Navigate The Future Of Identity And Access Management

by Eve Maler, April 7, 2014

KEY TAKEAWAYS

For Security With Agility, Enterprises Require Zero Trust Identity
The age of the customer is affecting how security and risk pros engage with the developers, users, and business stakeholders they serve. You can't slow the pace of change, so you need an IAM approach that withstands extreme heterogeneity in your business infrastructure so that you can support increased competitiveness with superior security.

Zero Trust Identity Is A Model, Not A Product
If you're starting from scratch, you may be tempted to buy your way into Zero Trust with a “cloud identity” solution, but you first need to conceive of IAM functions -- such as provisioning, authentication, and authorization -- as application programming interfaces. You can benefit by applying this model even to internal applications and users.

Zero Trust Identity Must Rest On A Solid Identity Data Foundation
In the loosely coupled regime of the cloud, you can expect every flaw in role governance to be magnified. Make your access control hygiene impeccable through the discipline of protecting information consistently with identity context (PICWIC) before you expect your Zero Trust identity approach to bear fruit.

Tackle Extended Enterprise Authentication Challenges With Next-Gen Technology
Security pros often struggle with the classic “security versus usability” tradeoff in reaching authentication goals.
Navigate The Future Of Identity And Access Management

Future Look: The Identity And Access Management Playbook
by Eve Maler
with Stephanie Balaouras, Andras Cser, John Kindervag, and Jennie Duong

WHY READ THIS REPORT

This is an update to the report of the same name originally issued to clients on March 22, 2012; it includes updated charts and new 2013 Business Technographics data and adds a discussion on Zero Trust authentication. This report outlines the future look of Forrester’s solution for security and risk (S&R) execs building an identity and access management (IAM) strategy for the extended enterprise. This report helps you understand and navigate the major business and technology management trends affecting IAM in the next five years. Increasingly in 2014, IAM has become a tool not just for security but also business agility. Competitive challenges push businesses into the cloud and encourage mobile device use even without full-fledged access controls in place. These trends create pressing provisioning, authentication, and authorization challenges for S&R pros while compliance requirements and breaches and other security threats continue to swell. This report recommends that S&R pros apply a Zero Trust information security model to IAM to unify and improve access control across the extended enterprise.

Table Of Contents

2 The Extended Enterprise Urgently Needs Better Access Management
3 Newly Agile Environments Highlight The Weaknesses Of Today’s IAM
6 Introducing Zero Trust Identity
8 Apply Three Rules To Achieve Zero Trust Identity
14 Enable Zero Trust Identity Step By Step

WHAT IT MEANS

15 Zero Trust Identity Does Much More Than Protect — It Enables
15 Supplemental Material

Notes & Resources

In developing this report, Forrester drew from conversations with over a dozen user companies, authentication vendors, and experts, including eBay, Intuit, Layer 7 Technologies, and Quest Software (now Dell).

Related Research Documents

Market Overview: Employee And Customer Authentication Solutions In 2013, Part 1 Of 2 December 30, 2013

Transform Your Security Architecture And Operations For The Zero Trust Ecosystem September 12, 2013

THE EXTENDED ENTERPRISE URGENTLY NEEDS BETTER ACCESS MANAGEMENT

Forrester clients are struggling with an IAM landscape that increasingly crosses enterprise boundaries. They tell us: “Software-as-a-service apps are making our existing methods of access management useless.” “We can't just ‘Kerberize’ our apps anymore.” “If we keep on doing security in domains, it's pointless.”

Forrester defines the extended enterprise as one for which a business function is rarely, if ever, a self-contained workflow within the infrastructure confines of the company. It presents unique IAM challenges in three dimensions simultaneously (see Figure 1). For example:

- **Resource sharing with partners is on a knife's edge between vital and perilous.** An automotive manufacturer is expanding its internal enterprise information portal to include a business partner audience, something it wouldn't have considered doing even a year ago but now needs for business agility. It wants to put in place extra-strict access controls, since most of its suppliers also deal with most of its competitors. However, it faces a challenge due to its inability to control suppliers' role-provisioning processes.

- **Security pros perforce pay less attention to cloud apps than apps they control directly.** When business owners rush to use software-as-a-service (SaaS) apps for email, expense management, and more, they sometimes skip over the fine details of security and access control, leaving security pros out of the conversation. We see some companies synchronizing user accounts to external apps on a relatively infrequent schedule through insecure file transfer protocol (FTP) or relying entirely on "front-door" authentication for access to wide swaths of app functionality. Organizations can lose all visibility into access events wherever users can access a SaaS-based business function through the open Internet from an unmanaged device or network without touching "home base" infrastructure.
NEWLY AGILE ENVIRONMENTS HIGHLIGHT THE WEAKNESSES OF TODAY’S IAM

Software decision-makers are telling Forrester they’re continuing to increase their SaaS app use — and every one of these apps represents a potential IAM challenge (see Figure 2).\(^1\) Three problems typify the disconnect between traditional IAM and the new extended-enterprise reality: 1) stumbling blocks in cross-domain user provisioning; 2) weakened control of authentication and authorization; and 3) siloed IAM approaches to different purposes and populations.
Figure 2: SaaS App Adoption Continues to Grow, Creating New IAM Challenges

“Using your best estimate, how many different software-as-a-service (SaaS) applications did your firm use/is your firm likely to use?”

<table>
<thead>
<tr>
<th></th>
<th>Europe (N = 297)</th>
<th>North America (N = 646)</th>
</tr>
</thead>
<tbody>
<tr>
<td>...12 months ago?</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>...today?</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>...12 months from now?</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>...two years from now?</td>
<td>20</td>
<td>12</td>
</tr>
</tbody>
</table>

Base: North American and European software decision-makers from companies with 20+ employees

Source: Forrester Research, Inc.

Problem No. 1: Cross-Domain User Provisioning Stumbling Blocks

Ideally, technology management should enable all legitimate access by workforce members to SaaS apps and by partners to internal apps — and block all illegitimate access. However, conveying the attributes and entitlements of joiners, movers, and leavers to remote apps continues to be a sore spot. The issues include:

- **Tight coupling to enterprise user stores.** SaaS apps often come prepared to connect directly to your organization’s lightweight directory access protocol (LDAP) or Active Directory (AD) store. However, this approach becomes complex and adds security and privacy concerns where it involves multiple or heterogeneous user stores, and it doesn’t scale well as the number of SaaS apps grows. Many times, firms need to work with business partners’ users whose identities they don’t want to store, since this entails added liability.

- **Reduced security due to latency when removing authorizations.** SaaS and partner apps that rely on too-infrequent synchronization to obtain authoritative user data tend not to catch status changes that should have resulted in denying access. This need becomes acute for sensitive apps accessible to competitors and supply chain partners, as is often the case in the automotive and aerospace sectors.
Reduced business agility due to latency when adding authorizations. Dynamism is key for agility and competitiveness. When a SaaS or partner app refuses access to legitimate new employees because the app’s synchronization process hasn’t caught up with reality, its value diminishes.

“Garbage in, garbage out” user data. As one large professional services firm told us, “The cloud has exposed the fact that even well-governed companies are not prepared.” SaaS apps are forcing businesses to confront the inadequate quality of the data in their user repositories, no matter how they convey the data to remote apps. In the loosely coupled regime of the cloud, you can expect every governance flaw to be magnified.

Problem No. 2: Scenarios That Allow Weakened Authentication And Authorization

Information workers are driving big bring-your-own-device (BYOD) moves; recent Forrester research reveals that 66% of North American and European info workers who use smartphones for work chose their own smartphones. Organizations are now beginning to take better advantage of the BYOD opportunity. One Dutch company exemplifies an increasingly common scenario by giving employees access to its legacy enterprise applications through specialized iPad apps. However, mobile and other extended-enterprise trends introduce the following challenges:

Mobile use eliminates classic Windows-based authentication options. Organizations’ “extreme mobile” users, typically salespeople and other field personnel, might never log into a Windows-based computer. This puts Integrated Windows Authentication (IWA), desktop-friendly smartcard readers, and desktop-to-web single sign-on (SSO) flows out of reach. Organizations’ authentication strategies must account for the plethora of new login flows in BYOD environments.

External apps’ local authentication options may not sync with organization requirements. Configuring each of your SaaS and partner apps to perform the types of employee or customer authentication you would normally require, such as multifactor authentication (MFA) or risk-based authentication (RBA), ranges from daunting to impossible. Popular apps such as salesforce.com may offer integration of various strong authentication methods such as RSA SecurID tokens, but long-tail apps are likely to offer only passwords.

It’s hard to give SaaS apps all the tools they need to make access decisions on your behalf. Your internal users have an overabundance of authorization-related attributes, whether in role, group, or other form. Sometimes getting the right ones to a SaaS application in the right form can be cumbersome and problematic.
Problem No. 3: IAM Silos For Different Purposes And Populations

Often, different business owners drive the decision-making around IAM functions for different populations, such as: 1) employees from various company divisions; 2) business partners; 3) consumers; and 4) developers of third-party applications that interact with corporate systems. This leads to divergent architectural choices and added complexity. As a VP of IT risk for a large computer systems firm noted simply, “Complexity drives risk.” The extended enterprise causes these scenarios to blend and merge, drawing attention to mismatches in infrastructure that add security risk and stall agile business moves. For example:

- **A change in employee status is sometimes a continuum rather than an event.** Mergers and acquisitions throw together technology management organizations that use different IAM platforms, leading to Band-Aid solutions on top of diverse user stores to begin the process of representing a unified employee base. When it's time to part ways, a similar problem arises: The firm mentioned above sold a major division in 2004, but because of remaining close business relationships, its IAM systems overlapped in hard-to-manage ways eight years later.

- **Federation looks very different in business settings versus consumer ones.** Many media and retail companies are moving rapidly to accept “social sign-in” from the likes of Facebook and Twitter, exemplifying identity federation for marketing and eCommerce purposes. Although the underlying mechanisms for providing consumer SSO are identical to SaaS and business-partner SSO, the corporate business owners — and the solution providers addressing these markets — tend to diverge radically. As data breaches and password stealing increase, hardening consumer IAM to levels expected in enterprise technology management and aligning infrastructure to reduce complexity look more attractive.

- **Many SaaS apps cater to businesses and individuals alike, forcing the unification issue.** Cloud service providers such as Google, Intuit, and salesforce.com work with individuals along with enterprises and small and medium-size businesses (SMBs) and must integrate with each other’s services for mashup scenarios as well. Organizations interacting with these services using different infrastructure for different use cases multiply their costs and security vulnerabilities.

INTRODUCING ZERO TRUST IDENTITY

Forrester’s Zero Trust model of information security eliminates the idea of distinct trusted internal networks versus untrusted external networks. It requires security pros to verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic. Thus, Zero Trust refers to an initial stance toward access. What, then, are the goals for a Zero Trust approach to identity? It must:

- **Center on sensitive applications and data.** Organizations’ perimeters aren’t going away, but they’re clearly not doing a good enough job; the Privacy Rights Clearinghouse has identified 947 data breaches from 2005 through 2013 due to “electronic entry by an outside party, malware
and spyware,” and only a few of the affected organizations reported absence of a firewall. For Zero Trust, every protected resource, whether it’s an older on-premises customer relationship management (CRM) app or a business SaaS app that launched last week, must be equally capable of assessing incoming access requests and treating each one as a potential threat.

- **Unify treatment of access channels, populations, and hosting models.** Organizations’ systems should always use the same robust and reliable mechanisms to determine and track access. They shouldn’t go easy on a request for access just because it comes from a physically badged-in employee sitting in the cubicle next to the server farm that hosts the app, rather than an external partner halfway around the globe using a newfangled mobile device to get into a SaaS app (see Figure 3). A key way to achieve this robustness is to use authentication methods that work even for external people on unmanaged devices trying to access SaaS apps. The authentication market has graduated from a hardcore high-security first generation to a mobile-fueled third generation that’s much better suited to Zero Trust (see Figure 4).

- **Prepare for interactions at Internet scale.** Google engineer Steve Yegge made waves with a public rant in late 2011 about Google’s failures in light of his former employer Amazon’s successes. The observation at its heart: Amazon’s success is due to one simple mandate, which begins, “All teams will henceforth expose their data and functionality through service interfaces.” The lesson applies not just to high-tech companies but also to every organization that wants to unlock the value of its data and services. Internet scalability enables integration and aggregation of business value but also points the way to a robust and repeatable approach to access control.

---

**Figure 3 Zero Trust Identity Accommodates Mix-And-Match Access Scenarios**

<table>
<thead>
<tr>
<th>IAM functionality</th>
<th>Authoritative user store</th>
<th>Provisioning, proofing, self-service</th>
<th>Authentication, session management, SSO, federation</th>
<th>Authorization, consent, access control</th>
<th>Attestation, delegated administration, audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>End user populations</td>
<td>Workforce</td>
<td>Business partners</td>
<td>Consumers and customers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protected resources</td>
<td>Organization apps</td>
<td>Business partner apps</td>
<td>SaaS apps</td>
<td>Consumer-facing apps</td>
<td></td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.
Figure 4 User Authentication Has Morphed In Response To Zero Trust Needs

APPLY THREE RULES TO ACHIEVE ZERO TRUST IDENTITY

To achieve Zero Trust identity, S&R pros must apply three important rules: 1) plan for both outward and inward identity propagation; 2) formalize and robustly protect the interfaces for IAM functions; and 3) use and advocate standards for IAM interfaces. If you only stick to traditional approaches suitable for the “unextended enterprise” of the past, you could pay — in integration costs, agility, or regulatory compliance — whenever users cross security domain boundaries to use technology functions that form a virtual part of your business.

Rule No. 1: Plan For Both Outward And Inward Identity Propagation

Zero Trust identity supports the goal of identity statelessness, allowing each app to consume just-in-time identity data and services coming from other organizational domains that are authoritative for them.9 Given the need for bidirectional flow, you can see the classic identity provider (IdP) and relying party (RP) roles as merely special cases of a generic security token service (STS) (see Figure 5). This rule requires a change in mindset, and it’s not a trivial one. The following are some business motivations for this bidirectional flow:
- **External identities need to be able to knock on an organization’s door for access.** A large consulting firm with a substantial IAM practice observed: “Some organizations are on the cusp of figuring out how to address identity in a cloud environment. Everyone comes with identity inside their house, and moving it outside the house is what we’re trying to address.” Living up to this goal, a US technology research firm is deliberately exposing its employee identities in a form that is “usable on both sides of the firewall” and is working to accept third-party logins from US federal government contractors who can present a Common Access Card (CAC) smartcard credential on a dynamic basis.

- **Business units and partners alike need to integrate at a moment’s notice.** Intuit has found that externalized authentication and authorization application programming interfaces (APIs) allow apps from different business units and third-party partners, such as QuickBooks, FreshBooks, Bill.com, and Expensify, to be nearly completely interoperable when it comes to access management, and it finds this ability to be effective in encouraging customers to use additional services. Its goal is to avoid asking its enterprise architecture (EA) team or its multitenant cloud service providers to do anything special when it’s time to integrate a new “identity channel,” such as a financial services firm.
Figure 5 Many Scenarios Require Two-Way Flows of Identity and Access Information

For functions internal to the organization:
- Organization serves as an identity server for business functions.
- A security token service (STS) handles token issuance, translation, and consumption.

For external partners and customers:
- Organization serves as an identity client of user stores.

Source: Forrester Research, Inc.
Rule No. 2: Formalize And Robustly Protect The Interfaces For IAM Functions

Many security pros tell us that for years they have exhorted line-of-business developers to stop baking access management logic into applications. Why is it more important than ever to externalize and centralize that logic? It's because the only safe prediction about the next application your organization will deploy, user it will serve, and device or network he or she will use is a Zero Trust prediction.

The secret to making progress is to push identity-as-a-service (IDaaS) to its logical limit — into the realm of the open web platform. Conceive of IAM functions as fully externalizable APIs that serve client apps in need of access protection (see Figure 6). Taking this step enables your intentions around rule No. 1 on a technical level.

In offering IAM APIs, your organization becomes, in a sense, an IAM cloud service provider. It must protect these APIs as it would protect any open web APIs offering core business functions, and the IAM services themselves can recursively play a role in this protection, further unifying your infrastructure. Intuit went through exactly this process by conceiving of and building a central identity authority, which could be hosted on-premises or as a cloud service. It then built a layer over all of its services that could test all inbound traffic.

The three primary IAM APIs we see enabling mix-and-match access scenarios are as follows:

- **Authentication.** This is a centralized service that performs identification, authentication, and attribute delivery of all users under your authoritative control. It has an open API, which internal and external apps can call when your user population needs to access them. This API lets your organization function as an IdP, enabling cross-domain SSO, login session management, federation, social sign-in, and similar use cases. Taking an API approach prepares for access by native mobile apps as well as web apps. Large enterprises can benefit from this API even in an internal federation scenario; our computer systems firm found that getting all of its apps to use one directory is a $200 million IT problem.

- **Provisioning.** This is an open API over your user stores that allows internal and external client apps to read and write identity information as appropriate, including deprovisioning accounts. This API enables account synchronization with internal, SaaS, and partner apps when federation is not an option, as well as internal provisioning workflows that work with your existing directory or database infrastructure in a loosely coupled way.

- **Authorization.** This is a centralized policy decision point (PDP) with an open API that internal and external business apps running on your behalf can consult before allowing access by requesters. This API enables business apps to serve as auditable policy enforcement points (PEPs) no matter where they are hosted. API management vendor Layer 7 (since acquired by CA Technologies) has been finding that, to the extent that these business apps themselves expose fine-grained features through their APIs, they can support arbitrarily fine-grained access control by this method. Least-privilege access is an important tenet of Zero Trust information security.
Rule No. 3: Use And Advocate Standards For IAM Interfaces

The Zero Trust identity vision and its open web emphasis play into a larger vision that some, including our technology research firm from above, label “Enterprise 2.0.” The goal: Couple your systems as loosely as you can, avoiding dependencies on IWA, AD, LDAP, or Kerberos identity technologies wherever you can. While enterprises often employ internal standardization of IAM APIs as a first step, they frequently report that forcing developers onto an API that the outside world doesn’t use merely delays extended-enterprise benefits and forces unnecessary implementation upgrades. Therefore, the best way to achieve Zero Trust identity is to use global standards that define well-accepted and loosely coupled messaging around IAM functions. For the standardization needs of the three key IAM APIs, we see the following solutions coming to the fore as Internet-scale and mobile- and API-ready interoperability standards (see Figure 7):
- **Service provisioning markup language (SPML).** Although it never reached pervasive deployment, this long-established provisioning standard uses a web services approach that is friendly to service-oriented architecture (SOA) environments.

- **Simple cloud identity management (SCIM).** This emerging web-friendly provisioning standard is appealing to cloud service providers and was developed rapidly over the past year and a half. It is entering a final standardization phase now but is already seeing product support from vendors such as UnboundID. Using SCIM as a jumping-off point is valuable even as it evolves.

- **OAuth.** This is a standard for user-authorized access by an API client to a web API. It provides security plumbing similar in purpose to the WS-Security standard or HTTP Basic Authentication. It is becoming a key method of protecting APIs — including IAM-related APIs such as SCIM and OpenID Connect — to the level required for Zero Trust.

- **OpenID Connect.** This emerging web standard, based on OAuth, focuses on SSO, session management, and identity claims retrieval. You can think of it as a lightweight SAML protocol that enables dynamic B2E, B2B, and B2C use cases in a way that’s of particular interest to efforts such as the National Strategy for Trusted Identities in Cyberspace (NSTIC). Its proposed final specifications entered public review in December 2013, and a fifth round of interoperability testing among many implementers, including Deutsche Telekom, eBay, Google, IBM, Microsoft, Ping Identity, and others is under way. Using OpenID Connect as a starting point for integrating with small partners that don’t have SAML chops can be valuable.

- **User-managed access (UMA).** This emerging web protocol, also based on OAuth, focuses on access control by third parties to arbitrary protected web resources. The initial use cases included enabling individual Web 2.0 users to share calendars, health records, and other data and content with friends, family, and organizations. Business-related use cases include enterprise oversight of employees’ use of cloud services. You can think of it as a lightweight XACML (without the policy expression language) that enables loose coupling between authorization decision and enforcement points.
Zero Trust identity is a model, not a product. If you’re starting from scratch, you may be tempted to buy your way into Zero Trust with a cloud-identity solution, but you can benefit by applying the model even to internal applications and users. Follow these four steps to enable and leverage Zero Trust identity in support of a more agile, competitive, and secure organization:

■ **Step 1: Map identity context to your data.** Remember: Garbage in, garbage out. Apply the practices of protecting information consistently with identity context (PICWIC) to ensure that your access control hygiene is impeccable before you expect your Zero Trust identity approach to bear fruit.13

■ **Step 2: Federation-enable your organization and its applications.** If you haven’t yet, become an IdP for your workforce so that you’re ready for SSO into business partner and SaaS apps, and plot a strategy for converting your business applications into RPs to leverage your new IdP. A large professional services firm has seen federation enablement pay off even for companies that haven’t yet taken the SSO plunge with a single strategic partner or cloud app. This is because competitive pressures inevitably demand quick SSO action, and you want to be ready with an enterprise-grade solution rather than a quick-and-dirty one that suffers from security and performance holes.

■ **Step 3: Create communities of developers to increase the attraction of your IAM services.** Preparing your IAM services for loose coupling provides a means of outsourcing security logic, but creating a developer community enables you to promote this goal actively. This can take a lightweight form, such as creating and evangelizing software development kits and sample...
“hello world” code, or it can involve a formal developer forum and portal, typical for an external developer audience. API management vendor Layer 7 advises forming an internal community first as a test audience; its own API Portal product is deployed in an inward-facing fashion more than 50% of the time. Focus first on enabling developers to turn apps into RPs.

- **Step 4: Push the edge of the envelope in externalizing authorization.** Elderly on-premises apps tend to control a great deal of their own security logic, delivering the desired fine-grained authorization but in a manner that quickly becomes unsustainable in an extended enterprise. A greenfield is your best chance of building better habits: Leverage your developer community to promote outsourcing authorization decisions from new apps to a centralized API. When you just can’t wait for the natural end of a legacy app’s life, build a façade that handles translation in and out on the basis of your PICWIC data classification.

**WHAT IT MEANS**

**ZERO TRUST IDENTITY DOES MUCH MORE THAN PROTECT — IT ENABLES**

Steve Yegge’s rant uses snark to highlight the seeming contradiction between accessibility — open interfaces — and security: “Accessibility is actually more important than Security because dialing Accessibility to zero means you have no product at all, whereas dialing Security to zero can still get you a reasonably successful product such as the PlayStation Network.” As a wise person observed, however, we have brakes on our cars not so that we can stop, but so that we can go fast. To extended enterprises, organizational domains become a secondary consideration — and so their IAM strategies must respond in kind.

Zero Trust identity does more, however. Moving to the cloud and enabling BYOD entail ceding control. Zero Trust identity brings it back, in finer granularity. If your organization can’t transition to this model, it won’t be able to apportion control — and responsibility — to the correct party, whether that party is itself, an employee, a business partner, or an external service provider.

**SUPPLEMENTAL MATERIAL**

**Methodology**

Forrsights Software Survey, Q4 2013, was fielded to 2,074 IT executives and technology decision-makers located in Canada, France, Germany, the UK, and the US from SMB and enterprise companies with two or more employees. This survey is part of Forrester’s Forrsights for Business Technology and was fielded during October 2013 and November 2013. ResearchNow fielded this survey online on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates. We have provided exact sample sizes in this report on a question-by-question basis.
Forrester's Business Technographics™ provides demand-side insight into the priorities, investments, and customer journeys of business and technology decision-makers and the workforce across the globe. Forrester collects data insights from qualified respondents in 10 countries spanning the Americas, Europe, and Asia. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

**Companies Interviewed For This Report**
- eBay
- Layer 7 Technologies
- Intuit
- Quest Software (now Dell)

**ENDNOTES**


2. Source: Forrsights Telecom And Mobility Workforce Survey, Q2 2013.

3. The strong authentication landscape has undergone tremendous churn in recent years as new mobile-fueled technologies have come online and as RSA, the premier vendor of hardware one-time password (OTP) tokens, experienced a breach. See the February 3, 2012, “TechRadar™ For Security Pros: Strong Authentication, Q1 2012” report.

4. If the current trust model is broken, how do we fix it? It requires a new way of thinking. The way we fix the old trust model is we begin at the beginning and look for a new trust model. See the November 15, 2012, “No More Chewy Centers: Introducing The Zero Trust Model Of Information Security” report.

   Once upon a time, security and risk professionals had defined borders to protect — a limited and highly restricted user community — and a visible set of threats, such as worms and viruses. Today, our organizations’ functional network has extended well outside of our controllable borders. See the August 5, 2011, “Applying Zero Trust To The Extended Enterprise” report.


6. The Amazon mandate in full, as related by Yegge, was as follows: “1) All teams will henceforth expose their data and functionality through service interfaces. 2) Teams must communicate with each other through these interfaces. 3) There will be no other form of interprocess communication allowed: no direct linking, no direct reads of another team's data store, no shared-memory model, no back-doors whatsoever. The only communication allowed is via service interface calls over the network. 4) It doesn't matter what technology they use. HTTP, Corba, Pubsub, custom protocols — doesn't matter. Bezos doesn't care. 5) All service interfaces, without exception, must be designed from the ground up to be externalizable. That is to say, the team must plan and design to be able to expose the interface to developers in the outside world. No exceptions. 6) Anyone who doesn't do this will be fired.” The rant is worth reading in full. Source: Google Plus (https://plus.google.com/112678702228711889851/posts/eVeouesvaVX).
Federated identity solutions enable “identity statelessness,” which we define as follows: networked services achieving access control and personalization goals by consuming just-in-time identity data and services from authoritative sources living in other organizational domains, at the moment users and applications approach, removing the need for long-term identity data replication. See the June 3, 2011, “The ‘Venn’ Of Federated Identity” report.

IDaaS architectures provide discrete but complementary and coordinating services that enable applications and portals to perform identity and access management functions. These services can work in a standalone fashion or be chained and orchestrated in the manner of an enterprise service bus. See the April 2, 2008, “Identity-Management-As-A-Service” report.

Open Web developers tend to use a variation of the façade pattern for their applications but refine the pattern to focus on standard web formats and protocols and services delivered via the Web — so we refer to it as the open Web façade. See the January 24, 2012, “Embracing The Open Web: Web Technologies You Need To Engage Your Customers, And Much More” report.

When it comes to web-based APIs, security professionals are coming under pressure in opposite directions: 1) to reduce the number of moving security parts, and 2) to manage the exposure of more APIs to a wider range of access, more dynamically. See the July 13, 2011, “Protecting Enterprise APIs With A Light Touch” report.

The new suite of OpenID Connect and JavaScript Object Notation (JSON) Web Token specifications brings another round of standards disruption but also promises a no-compromises approach to highly distributed identity and access management (IAM). See the October 26, 2011, “OpenID Connect Heralds The ‘Identity Singularity’” report.

More information about the NSTIC program is available at The National Strategy for Trusted Identities in Cyberspace’s website (http://www.nist.gov/nstic/).

Disclosure: The author of this report founded the UMA effort and serves as the chair of the UMA working group at the Kantara Initiative.

The identity life cycle contains four critical stages where you must set up and enforce policies regarding how you grant and revoke users’ (employees’ and business partners’) access to information. The fundamental premise of PICWIC is that you should assign data to business owners at all times. See the June 27, 2011, “Your Data Protection Strategy Will Fail Without Strong Identity Context” report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world’s top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION
To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT
For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester’s subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

SEAN RHODES, client persona representing Security & Risk Professionals