ADAPTIVE IAM: DEFENDING THE BORDERLESS ENTERPRISE

Digital identities move to the front lines in the battle for cyber security.

May 2013

SUMMARY OF KEY POINTS

Identity and Access Management (IAM), an established part of most information security programs, is attracting renewed interest as a way to secure today's borderless enterprise. As an organization's employees become the front line of cyber attacks, IAM systems must become the front line of defense: an adaptable, dynamic, situational perimeter for the borderless enterprise.

IAM solutions will evolve over the next couple years in two key ways:

1. IAM systems will patrol a dynamic, situational perimeter for the borderless enterprise, enforcing security wherever users interact with corporate data and resources. Security measures morph with the transaction, the parties and the value of data and assets in play.
2. Adaptive IAM systems draw on data from hundreds or even thousands of sources to conduct risk assessments of user behaviors and access requests. When suspicious activities are detected, next-generation IAM solutions stop users in their tracks with "stepped up" authentication or authorization requirements that users must satisfy before they can continue.

Contents

Security's "New Normal": The Borderless Enterprise and Advanced Threats 3
IAM Must Be Reinvented to Stay Relevant in Security 3
- Virtual population growth and duplicate identities 3
- Users expect greater convenience 4
- Extensibility to cloud and mobile platforms 4
- Difficulty in discerning deception 5

Adaptive IAM Secures the "Perimeter" of the Borderless Enterprise 5
- Rich user profiles 5
- Big data analytics 6
- User monitoring and risk-based intervention 6
- Consumer-level convenience, enterprise-level security 7

Transitioning to Next-generation IAM 8
Security Solutions from RSA 9

SECURITY'S "NEW NORMAL": THE BORDERLESS ENTERPRISE AND ADVANCED THREATS

The convergence of several business and IT trends has caused massive disruptions in the practice of information security:

1. IT outsourcing, cloud services, workforce mobility, bring-your-own-device (BYOD) and the opening of corporate applications and data to outside partners have dissolved traditional enterprise boundaries. They have also multiplied potential points of breach and challenged organizations to figure out how to secure IT assets they often don't own or operate.

2. Highly targeted advanced threats such as APTs pose unprecedented risks to valuable corporate information and IT assets. Cyber adversaries often gain illicit entry into the enterprise by falsely assuming the digital identities of employees or trusted partners. By masking themselves as legitimate users, adversaries can deflect suspicion when conducting reconnaissance on the IT environment and while staging their attacks.

3. Advanced threats and dissolving enterprise boundaries are placing unprecedented strain on the ability of organizations to protect what matters most to their business: valuable proprietary information. Such information increasingly resides on infrastructure that's not directly controlled by corporate IT departments. Absent such control, *the best way to safeguard corporate information is to control how users interact with it*. Control means verifying that users, whether human or machine, are who they claim to be and that they're doing only what they should.

IAM MUST BE REINVENTED TO STAY RELEVANT IN SECURITY

The task of ensuring that the right users get access to appropriate enterprise IT resources has traditionally been the realm of identity and access management (IAM). IAM encompasses all the policies, processes, procedures, applications and tools that help an organization manage access to enterprise information. IAM solutions verify that users attempting to access systems are who they say they are via a variety of authentication methods.

IAM, long an established part of most information security programs, is attracting renewed interest as a way to secure today's borderless enterprise. IAM is also evolving into a tool to thwart the escalation of advanced threats. Cyber adversaries often exploit stolen corporate identities to gain virtual entry into organizations. *As people's identities become the front lines of attack, IAM systems must become the front line of defense*: a dynamic security perimeter for the borderless enterprise.

Traditional IAM systems, however, have a long way to go before they can reliably serve as the new front line of defense. Most IAM solutions today face serious challenges in this new world.

Virtual population growth and duplicate identities

Organizations are experiencing a "virtual population" boom. A single enterprise user can spawn multiple digital identities: a corporate log-in, and separate identities for various enterprise applications and web services. Multiply these disparate identities with the number of access devices used by each employee (office laptops, home computers, tablets, mobile phones) and the dozens of IP addresses each device could be using, and it's clear organizations face an explosion of identity-related information.

Most traditional on-premise IAM systems, however, cannot easily scale to accommodate larger, more diverse user populations. They cannot integrate and correlate siloes of identity information created by new applications and services, especially those hosted outside the organization. Also, as many industries continue consolidating, mergers and acquisitions are requiring IT departments to extend their IAM systems to include new locations, departments and employees and forcing them to make sense of disparate attributes, roles and policies. As a result, developing an authoritative, single source for identity information has become very difficult.

Users expect greater convenience

Organizations expanding their use of enterprise applications and cloud services have seen the number of user identities and the repositories supporting them multiply accordingly. Traditional IAM systems cannot easily integrate these disparate repositories. As a result, enterprise users must keep track of and use different user names and passwords to log into different systems, applications and services, each of which rely on separate databases for identity verification. This approach is good for neither the organization nor the user and is unsustainable in the long run.

In the same way that enterprise users forced bring-your-own-device (BYOD) policies upon corporate IT departments, organizations face a similar sea change in expectations when it comes to identity management. People are acclimating to the convenience of signing onto multiple websites using online "passports" such as their Facebook ID, Google sign-in or Microsoft® account. It's just a matter of time before people expect similar or even greater levels of integration when signing into corporate IT services. They won't want to keep track of dozens of log-in credentials for work.

Also, people have come to realize that high levels of security can be delivered with minimal intrusion into their online interactions. For example, most consumers bank online and send payments through mobile devices and public networks. They expect their financial institutions to keep tabs on their assets and keep them safe. These high expectations are permeating into work environments. IT departments and security teams must learn to elevate the enterprise IAM experience so it more closely resembles the utility and convenience users have grown accustomed to on the consumer side.

Extensibility to cloud and mobile platforms

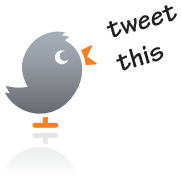
IAM systems will need to extend authentication, authorization and federation services to cloud and mobile platforms, which are now popular ways to deliver business applications and data. IAM systems will also need to assimilate information from cloud and mobile services to enrich user profiles and to enhance how identities are verified in the enterprise. For example, in the future, location data from users' mobile devices could be compared to other information sources (e.g., IP address location, the number of user identities logging in from a specific device within a particular timeframe) to corroborate remote log-ins.

For many organizations, extending the reach of enterprise IAM to cloud and mobile platforms will compel them to host IAM services in the cloud. By placing certain IAM services in the cloud and integrating them with corporate identity repositories managed behind the firewall, organizations can achieve secure authentication, authorization and federation value faster.

Difficulty in discerning deception

Traditional IAM assumes that users providing the right credentials can be trusted after their initial authentication, regardless of what they subsequently attempt to do. Once sessions are established, trust isn't challenged or re-verified, even when users' actions fall outside regular behavior patterns.

Trust cannot be established solely on the basis of a successful log-in; trust must be continually verified. To do this, IAM systems, like most categories of security tools, will need to integrate advanced capabilities in data analytics. In addition to traditional classifications such as application sensitivity or network location, broader data sets should be considered to help IAM tools dynamically assess risk. Risk factors could include data type (image, file, voice print), geographic and jurisdictional restrictions, security configurations for the data environment and other measures of information sensitivity.



IAM systems will need to be reinvented to meet the changing needs of enterprise IT departments. RSA predicts in the next two years *next-generation authentication and identity management systems will pivot on a new capability: adaptive IAM*.

ADAPTIVE IAM SECURES THE "PERIMETER" OF THE BORDERLESS ENTERPRISE

Adaptive IAM patrols a dynamic "situational perimeter" for the borderless enterprise, enforcing security wherever users interact with corporate data and resources. Security measures within this situational perimeter morph with the transaction, the parties and the value of data and assets in play.

Next-generation IAM systems draw on data from hundreds or even thousands of sources to help organizations better detect deception and danger. When high-risk activities are spotted, next-generation IAM systems stop users in their tracks with "stepped up" authorization or verification requirements that users must satisfy before they're allowed to continue.

Adaptive IAM is built on four emerging capabilities.

FIGURE 1: GUIDING PRINCIPLES FOR ADAPTIVE IAM

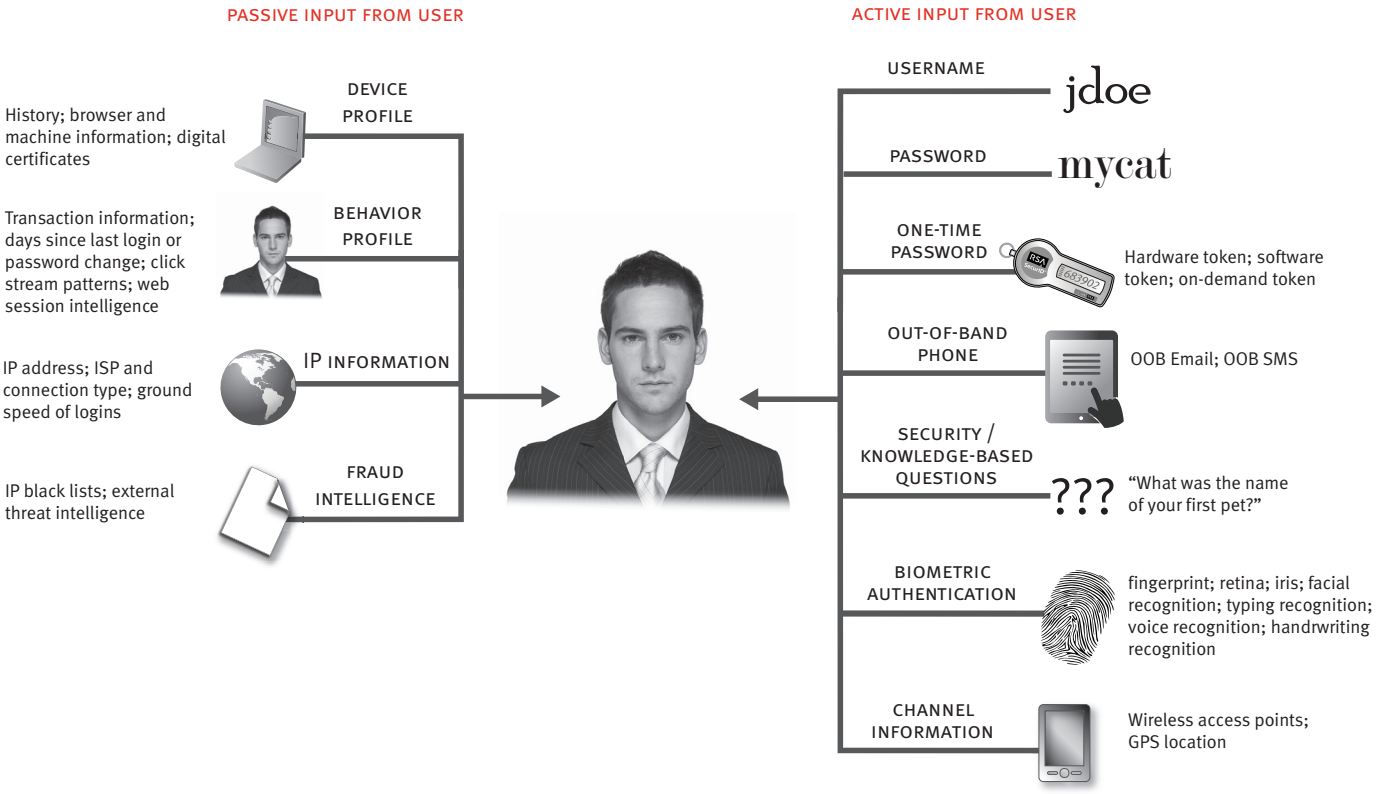
Rich user profiles

Adaptive IAM profiles each user to spot significant deviations from "normal" behavior, which can often signal security problems.

User profiles draw from many attributes that can independently corroborate the trustworthiness of users and their activities. These identity attributes, shown in Figure 2, represent composite data from a variety of sources. These rich user profiles empower adaptive IAM systems to verify identity using hundreds, if not thousands, of factors—not on a single factor alone such as a correct password.

Rich user profiles help next-generation IAM systems create a unified view of users and their entitlements across the organization. This unified view establishes a single authoritative source for authenticating, authorizing and federating the organization's user identities across IT systems and services. Unified profiles also provide richer context for evaluating user behaviors to measure risk and to determine appropriate user privileges. Each profile contributes to a composite baseline of behavioral norms for the entire user population while providing sufficient granularity to customize assessments of what's considered "normal" for the particular user.

Figure 2: Adaptive IAM builds rich user profiles



Big data analytics

Big data analytics will inject next-generation IAM solutions with the intelligence required to assess risks, detect problems and interrupt users attempting unsafe activities. Creating the intelligence needed to distinguish good behavior from bad will require IAM systems to integrate and analyze vast volumes and varieties of user-related data. Data from internal sources, external intelligence feeds, and mobile and cloud environments will all be used to enrich user profiles and to enhance behavior modeling. This approach can also be instrumental in comparing user behaviors with observed historical norms, interpreting deviations from normal baselines as potential problems.

Next-generation IAM solutions will need to integrate and interoperate with diverse IT components and to ingest data from a wide variety of sources. Analytics for adaptive IAM systems must perform at the scale and speed needed to affect security outcomes in real time.

Next-generation IAM systems will layer risk analytics on top of existing on-premise authentication systems to protect access to software-as-a-service applications, federated web services and other cloud services. IAM capabilities will also authenticate and secure access from mobile devices. Adaptive IAM systems will consider contextual factors in making authentication decisions such as whether a user has previously logged in from a particular mobile device and whether the data being accessed has a high degree of sensitivity.

With adaptive IAM, organizations will be able to easily manage risk-based authentication as a service across mobile devices, tablets and PCs, with intuitive policy management and simple installation of on-premise connectors.

User monitoring and risk-based intervention

Adaptive IAM systems monitor user behaviors and adjust access controls based on real-time risk assessments. At first, user monitoring and access controls for next-generation IAM systems will start at an application boundary such as a financial application, enterprise web application, SaaS application, remote access gateway or mobile application. Over time, organizations will be able to evaluate risk and establish trust for online activities throughout the web of connections to enterprise data, not just within a particular network or application. Enterprise IT and security teams will be able to create trust zones and connections that define situational perimeters based on the activities being attempted, not on static boundaries. Enforcement becomes contextual, adaptive and dynamic.

Adaptive IAM systems also adjust to changing risk levels as users travel to remote locations, enter through untrusted networks or access cloud and web-based applications. While even the best authentication systems can succumb to phishing, man-in-the-middle, man-in-the-browser and other attacks to steal user credentials or hijack secure sessions, adaptive IAM approaches wrap security around a session—both the user and the data—inspecting the session nonstop and adjusting security procedures to observed behaviors. If the analytics system spots users engaging in suspicious or high-risk activities after authentication, users are interrupted until they can present additional proof of identity or authorization.

Consumer-level convenience, enterprise-level security

Today, organizations make tradeoffs to balance security with end-user convenience. Next-generation identity protection removes the need to choose: it allows organizations to achieve higher security and convenience at the same time.

IAM systems are morphing to make identity controls and analytics invisible to corporate end users. Initial authentication is simple and straightforward, and the user experience is streamlined with federated single sign-on for IT services not directly hosted by the organization. User interactions with corporate resources are interrupted only when unacceptable activities or levels of risk are detected. Nevertheless, behavior monitoring and risk assessments occur behind the scenes to provide security teams with visibility and control over how users interact with corporate resources.

Going further, users will be able to manage fewer log-in credentials as enterprise user identities consolidate into a smaller number of identity stores. While a universal ID is probably not in the foreseeable future, next-generation IAM systems will facilitate a more convenient work experience for enterprise users.

TRANSITIONING TO NEXT-GENERATION IAM

Going from the current state of IAM to next-generation offerings will require the security industry to work out a smooth migration path.

Most organizations may not have the in-house expertise or resources to integrate the diverse technologies, data stores and analytics models needed to build next-generation IAM systems. Because of this, many will likely turn to cloud-based services as a turnkey alternative to in-house IAM deployments.

Regardless of whether adaptive IAM services are delivered from the cloud or from enterprise data centers, next-generation IAM systems must plug easily into existing enterprise environments. They must offer open APIs for third-party integration and include management, reporting and auditing tools for IT administrators. Perhaps most importantly, user authentication and other IAM services need to be delivered at the same performance and quality levels that users have become accustomed to experiencing on the corporate network, regardless of the number of identities managed or the scope of the system.

In the coming years, adaptive IAM can help organizations build a unified view of user identities, whether human or machine. Adaptive IAM systems can also scale security to the fast-growing numbers of users coming from cloud and mobile platforms. By becoming much more aware and discerning of risks associated with various user behaviors, adaptive IAM systems can better detect fraudulent or malicious attempts to access corporate IT resources, thus providing intelligence-driven and dynamic protection for valuable enterprise information wherever it's needed in today's borderless enterprise.

SECURITY SOLUTIONS FROM RSA

The products and services described below are designed to align with the best practices described in this RSA Technology Brief. This security solutions overview is not intended to provide a comprehensive list of applicable solutions. Rather, it's intended to serve as a starting point for security technology practitioners wanting to learn about some of the options available to them.

RSA® Access Manager is engineered to secure access to web applications with transparent, single sign-on (SSO) access based on coarse- to fine-grained access control policies. RSA Access Manager is designed to integrate with a broad range of authentication methods or combination of methods based on your acceptable level of risk. These include Integrated Windows Authentication (IWA), x.509 certificates, RSA SecurID® two-factor authentication and RSA Adaptive Authentication, which includes out-of-band phone and out-of-band email, among others. RSA Access Manager also is built to integrate with RSA Adaptive Directory so that organizations have a logical view of all identities and attributes listed in one place to ensure safer authorization of access to all their web applications.

RSA® Adaptive Authentication, with its advanced self-learning risk engine, is designed to calculate a risk score based on the user behavior profile, the device profile and the eFraudNetwork match. This risk score is provided to a policy engine and the user is either granted access, required to provide an alternate authentication credential or denied access. Today, RSA Adaptive Authentication is used by thousands of organizations to protect more than 250 million identities worldwide.

RSA® Adaptive Directory is built to create and secure a single authoritative identity directory from disparate and distributed directory infrastructures for authentication, authorization and federation. Users who exist in more than one source now have a single profile of all attributes without duplication. This gives you one virtual view of all users and entitlements — on top of your existing identity infrastructure.

RSA® Adaptive Federation is engineered to provide easy-to-use, federated single sign-on for both identity provider and service provider models to popular SaaS applications. As a cloud-based service, RSA Adaptive Federation provides flexible, scalable support without additional hardware, software, agents or data stores—enabling, faster, simplified deployments. For better security, user credentials are not stored in the cloud; rather, existing user credentials in Microsoft Active Directory® can be extended securely to the cloud without leaving your organization's IT environment through an enterprise connector. For two-factor authentication, RSA Adaptive Federation also integrates with RSA SecurID solutions.

RSA® Authentication Manager 8.0 delivers the world-class strength of RSA SecurID® Authentication technology and now also offers a risk engine designed to meet the challenges and needs of today's organizations. The RSA Authentication Manager virtual appliance is engineered to provide the flexibility to support a wide range of authentication methods, an advanced risk engine, ease of manageability and interoperability with industry-leading products and vendors.

RSA® Digital Certificate Manager has interoperable modules for managing digital certificates to automate and centralize the management of cryptographic keys. It is based on public key infrastructure (PKI) technology.

RSA® Federated Identity Manager is built to install on-premise and provide federated single sign-on for both identity provider and service provider models. It has a flexible and extensible architecture for enhancing user productivity, enforcing internal identity security policies to make stronger security at the SaaS layer, and for consistent and faster identity integration with business partners.

RSA SecurID® technology is a market leading two-factor authentication solution. It is designed to solve the "weak link" issue of poorly chosen user passwords by enforcing strong, multi-factor authentication. The RSA SecurID authentication mechanism consists of either a hardware or software token that is engineered to generate unique authentication codes at fixed time intervals using the token's factory-encoded random key.

H11803-IAMV2_BRF_0513

www.rsa.com

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps organizations solve their most complex and sensitive security challenges by bringing visibility and trust to millions of user identities, the transactions they perform and the data that is generated. RSA delivers identity assurance, encryption & key management, SIEM, data loss prevention, continuous network monitoring, and fraud protection with industry leading GRC capabilities and robust consulting services. www.RSA.com

RSA