Forrester's Risk-Driven Identity And Access Management Process Framework

Process: The Identity And Access Management Playbook

by Andras Cser

January 6, 2017

Why Read This Report

Identity and access management (IAM) processes have always been convoluted. They affect many people (both customers and employees), systems, and teams, and this complexity makes it difficult to protect against new or emerging threats, whether from the outside or the inside. This report describes how security and risk professionals (S&R pros) can apply risk concepts across the entire IAM process portfolio and use behavior-based trending methods to reduce security exposure, ease the burden of IAM policy management, and improve the user experience.

This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Key Takeaways

Only Risk-Based IAM Can Protect Against New And Unknown Threats

S&R pros can only formulate explicit IAM policies to deal with threats that they have identified, understand, and know how to mitigate — but new and emerging threats hit quickly, before you can fully understand them. Risk-based IAM allows security teams to identify anomalous and potentially insecure behaviors and defend against these threats.

Risk-Based IAM Alleviates Policy Management Burdens

Explicit policies containing a large number of IAM control points are difficult to formulate and expensive to manage. Risk-based IAM tracks user behavior and constantly updates user and group profiles, thereby reducing — but not eliminating — the need to maintain explicit IAM policies.

Risk-Based IAM Makes Employees Happier

Let's face it: No one likes to perform attestations or navigate around obstacles to access. Risk-based IAM makes access policy enforcement invisible, allowing employees to focus on their core job functions.

Forrester's Risk-Driven Identity And Access Management Process Framework

Process: The Identity And Access Management Playbook

by Andras Cser
with Stephanie Balaouras, Alexander Spiliotes, Salvatore Schiano, Bill Barringham, and Peggy Dostie

January 6, 2017

Table Of Contents

Notes & Resources

Forrester drew insights from numerous vendor and enterprise companies through Forrester briefings, inquiries, and primary research interviews in 2015 and 2016.

Related Research Documents

Q&A: 10 Questions To Ask Before Deploying Customer Identity And Access Management

Top 13 Technology Trends S&R Pros Should Watch: 2016

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Today's IAM Processes Are Slow To Adapt To Threats And Disruption

Traditional IAM tools have come a long way during the past five years. They integrate much better with cloud and on-premises applications and can automate identity life-cycle management processes, thus reducing identity administration costs. However, they still have several shortcomings:

- **Cumbersome IAM processes detract from customer experience.** When IAM systems force customers to authenticate repeatedly or unnecessarily, it affects the customer's experience. Customers may decide to go where they get a more pleasant security user experience.[1]
- **S&R pros can only set policies to defend against threats they know and understand.** Before they can protect against them, S&R pros must be aware of and correctly identify new zero-day threats as they emerge. With new types of malware and fraud methods appearing every day, this is an uphill battle — to put it mildly.
- **New threats require explicit coding of policies and rules and affect productivity.** After identifying a threat, S&R pros must code explicit policies to mitigate or intercept it. To prevent users from logging in from rogue countries and potentially committing fraud, S&R pros have to create and manage a list of such countries in their policies, adding new ones to the list any time a country emerges as a significant threat. Having to code explicit policies and rules puts an unnecessary burden on IAM administrators and limits the potential of digital operational excellence.[2] It also severely limits the firm's ability to do business with legitimate customers from higher-risk regions — missing out on business opportunities.
- **IAM policy management costs soar when supporting multiple user populations.** Most security teams use different IAM instances for customers, business partners, and employees. To protect against new threats, S&R pros have to design, implement, test, and maintain IAM policies in all three environments — plus the corresponding nonproduction environments. This leads to an explosion in the number of policy artifacts and the work required to keep those artifacts current.
- **There's little sharing of risk and threat information.** Stovepipes of identity management, access governance, access management, and log management policies prevent S&R pros from using threat information created in one system in another. For example, even if the access control system clearly shows that a user only accesses a certain application feature or entitlement very rarely, the access governance and recertification (attestation) system may never expose this fact to a reviewer who could consider revoking the unused privilege. Static policy management keeps companies from learning how other firms defend themselves against certain threats.
- **They can't always intercept access to cloud applications.** Users don't just access software-as-a-service (SaaS) line-of-business (LOB) applications via the corporate network; they also use personally owned devices to do so from off-premises locations like coffee shops and home offices. As a result, access controls implemented as an on-premises federation or single sign-on (SSO) system — or even as a cloud SSO portal — may have trouble enforcing access policies and

tracking user activity.[3] Identity administration and policy management tools are notoriously difficult to integrate with SaaS LOB applications. While cloud data protection solutions provide some level of discovery of nonsanctioned SaaS applications, they do not yet address access risks.[4]

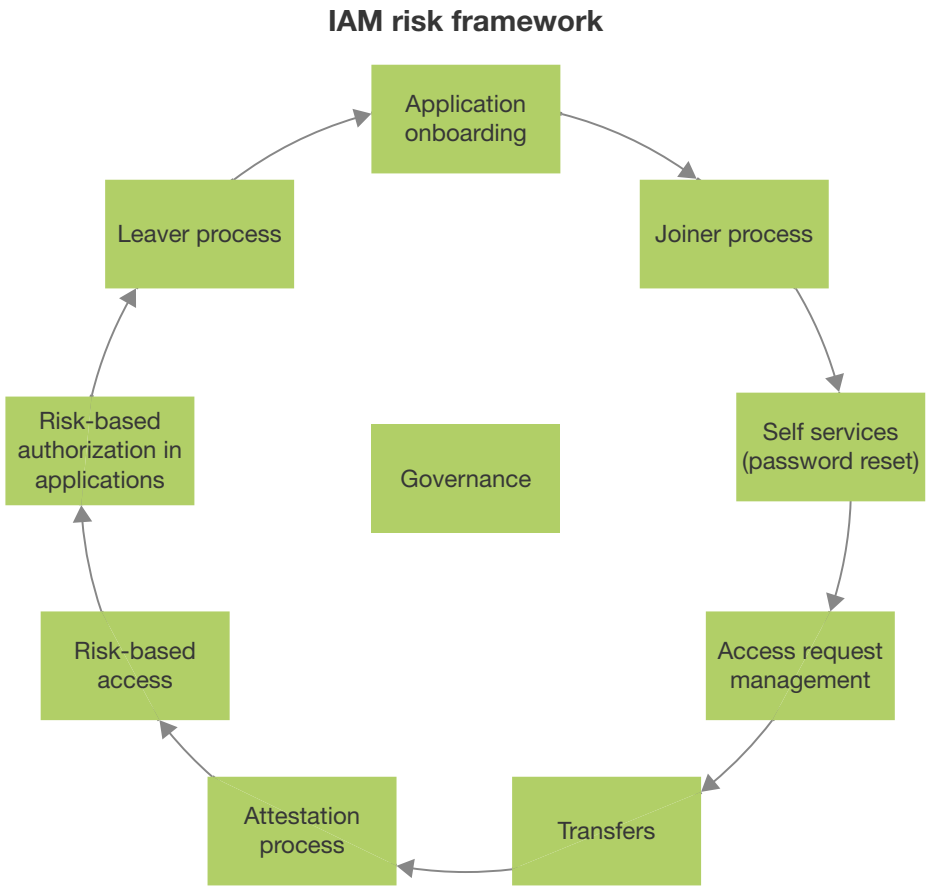
Introducing The Forrester Risk-Based IAM Process Framework Tool

To mitigate the above issues and provide better, holistic, layered controls, Forrester proposes a risk-based IAM approach. That said, understanding a broad overview of the IAM risk-based processes is also a key component in effectively utilizing our suggested framework tool (see Figure 1). This framework provides a simple, coherent self-assessment; based on the gaps it identifies, an organization can (re)define its risk-based IAM processes and manage identity and access risk more effectively. This tool:

- **Provides a comprehensive look at risk across various tasks in IAM processes.** Assessing risk in some processes but not others may leave holes in a company's defense strategy. For example, a firm may use network fraud management or risk-based authentication (RBA) for customer access but not for registration, or it may understand risks around the joiner process but not look at the attestation or mover process. You should follow identity and access life cycles from cradle to grave — not only for on-premises applications, but also for SaaS LOB applications.
- **Encourages collaboration between marketing and security.** Customer-facing IAM processes have long included risk-based IAM approaches and tools such as RBA and back-end transaction fraud monitoring.[5] Forrester clients have made it clear that they want the teams responsible for external-facing customer IAM (security, marketing, customer contact center, fraud) and those responsible for internal workforce IAM (security, HR, application developers, help desk) to share their experience and knowledge with each other. This is in response to customer-facing IAM and verification methods and tools being increasingly sought after for internal IAM as well. Specific CIAM solutions, such as Gigya, ID.me, Janrain, SheerID, Socure, and Stormpath, also offer risk concepts (IP address geolocation, user identity verification) in their policy definition features.
- **Enhances communication between risk-based measures and policies across IAM.** Based on contextual information and identity relationships, each IAM process should have an automatically generated risk score associated with it. Our model encourages S&R pros to think through how risk scores propagate among the various processes and tools. In the light of past data breaches, security teams increasingly draw data from cyberthreat intelligence solutions.[6]
- **Allows S&R pros to look at context beyond a single transaction.** As risk-based, behavioral methods and techniques almost always require building an identity and peer group profile, by definition, risk-based IAM has to look at the past behavior of the user and his or her peer group to assess whether the observed current behavior is anomalous. IAM tools, especially for access governance, can ingest security information management (SIM) information and intelligence.

› **Directs customers to vendors with built-in automatic IAM risk-scoring capabilities.** Creating risk scores automatically throughout all IAM processes allows S&R pros to focus on enhancing their risk-scoring algorithms rather than manually creating risk scores. S&R pros should ask vendors how they support true automatic risk score generation; preferably, they will use statistical algorithms and rely only minimally on defining and maintaining rule sets.[7] Security user behavior analytics (SUBA) solutions such as E8, Exabeam, and Securonix provide excellent linked context between identity activity and network traffic.[8]

FIGURE 1 Step Through An IAM Risk Framework



Infuse Every IAM Process With A Concept Of Risk

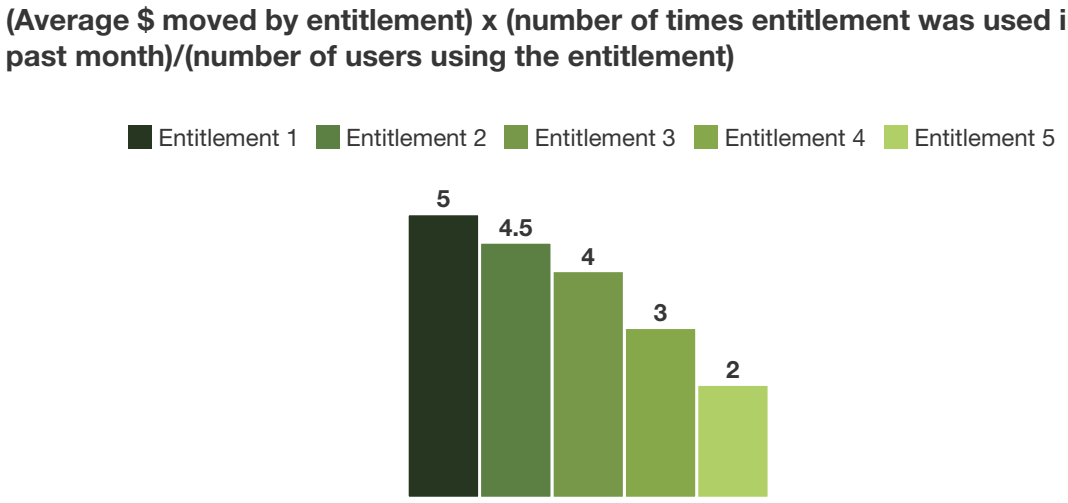
Risk-based concepts in IAM are quickly becoming ubiquitous: Most identity management and governance (IMG) vendors offer some level of machine-learning-based risk assessments in their provisioning and attestation solutions.[9] Modern IMG solutions allow you to look at the whole IAM life cycle from the identity's creation to the "death" or deletion (or disabling) of the identity.

Create Priorities For Application Onboarding

Onboarding applications into the risk-based IAM framework requires disciplined thinking. S&R pros must:

- **Create application priorities.** S&R pros should prioritize applications according to the value of data stored in them, the difficulty of managing identities and their entitlements in them, and the difficulty of managing access (authentication and authorization) in them.
- **Create a static proxy metric for application financial risk.** Scoring the financial risk of an application should be an automated, clear-cut, and objective process. While it's difficult to automate, Forrester recommends creating a metric that's a proxy of risk. Look at how many people are moving how many dollars in the application, and multiply the two figures. The higher the value, the riskier the application is financially. Then create a frequency chart of financial risk in the application (see Figure 2).[10]
- **Create a dynamic proxy metric for overall risk.** Using a SUBA or cloud security gateway (CSG) solution helps you figure out who is accessing which on-premises and cloud application from where, how much data they normally download and when, etc. These solutions also prioritize their findings and attach risks factors to applications as well as to people. Using a historical and current view of these dynamic application risk trends also helps to determine application risk.
- **Factor in compliance criticality.** Data breaches are not just bad for goodwill and customer retention but raise compliance questions as well. If the application falls under a major regulatory compliance mandate that your organization must follow, it should definitely be higher on the application onboarding priority list. If the application is in the cloud, consider using Forrester's Cloud Security Compliance Checklist.[11]

FIGURE 2 Use A Frequency Chart To Prioritize The Riskiest Application Entitlements



Base: 42 IT decision-makers
Source: Forrester/University Of British Columbia Access Certification Survey 2013

Vet Users And Limit Privileges In The Joiner Process

It all begins with who S&R pros allow to access applications. Forrester's interviewees emphasized that, in a risk-based joiner process, you should:

- **Realize that your identities are only as strong as your vetting process.** If you don't conduct background checks on employees and identity verification on customers (using data and solution providers such as Equifax, Experian, IDology, LexisNexis, or TransUnion), or if you don't have a knowledge-based authentication (KBA) process for customers that already have a relationship with the company, the identities you onboard may very well be fraudulent or synthetic — something you definitely want to avoid. Even Facebook or LinkedIn profiles can be used to predict job performance (one of the reasons Microsoft acquired LinkedIn) — use them![12]
- **Understand the concept of least privilege.** In theory, the fewer rights and entitlements that users have in applications, the lower the likelihood of separation-of-duties violations, data breaches, sanctions, and fines. However, in reality, users need entitlements to do their jobs, and giving them too few can cause frustration. It's a good idea to understand how existing users in similar job roles use their entitlements and to use trimmed-down roles to grant new users access only to those entitlements they're likely to use. SUBA solutions such as Bay Dynamics, Feedzai, Gurucul, NuData Security, and Securonix help with finding common least privileges, as do newer IMG and privilege identity management (PIM) tools from almost all vendors.[13]

› **Get data from your attestation platform to score the risk for all new access requests.** Managers and new employees often request too much access — or request that they get a copy of an already overprivileged user's entitlements. To limit the number of overprivileged users due to user profile copying, create a risk score for a joiner access request form based on the aggregate risk score of the requested entitlements and what privileges the new employee's peers have. Then provide this risk score and any red flags to the approvers — such as managers, application owners, and help desk personnel. This process is equally applicable for business and privileged users.

Assign Risk Scores To Every Self-Service Task

Self-services like user ID and password recovery and security profile updates are important tasks that have usually been fairly static: Answer your security questions correctly and — voilà! — you can reset your password. Forrester recommends that companies shift their authentication mechanisms from static methods to risk-based methods in the following ways:

› **Extend adaptive authentication mechanisms to risk-score self-services.** Treating answering security questions with the same level of risk awareness as users actually entering their passwords is a great start. You can use your existing RBA tools to cover all self-service entry points.[14] Be sure to review the rules and statistical models to ensure that a tool can cover this use case adequately and won't provide false positives. Geofencing this task or using geographical context like geolocation from browsers or mobile apps can also contribute to a reliable risk assessment.

› **Assign risk scores to transactional information to authenticate users.** Companies have long used transactional data to authenticate users in customer-facing KBA — such as, "How much was your last deposit?" or "What was the amount of your last bill?" Employee- and partner-facing IAM now use similar questions — such as, "With whom do you have a standing meeting on Tuesdays at 3 p.m.?" — that are based on knowledge of the user's work environment rather than relying on purely static information like employee number, cubicle number, or hire date.

› **Vary the data fields you use to authenticate users.** To manage fraud caused by an employee committing occupational or internal fraud — such as accessing other employees' accounts or collecting data without authorization — don't always ask the same questions at the help desk to authenticate users. Vary the knowledge-based questions or ask for a character or digit from a different position of a verbal password. Consider replacing traditional security questions and answers with KBA or asking the customer for transactional data, such as, "What was the range of your electric bill in the past 12 months?"

› **Look beyond the single transaction.** Self-service transaction risk is also a function of the user's behavior in the online channels (web, mobile, app, etc.): If a user behaved erratically online before a self-service transaction (i.e., navigating on the website in a suspicious manner before trying to perform a self-service transaction), then the risk level of the transaction should also be high. As with enterprise fraud management, where each channel understands a user's actions on other

channels, a risk-based self-service application should know about the user's transactions on the other channels. When the user is requesting a phone-based password reset, the phone application should be aware of the user's other recent self-service requests.

Access Request Management Should Always Look At Context And Identity Relationships

Access request management is the automated process of submitting forms and workflow items in an IAM or help desk system and routing these requests to managers and application owners for approval. To imbue risk concepts into the access request management process, S&R pros need to:

- **Risk-score every access request and approval item.** When creating risk scores, many companies look at the monetary value of the requested entitlement, the number of users with the entitlement and what job roles they have, the location from which the request was submitted, and the risk associated with the data to which the requested entitlements will provide access. Using a glossary and description of entitlements to put it into a business context will also help the reviewer.
- **Preventively detect separation-of-duties violations.** When looking at a user's shopping cart, the workflow should proactively detect separation-of-duties violations between the entitlements that the user requested. Some organizations told Forrester that they don't allow users to select conflicting entitlements at all. Separation-of-duties violations should also be dynamic. For example, the sensitive, high-risk entitlements needed to perform the duties of an accounts receivable clerk should conflict with the sensitive, high-risk entitlements needed by an accounts payable clerk — even if the lower-level entitlements for the two roles do not conflict.
- **Provide as much contextual and risk score information as possible at runtime.** Help the approver understand the context of the request by translating a risk score into approval items marked red, yellow, or green based on risk factors such as how many other users on the team have the requested entitlement, how and when they use the requested entitlement, and why the requested entitlement has been revoked from users in the past. This will help the reviewer spend much less time on reviews, allow him to make the right decision, and not grant unnecessary privileges to users. Show him a user's previous requests and whether those were approved or rejected to provide even more context.
- **Watch for signs of collusion.** If a user has a relationship (peer or hierarchical) to another user who is already involved in confirmed internal fraud, or if a user requesting risky privileges is related to another user who already has excessive privileges, it means that the identity management and governance platform should raise the requestor's risk score and warn approvers accordingly.
- **Watch the guards.** It's not unheard of to have a fraudulent approver in the organization, someone who grants highly sensitive entitlements to a user in a collusion scheme or fraud ring. Understanding how reviewers approve entitlements will help flag outliers and prepare S&R professionals, internal fraud management, and compliance departments to ask the right questions or launch an investigation. When it comes to data protection in SaaS cloud applications, bring your own data protection platform and key management.[15]

Transfers Should Highlight Risk Of Accumulated Entitlements

When employees transfer or move between jobs, they should lose the entitlements and data access associated with their old role and gain new ones tied to the new role. In reality, many organizations let users change jobs without ever looking into or truly understanding the entitlements they've accumulated or allowing excessive overlap periods (over 90 days) for the user to keep both their old and new set of privileges. This results in very excessive user entitlements and separation-of-duties violations: Old access rights the user had for the old job conflict with new access rights he or she acquired for the new job. Here's how using risk concepts during the transfer process can help limit exposure:

- **For all transfers, create a risk score based on old and new job roles and entitlements.** This is especially useful if the user is leaving a job that carries more risk than the new one. Creating a risk score by looking at the entitlements and data for both the old and new position immediately helps frame the conversation and set the urgency with which the company should revoke the access rights associated with the old position. Some teams automatically increase the risk score of users who have a lot of entitlements or who are related to other users who have a lot of entitlements or who work in positions where their access to data represents a high risk such as finance or HR. CA Technologies, RSA/Aveksa, SailPoint, and Savyint can help formulate risk scores without administrator intervention.[16]
- **Spawn an automatic access recertification or attestation campaign on all transfers.** Risk scores are of limited value if no one acts on them. Creating an automatic attestation and self-attestation campaign with the risk scores and routing it to the new manager and application owners, as well as to the moving employee himself, helps create an informed access review of the moving user, and it reduces the likelihood that the user will collect entitlements during his tenure in the organization.
- **Look at data asset risks, not just entitlement risks.** Even organizations that have an excellent understanding of application entitlement risks often make the mistake of omitting data risks. Data governance solutions like Imperva or Varonis Systems can help establish the common pathways and patterns of data access; the IAM user account provisioning system can use these inputs to automatically define and update the data-associated risk scores. These solutions increasingly help with out-of-the-box machine learning algorithms to define risk of data assets based on the assets' use.

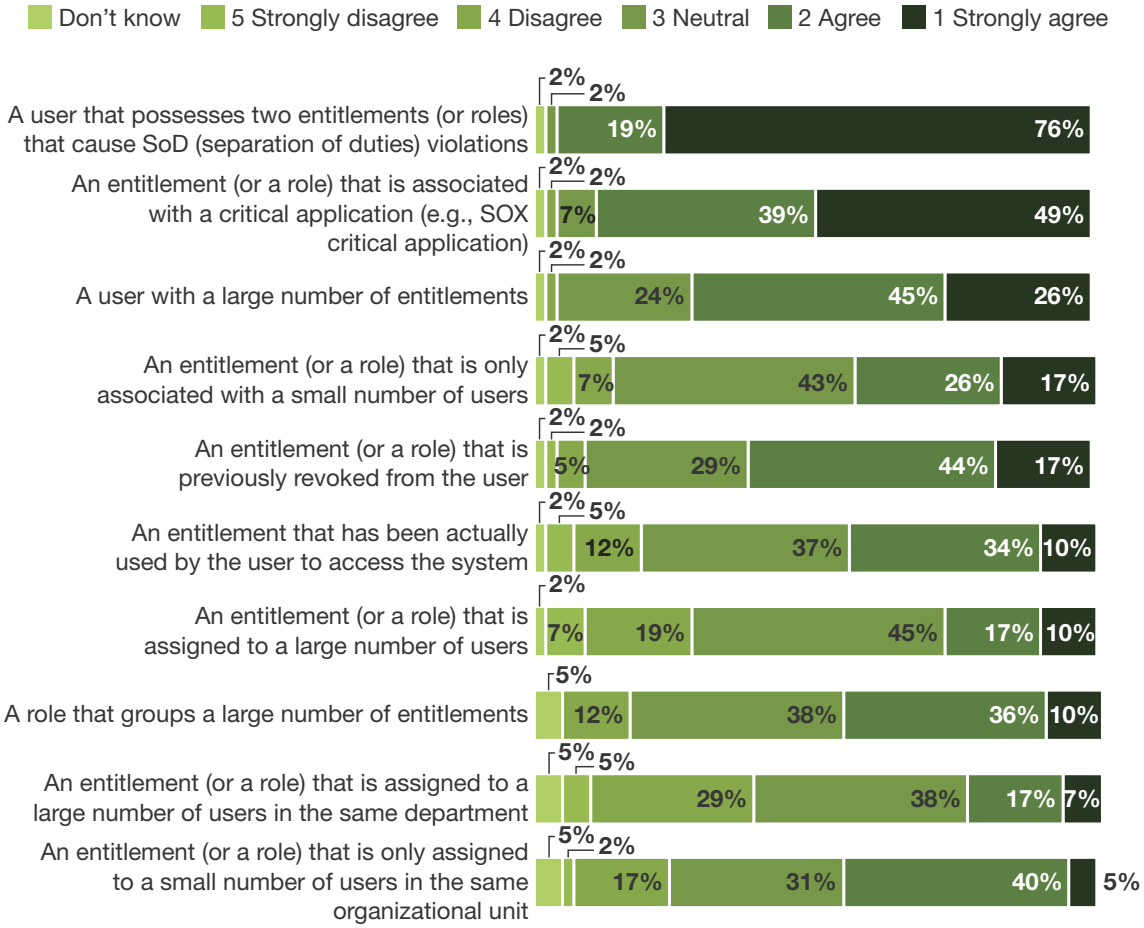
Well-Described Roles And Entitlements Are A Must For Understanding Attestation Risk

The most effective and direct way of controlling users' burgeoning access to application entitlements and data assets is a periodic attestation campaign, including access review, identity audit, and access (re)certification. In this quarterly, semiannual, or annual process, the users themselves, managers, application owners, compliance personnel, and others review and assess the risk of each user's application entitlements and data access and make a call on whether the user can keep the entitlement moving forward. A survey conducted by the University of British Columbia found that there are several key metrics to look at when determining how risky a user's access is (see Figure 3):[17]

- **A list of the enterprise job roles and application roles the user is assigned to.** Ideally, a user should only be a member of one enterprise job role, but this isn't always the case in reality. What's more, many companies have not implemented an enterprise role system, meaning that users are often directly placed into application-level, functional IT roles. Some roles' functions, such as approving a pay raise in an HR application or making a large payment in a corporate banking application, carry a higher risk, and this should be reflected in the risk score that membership in the role assigns to a member.
- **A list of the user's entitlements.** The sheer number of entitlements that a user has is a clear indicator of risk. However, conversations with Forrester clients reveal that users — especially in knowledge worker positions — sometimes need many entitlements to do their job well. This is why it's important to discover risky entitlements and assign risk scores to them.
- **A description of each entitlement.** Reviewers need a business-language definition of what entitlements really mean. Creating a dictionary of what various attributes and their values mean in layman's terms — for example, "Active Directory group ESAP0123 means that the user has write access to the enterprise resource planning system's general ledger" — will provide a lot of background and help the reviewer make an informed decision.
- **The criticality and risk of each entitlement.** This is the hardest problem to solve. S&R pros need to perform an automatic risk discovery and assignment process for each entitlement and refine the results. And not all entitlements are created equal: You have to understand the fiscal risk and value of each entitlement and imbue the attestation process with this information. Modern access governance tools, such as Avatier AIMS, CA Technologies GovernanceMinder, Courion ComplianceCourier, Oracle Identity Analytics, RSA Aveksa (an EMC company), and SailPoint IdentityIQ will help automate this process.

FIGURE 3 Indicators Of Risk During Certification

"Assume you are reviewing and validating possession of an entitlement (or assignment of a user to a role in case of role-based access control) during access certification. How much do you agree that each of the following observations is an indication of risk?"



Base: 42 IT decision-makers (percentages may not total 100 because of rounding)
Source: Forrester/University Of British Columbia Access Certification Survey 2013

Use Layered, Risk-Based Methods To Control Access

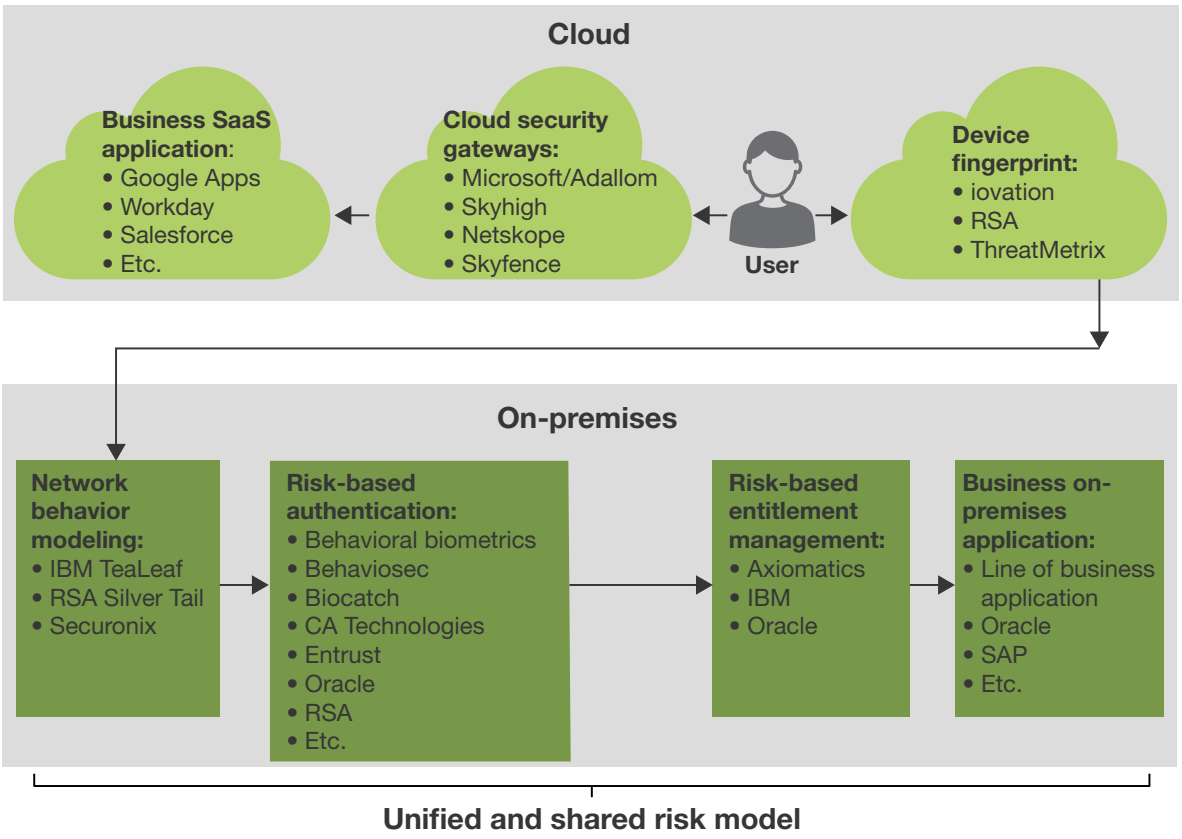
Third-generation risk-based access controls are on their way to replacing legacy first- and second-generation two-factor access control and authentication systems. Why do we see this trend? It's simple: As the use of mobile devices expands, the old-style "Let me send a text message with a one-time password (OTP) or push notification for two-factor authentication to your mobile phone"

methodology is of limited value; it's no longer out of band. The endpoint that accesses a mobile app is the same endpoint at which the user receives the OTP — hence the need for risk-based access controls. Forrester sees the following technologies emerging to mitigate this problem:

- **Cloud security gateways detect risky behavior.** Vendors like Bitglass, Cisco/CloudLock, Imperva/Skyfence, Microsoft/Adallom, Netskope, Skyhigh Networks, and Symantec/Blue Coat offer solutions that intercept API calls and also proxy corporate user authentication and network traffic and look for suspicious patterns while a user is using a SaaS business application like Google Docs, Salesforce, or Workday. Most of these solutions allow discovery of SaaS applications, offer self-learning and unsupervised baseline building, and monitor and alert for suspicious behavior.[18]
- **Network behavior modeling understands and risk-scores network access patterns.** Solutions from IBM Tealeaf, NuData Security, RSA Silver Tail Systems, and Securonix intercept mainly HTTP and HTTPS traffic and build a baseline of normal access patterns on a website or in a mobile application over the past 1 to 4 hours. If the solution sees anomalies in timing (for example, a robot can access different areas of the site much faster than a human can) or access sequence (a sure sign of site-scraping or botnet activity), then it alerts the administrators and can optionally block access.
- **Device fingerprinting solutions score the risk and reputation of endpoint devices.** Solutions from vendors such as BlueCava, Experian/41st Parameter, iovation, Kount, and ThreatMetrix — often with a fraud management pedigree — and open source solutions like ViewWho — are mostly customer-facing SaaS, but enterprises increasingly want to employ them to create device reputation and risk scores for their employees. Many RBA vendors also offer device fingerprinting mechanisms. The benefit: improved tracking of fraudsters' and cyberattackers' devices and the ability to create a stronger layer of defense against them.
- **RBA factors context into increasingly continuous authentication . . .** Traditionally, solutions like CA Risk Authentication, Entrust/DataCard IdentityGuard, IBM Verify, Oracle Adaptive Access Manager, and RSA Adaptive Authentication looked at IP address geolocation, distance traveled (if a user logged into the website 10 minutes ago from China and now they're logging in from the US, that's definitely suspicious behavior), device fingerprint, and time of day to create a risk score around authentication. More recently, these solutions, and new vendors' solutions (Behaviosec, Biocatch, NuData, etc.), have gained the ability to look at these context and behavioral indicator variables as well as behavioral biometrics (how the user holds the device or swipes the screen) continuously during the user's session and terminate risky sessions or transactions. Increasingly, Forrester clients also ask about using RBA for employee-facing and partner-facing authentication, not just customer-facing use cases.[19]
- **. . . uses the concept of high-risk transactions for additional authentication . . .** Understanding which transactions are high risk and high reward is critical when trying to protect them. Using RBA to define a risk score around the transaction, not just at login, and then prompting the user for additional authentication credentials if the risk score exceeds a certain threshold will provide additional protection for these transactions.[20] If you monitor how user profiles' risk scores change over time, you can create additional user segments to further refine the risk-scoring environment.

› **. . . and actively shares access-control risk scores.** Most RBA solutions can import or consult external data as an input to the risk score they generate. Creating a network of cloud interception solutions, network behavior modeling, device fingerprinting, and RBA through which risk scores can propagate will coordinate those scores for layered defenses (see Figure 4).

FIGURE 4 Layered Defenses In Risk-Based Authentication Solutions And Cloud Services



Look At The Amount Of Money Moved When Defining Risk During Authorization

Risk-based authorization in applications tries to mitigate the problem of defining least privileges in a knowledge worker environment. Instead of limiting the user's ability to do her job by revoking privileges during attestation campaigns, risk-based authorization subscribes to the notion that under normal circumstances, this user — working at her desk, during normal business hours, performing a routine sequence of transactions — should be able to use all entitlements to get her job done. However, if she transacts from a risky location, outside of normal business hours, or out of her normal sequence,

entitlements may not be available and the application may temporarily not grant them to her, but instead ask her to apply for authorization from her supervisor or to move to a less risky location. Risk-based authorization can be difficult because:

- **Applications may cache user repository attribute values that define entitlements.** Even if your risk-scoring mechanism can figure out which attributes it needs to change to ratchet down user permissions, doing so in real time is not that easy. A lot of commercial off-the-shelf (COTS) and in-house-built applications cache user store attribute values at startup, making dynamic changes to entitlements at runtime difficult.
- **Entitlement management platforms' policy definitions lack the concept of risk.** Apart from providing little or no support for COTS applications, today's entitlement management systems provide little ability to look at risk scores from other environments and tools.[21] Entitlement management platforms come into play mainly when replacing or refactoring in-house-developed on-premises applications.
- **Entitlement risk definition requires careful planning, automation, and normalization.** Our interviewees proposed a simple calculation for automated entitlement risk assessment. It defines the risk of an entitlement as the average number of dollars that the user moves multiplied by the number of times that the entitlement has been used in the past 31 days divided by the number of users using it. This gives the average value of the entitlement in the past 31 days, which correlates closely with the risk the entitlement represents. To focus on controlling these entitlements (in terms of attestation, provisioning, and dynamic entitlement management), financial services companies (banks) have created a frequency chart of the riskiest entitlements.
- **Network-level entitlement management allows for minimal invasion in applications.** Vendors like BayShore Networks and Cisco Systems (through its acquisition of Rohati and, more recently, CloudLock) can intercept access to resources and apply policies. Forrester expects that SaaS traffic interception vendors like Microsoft/Adallom, Netskope, Skyfence/Imperva, and Skyhigh Networks will also help proxy traffic to on-premises applications and effectively apply risk-based entitlement policies.

Ensure You Factor In Risk Of Shared Accounts In The Leaver Process

In theory, the leaver process is simple: S&R pros need to revoke entitlements and access rights from a departing user. Typically, it begins with disabling the leaver's network (cloud or Active Directory) access. However, if the leaver has shared his application-specific user ID and password with someone who stays, then the company needs to know about it and disable the leaver's user ID across all applications. Usage patterns for application entitlements, web SSO, federation, mobile applications (OpenID, OpenID Connect) eSSO, and cloud-based IAM systems are an excellent way to understand the risk of shared credentials and help set the priorities for disabling the leaver's access rights across affected applications. Static and dynamic application entitlement risk scores can also help define priorities and focus on where the leaver's credentials need to be disabled or terminated.

Recommendations

Governance Is Key To Imbuing Business Processes With Risk

Getting risk concepts into IAM processes is no small task. At a minimum, S&R pros must:

- **Engage application developers.** While using an XACML-based entitlement management platform may not always be a reality, application developers need to create hooks that allow their applications to consume external risk scores and dynamic entitlements. If at all possible, create a checkpoint in your in-house secure application coding standards to mandate this.
- **Understand and quantify the administrative and business benefits of risk-based IAM.** Nothing beats a good business case. Try to quantify the avoided costs of managing long lists of explicit policies across multiple applications and environments. Factor in the lessened burden of attestation reviews on managers and application owners as well as the improved ability of users to fully realize their potential by not being hampered by too few entitlements in applications.[22]
- **See how you can exchange risk scores with your cloud providers.** Many cloud SaaS providers, such as Amazon Web Services, IBM, Microsoft, and RSA, already offer risk-based concepts in their platforms and portfolios. Adopting and building on these risk-based concepts is easier than building a risk-based IAM framework on your own from the ground up. CSG solutions help a great deal with this as well.
- **Look at risk-based IAM as a sequence of processes.** Tools for risk-based access and attestation are readily available. It's wise to start with those areas and expand into others as you master the concept of risk-based IAM.
- **Include access policy governance and enforcement of privileged identity management.** Privileged access is often behind data breaches: Hackers can wreak the greatest havoc and steal the maximum amount of data if they compromise root and administrator accounts. New privileged session monitoring (PSM) solutions (Balabit, BeyondTrust, CA/Xceedium, CyberArk, ObserveIT, and Wallix) have been innovating to provide ongoing risk scores of admin users based on their privileged user activity. Controlling privileged access, periodically reviewing who has sensitive access to infrastructure and applications based on how risky data is stored in those applications, goes a long way toward reducing the risk around privileged access.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iPhone® and iPad®
Stay ahead of your competition no matter where you are.

Supplemental Material

Survey Methodology

Forrester Research collaborated with two researchers from the Laboratory of Education and Research in Secure Systems Engineering at the University of British Columbia in 2013 on a research project focused on identity and access management tools in organizations. Forrester Research and the University of British Columbia fielded an online survey titled "Forrester/University Of British Columbia Access Certification Survey 2013." This survey was fielded online in 2013, and we received 42 anonymized responses. The respondents' participation in this study was entirely voluntary.

Endnotes

[1] Customer identity and access management (CIAM), if done well, can help business owners achieve increased customer engagement and sustained brand loyalty while maintaining customers' security and privacy. For the considerations to take into account, see the Forrester report "Q&A: 10 Questions To Ask Before Deploying Customer Identity And Access Management."

[2] Your customers, your products, your business operations, and your competitors are fundamentally digital. While 74% of business executives say their company has a digital strategy, only 15% believe that their company has the skills and capabilities to execute on that strategy. A piecemeal strategy of bolting on digital channels or methods is no longer sufficient. Instead, you must think of your company as part of a dynamic ecosystem of value that connects digital resources inside and outside the company as needed to compete. You must harness digital technologies, both to deliver a superior customer experience and to drive the agility and operational efficiency you need to stay competitive. For more information, see the Forrester report "The Future Of Business Is Digital."

[3] While cloud security gateways (CSGs) provide visibility into cloud application traffic, they are often limited to line-of-business cloud apps only accessed from corporate owned or managed devices. For the eight most significant CSG vendors in the space, see the Forrester report "The Forrester Wave™: Cloud Security Gateways, Q4 2016."

[4] Security and risk (S&R) professionals must protect data that business and technology management leaders store in cloud services — services that they have little control over or visibility into. However, even though companies may transfer sensitive data to the cloud, they cannot transfer liability. They remain the data custodians legally mandated to protect data they collect, process, and store — regardless of its location. Security and privacy concerns remain the biggest inhibitor to cloud adoption. As a result, cloud providers have begun to offer enhanced security features and new capabilities to enforce data residency. However, many security teams and their CIOs remain uncomfortable having to trust and rely on the cloud providers' capabilities. Thus, a new crop of startups has emerged, hoping to empower S&R pros with their own tools for visibility and control of their cloud-resident systems and data. For more information, see the Forrester report "Market Overview: Cloud Data Protection Solutions."

[5] Forrester conducted two extensive Forrester Wave reports to help security professionals find the right solution for their authentication requirements and fraud management initiatives. See the Forrester report "The Forrester Wave™: Risk-Based Authentication, Q1 2012" and see the Forrester report "The Forrester Wave™: Enterprise Fraud Management, Q1 2016."

[6] Cyberthreat intelligence (CTI) has emerged as a potentially powerful tool for S&R professionals who must defend their digital business from cybercriminals seeking to disrupt their operations and steal their most valuable information — their customers' data and their intellectual property. CTI promises to give S&R pros advance warning of cybercriminals targeting their region, their industry, or even their specific firm — with enough time to do something about it. Investors are eager to capitalize on the strong demand for CTI solutions and services: Since October 2014, CTI vendors have raised $102.5 million, and there have been three acquisitions. The vendor landscape is overwhelming, and S&R pros must separate fact from hype when it comes to investing in CTI offerings. For more information, see the Forrester report "The State Of The Cyberthreat Intelligence Market."

[7] Forrester evaluated nine vendors across 16 criteria in order to help S&R professionals find the right partner for their enterprise, business-to-business, and consumer-facing IAM deployments. For more information, read the risk-based criteria from the following Forrester report. See the Forrester report "The Forrester Wave™: Identity And Access Management Suites, Q3 2013."

[8] Security user behavior analytics (SUBA) solutions promise to provide security and risk professionals with a unified view of employee activity across networks, devices, and apps and the ability to detect suspicious activity — quickly. For an overview of critical capabilities, see the Forrester report "Vendor Landscape: Security User Behavior Analytics (SUBA)."

[9] Identity management and governance (IMG) solutions give security and risk (S&R) pros the ability to provision all users with the appropriate level of access to critical applications and systems, thereby minimizing the risk of users with excessive privileges or orphan accounts which hackers frequently target to exfiltrate sensitive data. In our 17-criteria evaluation of IMG providers, we identified the nine most significant and researched, analyzed, and scored them. To see who the lead the pack, see the Forrester report "The Forrester Wave™: Identity Management And Governance, Q2 2016."

[10] Source: "Base SAS Glossary," SAS (http://support.sas.com/documentation/cdl/en/mastergl/62860/HTML/default/viewer.htm#glossary.htm).

[11] In the swift adoption of cloud technology, assessing a cloud provider's security is sometimes an afterthought, an undertaking for which sufficient time and resources don't exist. But these cloud providers are assuming responsibility for the delivery, availability, and, possibly, recovery of your data. This requires a level of scrutiny that is proportionate to the type of data and services being supplied. This checklist can help S&R professionals validate their approach to security and risk management controls of cloud providers by making sure they have not overlooked key areas of concern. For more information, see the Forrester report "The Forrester Cloud Security Compliance Checklist."

[12] Source: Aaron Sankin, "Facebook Profiles Can Predict Work Performance," Mashable Asia, April 17, 2014 (http://mashable.com/2014/04/16/facebook-profile-work-performance/).

Social identity and eligibility verification (SIDEV) vendors such as ID.me, SheerID, and Socure help with matching the user's attributes against the user's digital exhaust on social media (Facebook, LinkedIn, etc.) to risk-score the user's asserted attributes' match to a real human. For more, see the Forrester report "Breakout Vendors: Social Identity And Eligibility Verification (SIDEV)."

[13] Forrester has conducted Forrester Wave evaluations on both identity management and governance (IMG) providers and privileged identity management (PIM) providers. To read about the vendors who came out on top and what their differentiating factors are, see the Forrester report "The Forrester Wave™: Identity Management And Governance, Q2 2016" and see the Forrester report "The Forrester Wave™: Privileged Identity Management, Q3 2016."

[14] Forrester evaluated seven enterprise fraud management vendors across 15 different criteria to help security professionals select the right partner for their fraud management initiatives. For more information, see the Forrester report "The Forrester Wave™: Enterprise Fraud Management, Q1 2016."

[15] Security and risk (S&R) professionals must protect data that business and technology management leaders store in cloud services — services that they have little control over or visibility into. However, even though companies may transfer sensitive data to the cloud, they cannot transfer liability. They remain the data custodians legally mandated to protect data they collect, process, and store — regardless of its location. Security and privacy concerns remain the biggest inhibitor to cloud adoption. As a result, cloud providers have begun to offer enhanced security features and new capabilities to enforce data residency. However, many security teams and their CIOs remain uncomfortable having to trust and rely on the cloud providers' capabilities. Thus, a new crop of startups has emerged, hoping to empower S&R pros with their own tools for visibility and control of their cloud-resident systems and data. For more information, see the Forrester report "Market Overview: Cloud Data Protection Solutions."

[16] Identity and access management (IAM) professionals need to protect information and prevent unauthorized users from accessing business-critical systems in an increasingly complex IT environment. They must not only control employee access but also enable the extended enterprise to share data and intellectual property securely despite an ever-increasing variety of user-owned consumer devices. Identity intelligence connects fraud management, data protection, and IAM processes using pattern recognition, allowing S&R professionals to not only stay ahead of fraudsters but also generate tangible business benefits by turning actionable identity intelligence into business intelligence. For more information, see the Forrester report "Actionable Identity Intelligence Protects Big Data And Zero Trust Identities."

[17] Source: Forrester/University Of British Columbia Access Certification Survey 2013.

If you have questions or comments about this survey, please contact either of the research team members: Pooya Jaferian, Ph.D., (pooya@ece.ubc.ca); or Konstantin Beznosov, associate professor (beznosov@ece.ubc.ca), from the Laboratory of Education and Research in Secure Security Engineering, University of British Columbia.

[18] As companies move their workloads and data to the cloud, the question is no longer "Should we move our data to the cloud?" but rather "What security precautions should we take to move our data to the cloud?" For a comprehensive assessment of the top CSG providers, see the Forrester report "The Forrester Wave™: Cloud Security Gateways, Q4 2016."

[19] Behavioral biometrics continuously monitors user behavior, such as typing speed, mouse movements, and touchscreen interactions, to build a baseline profile from which security and risk professionals can identify and intercept suspicious activity. For an overview of behavioral biometrics vendors and their capabilities, see the Forrester report "Vendor Landscape: Behavioral Biometrics."

[20] Traditional authentication-related solutions are no longer a good enough standalone function for the changing populations and user interaction channels. As such, emerging authentication-related solutions are becoming more popular in order to address the usability, deployability, and security needs of a business. For more details on authentication and access management, see the Forrester report "Market Overview: Employee And Customer Authentication Solutions In 2013, Part 1 Of 2" and see the Forrester report "Market Overview: Employee And Customer Authentication Solutions In 2013, Part 2 Of 2."

[21] Entitlement management solutions are maturing in the market and likely to become more integrated into IAM and DLP in the long term. For more information, see the Forrester report "Market Overview: Entitlement Management."

[22] Anything is better than manual IAM processes. Forrester found, without looking at net present values and evaluating IAM costs for three years, that build-your-own, COTS, and IDaaS solutions provide triple-digit ROI percentages over manual IAM processes. For a full comparison, including an Excel tool which calculates ROI, see the Forrester report "Making The Business Case For Identity And Access Management."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

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.