G00313643

2017 Planning Guide for Identity and Access Management

Published: 13 October 2016

Analyst(s): Mark Diodati, Homan Farahmand, Paul Rabinovich, Lori Robinson, Mary Ruddy, Erik Wahlstrom

The shifting of users, applications and management to the cloud, and the acceleration of IT innovation, has forever altered the IAM landscape. In 2017, technical professionals must focus on IAM initiatives that deliver rapid time to value but avoid "technical debt."

Key Findings

- Identity and access management (IAM) initiatives have traditionally required multiyear implementations before delivering full organizational value. But in the digital age, lengthy IAM deployments are unacceptable. In 2017, organizations will deploy agile IAM technologies that deliver business value within 12 months or less.
- While organizations should focus on time to value in 2017, they should begin initial assessments to exploit the value of emerging technologies, such as blockchain and the Internet of Things (IoT).

Recommendations

- **Create** scalable Office 365 IAM practices, including on-premises preparation, user management, license management and authentication management. If done correctly, your organization will be successful with Office 365 and future initiatives like infrastructure as a service (IaaS), enterprise mobility management and SaaS single sign-on (SSO) — while reducing costs and improving security.
- **Leverage** IaaS virtualized Active Directory (AD) services for "lift-and-shift" application migrations, instead of deploying AD domain controllers into virtual machines. Test your applications in advance because the services are nascent and application incompatibilities may exist.
- **Adopt or migrate** to mobile push authentication. Compared to second-generation authentication methods like one-time password devices and SMS, mobile push authentication delivers significant cost reduction while improving usability and security — and offers faster time to value.

- **Incorporate** identity analytics capabilities into both admin-time (identity governance and administration [IGA]) and runtime (multifactor authentication [MFA] and SSO) IAM. They are here to stay due to their ability to reduce administrative workload and security risk while improving the end-user experience.

Table of Contents

List of Tables

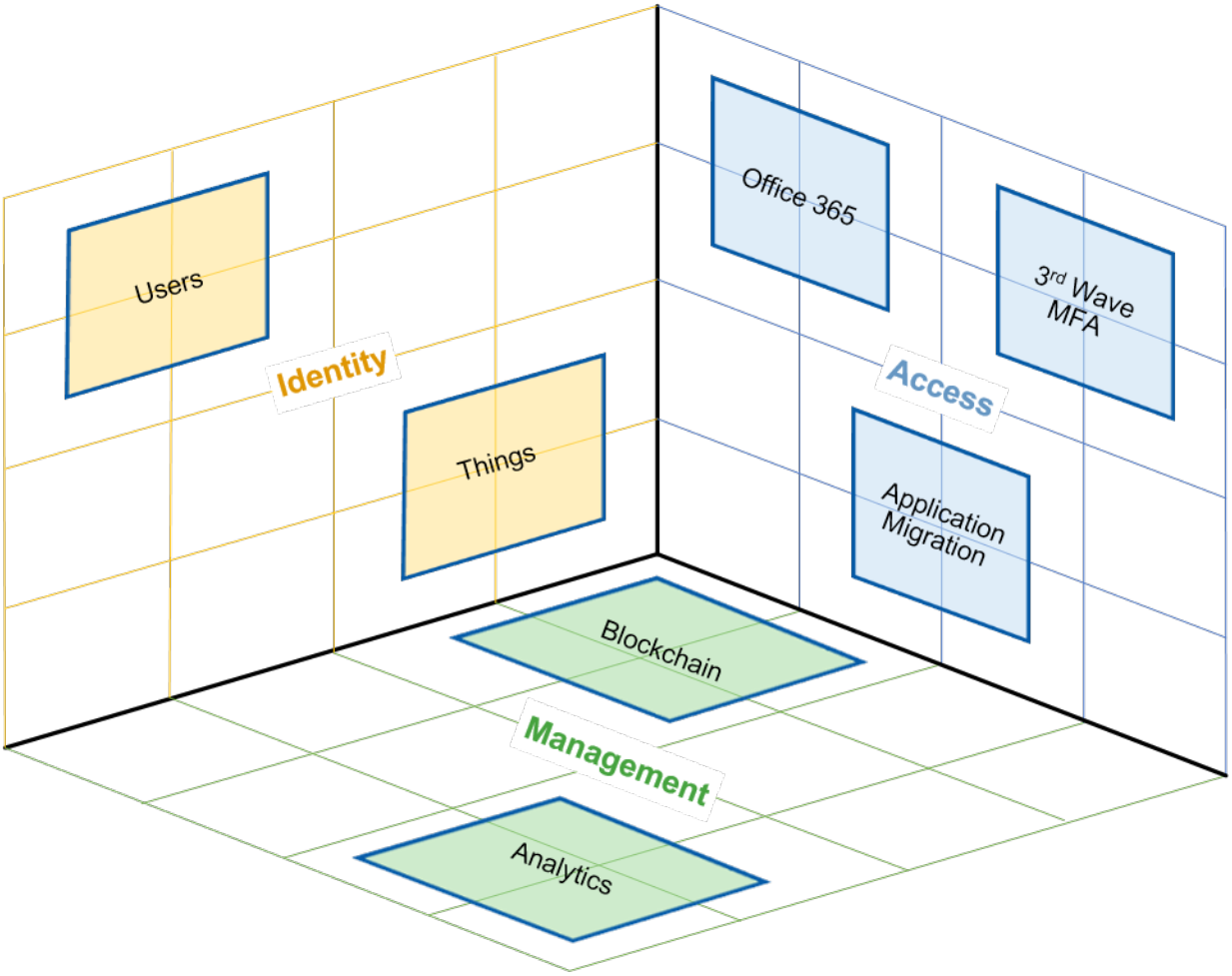
List of Figures

Identity and Access Management Trends

Two trends have forever altered the calculus of success for identity IAM: the shifting of users, applications and management to the cloud, and the acceleration of digital business innovation.

Unfortunately, IAM initiatives have traditionally required multiyear implementations before delivering full organizational value, and the value of IAM has always proven difficult to articulate to executives and the lines of business. Finally, the economics of modern IT are at odds with multiyear initiatives; the mantra of "rapid time to value" means that acceptable time-to-value expectations rarely exceed 18 months. But 2017 may be the year that IAM delivers faster time to value — provided that the organization bets on the right IAM initiatives. Figure 1 illustrates the IAM technical planning trends and associated initiatives discussed in this document.

Figure 1. 2017 Identity and Access Management Trends



Source: Gartner (October 2016)

However, selecting the right initiatives will not be enough to ensure success. Organizations must avoid the enterprise equivalent of technical debt, where corners are cut to shorten execution. Technical debt will need to be paid off in future years at the expense of other organizational objectives. Table 1 summarizes IAM initiatives that provide the opportunity to provide rapid time to value in 2017, along with associated technical debt risk.

Table 1. IAM Initiatives With 2017 ROI Opportunities

Technical Planning Trend	IAM Initiative	Technical Debt Risk
Office 365 IAM	Seamless extension of enterprise IAM to support Azure Office 365. Initiative requires four successful milestones: on-premises IAM preparation, basic user management, license management and authentication management.	Organizations should carefully balance future Active Directory forest consolidations against faster Office 365 adoption. The Microsoft stack will support duplicate identities from different forests, but forest consolidation becomes more challenging after moving to Azure.
Rise of Third-Wave MFA	Migration from second-generation authentication systems (for example, one-time password device systems) to mobile push authentication can deliver a 70% reduction in total cost of ownership (TCO) in a short time frame, while improving security, usability and platform support.	Organizations should take care to implement adequate identity proofing to protect their authentication investment. If not, it may cost up to 10 times the initial deployment cost to fix it.
IaaS Identity Services for Application Migration	Organizations can reduce software, hardware and administrative costs with a "lift-and-shift" approach for application migration to IaaS. Both AWS and Azure have recently added virtualized Active Directory services to support the applications.	The "lift-and-shift" approach requires minimal application changes compared to application refactoring. But organizations should test important applications on both AWS and Azure because there are application incompatibilities with both flavors of virtualized Active Directory services.

AWS = Amazon Web Services

Source: Gartner (October 2016)

Some IAM initiatives require proactivity to reduce organizational risk and have the opportunity to deliver time to value in the 18-month time frame (Table 2).

Table 2. IAM Initiatives With 18-Month Time to Value

Technical Planning Trend	IAM Initiative	Technical Debt Risk
Identity of Things	IAM architect participation in organization's IoT center of excellence.	Organizations should ensure that things have adequate authentication credentials as part of the initial deployment "in the wild." Expensive, high-touch resetting of device credentials can be avoided.
Inevitability of Identity Analytics	The adoption of identity analytics for both "admin-time" (that is, identity governance and administration) and runtime (authentication and single sign-on) will reduce organizational risk and administrative efforts, while improving user experience (UX).	Insufficient evaluation of IGA, SSO and authentication products — both current features and product roadmaps. Products without analytics capabilities will place additional administrative burden and may result in undiscovered security risks.

Source: Gartner (October 2016)

Office 365 Continues to Disrupt Enterprise IAM

Office 365 continues to be a major disrupter for IT departments worldwide. Seventy-eight percent of Gartner clients have either implemented Office 365 or plan to implement it in the near future.[1] The most popular Office 365 services are Exchange Online, OneDrive for Business, SharePoint Online and productivity applications (Office 365 ProPlus), in that order. The benefits are compelling, from significant cost and technical resource reduction to enhanced usability and security.

But adoption of Office 365 is disruptive to IAM because it shifts applications into a hosted environment — and, as a result, puts the organization in the hybrid identity game. In a recent Gartner survey, 20% of respondents cited identity integration with Office 365 as one of the top-three technical problems they encountered.[2] Identity integration with Office 365 necessitates planning and execution in four key areas:

- On-premises preparation
- User management
- License management
- Authentication management

Planning Considerations

Office 365 applications require the care and feeding of a new identity subsystem — Azure AD. Start Office 365 planning early. One of the most pervasive reasons for Office 365 implementation problems is lack of planning and coordination between the IAM team and the IT and cloud teams responsible for delivery. Organizations should plan early and make sure IAM architects are involved in the project from the start.

Your ability to meet the business' needs for Office 365 at scale requires the following four processes:

- **Active Directory preparation.** Ensure that each user's email address and logon name are the same. It is possible to adopt Office 365 without doing it, but you will likely need to hire more help desk personnel to assist users in negotiating Azure-based logon screens, for both web and native applications. Use IdFix and home-built PowerShell cmdlets to identify and correct user attribute anomalies. Finally, if you have multiple forests, consider the normalization of duplicate user accounts across the forest. For the most part, Azure AD and Azure AD Connect will survive with duplicate accounts, but you will find that future forest consolidation projects become more painful in a post-Azure AD world.
- **User management.** Most organizations opt to use the Azure AD Connect directory sync tool to enable management of Azure AD users from the on-premises world, regardless of how users are authenticated (e.g., passwords, Security Assertion Markup Language [SAML] or Azure MFA). If a strategic IGA system exists, it can be used to provision users to AD, then let AD Connect finish the job of managing the users in Azure AD.
- **License management.** Most organizations have yet to recognize the value of IAM in managing Office 365, Microsoft Enterprise Mobility + Security, and other Azure-based licenses. At scale, licenses are particularly expensive, and timely license management can provide significant cost savings. Additionally, poor license management results in excessive access because unnecessary service plans can be enabled by default within the license. Currently, there are no native Microsoft tools for Azure AD license management. Create (or borrow) PowerShell sync scripts that can update user licensing based upon user attributes or group membership. PowerShell has quickly emerged as the workhorse for managing Azure at scale, and license management is no exception. PowerShell can be combined with Azure Automation to provide complete in-the-cloud license management.
- **Authentication.** MFA for Office 365 remains a hot topic for Gartner clients because they are concerned about password (credential) theft. If you choose to implement MFA, there are several approaches. You can use Azure MFA if your needs are limited to Azure AD-protected resources (like Office 365). You can also deploy third-party authentication products that integrate with Azure AD via SAML, and with your on-premises applications via Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial-In User Service (RADIUS) proxy capabilities.

Third-Wave Authentication Will Accelerate

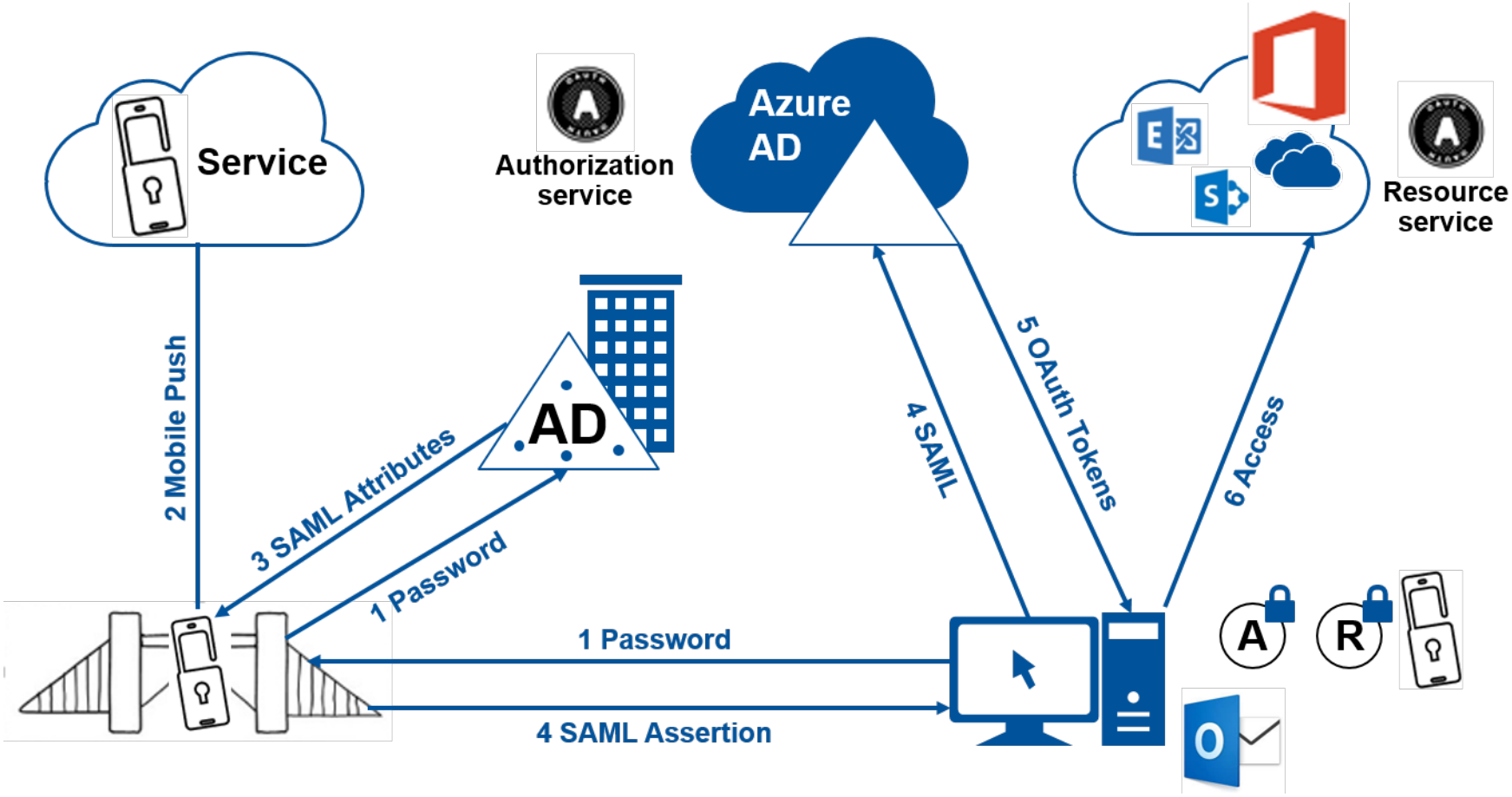
The enterprise authentication landscape has been altered by the arrival of smartphones — that's hardly news. Mobile push authentication, which leverages notification services, dramatically reduces costs while improving security and UX. In addition, adaptive authentication can be combined with many authentication methods while improving usability. Local biometric authentication shows potential but will require time because the Fast IDentity Online (FIDO) standards are still evolving.

Mobile Push

Mobile push has emerged as the default commercial MFA method. It is more secure than one-time passwords (OTPs) because there is no passcode interception. It is more user-friendly than OTPs because the user need not type in long passcodes. Many services display login or transaction details to provide users with context. Most implementations use the single-click acknowledgment mode, where users only need to push a button to confirm they received the push notification. But some implementations provide even higher assurance by asking users to authenticate before acknowledging the message using local authentication capabilities such as the phone PIN or the fingerprint. Mobile push's TCO can be up to 70% lower than that of other MFA solutions.

Figure 2 illustrates the use of mobile push to Office 365. The authentication vendor's SAML identity provider enables the integration with Azure AD and therefore Office 365.

Figure 2. Mobile Push to Office 365 via SAML Integration



Source: Gartner (October 2016)

Identity Proofing

The use of stronger credentials must be coupled with stronger credential management processes, including issuance. Identity proofing (also called identity verification) should be used as a compensating control to ensure the enrollment session provides assurance of password authentication. Identity proofing can include dynamic knowledge-based authentication, device identification, presentation of a government-issued photo ID, demonstration of ownership of an online account and other techniques.

FIDO

The Fast IDentity Online (FIDO) Alliance has strong support from over 100 members, many of which are enterprises and financial service providers. Currently, the FIDO standards are at the 1.0 level, with two separate specifications in play. The first specification is the Universal Authentication Framework 1.0 (UAF), which focuses on passwordless local biometric authentication via a mobile device (as exemplified by Nok Nok Labs products). The second specification is Universal 2nd Factor 1.0 (U2F), which focuses on hardware second-factor authentication (exemplified by Yubico products).

FIDO is currently in transition. The v.2 standard isn't yet defined; it will unite UAF- and U2F-style authentication methods under a single specification. The expected completion for the standard is the first half of 2017. FIDO is also working with the World Wide Web Consortium (W3C) to develop an API for interoperability with web-based applications. The charter for the W3C working group is expected to conclude in February of 2017. Interoperability between existing FIDO UAF 1.0 products and the upcoming FIDO 2.0 specification is unclear.

In advance of the FIDO v.2 standard, Microsoft introduced Windows Hello, which delivers true native biometric authentication to Active Directory. Windows Hello is truly an important development because MFA authentication (apart from smart cards) was an impossibility within the Windows workstation/Active Directory ecosystem. But Windows Hello is "FIDO-aligned"; it does not support the FIDO UAF 1.0 standard, and the FIDO 2.0 standard isn't here yet. Further, most of the benefits for Windows Hello require Windows Server 2016, something that became generally available in the September of 2016.

Planning Considerations

Gartner recommends the following steps to provide fast ROI, while simultaneously improving security and trust, increasing user satisfaction and controlling costs:

- **Migrate or adopt mobile push.** Organizations should take advantage of the mobile-push-based multifactor authentication at the expense of other out-of-band modes such as SMS and voice OTPs. New deployments should use mobile push from the start. Existing SMS- and voice-based OTP mechanisms can be replaced with mobile push over time. LDAP-, RADIUS- and federation-based systems are especially good candidates for migration and can achieve fast time to value.
- **Implement robust identity proofing.** Organizations must ensure that enrollment for higher-assurance credentials is accompanied by adequate identity proofing. Otherwise, the security

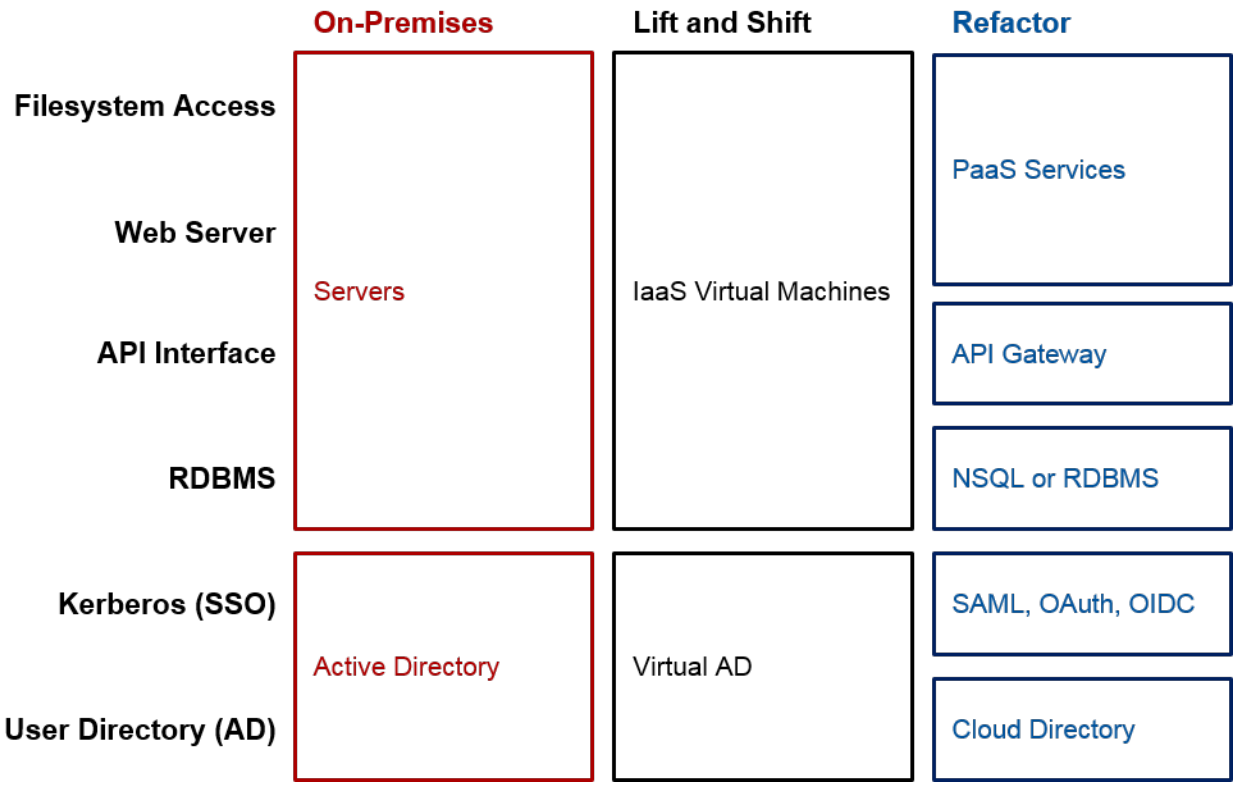
value of the MFA solution will be lost. Choose technologies and vendors that provide adequate identity assurance as well as high acceptance rates for legitimate users.

- **Develop a local biometrics strategy.** Local biometrics via smartphone is inevitable, because it leverages the existing capabilities of the user's mobile device, provides good usability and higher identity assurance. But most organizations should wait on FIDO, until the 2.0 specifications are complete and there is a track record of Windows 10/Server 2016 deployments.

IaaS Identity Services for Application Migration Become a Reality

The enterprise has become more comfortable with moving applications to the cloud. The "lift-and-shift" approach is the predominant method because it enables movement of the application to the cloud with minimal changes and refactoring, and therefore faster time to value for the organization (see Figure 3). Depending upon the application, organizations use lift-and-shift as a transitional step toward refactoring, or stop at lift-and-shift.

Figure 3. Application Migration Paths



NSQL = Nonstop SQL; RDBMS = relational database management system

Source: Gartner (October 2016)

The lift-and-shift approach typically requires virtual machines (VMs) and perhaps a set of Active Directory-centric identity services, including a user directory and authentication services. Both of the IaaS Magic Quadrant leaders (that is AWS and Azure) recently introduced virtualized AD services for their VMs.

Planning Considerations

When using the lift-and-shift application migration approach, leverage the IaaS virtual identity services. It may not succeed in all cases, however, primarily due to incompatibilities with the IaaS platform's virtualized AD implementation.

But before you walk the path, recognize that it is possible that your application will not run due to incompatibilities with the IaaS platform's virtualized Active Directory implementation. Because of these constraints, organizations should use lift-and-shift for simple applications and consider other options for more complex ones.

Also, note that the current virtualized Active Directory services are designed for application migration, not a wholesale migration of your on-premises Active Directory environment. Finally, you should avoid managing your own domain controllers inside IaaS VMs to meet your needs, because they require care and feeding, and result in technical debt that you will need to clean up in the future.

Advanced Analytics Will Permeate IAM Services

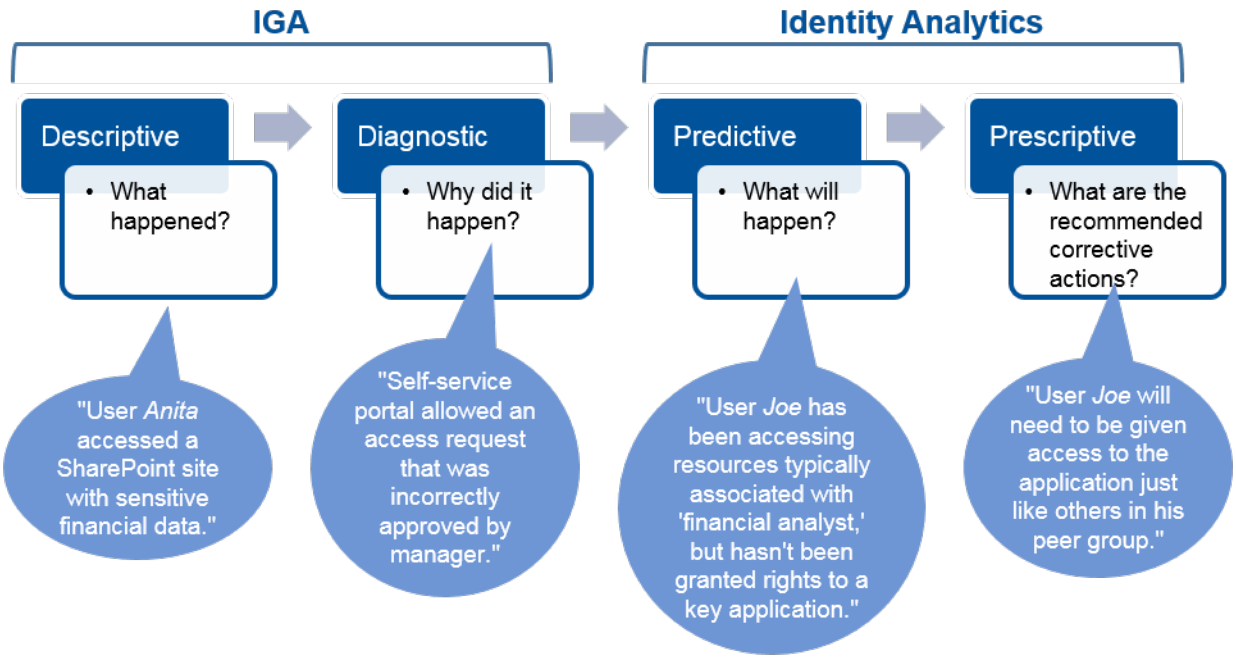
Analytic capabilities are everywhere, and the IAM marketplace is no exception. IAM vendors are increasingly adding analytic capabilities to their product offerings. Identity analytics have the potential to significantly improve IAM services. Simply said, analytics make IAM smarter.

Identity analytics is the discipline that applies science to identity and access data to provide insights for making better IAM decisions. Identity analytics tools enable organizations to take a contextual, dynamic, risk-based approach to IAM. With identity analytics, the organization can bridge the gap between administrative controls and runtime access, add context and risk awareness to access decisions, and continuously monitor, detect, and remediate malicious behavior.

2016 marked the year that identity analytics became a reality, as numerous IAM vendors added analytic capabilities. Most vendors, however, offer only descriptive and diagnostic analytic capabilities. Descriptive analytics describe what happened in the past, and diagnostic analytics determine why it happened.

In 2017, Gartner expects to see IAM vendors offer more-advanced analytics that move the market toward predictive and prescriptive analytics that automatically predict trends and behaviors, identify what may potentially happen and make recommendations for corrective action (Figure 4).

Figure 4. Identity Analytics: Descriptive, Diagnostic, Predictive and Prescriptive



Source: Gartner (October 2016)

Advanced analytics will require IAM vendors to integrate with more data sources, aggregate and process larger amounts of identity-related data, employ behavioral and machine learning analytic engines, and provide algorithms optimized for the identity domain.

By using advanced analytics, IAM vendors will enable the following key features:

- **Risk scoring, computation and analysis:** Ability to not only evaluate risk based on static risk inherent to an entitlement or an account, but also dynamic risk derived from context, behavioral analytics and risk information gathered from external systems.
- **Identity correlation and profiling:** Ability to detect and recognize uncorrelated users and establish a baseline (normal) behavior profile of a user.
- **Behavioral and data analysis:** Ability to perform peer-group analysis, detect anomalous behaviors, identify users with excessive access, etc.
- **Continuous monitoring and alerting:** Ability to spot anomalies and vulnerabilities in real-time (or near real-time) and take immediate action.
- **Data presentation and visualization:** Ability to provide visual dashboards and tools that expose identity data in a business-friendly manner.

In 2017, analytics will permeate the IAM market in three key areas: identity governance and administration, adaptive access control, and privileged access management.

Identity Governance and Administration Analytics

Identity analytics in the context of IGA is largely driven by the need to improve access certifications. Many organizations have what Gartner calls "access certification fatigue." Access reviewers do not have the information and context necessary to make informed access-review decisions.

To ensure effective access certifications, organizations must add identity analytic data to their access certification process. Analytic data such as rogue or outlier access identification, peer group analysis, risk scoring, orphaned and dormant account identification, and usage patterns provides context to help managers make faster, more-informed access review decisions. Gartner expects identity analytics to enable organizations to move from frequent, full certifications to continuous microcertifications.

Identity analytics also helps organizations make smarter IGA policy decisions. For example, identity analytics enable more sophisticated role models that are based on usage patterns, peer-group analysis and role effectiveness. Identity analytics also provides contextual data that simplifies the access request and approval process.

Gartner believes that identity analytics is the next evolution in the IGA market. While there are some niche vendors that offer advanced identity analytic capabilities, today most IGA vendors offer only basic analytic capabilities (descriptive/diagnostic). We expect IGA vendors to innovate and invest heavily in analytic capabilities in 2017.

Adaptive Access Control

Identity analytics also plays a crucial role in reducing runtime access risk and improving user login experience. Compromised identity credentials, including credential phishing, are the biggest cause of cloud security failure. It is not enough to establish a user's right to access an application at administration time. Organizations must also detect and respond dynamically to attempted breaches in real or near real time by evaluating that the context of the request is appropriate.

For example, if a relationship manager, whose job routinely requires him or her to access dozens of customer records in the office during the business day, suddenly requests thousands of customer records in another country at three o'clock in the morning, then a system that incorporates user and entity behavior analytics (UEBA) information into its risk-based access policy logic would be able to flag this request as high-risk and block access until the user provided additional authentication factors. If this account manager is a salesperson who travels frequently across multiple time zones and routinely mines customer data to discover successful sales patterns, the same smart adaptive access system could leverage policy that recognizes that salesperson's behavioral patterns as normal for him or her and treat the request differently.

Planning Considerations

- **Organizations evaluating new IAM solutions should look for vendors that incorporate identity analytics capabilities.** Look for vendors that have already incorporated basic analytic techniques, and inquire about support for more advanced, proactive and prescriptive capabilities in vendor roadmaps.

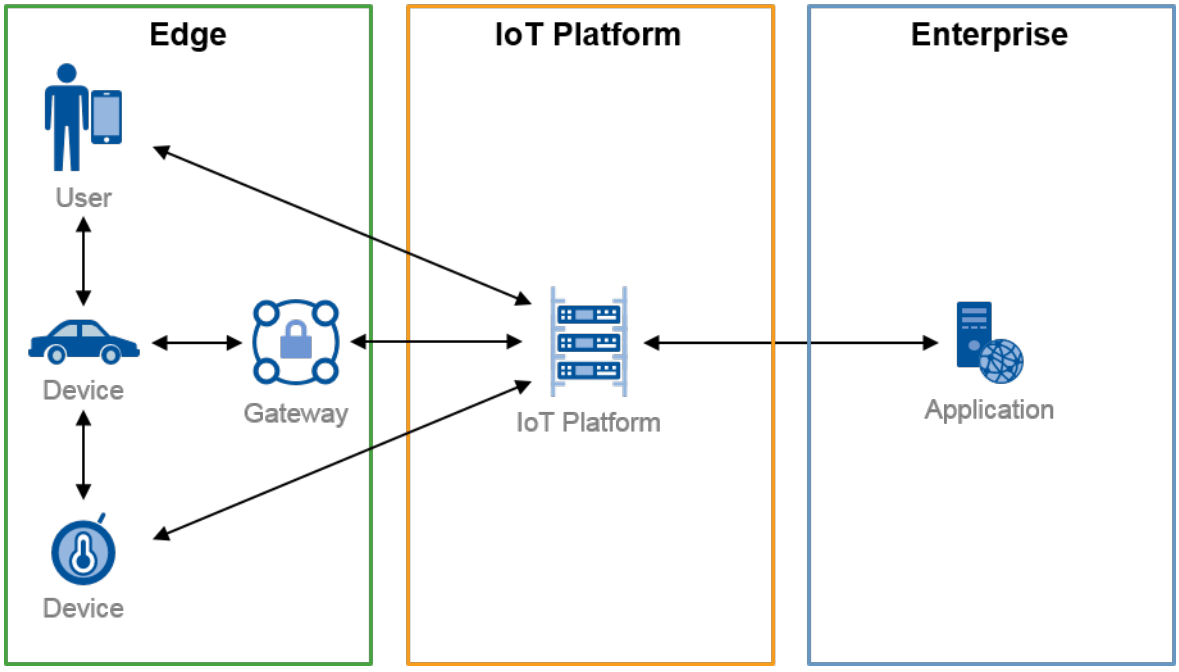
- **Choose authentication and SSO solutions that provide robust support for risk-based adaptive access.** Look for vendors that not only support the evaluation of basic context attributes such as time and geolocation, but also identity analytics insights that provide historical context. Adaptive access engines should have APIs that can accommodate input from multiple analytics sources both inside and outside the organization.
- **Develop your adaptive analytics policies to adjust to changes in use cases and evolving threats.** Adaptive analytics is an evolutionary approach. Continually assess whether your adaptive access is configured too narrowly, so that legitimate behavior is flagged as too risky, and also whether in hindsight some requests were approved that should not have been. Adaptive access techniques are a key tool for dynamic threat detection and response.
- **Leverage identity analytics incrementally to make your overall IAM systems smarter.** Identity analytics is not an all-or-nothing technique, but an evolving set of tools. Incorporate identity analytics techniques as part of a layered approach to solving your more difficult and subtle IAM challenges.

The Internet of Things Will Raise the Stakes for IAM

The Internet of Things is a technology transformation with potential for groundbreaking revenue models and optimizations. IoT transformations often start with research, trial and error and innovation at the lab or within an IoT center of excellence.

The diversity of the IoT makes Identities of Things (IDoT) hard to architect and manage for IoT solution architects. Users, devices, gateways, platforms, applications and services all have a part to play in IoT solutions and need identities to form a secure and trusted IoT. Figure 5 illustrates the seven identity-infused interactions within IoT.

Figure 5. Identity-Infused Interactions Within IoT



Source: Gartner (October 2016)

However, the approaches to molding identity into the IoT differ. Hardware security module (HSM), public-key infrastructure (PKI), IAM, API gateway, networking, hardware and IoT platform vendors state that they have an important part to play when it comes to IDoT. In most cases, that's very true. The functionality provided by these products is often required to meet all the requirements for molding identity into the IoT. You will not find one flow, credential, bootstrapping method, authentication or authorization method that will solve all needs. Instead, a portfolio of tools is required.

Identity Is Hard to Architect and Maintain

IoT solutions are greater than the sum of their parts, and they are built up of many pieces and vendors. There is, however, a disconnect between the different vendors, where each part is busy trying to become great standing on its own. Long-lived, adaptive, scalable and maintainable solutions require integrations, especially for the IDoT, where new and existing policies, authentication methods, federations and trusts needs to be used and reused to limit the amount of vendor lock-in and new identity islands.

The Invention of New, Not Always Rounder, Wheels

IoT platforms reinvent IAM to meet scale requirements and to manage new types of objects. Sadly, it is not always an improvement. The newly invented "stock wheels" within IoT platforms are not always as round as they should be. The dreaded password is making a comeback on IAM teams'

radar within IoT. This time it is deployed at the edge of the networks, often out of reach and out of sight.

A one-size-fits-all credential type does not exist for all assurance needs in IoT solutions, but a good and modern credential is both bound to hardware and is life-cycle-managed (that is, can be updated and revoked).

Scale

New objects as the plethora of different device types, devices, gateways and IoT platforms need to be maintained because they are decentralized trust servers of the organizations using them. Management and governance enables organizations to meet both compliance and business requirements. Will your IAM system handle the increased number of relationships between users, devices, services and policies?

A client expressed the following analogy while assessing its PKI infrastructure against modern needs:

> "It feels as we went to the car mechanics and asked for an oil change, but it ended up in us needing a brand new motor."

Planning Considerations

In response to IoT trends, consider the following actions when planning for 2017:

- **Put an IAM architect in the IoT center of excellence.** Hastily deployed pockets of identity infrastructure need to be maintained for the full lifetime of the devices. You do not want to set a presence of systems with low assurance levels that an organization later must handle. Do you need end-to-end authentication and authorization? Do you need to centralize policy management but still connect to offline devices? Identity affects your entire architecture. Put an IAM architect within the IoT center of excellence that can assess and, early on, take ownership of the IAM functionality.
- **Follow the path of the six identity-infused interactions.** Each of the interactions opens up new requirements and considerations when architecting your IoT solutions. By following the path, you will see how the interactions affect your devices, protocols used, communication security and credential types. While following the paths, ask yourself:
  - Can I reuse my existing identities and access policies?
  - Do I need end-to-end encryption?
  - Should the component act on behalf of itself, or on behalf of someone else, like a user or a device?
  - How will I manage this component?

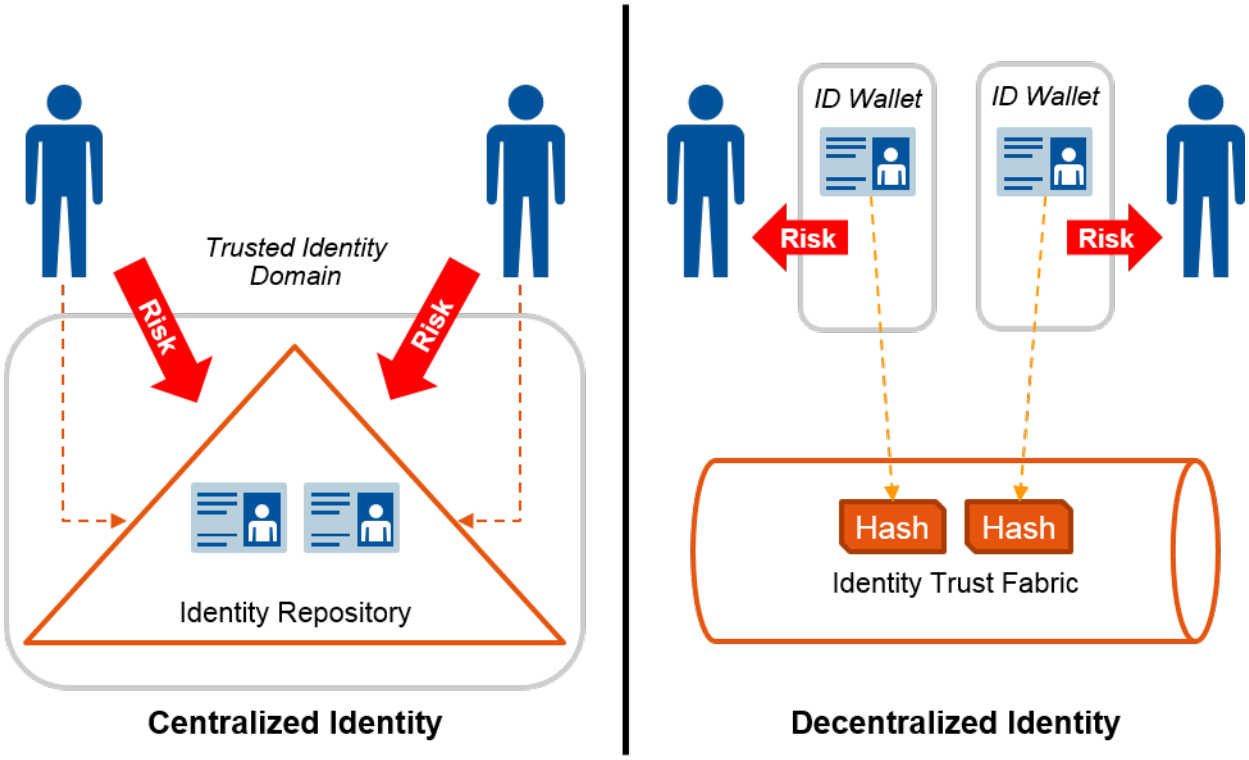
    - How can I centralize my authorization policy management for this interaction?
- **Define and meet your assurance levels, for now and forever.** If your devices live for decades, are you sure that you can trust the network that the devices are connected to for the full lifetime of the device? Define your assurance levels not only with today's requirements, but also with future potential requirements in mind. An example: A credential, bound to physical hardware, and through which life cycle is managed, can meet your defined and required assurance levels longer than that static password can.
- **Think of your IoT platforms as identity technology.** The IAM maturity level of the IoT platforms varies because identity is not always in its DNA. Onboarding, and automated life cycle management of the devices and gateways connected to your network, will be important while unraveling your IoT projects. For all components in an IoT solution, look for certificates and Identity 2.0-based protocols, such as SAML, OpenID Connect, OAuth2 and System for Cross-Domain Identity Management (SCIM). Important questions include:
    - Can I live with the built-in capabilities of the IoT platforms?
    - If not, can I integrate my IAM and IGA systems?

Blockchain Will Advance Decentralized IAM

Blockchain fever has accelerated a movement toward a decentralized identity model, enabling user entities to manage their own identity and profile attributes. Gartner believes a decentralized identity model that is built on a common identity trust fabric will become more feasible in the coming years.

Blockchain platforms have provided a suitable environment for developing an experimental identity trust fabric that enables decentralized identity solutions, even though the results are not fully ready for general industrial adoption. The goal of these solutions is to decouple trust management from central authorities and disaggregate risk by gradually reducing the role of identity providers in managing identity data. This is a key evolutionary step, following the introduction of identity federation and mobile identity, to bring identity management closer to user entities. In doing so, the decentralized identity model (see Figure 6) is a fundamental shift that balances the accountability and responsibility of digital identity management across the value chain participants.

Figure 6. Centralized vs. Decentralized Identity



Source: Gartner (October 2016)

The key drivers are to minimize the security and privacy risk of managing identity profiles centrally. From a business perspective, it is an opportunity to address the ongoing challenge to establish trust between multiple domains. This has been a major challenge for organizations implementing a federated identity model. The decentralized identity model is enabled by a more inclusive identity trust fabric that can streamline cross-domain business processes integration, regardless of where identities are originated. This property simplifies the flow of data and transactions to enhance business agility and customer experience. However, organizations are cautioned that decentralization is not all-or-nothing. Organizations should consider this phase of identity decentralization as a steppingstone.

Currently, many large organizations have engaged their innovation teams to identify potential use cases. Gartner expects this trend to accelerate as more organizations take a similar approach in the coming year and look for adoption opportunities beyond the blockchain hype. The key objective is to support the modernization of the core business processes, specifically in B2C and B2B scenarios that manage sensitive or regulated identity data or carry higher operational risk, both from the user experience and compliance perspectives. Organizations are trying to address the following key issues:

- How to generate, prove, bind and manage a decentralized identity in an identity wallet.

- How to register and attest to a decentralized identity and its attributes on an identity trust fabric.
- How to protect identity wallets and enhance user experience using an identity custodian.
- How to verify identity and entitlement attributes for granting access in a digital transaction.
- How to ensure interoperability between like components and establish integration standards.

Organizations should develop robust logical and physical architecture to address these issues for regular and exceptional use cases. Decentralized identity systems consist of two key architectural components:

- **Identity trust fabric:** An identity trust fabric enables the appropriate sharing of identity assets across people and organizations. Blockchain-based platforms run by groups of organizations operating in a (preferably) trusted network are playing a key role in enabling the current generation of identity trust fabrics. The level of trust in these systems highly depends on the quality of distributed consensus algorithms. There are currently open questions on the long-term viability of blockchain proof-of-work or proof-of-stake distributed consensus algorithms for identity trust fabric use cases. The key issues boil down to performance, efficiency and the probabilistic properties of these algorithms. Many vendors are working on addressing these issues. Hashgraph is an emerging alternative to blockchain proposed to address these issues natively. However, hashgraph approaches are still in the early stages of industry review, and have much less exposure than blockchain.
- **Identity wallet:** The user entities' identity wallet is another key component that directly affects the user experience. The identity wallet enables the user to manage the storage and presentation of their identity data, which involves the wallet owner in administrative activities. There is a general concern that in the case of a lost or compromised wallet the user's identity history may disappear. These issues have raised the importance of the key management and application integration framework used by the wallet. Proprietary approaches to address these issues are emerging, such as multisignature and escrow models that provide a wallet recovery mechanism, but standards do not yet exist. There are business models in which an identity custodian securely stores the wallet data in its environment to enhance the availability and recoverability of decentralized identities.

Planning Considerations

Gartner expects examples of decentralized identity solutions to become available within one to two years. In 2017, IAM teams from organizations that could benefit from a distributed IAM model should start investigating decentralized identity solutions by defining and executing on limited-scope, proof-of-concept projects. The following list summarizes key considerations:

- **Establish a focused identity decentralization team.** The identity decentralization team should consist of IAM architects and business analysts, with representatives from sponsoring business unit, digital business, legal and compliance, risk management, privacy and security teams.
- **Investigate decentralized identity solutions.** Organizations gain institutional knowledge by defining and executing on limited-scope, proof-of-concept projects.

- **Create a blockchain center of excellence.** In addition to establishing an identity decentralization team, organizations should create a block learning repository, run pilot programs and track industry activity.

Setting Priorities

You should focus on IAM priorities that deliver faster value to the business in 2017.

Scalable Office 365 IAM

Most of Gartner's clients are at varying stages of Office 365 adoption. Their success requires tackling four milestones: preparation, user management, license management and authentication — all at scale. If addressed, organizations will be set up for success with Office 365 and future IaaS and enterprise mobility management deployments.

Getting Office 365 and Azure AD "right" requires the acknowledgment that license management is a core IAM function, just like any other entitlement. Organizations should not be afraid to use PowerShell to integrate IAM with license management; PowerShell has emerged as the workhouse for scalable management of users and resources in Azure. If license management is done correctly, the organization not only improves security but also saves money by reducing costs.

Mobile Push Authentication

As to other commercial MFA systems, mobile push is making dramatic improvements across the dimensions of security, cost and usability. Organizations looking to achieve fast time to value in 2017 should consider moving to mobile push by taking the following actions:

- Inventory applications to determine if they are compatible with federation (SAML OpenID Connect), LDAP or RADIUS.
- Determine if the majority of the users have smartphones.
- Assess OTP coexistence needs.
- Use good identity-proofing processes.

IaaS Identity Services for Application Migration

The lift-and-shift approach to application migration has emerged as a popular approach due to faster time to value. The approach usually requires IaaS virtual machines and Active Directory-centric identity services. Both of the "up and right" IaaS providers (that is, AWS and Azure) now offer them.

But before walking the path, organizations should recognize that application incompatibilities are common. Also, the current capabilities of the IaaS VMs and virtualized AD services are designed for application migration, not relocating on-premises Active Directory environments to the cloud.

Finally, organizations should avoid deploying domain controllers inside IaaS VMs because this negates most of the value of moving to IaaS in the first place.

Identity Analytics

Leverage identity analytics incrementally to make your overall IAM systems smarter. Identity analytics is not an all-or-nothing technique, but an evolving set of tools. Organizations should leverage analytics for both admin-time (that is, IGA) and runtime (SSO and MFA) processes. When evaluating solutions, organizations should look for offerings that have incorporated analytics into their platform:

- Incorporate admin-time basic analytic techniques and inquire about support for more advanced, proactive and prescriptive capabilities in vendor roadmaps (IGA).
- Evaluate runtime contextual attributes such as time, geolocation, IP address blacklisting, and device identification (SSO and MFA). Most mobile push MFA vendors support contextual/ adaptive authentication.

Identity of Things

For many organizations, IoT provides compelling benefits, from improving customer retention to providing better visibility and control over core infrastructure. For 2017, be proactive:

- Assign an IAM architect to IoT initiatives. IoT requires solid IAM disciplines.
- Ensure that you are authenticating things with adequate assurance. Once the thing is in production, fixing it is an expensive and time-consuming proposition.

Gartner Recommended Reading

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

"Molding Identity Into the Internet of Things"

"Solution Path for Implementing Single Sign-On"

"Making the Right Identity Choices for Azure AD and Office 365"

"Blockchain — The Dawn of Decentralized Identity"

"Magic Quadrant for Cloud Infrastructure as a Service, Worldwide"

"Implementing Office 365: Gartner Survey Results and Analysis, 2016"

"Building a Risk-Aware IAM Environment With Identity Analytics"

Evidence

[1,2] "Implementing Office 365: Gartner Survey Results and Analysis, 2016"

More on This Topic

This is part of an in-depth collection of research. See the collection:

- 2017 Planning Guide Overview: Architecting a Digital Business With Sensing, Adapting and Scaling

GARTNER HEADQUARTERS

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

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

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