integration offered by traditional on-premise IAM offerings. This will be necessary to manage the largely hybrid environments we expect will be maintained in most large enterprises over the next five years and this is the direction we believe most large enterprises should be moving towards.

*full-service IDaaS”
offering that combines
the scalability of an
cloud-based service
with the governance,
provisioning and
integration offered by
traditional on-premise
IAM offerings*

Identity and Security Integration

Identity and security are joined at the hip and will continue to be over the next five years. The reasons are pretty simple. Security is required to ensure that the identity system is not compromised and identities are the foundation for describing the resources to be secured. You can't have traditional security without an identity system because you will not know who is entering the system or what their rights are. You also can't protect assets enough to do identity in the first place.

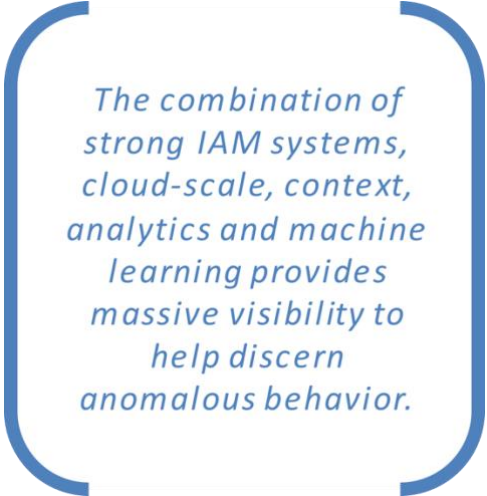
Identity and security will increasingly leverage context, machine learning and AI to be

more proactive in addressing security threats. The future of security will have to be much more proactive as the attack and attacker sophistication grows exponentially. Given the evaporating perimeter it will be necessary to fully understand the identities being managed, the context of those identities relative to what they are trying to do and the resources the enterprise wants to protect. As firewalls are largely going away, there needs to be a means of ensuring the accuracy of identities initiated within and outside of the organization and fully integrating IAM into security and risk programs.

As mentioned earlier, behavioral-based security and context-based security will be core elements of future security programs and it is all premised on getting identity right. Successful implementation of the 21st Century IAM program explained above will provide the foundation necessary to support the next generation of security/risk programs. Cloud-based IAM and the integration of IoT identities are also a necessary pre-requisite to next generation security programs.

Security breaks down when IAM systems are not complete or reliable. The proliferation of identity silos create huge security holes that must be addressed ASAP. Virtual directories will be an important mechanism to create a normalized view of heterogeneous Identity Management systems. This is captured by Michel Prompt from Radiant Logic in characterizing successful IAM systems as needing to start with “one version of the truth.” Pulling together this scattered identity information and creating this organizational version of the truth is critical to limiting attack points and driving strong security programs.

The combination of strong IAM systems, cloud-scale, context, analytics and machine learning provides massive visibility to help discern anomalous behavior. Patterns across multiple companies, geographies and user profiles helps to establish this baseline. Further analytics include authentication events, application usage and privileged activity monitoring which helps to feed the security systems and will be inextricably tied to the IAM systems.



The combination of strong IAM systems, cloud-scale, context, analytics and machine learning provides massive visibility to help discern anomalous behavior.

Scaling Identity Systems

Identity management systems must rapidly scale over the next five years in response to IoT, new identity-aware applications, big data, context-based identity management systems, consumer identity integration and rapidly evolving security requirements. Cloud based identity and graph databases will help to support the scale and flexibility needed to enable future identity management systems. The movement from on-premises Identity Management to cloud-based and hybrid IAM is key to supporting the scaling next generation Identity Management systems will require.

Specific areas to focus on to meet the massive scale required over the next five years

include:

- Standardizing on an Identity Data Service
- Identity consolidation: eliminate redundant directories and data stores
- Standardization: OAuth, SAML, OpenID CONNECT, User Managed Access (UMA)
- IoT Identities on the chip
- Graph databases and Graph APIs
- Cloud-based Identity
- Virtual directories
- Packaged pre-defined business processes
- Replication for both reliability and performance
- Leverage consumer facing identity solutions

As we look to the future, Identity Management systems will scale by minimizing redundancies and heavily leveraging cloud-based services. Consumer identities will largely be managed by services that specifically focus on cloud-scale such as those provided by Amazon Cognito, Facebook Parse, Google Identity tool kit or the Microsoft Azure B2C offering. Enterprises will increasingly depend on cloud-based identity vendors such as Okta, ForgeRock, IBM, Janrain and Ping Identity to support the increased scale required by enterprise IAM solutions. Microservice-based Identity Management providers such as Cloudfity will achieve scalability with a “Netflix-like” approach of providing services when needed.

The underlying database technology will also largely move to graph databases and graph APIs to handle increasingly complex relationships and dramatic increase in scale required by next generation Identity Management systems.

Identity Governance

Identity Governance and Administration (IGA) has not always been given adequate attention and funding within the context of enterprise identity programs. This needs to change as the effective management and governance of identity services is a key to enterprise security and essential to the efficient operation of the identity services.

Enterprises need a consistent framework for operationally managing and governing their rapidly expanding digital ecosystem and IGA is an important piece. At its core, the goal behind IGA is simple: Ensuring appropriate access, when and where it is needed.

A key component of IGA is, ultimately, the automation of the identity lifecycle through an identity provisioning infrastructure. This helps both fulfillment and the enforcement of access decisions. The automation and enforcement helps prevent deviation from these decisions and reduces the amount of effort required for the next round of access reviews.

IGA is much more than technology, but can be thought of as an ongoing means of governance through a set of controls, processes, and actions related to the determination and enforcement of appropriate access throughout the organization's environment. This is a continuous process of grooming, review, decision making, documentation, and enforcement for how access privileges are issued.

IGA combines entitlement discovery, decision-making processes, access review and certification with identity lifecycle and role management. IGA operates in the intersection of business process management and access automation allowing people and systems communicate with each other, fulfilling day-to-day operational needs. It focuses on the process and operational components of Identity and Access Management. From a technology perspective, from a governance perspective and from a process perspective, the governance, administration and lifecycle management areas need to be a significant area of investment for most enterprises over the next five years. It is key to an effective and usable IAM program and also critical to properly managing enterprise risk.

Identity as a Privacy Enabler

Identity Management systems and services tied with contextual data, analytics, AI and ML can provide unprecedented information about individuals; more data than most would consent to. We're at a tipping point where the management of identity data must be improved dramatically, and most likely this will need to happen by not adding more of the same identity management approaches, but radically different ones instead. For instance,

- We must change our way of storing and using sensitive personal identifiable information (PII). There will be more centralization of core sensitive information into closely guarded data "vaults."
- Each citizen, employee, customer (i.e., "user") will maintain personal identification information in a similarly protected data vault.
- Abstraction of existing sensitive data, whether user identity information, sensitive personal information, sensitive corporate information (e.g. intellectual property) will become the norm, reducing the amount of proliferation of the actual sensitive data.
- The use of blockchain and verifiable claims with zero knowledge proofing to limit the propagation of PII.
- Compliance with GDPR and other privacy regulations

It isn't all about regulatory compliance and fines; organizations are being increasingly aggressive in collecting, correlating and acting on PII which is, increasingly alienating prospects and customers. So enterprises need to determine how Identity Management systems can support privacy while maintaining business goals. We believe it starts with separating the identity information from other PII and carefully controlling access to the core identity data. PII requested and retained will increasingly be limited to data with consent explicitly granted for storage and use. Consent will need to extend to how the data

will be used and to who it will be disclosed.

Context-based identity can also be a privacy enabler even though it may require storing or accessing additional data. The key is having sufficient context to establish a base line of normal behavior and then only track anomalies. This means that threat detection will only require deeper probing if there is a flag rather than broad surveillance. A long-term goal is to dynamically generate context to avoid creating new static sources of correlations between users and actions that can lead to subsequent privacy issues.

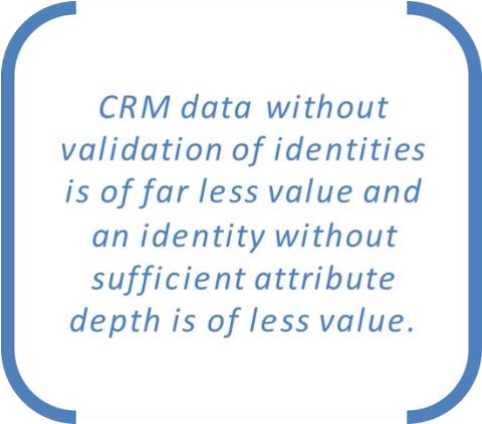
Privacy is a major coverage area for TechVision Research and will include technical aspects, legal issues, regulatory issues and ideas about how organizations can gain a competitive advantage through a well-designed privacy program.

Identity as a Business Enabler

The next generation of Identity Management will increasingly support strategic and tactical business needs and create major opportunities for organizations that best connect their technology programs to major business initiatives. One of the biggest challenges organizations face today from an IAM perspective is walking a fine line between collecting information about customers from multiple sources and using that information in a way that both serves the businesses needs and is not perceived as invasive to the prospect/customer as we discussed above.

Predictive analytics tracking behavior and correlating information from multiple sources can help an organization better serve its existing customers and find new customers. That said, knowing too much without authorization is viewed as “creepy” and may not be legal. IAM can provide greater focus, greater assurance of a participant’s identity and provide a platform for intelligent decision-making without crossing privacy and legal lines. The trend towards self-sovereign identities will likely clash with the current data mining and so-called predictive analytics (marketing) capabilities many organizations currently employ. Because of this, we underscore the necessity to look closely at the future of IAM as we are outlining in this report. This trend will bring about much disruption to current business analytical models.

A key component of next generation Identity Management systems will be increased integration with business systems and business goals. This is core to the real value of most digital transformation initiatives. For example, coupling IAM with CRM will be of value in identifying sales opportunities, customer needs and driving additional revenue. CRM data without validation of identities is of far less value than an identity with validation and sufficient attribute. Coupling CRM and Identity systems will be of tremendous value to businesses.



*CRM data without
validation of identities
is of far less value and
an identity without
sufficient attribute
depth is of less value.*

As described earlier, context-based IAM coupled with machine learning can be a critical

part of the next generation of security and threat detection. The business benefits of protecting confidential client data and IP will be major areas of competitive advantage (or at least avoid a serious competitive disadvantage) in the future.

The opportunity to have rich client data and business analytics without crossing “privacy boundaries” is the sweet spot for most enterprises and enterprises that are successful in this space will have a major competitive advantage.

Customer IAM (CIAM)

There is an accelerating need to store, analyze, manage and present customer and prospect data in a more sophisticated and user-friendly way than exists in most enterprise-focused IAM solutions. The gradual transition from on-premises facilities to the cloud has opened up a world of possibilities, as is apparent from the number of enterprise vendors who are extending the reach of their solutions.

There is increasing momentum, and will be for the next several years, toward a separate, specialized IAM category focusing on customers we call CIAM. This has been going on for several years with vendors such as Janrain, Gigya and iWelcome as specialty CIAM vendors, vendors such as ForgeRock and Ping providing scalable CIAM solutions, vendors such as Cloudentity and Okta offering microservices for the developers and vendors such as Radiant logic providing a means of bringing multiple data sources into a common context. That said, this space will rapidly expand with significant investment over the next five years...and this will be a major coverage area for TechVision.

The basics for the growth and future of this space are easy to see; the connection with customers is a core part of any broader digital transformation program and is becoming a business necessity. Enterprises will accelerate their investments in providing a secure, seamless and unified customer experience across multiple channels – and the way to achieve that is through deploying the right customer IAM (CIAM) solution. The immediate benefits to the customer are to reduce friction through multiple login options and increase and improve engagement through self-service and progressive profiling. This leads to greater transaction satisfaction and the likelihood of brand loyalty along with the development of a mid- to long-term relationship.

From the organization’s perspective, the upfront investment in CIAM offers faster time to market, a reduction in administrative overhead and ultimately an ongoing increase in revenue. The opportunities to get to know customers better are provided not only by cataloging preferences from their engagement history and self-provisioning.

Recommendations

In this report we cover many approaches, initiatives and trends and there are some common over-arching themes that are crucial for all organizations to consider:

The IAM architecture principles identity data services, federation, loose-coupling and standards-based integration as fundamental keys for successfully addressing today’s and tomorrow’s IAM burden.

An architecture built on these principles will help one become ready to quickly integrate emerging BYOID approaches including blockchain, OpenID Connect and OAuth. Additionally, such an architecture provides the scalability and elasticity to effectively support the Identity of Things by eliminating the monolithic, single-purpose approaches that incorporate specific groups of things as one-off solutions.

- Embrace the cloud – it is here to stay. These architecture principles will help one become cloud-ready, and may in fact enable moving the IAM infrastructure from on-premises into the cloud.
- Be bullish about standards and do not let any vendor (large or small) steer you away from standard protocols and interfaces. We are now in an era of ‘progress, not perfection’, meaning that absolute perfection comes at the expense of interoperability. In other words, you may find yourself painted into a corner by relying too extensively on one vendor’s ‘perfect’ solution. Think big picture and set your organization up for more flexible, governable and scalable identity management functions that will yield benefits now and far into the future.

With these principles in mind, many organizations must rethink their current IAM strategies. The tactical efforts to data a process problems that have proliferated over the past few decades has left many organizations with a hodge-podge of silo’d, poorly or non-interoperable IAM functions that become impossible to govern properly and hinder proper risk management. Doing the same things the same way by just throwing more money at it doesn’t solve the root of the problem, which is the need for a cohesive, well-designed architecture strategy that takes into account flexibility, scalability and cloud readiness. The next section will leave the reader with a summary set of actionable set of priorities and program principles to be considered in “future-proofing” your IAM strategy.

Conclusion

In this report we present TechVision Research’s vision of the future of Identity Management including thought-provoking perspectives from many of the leaders in the industry. To summarize, these are the most salient points to consider as you evolve your IAM program in the context of where TechVision Research sees the industry going:

- The Internet of Things (IoT) will require scalable and reliable infrastructure for establishing identities for these Things. Enabling appropriate access for these identities throughout the connected ecosystem is stretching identity to new limits.
- Big (IAM) data enters the fray as pervasive social media/data brokering and sophisticated predictive analytic engines drive the hunger for and availability of more and better user data.
- Privacy is and always will be a top concern, and identity data requires stringent protection and closely governed usage.
- Cloud computing will continue to gain momentum and cloud-based IAM must be strongly considered as a viable means to store identity information, authenticate

users – both internal and external and provide at a minimum coarse-grained authorization services.

- An improved Dev/Ops model building and deploying IAM in the form of secure microservices will hasten your organization's ability to thoughtfully move your environment to the cloud without the risk of 'forklift IT migration' and its inherent risk to identity data.
- The advent of mobile has major ramifications for both identity management and security. IAM architectures can and should embrace the mobile user (and device) landscape. BYOD, wireless and mobile means identification based on static location (or a corporate device) is no longer an option.
- Artificial Intelligence is beginning to help organizations consume and derive value from big data and drive decision-making through powerful analytics, and more robust context-aware runtime authorization decisions.
- Security and IAM are inextricably linked, with IAM becoming perhaps one of the most important facets of the organization's security program to 'get right.'

Addressing these trends requires considering these IAM architectural and program principles:

- Embrace Identity Abstraction to enable looser coupling, better data protection and a reliance on stable authoritative source identity data.
- Leverage Identity Federation to enable cloud integration, looser coupling and better user current affiliation reliability.
- Plan for Bring Your Own Identity (BYOID) to foster standard identity verification, reduce internal user identity processing and facilitate cloud integration.
- Deploy Privileged Access Management to protect the most important information assets within your organization.
- Establish an Identity and the Internet of Things Architecture Strategy to ensure scalability, reliability and security of the things that are going to be increasingly entering your network.
- Evolve to Relationship and Context-based Identity to better verify identities at run-time and more granularly control access privileges.
- Expect Deprecation of Traditional Enterprise Directory Services and don't stake your long-term future on Active Directory or LDAP.
- Consider Cloud-based IAM in order to simplify your architecture, reduce deployment/maintenance costs and foster quicker adoption of fast-moving standards like OAuth 2.0, OpenID CONNECT, UMA and others.
- Begin to evaluate and leverage new, more disruptive approaches including self-sovereign identity, distributed identity, blockchain-based IAM, verifiable claims and

microservices concepts applied to Identity services.

- Make Identity Management a Linchpin of your security program.
- Scale IAM by avoiding short-term vendor-influenced shortcuts by supporting standards, embracing the cloud, developing a loosely-coupled architecture, provide as-a-service and federating.
- Make Identity a Privacy Enabler by reducing identity data proliferation and abstracting identity data.
- Make Identity a Business Enabler by treating it like (properly protected) big data and implementing delegated access management standards such as UMA, when ready.

There's no magic pixie dust or silver bullet, but these are principles that will assist you in getting ready for the future of identity management, because the future is now.

Industry Expert Perspectives on the Future of Identity Management

We've been fortunate enough to assemble a great team of consulting analysts at TechVision Research. Most of us have been working in Identity and Access Management for decades. A couple of us worked together on the first Lightweight Directory Access Protocol (LDAP) implementation back in 1991, drove early multi-vendor directory pilots in the 1980s and participated in industry efforts to develop standards and solve early directory problems. Several of us have led industry initiatives and built many of the services we describe in our research. Our efforts of late have been in analyzing new identity models such as self-sovereign identity and we have actually helped to develop these concepts, working with our large clients in helping to architect their next generation IAM architecture and continuing to lobby for the products, services, pricing models and integration plans that best serve our end user clients.

That said, predicting the future of any market or technology is an inexact science at best. To sharpen our prognostications, we are leveraging insights from several great technologists and industry leaders. The following section summarizes the results of five interviews with the key leaders in Identity Management. Note that we asked interviewees to limit their vendor-specific comments, but we did allow examples that demonstrate execution of the vision with specific investments being made by their companies. Unlike our first version of this report released a few years ago where we interviewed 12 experts, we are limiting our interviews in this report to a selected group of thought leaders that have specific expertise and insights in areas we believe are critical to the future of Identity Management.

For example, we interviewed Michel Prompt of Radiant Logic given his expertise and insights into integrating, federating, normalizing and virtualizing the growing base of identities to part of any well managed identity service. We interviewed Lasse Andresen from ForgeRock given his insights into scaling identity systems and approach to integrating IoT into IAM. We talked with Nathanael Coffing from Cloudfity to gain his perspective on the increasingly important role microservices and DevOps will play in IAM. We interviewed Phil Windley from the Sovrin Foundation and Brigham Young University to garner his well-founded perspective on blockchain-based IAM, self-sovereign identity, verifiable claims and a new governance model. And we talked with Jackson Shaw from One Identity and got his perspective on the need to continue to recognize and manage hybrid environments (despite all the cloud momentum) for the foreseeable future; as on-premise IAM will be here for a long time.

After each individual summary we've included a few takeaways that represent key points the reader may want to leverage from the interview summaries. In a similar fashion, we'll now summarize some key overall insights garnered from these industry leaders.

We'll now look at the interview summaries from our esteemed industry thought leaders that were kind enough to share their valuable perspectives with TechVision Research

Nathanael Coffing, Cloudfinity

Nathanael is the CEO and Founder of Cloudfinity, a firm building a cloud-native identity platform crafted entirely in microservices that support distributed, multi-cloud and edge based architectures with lifecycle management for users, applications and things.

Nathanael started by making a few observations about the static, monolithic applications and user centric data models that serve as the baseline for Identity and Access Management (IAM) platforms today. He discussed the need for IAM and other security applications to evolve to microservices, identity grids, and entity centric data models.

His believes that the traditional centralized data-center perimeter is dissolving and identity is the core of the evolving distributed perimeter. Nathanael went on to say that identity management systems today are “needlessly complex, brittle and they require substantial administration for which most teams are horrifically understaffed”. He sees a continued acceleration in the shift to cloud-native and cloud-first strategies where many/most of the legacy platforms will be radically transformed, through decomposition into microservices or re-architected to support the API economy and containerization.

At the center of this evolution is the Developer community whom, Nathanael advocates, is often times ignored. Applications are evolving at rates well beyond what traditional approaches to IAM can support. The Developer community will be key to future-state Identity Management systems and services. He added that DevOps and microservices are reshaping application development and they will be equally important in reshaping IAM services as developers push the boundaries by utilizing new technologies like IoT, multi-cloud and edge architectures.

With the current state challenges as a backdrop, Nathanael described a future state Identity microservice model in which Identity platforms and business applications are decomposed into microservices co-located in containers for embedded security. He sees this model extending to cloud-based identity services. Nathanael explained that everything is moving to the cloud and he ultimately sees this extending to service meshes, server-less and function specific computing infrastructures with an embedded identity/security layer to secure the underlying business functions.

He further described the microservices model extension in the identity space as similar to what we are seeing in the application arena; providing a ubiquitous utility that can support any device, at scale, everywhere with low latency and highly secure. Leveraging microservices in an IAM environment is fundamental to achieving the scalability needed for the next generation of identity systems as objects such as IoT devices are brought into the mix, Nathanael added.

He sees these business microservices being protected by micro-API-gateways and container-sidecar via a micro-perimeter that offloads both Identity and high level data security functions to protect East/West transactions—events and communications between API’s, microservices and containers and North/South transactions between edge devices and service meshes.

Nathanael believes this can be a viable self-healing and self-protecting service with minimal administrator intervention. He called it a “bend but don’t break” model based on the usage of circuit breakers, adaptive/intelligent distributed authorization services for Policy Definition, Policy Decision and Policy Enforcement. He added that this creates an integrated security layer designed to protect business functions while liberating developers from the complexities of federation, data queries, user/service/thing management, traffic inspection, authentication and fine-grained authorization.

He sees the next generation of IAM moving towards event-based services creating a light-weight model for data movement and just in time delivery of verified claims. He acknowledged the biggest weakness is the inclusion of a service registry that provides unique identities to applications allowing them to authenticate/authorize each other and maintain the context of external parties (users) consuming these services which must be included in the next generation of IAM systems.

Key takeaways from Nathanael include:

- Identity Management will be moving to a utility-type model.
- IAM systems must follow applications in moving to a stateless, cloud-native microservices model leveraging containers.
- Developers require a frictionless development experience and offloading the complexities of IAM, API inspection and validated data access away from the business functions.
- Business Microservices will be protected by micro-gateways and micro-perimeters that provide the core IAM functionalities and API inspection capabilities allowing security teams to approve and contribute to new functionalities faster within SecDevOps processes.
- IAM will be responsible for managing and maintaining identities, authentication, and authorization for all entities; Users, Microservices, API’s, Devices and Things.

Lasse Andresen, ForgeRock

Lasse Andresen is the CTO, Founder and Board member at ForgeRock, former CTO at Sun in central/northern Europe and founder/CTO at GravityRock. He is a thought leader in Identity Management and has helped build several companies that execute on his vision.

Lasse started with an observation that companies are starting to understand the value of identity—not just user name and password—they know their customers, know the devices that are attached to their customers and, in turn, leverage this to generate new revenue opportunities, connecting users with devices with applications and the only way to do that is identity.

He described Identity Management as the “holy grail that brings everything together and there is huge money to be made combining these things...not just scale, but need to be extremely context aware, and support for hyper-personalization for a customer”.

He added when discussing context awareness that “role-based access control is a dream that never worked”, so customers are looking for relationship-based access control at scale supporting run-time decisions.

Lasse then turned the discussion to IoT and how important Identity is for IoT be successfully and securely deployed. He described a challenge with IoT systems in that they have largely built their own silos; first it was all about connectivity and now they are trying to figure out security and updates; for example “how do you keep IoT firmware updated. IoT platforms need to step up and not only do the first mile but figure out how they are connected to business process users and the revenue stream.

In the Identity space he described the increasingly important concept of distributed architectures; explaining that there are pros and cons of storing everything in the cloud—and everything will not and should not move to the cloud. He cited an example in the car industry in that they design off-line first and that identity and access decisions will actually be made in the car. Policy Decision Points (PDPs) will move out to the edge he believes and the industry will no longer be limited to only centralized identity systems.

Lasse also sees a rise of Machine Learning (ML) and Artificial Intelligence (AI) as supporting smarter ways of making and executing real-time decisions. He sees an environment with learning, policy servers built, in part, by ML. This will hit the identity space in a big time way per Lasse.

Lasse sees this supported by distributed policy engines with distributed policy enforcement points and support for distributed Identity systems in general. These distributed policy engines will make authorization decisions at the edge devices which will also support the increasing proliferation of external (BYOI) identities that will need to be included.

He sees the future of Identity Management supported by three key trends that he recommends customers invest in. They are:

- Relationship-based architecture

- Machine Learning and Artificial Intelligence
- Distributed identity architectures

Jackson Shaw, One Identity

Jackson Shaw is the VP of Product Management at One Identity and a long-time Identity Management thought leader and visionary. Jackson has been driving identity programs at Microsoft, Quest/Dell/One Identity, Zoomit and others for the past 25 years.

Jackson started by talking about the pendulum shifting from a traditional enterprise on-premise focus to a pervasive movement to the cloud. That said, he explained that the cloud transition will take years or decades to fully happen and, in the interim, most enterprises will have to deal with a largely hybrid environment.

He explained that this largely hybrid environment presents a huge set of problems/challenges that should be a key area of enterprise focus. For example, managing hybrid identity and hybrid security is exponentially more difficult than managing traditional identity systems. He added that the minute an application and its associated identities are moved to the cloud everything is an order of magnitude more difficult. This applies to enterprises and also to vendors that are trying to manage this largely hybrid world as Jackson is with One Identity.

Jackson believes that the future of IAM must include a fundamentally better way of managing personal identities. He explained that there isn't a day that goes by when he doesn't have a password that needs to be reset and he thinks that this is the norm. He described this as a major problem that needs to be solved over the next several years but isn't sure exactly how it will be addressed; perhaps FIDO can play a role he added.

Jackson also explained in the context of stronger authentication the tide has changed with respect to biometrics; He contends that Apple has played a major role in making fingerprints an acceptable form of authentication. He also sees the FIDO alliance and others standardizing mechanisms for authenticating and being increasingly open to sharing this information. He sees facial recognition and other forms of biometrics being leveraged in supporting PAM as well.

He sees another major shift in the area of identity analytics; with Machine Learning playing a key role going forward. He sees early examples Amazon's and Microsoft's implementation of identity analytics.

In terms of some of the more disruptive trends such as microservices and blockchain he is more impressed with the value behind the microservices concept and sees microservices as playing a role in solving the hybrid problem he described earlier. With respect to blockchain Jackson stated that there is little going on around the use of blockchain-based identity solutions in scenarios related to enterprise IAM. That said, he believes there is a lot of potential outside of the enterprise. He added that "one of the fundamental problems that blockchain solves is providing trust where there is no trust, and in the enterprise, that is a given, generally".

Jackson believes that most vendors and end-users need to resign themselves to being a relying party and taking attributes from others. He added that, for example, firms Microsoft, Amazon, Facebook and Google are in the position to be identity providers, but

most vendors and end-users don't have the ability and governance models to be identity providers. So he believes that other vendors and end-users need to be pragmatic and simply accept vetted identities from the few select identity providers that are properly positioned to do so.

In summary, key takeaways from Jackson Shaw include:

- Managing hybrid identity systems and services should be critical areas of focus for the next decade
- Most organizations need to give up on the dream of being identity providers
- He sees microservices as increasingly important in IAM, but blockchain as being more of a solution looking for a problem

Michel Prompt, Radiant Logic

Michel Prompt is the CEO and Chairman of Radiant Logic, a company he founded in 1996. He is also a long-time thought leader in identity and access management, virtual directories and contextual identity services. TechVision first interviewed Michel two years ago in support of our first Future of Identity Management report.

Michel started by validating and expanding upon prognostications he made in our initial report. First he explained the trend towards tighter integration of identity management and security is even more critical. Michel added that the threats are accelerating and they are being better addressed by leveraging context-based identity management and semantic data. He described contextual awareness and strong integration as “foundational elements” in thwarting identity-related breaches. Another accelerating trend is increased scalability for an increasingly diverse set identity services. Identity services need to be always available to users and applications across heterogeneous environments.

Michel believes that identity management will, and should be, right in the center of the Internet universe and is, perhaps, the most critical component driving successful digital transformation programs. He also explained that the infrastructure in support of this Internet universe is moving to the cloud and there is a need for “establishing, securing and migrating to the cloud and IAM providers must be responsive to this need”. There is a need to synchronize identity information to the cloud and to provide secure access to applications and services living in the cloud and identity services must support both he explained.

Michel then added that areas such as IoT are creating new challenges for IAM. For example self-driving and connected cars create a complex set of relationships and objects to be identified. This creates IAM challenges in terms of scaling, but also creates an opportunity to leverage new categories of contextual data in support of digital transformation programs.

TechVision then asked about identity-centric roadblocks limiting enterprise business transformation programs and Michel explained that the opportunities associated with digital transformation are based on providing a single version of the truth, but that is often easier said than done. He used group management and administration as an example of a particularly difficult area to integrate and normalize. Michel suggests that organizations will often need to reverse engineer and audit existing groups and, based on the results, develop a new group foundation that is internally and externally aligned.

Michel also talked about real-time access to identity data across increasingly complex environments in light of need for enterprises to provide just-in-time provisioning services. This will involve new microservices-based approaches to IAM and integration with environments such as Microsoft’s Active Directory/ADFS and cloud platforms such as Okta.

Michel summarized by describing a future state that will be increasingly complex, but will need to be properly integrated and managed to mask that complexity.

In summary, key takeaways from Michel Prompt include:

- Managing context-based identity and semantic data identity are critical elements in the future of identity services
- The emergence of Amazon and Microsoft cloud platforms requires IAM integration and support for these environments
- Reverse engineering groups is often overlooked and is a key to integration
- Identity systems most fully support just-in-time provisioning
- Future scalability requirements will drive a movement to graph databases

Phil Windley, Sovrin Foundation and Brigham Young University

Phil Windley is a long-time thought leader in Identity Management; he is currently an Enterprise Architect in the Office of the CIO at Brigham Young University, chair of the Sovrin Foundation, co-founder and organizer of the Internet Identity Workshop, serves as an Adjunct Professor of Computer Science at BYU and widely published technology author.

Phil started the discussion with an observation that he had started the Internet Identity Workshop (IIW) with Doc Searls and Kaliya Young thirteen years ago to provide a forum for the development of user centric identity. He felt that despite the community efforts over the years, that this is the first time we are seeing people in the “center” of transactions.

Phil made the observation that most physical world identity transactions are self-sovereign. He explained that physical transactions put people in the center using decentralized credentials (ID, credit card) to transfer trustworthy attributes about the identity owner. The naturally support scalable, flexible, private interactions that take place with the identity owner's consent. He explained that the Internet introduced the proximity problem (proving you are you) and this is the problem the industry has been trying to solve

TechVision asked Phil what has changed over the last few years that makes him believe that user centric identity is finally viable and he said “Blockchain”. He then explained that one of the biggest challenges for an Identity Management system is efficiently looking up identifiers; and in the past this has been controlled by a centralized directory or federator. He added that with blockchain, we can “get rid of the centralized directory and that changes everything”. He believes that this provides a degree of freedom, flexibility and autonomy that does not exist with a centralized identity system in the “middle” of every transaction or query.

He described this new model of blockchain-based Distributed Identifiers (DIDs) as providing a method as part of the identifier itself as (contained as part of the methods name) that tells what blockchain to look up. He added that now you know where to look it up (which blockchain), how to look it up, and what to expect back without requiring a central directory. He explained that once the requestor gets the identifier, he also gets the associated public key and the end points that the requestor can talk with. Phil stated that this is perfect for IoT.

He described the problem with IoT as being that they are in silos today for every IoT device they want to register. Phil explained that it is too hard to manage IoT devices and, of course, Amazon has a solution that everything comes through Amazon—certainly what they have and they have pretty good device shadow model. He wouldn't discount Amazon by providing the underlying consistent infrastructure but the other alternative is to is a blockchain-based distributed system via something like the Sovrin Foundation.

He believes the primary use case for blockchain ID use case for banks is Know Your Customer (KYC) and he believes that is a huge area for banks. Another problem is the call center Identity problem...so they ask you a bunch of questions that anyone can answer if you have access to Equifax data and as Phil said, of course now you do.

In summary, key takeaways from Phil Windley include:

- Blockchain changes everything when it comes to support for user-centric identity and will be a core part of the Identity ecosystem within the next five years
- The management of IoT identities will be enhanced by decentralized identity systems or everyone will come through Amazon
- Early distributed Identity use cases in banking include KYC and call-center identification
- DIDs provide security as scale without requiring a central directory

About TechVision

World-class research requires world-class consulting analysts and our team is just that. Gaining value from research also means having access to research. All TechVision Research licenses are enterprise licenses; this means everyone that needs access to content can have access to content. We know major technology initiatives involve many different skill sets across an organization and limiting content to a few can compromise the effectiveness of the team and the success of the initiative. Our research leverages our team's in-depth knowledge as well as their real world consulting experience. We combine great analyst skills with real world client experiences to provide a deep and balanced perspective.

TechVision Consulting builds off our research with specific projects to help organizations better understand, architect, select, build, and deploy infrastructure technologies. Our well-rounded experience and strong analytical skills help us separate the "hype" from the reality. This provides organizations with a deeper understanding of the full scope of vendor capabilities, product life cycles, and a basis for making more informed decisions. We also support vendors in areas such as product and strategy reviews and assessments, requirement analysis, target market assessment, technology trend analysis, go-to-market plan assessment, and gap analysis.

TechVision Updates will provide regular updates on the latest developments with respect to the issues addressed in this report.

About the Authors



Gary Rowe is a seasoned technology analyst, consultant, advisor, executive and entrepreneur. Mr. Rowe helped architect, build and sell two companies and has been on the forefront the standardization and business application of core infrastructure technologies over the past 35 years. He was President of Burton Group from 1999 to 2010, the leading technology infrastructure research and consulting firm through the sale of Burton to Gartner.

Mr. Rowe has personally led over 100 consulting engagements, 50+ educational seminars, published over 50 research reports/articles and led three significant technology industry initiatives. His combination of business skills and his deep understanding of technology provide a balanced perspective for clients. Core areas of focus include identity and access management, directory integration, cloud computing, security/risk management, digital transformation, IT business model changes, privacy and blockchain/distributed ledger."



Nick Nikols has more than 25 years of experience in the software industry, architecting solutions and developing innovative products for identity, security and compliance management, as well as directory services and directory/application integration.

Before working with TechVision Research, Nick was Senior Vice President of Product Management and CTO of Cybersecurity at CA Technologies, where he was responsible for CA's Cybersecurity Product Strategy and Roadmap. At CA, he was particularly focused on modernizing CA's Identity-centric Security portfolio and successfully promoted CA's Identity Manager and Access Governance solution into a leadership position within Gartner's Magic Quadrant for Identity Governance and Administration.



Doug Simmons brings more than 25 years of experience in IT security, risk management and identity and access management (IAM). He focuses on IT security, risk management and IAM. Doug holds a double major in Computer Science and Business Administration.

While leading consulting at Burton Group for ten years and security, and identity management consulting at Gartner for five years, Doug has performed hundreds of engagements for large enterprise clients in multiple vertical industries including financial services, health care, higher education, federal and state government, manufacturing, aerospace, energy, utilities and critical infrastructure.

Related Reports

The following reports might be helpful in your continued exploration of this domain:

[How Microservices Can Improve Your IAM Strategy](#)

Authors: Doug Simmons – Managing Director, Consulting /
Principal Consulting Analyst,
Nick Nikols – Managing Director, Research / Principal Consulting Analyst,
Gary Rowe – CEO/ Principal Consulting Analyst,

[Identity is the New Perimeter](#)

Authors: Doug Simmons – Managing Director, Consulting /
Principal Consulting Analyst,
Nick Nikols – Managing Director, Research / Principal Consulting Analyst,
Gary Rowe – CEO/ Principal Consulting Analyst,
Gary Zimmerman – CMO / Principal Consulting Analyst

[Cloud-based Identity Management](#)

Authors: Nick Nikols – Managing Director, Research / Principal Consulting Analyst,
Gary Rowe – CEO/ Principal Consulting Analyst

[Banking on Identity](#)

Authors: David Goodman, D. Phil - Principal Consulting Analyst
Rhomaïos Ram - Principal Consulting Analyst

[Getting to Know Your Customers: The Emergence of CIAM](#)

Authors: David Goodman - D. Phil, Principal Consulting Analyst

[Blockchain-based Identity Management](#)

Authors: Doug Simmons – Managing Director, Consulting /
Principal Consulting Analyst
Gary Rowe – CEO, Principal Consulting Analyst

[Context-based Identity Management](#)

Authors: David Goodman, D. Phil - Principal Consulting Analyst

[Enterprise Privacy Guidelines in a Changing Regulatory Environment](#)

Authors: Jill Phillips - Principal Consulting Analyst