The nexus of forces (cloud, mobile, information, and social) is driving complex shifts in identity and access management. In this article the author describes a set of five key predictions for the future of identity and access management, setting a horizon date of the year 2020.

By Ray Wagner

Why this prediction will be true
- Cloud service adoption growing
- Some IAM functions commoditizing
- Social media and BYOD are propelling consumer-grade identities
- Providers excelling in consumer-centric IAM are entering the market

Why this prediction might be false
- Legacy architectures cannot be replaced this quickly
- Vendors find ways to add new valuable features and differentiate
- Consumer-centric IAM vendors avoid getting into market for advanced identity governance and administration functions

Every user is a consumer
By year-end 2020, the majority of user access will be shaped by new mobile and non-PC architectures that service all identity types regardless of origin.

As much as globalization makes a country’s borders more open, adoption by the enterprise of cloud and other external services opens the “identity border” of enterprises and demands simpler, more consumer-oriented approaches for access. Commoditization of some identity functions coupled
with the explosion of available applications is driving complexity and pushing enterprises to seek more scalable options for identity. At the same time, embracing social media, mobile technologies, and bring your own device (BYOD) practices within the enterprise in support of collaboration and consumer access is leading to a convergence in the management and use of all identities for simplicity and business effectiveness.

As a result of these changes, providers excelling in consumer-centric IAM will enter the market to replace current enterprise IAM vendors. Current enterprise IAM vendors will need to adapt or disappear as a sea change in IAM consulting and integration services expands the availability of guidance for consumer-style architecture, design, and implementation.

Scalability, deployability, and mobility needs are driving a redesign of most enterprise IAM offerings to keep pace with enterprise changes. Enterprises will be able to view and manage all users (enterprise or consumer) as they view consumers today, resulting in simpler and faster IAM deployment. Social media and IAM firms specializing in mobile devices and applications will collaborate to produce simple and easy-to-use authentication, provisioning, and access governance functions on different device platforms. Microsoft’s Active Directory will continue to play a role in some mobile and application needs but will not drive future consumer-centric IAM architecture.

**A competitive marketplace for identities**

By 2020, most digital identities interacting with enterprises will come from external identity providers through a competitive marketplace.

The use of externally provided identities to access applications serving enterprise consumers has already begun. Social identities are being used in a number of applications with notable examples in retail, banking, and media through ubiquitous use of GoogleID, Facebook identity, Paypal ID, etc., across industries. Consumers use these identities for convenience, and enterprises support this for business advantage. Identity provider services are used to support several industry consortia, for example, healthcare, automotive, oil and gas, and aerospace and defense, while several national governments use third-party identity provider services to support national ID initiatives or citizen e-service access such as SecureKey Concierge, Canada; Identity Assurance Programme, UK; and BankID, Norway.

There is already a competitive marketplace for a portion of the identity ecosystem: identity proofing and fraud prevention services. Credit bureaus, governments, financial institutions, telcos, fraud prevention vendors, and other service providers leverage a variety of data sources and network relationships to provide identity assurance services to relying organizations. These services help provide risk scores for a sets of attributes and help enterprises gauge confidence in asserted identities.

---

**WHY THIS PREDICTION WILL BE TRUE**

- Social ID use increasing
- Established government third-party ID initiatives
- Adaptive access and mobile devices improve assurance

**WHY THIS PREDICTION MIGHT BE FALSE**

- Lack of equitable business models
- Adaptive access administration practices improve
- Users and enterprises do not trust third-party identities

---

This commercial identity marketplace combined with digital identity providers already used by consumers will grow in scope and in number of providers. Identity verification, registration, authentication, and attribute services will be disparate, complementary parts in an overall digital identity marketplace and infrastructure. However, to date, no identity proofing or authentication system has proven to be infallible. Even as a marketplace grows for identity providers, each provider will have inherent limits with regard to the level of trust in identities, attributes, and contextual or environment data they can assert to support a vast array of potential use cases. Therefore, a combination of externalized identity provisioning, on-hand data, contextual data, and adaptive processes for registration and access will need to be used to help enterprise-relying parties to defend themselves.

Disparities among industries and jurisdictions with regard to legal, regulatory, privacy concerns, and other factors will lead to identity marketplace synergies based on communities of interest. Individuals will not have one ID. They will have several, but fewer than today, which can be leveraged for interactions and transactions within communities that share common requirements.

The death of least privilege

By 2020, most enterprises will allow unrestricted access to non-critical assets, up from less than five percent today, reducing spending on IAM by 25 percent.

Why this prediction will be true

- Least privilege is inefficient
- Least privilege actually creates security gaps
- Analytics can help fill gaps
- End of least privilege – rise of people-centric security

Why this prediction might be false

- Auditors prevail
- Low priority
- Attempts at undoing current complexity lead to more security gaps

Least privilege is a generally accepted security principle granting users only the access that they need to do their work. The principle of least privilege is fundamentally ill-suited to commercial organizations and a costly security control. Like many established security principles, least privilege originated in government and military information security. Asking an enterprise to embrace the same principle obliges it to manage access with high granularity so that all users have only what they need to do their work and nothing more. This approach encumbers enterprises with convoluted change management processes and high administrative overheads despite investment in automation tools. This will be exacerbated as enterprises make use of mobile and cloud computing in the coming years.

Relaxing the principle of least privilege and giving “all” users unrestricted access to each non-sensitive, non-critical applications and data they need will greatly simplify things, enabling enterprises to focus on managing the access that matters more efficiently and effectively. This is a graceful compromise that has the enterprise accept lower-level risks to enable it to attend more rigorously to higher-level risks.

The second key reason for relaxing least privilege approaches is the projected rise of people-centric security (PCS). PCS enables enterprises to reduce overall risk while simultaneously reducing the number of preventative controls that impede user discretion and creativity. PCS maximizes agility and the level of transparency regarding users’ information access and behavior. PCS implies that enterprises must implement detective and corrective controls that enable granular monitoring of user activity in order to identify and appropriately respond to anomalous or abnormal user behaviors. Improved, context-based integration of monitoring technologies and after-the-fact analytics will be fundamental in a PCS environment.

While PCS will likely involve non-automated (human) monitoring by individuals as part of their responsibilities, improvements over the next six years in the power and sophistication of identity analytics and intelligence (IAI) tools and security intelligence toolsets will be a key enabler of PCS. With proactive use of these tools, enterprises will be able to mature from the principle of least privilege while simultaneously reducing overall risk.

Attributes are “how we role”

By 2020, the majority of enterprises will use attribute-based access control (ABAC) as the dominant mechanism to protect critical assets, up from less than five percent today.

Why this prediction will be true

- Attributes and context required for access control
- Role-based access control is too limited
- Legacy applications do not understand context
- Good identity governance requires attention to attributes
- Application vendors will start to get it!

Why this prediction might be false

- Lack of needed identity governance maturity
- Application developer culture
- Legacy applications live on
- Access control vendors don’t make this easy
The nexus of forces will have a profound impact on how users interact with and within an enterprise. The number of devices and applications that are used to process the same data will increase. Social media will bring more users from more places. Big data will generate more information about users. As the number of possible interactions between users, devices, services, data, and the external environment increases, so does the volume of contextual information used to describe the interactions through a set of attributes.

Protecting data will become a multi-dimensional exercise. Traditional role-based access control (RBAC) is one-dimensional because it cannot take context in the equation and will therefore fail to address the challenges. The problem is that most systems today control access through one piece of information—usually as a role. They are thus ill-prepared to address the challenges that come with the opportunities offered by the nexus of forces, because they are unprepared to take the contextual information into account when making access decisions.

ABAC will replace RBAC. Roles will be just another one of the attributes that form the context, and rules will make decisions based on the context. Attributes will become the new currency of access control.

Systems will increasingly support ABAC. This trend is evidenced by examples in popular software vendors’ product strategies: Dynamic access control within Microsoft Server 2012, the claims-based architecture in Windows Identity Foundation, and Oracle’s Fusion middleware. Systems that support at most RBAC will become legacy and—if they hold critical data that needs to be protected and used within the nexus of forces at the same time—will be increasingly difficult to support.

Software development methodologies must evolve to embrace best practices around ABAC. This enables developers to externalize authorization completely or at least better handle and simplify the access to contextual attributes when authorization is still hardcoded. The need for external attribute providers will grow as part of the competitive market for identities. Some identity-proofing companies already provide risk scores to relying parties as of today, and this practice is expected to grow in volume and significance and extend to an external marketplace for identities.

Managing identity includes the Internet of Things

By 2020, the Internet of Things will redefine the concept of identity management to include what people own, share, and use.

**WHY THIS PREDICTION WILL BE TRUE**
- Things must be identified and their access managed
- Things contribute context to human access decisions
- Things will be a unifying identifier

**WHY THIS PREDICTION MIGHT BE FALSE**
- Things lack IAM interfaces and smarts
- Existing IAM cannot manage things
- We may think the Internet of Things and identity have more in common than they do

The Internet of Things (IoT) links people, places, things, systems, and information sources into activity streams, deriving value for those interactions and relationships by using the context of combined “identities” (people, devices, and other “objects”), their attributes, and uses. This effect is not con-
fined to the traditional Internet but is also true of private networked systems as well.

Everything in the IoT has an identifier, attributes describing that identity, and experiences involving that identity. As more combinations of people and objects interact with the environment and one another, the identity gains and loses attributes to describe the current state of “people identities” based on their activities. These attributes and relationships provide context to aid in, for example, access decisions to information or the ability to use objects or services.

IoT identifiers and relationships will be the unifying element of people, places, things, and information, providing a platform for “entity interaction management” and a means to develop and deliver infrastructure, services, and applications in combinations that create new lines of business and ensure the appropriate access to business services.

Conclusion

As the definition of IAM evolves, tools and services for IAM will evolve to include capabilities in mobile devices, application and information management, asset management, and service management, consolidating some markets and modifying others. Massive changes in IAM scale and performance will occur to deal with the global scale of the Internet of everything (IoE) and the billions of new “identities,” resulting in changes to providers of identity and mechanisms for securing identities and an expansion in analytics and intelligence to accommodate expanded services.

For enterprises with increasingly intelligent devices and other endpoints (such as sensors, electronic tags, process and distributed control) a revision in strategy, architecture, and operations for IAM to accommodate new activity streams and relationships will be required.

Fear, uncertainty and doubt have limited value. Remember, you do not control the threat, but you do control your organization’s readiness, so that is the place to focus attention.

About the Author

This article is based on research by the Gartner for IT Leaders IAM research team, including Ant Allan, Gregg Kreizman, Felix Gaehtgens, Earl Perkins, Ray Wagner, and Neil Wynne.

Ray Wagner, PhD, is Managing Vice President of the Secure Business Enablement group, which is part of the Information Security and Privacy research organization of Gartner Research. Dr. Wagner focuses on a wide range of security issues, including identity and access management, web services security, public-key infrastructures, digital rights management, the information security organization, and information security issues within emerging technologies. He may be reached at ray.wagner@gartner.com.

The Curmudgeon

IDENTITY MANAGEMENT: now there’s a service I could use. I have so many identities, it’s getting hard to keep track of them. Says the patient: “Doctor: If you were absolutely sane, but imprisoned in an insane asylum, how would you prove that you were sane?”

What, exactly, is an “identity”? Is it the “online activities” we do? The “public identities” we leave as trails in our bills, finances, subscriptions, cell phones, travels, credit card records, daily habits, and interpersonal communications? Is it “us” at work? “Us” at home? “Us” at the Boy/Girl Scouts or church? The wonderful thing about our unique identity is: there are so many of them! And they converge and can be tracked.

May I tag you with something the NSA would dream up? It has a GPS tracker, accelerometers, four RF interfaces, two cameras, and a microphone. It can record your surroundings, captures everything you do, what you say, where you go, what you purchase or “show-room.” Would you carry that thing voluntarily?!

Yup! It’s called a “smartphone”!

That thing you use to control your automated home: garage door, door locks, thermostats, calendar, appointments, quick-codes for aircraft tickets? Who and what you communicate with (phone, text, email, web, Bluetooth). That shows the last several access points you used? It spews your IP, MAC, physical location, EIS and lots more. “They” want to “lock” these devices using biometrics. Look up Chaos Computer Club and how it defeated fingerprints, iris scans, and the requirement for a “live” presence for both.

Do you really think you are secret, unknown, untraceable? That no one knows your IP, MAC, which access points you use, what you work on, what you do? The USA just issued indictments against five people who never left their country for malicious hacking on a national scale.

Your Mom needs to know where you really were last night! Do you want your current main squeeze to know you were shopping in a certain lingerie store (but you didn’t deliver to him or her)? Your future squeeze to know you got treated at the community STD clinic? Your employer to know your “sick day” included a fishing trip (complete with GPS coords and images of the near-trophy catch you wished you had caught)? Your (current) employer to know about your lunch with your (future) employer? Your participation in the 2000 person drunken party in this certain “mansion” that caused $70k in damage? Your car to report your daily driving habits, including speed, location, speed limits, and any “modifications” to the hardware to your insurance company? Or the rental company (so they can charge you more)?

Do you really trust your ID to <cough>Target</cough> or any other major retailer <hack>TJX</hack>? Eeww. Hairball! Run the math: “They” value ten years (10 YEARS) of your life at about USD$0.70. Without inflation. I mean, really, would you work for 10 years, for $0.70? Total? Just so you could go back to work?

You really ought to talk to my cube mate.

Your local, grumpy, tie-wearing, un-impressed and suspicious Curmudgeon