RSA

DELIVERING CONVENIENT & SECURE ACCESS

TO THE MODERN WORKFORCE

BUSINESS-DRIVEN SECURITY™ SOLUTIONS

GOOD INTENTIONS AND UNINTENDED CONSEQUENCES

Faced with the threat of increasingly sophisticated and devastating terrorist attacks, countries around the world have repeatedly ramped up airport security screening. The debate over how much safer we are (or aren't) continues, but some effects are clear: long lines, frustrated passengers—and a host of unintended consequences.

A 2007 study investigated the five-year impact of new U.S. Transportation Security Administration (TSA) screening procedures, with results including a 6% decrease in air travel volume and more than $1 billion in lost revenue.[1]

Even when it's not a matter of life and death, unintended consequences aren't limited to airport security. Businesses need to protect their information, but they must do so in a way that maximizes effectiveness and minimizes corollary effects that can undermine their goals. The devil, as they say, is in the details.

[1] *The Impact of Post-9/11 Airport Security Measures on the Demand for Air Travel*, Garrick Blalock, Vrinda Kadiyali, Daniel Simon, Cornell University, April 30, 2007.

CONVENIENCE VS. SECURITY: A TUG-OF-WAR

In any security situation, users and IT professionals often have competing goals. Business users want convenience—quick and easy access to the data they need, from the cloud, the web or a mobile application. Users also want to deploy new apps and gain access to the latest technology without being slowed down by security policies and reviews. The CIO, meanwhile, wants security. This requires visibility across all applications and resources, as well as consistent, centrally enforced policies that reassert control over a disrupted perimeter and islands of identity.

But the more you attempt to secure critical information by restricting access, the more end users will seek out "creative" solutions to get their jobs done. This can be as simple (and as common) as sending work-related files from personal email accounts, adding a "1" to the end of an expired password, or using the same password across multiple accounts. And so it goes: Despite your best efforts and intentions, tighter controls often have a net negative impact on security and operations.

SECURING ACCESS IN A KINGDOM WITHOUT BOUNDARIES?

It used to be so easy. Give a small number of privileged administrators and road warriors secure, remote access to the corporate network, and you'd be done.

But in today's world without boundaries, applications reside both on premises and in the cloud. Users have rapidly expanded beyond the employee to include business partners, suppliers and customers—all of whom need on-demand access to software and data. Mobile users switch between personal and company-issued devices throughout the day. The goal of secure access is the same, but the kingdom's walls have come down.

To succeed, access for the modern workforce must be:

- Convenient and secure
- Available for any user, from anywhere, on any device
- To any resource, system, application or data, on premises or in the cloud

BE SURE WITH IDENTITY ASSURANCE

For most organizations, the answers lie in an authentication strategy. They're asking "How do we make authentication better?" Instead, you should be answering a different question: "How do we ensure that users are who they claim to be?"

Authentication is simply a technical control that validates an identity claim; taken out of context, it loses its effectiveness. The goal isn't to simply authenticate each user, but to **keep security strong while providing fast, convenient access.**

When you grant access, how sure are you that users are who they claim to be? Are you erecting more security hurdles when users travel, work from a mobile device, or simply need to do multiple tasks at once? Are you matching authentication methods to users' particular needs?

Maybe it's time to reimagine your approach to authentication—and move toward **identity assurance** as the end goal.

Just as the TSA discovered in securing air travel, security professionals need to take a **risk-based approach** to identity assurance to secure access to critical applications and data. Instead of just a single data point (does the user have the right password or token code?), identity assurance incorporates multiple data points, leveraging context and user characteristics to help make better access decisions. For example, when the risk analysis warrants, enforce step-up authentication or, conversely, if access is deemed low risk, allow the user to conveniently pass through. By understanding the context of users, data and applications, then evaluating patterns and signals to isolate high-risk requests, you can minimize dependence on interactive authentication. Focus on what matters most, and you'll improve user convenience while strengthening security.

SIX KEYS TO SUCCESSFUL RISK-BASED IDENTITY ASSURANCE

Consider these six characteristics in your authentication strategy, to help you adopt a risk- and context-aware approach that improves information security while optimizing the user experience.

Business context

The information used to form baseline assumptions about each access request

Anomaly detection

Watching behavior to determine what's normal and what's not

Machine learning

Continuous authentication that immediately recognizes changes in how the user interacts with the device

A broader ecosystem

Capturing the most information to inform access decisions

Consistent experience

Generating a user experience that is intuitive, predictable and easy

Flexible authentication

Flexible authentication for a diverse set of users and use cases

#1: BUSINESS CONTEXT

This is the information you use to form baseline assumptions about each access request. Business context breaks down into three fundamental pieces:

1. The data

What is being accessed? Everyone agrees that sensitive data (such as intellectual property) deserves more protection than, for example, the company holiday calendar. But in an age of enterprise SaaS applications and hosted data centers, either could be stored in your corporate data center or in the cloud. Companies are left with multiple on-premises and cloud applications, each containing a set of user identities with different, disjointed authentication requirements unaligned to the sensitivity of the information they contain.

2. The person

Who is requesting access? Is the user an IT administrator or an end user? Or a partner or customer? Different types of users need different levels of assurance to gain access. Organizations must leverage data from multiple identity repositories to ensure that appropriate security is applied.

3. The environment

What is the session context of the request? Is the user's device registered, known for this user, managed by the company? Companies must also evaluate session context attributes including trusted networks, trusted locations, and blacklisted locations and IP addresses. Each piece of contextual data contributes to the decision whether to allow access—and what level of additional assurance a user must provide to gain that access.

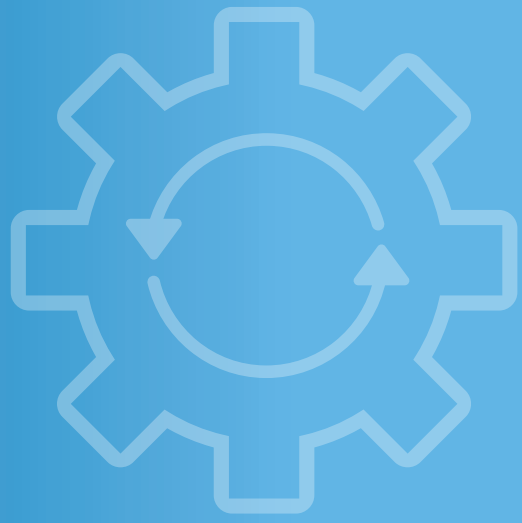
#2: ANOMALY DETECTION

Watching behavior to determine what is normal and what is not—anomaly detection—can unleash broader capabilities, which can in turn improve both the user experience and security.

A multifactor authentication solution should be able to perform basic anomaly detection: isolate a bad IP address, recognize velocity anomalies and flag untrusted locations. If these capabilities are built into an identity system, policies can leverage this information to deny access or require additional authentication.

Patterns across attributes such as device, location, network, and time of day and access can also help recognize and codify normal patterns of usage—crucial information for building intelligence in identity and access management systems.

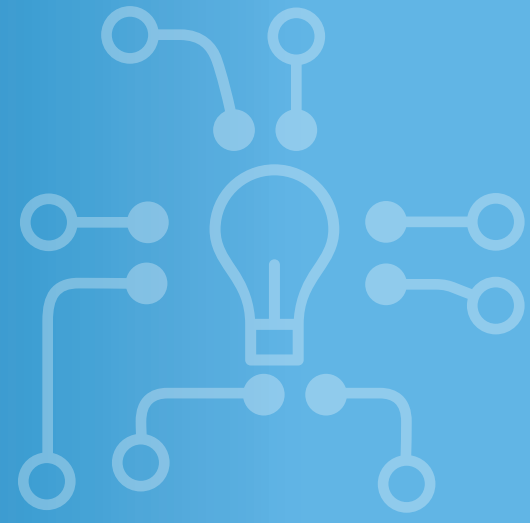
#3: MACHINE LEARNING



Machine learning helps further track and identify user patterns. When tuned for behavioral recognition, machine learning results in higher confidence in a user's identity while improving both the end user experience and security.

Machine learning identifies user patterns such as data accessed, time of day, location and device, but this is just the start. Many other, more personal behaviors, such as keystroke dynamics and pattern recognition, can help identify users by how they interact with their devices. These types of learning provide an even better, more seamless experience with higher security. In addition, machine learning technologies provide continuous authentication since changes in how the user is interacting with the device are immediately recognized, allowing for an instant challenge if behavior changes.

#4: A BROADER ECOSYSTEM



A broad ecosystem helps you capture the most information you can, better informing your access decisions. For example, information from a threat detection system should be leveraged by the identity system.

When the threat detection system receives an alert for a user or a resource, the identity system should respond. If these two systems are part of a broader ecosystem and tied closely together, you have a real-time, two-way information exchange. Your identity and access management (IAM) data should help inform how you analyze for threats, while alerts trigger anomaly detection on the IAM system in real time. A broad ecosystem allows you to get data from as many sources as possible, helping enrich context, improve security and reduce end user friction.

#5: CONSISTENT EXPERIENCE

Users are creatures of habit. In a security situation, consistent behavior should produce consistent results—generating a user experience that is intuitive, predictable and easy.

Security solutions should not result in a system that leaves users perplexed or confused. If a user behaves one way today and gets specific results based on that behavior, he or she will likely expect that behaving the same way tomorrow will elicit the same results. Preferences—for example, "remember this device" or "remember this location"—help keep the user experience consistent and simple.

#6: FLEXIBLE AUTHENTICATION

One-size authentication does not fit all. For a risk-based identity assurance strategy to be successful, you need flexible authentication for a diverse set of users and use cases.

For example, you may need hardware tokens for privileged administrators, mobile OTP for your road warriors, and push notifications for business partners and customers. By having a variety of authentication methods available, you can choose which one works best for your users and their environments. Select the method that best addresses perceived risk and aligns with your authentication strategy to create a seamless, friction-free experience for users.

BRING IDENTITY ASSURANCE INTO FOCUS

Identity assurance changes the security game. At RSA, we balance the risk associated with each user's actions with the assurance that they are, in fact, who they say they are.

Organizations need to provide convenient yet secure access—connecting users with the information they need, whether on premises or in the cloud. RSA uses risk analytics and context-based awareness to provide seamless, robust authentication based on proximity, device, location and behavior.

The result: Work gets done, users are happy—and you have the confidence that people are who they say they are.

RSA SecurID® Access, the industry's most advanced multifactor authentication solution, gives your users the ability to innovate, accelerate and collaborate. And it gives you the security and control to prevent identity risks from becoming a drag on your business.

INNOVATIVE AUTHENTICATION TECHNOLOGY FUELS BUSINESS GROWTH

RSA SecurID Access can help you manage access for any resource on premises or in the cloud, allowing you to:

- **Get authentication your way:** You can deploy RSA SecurID Access in the cloud and get our industry-leading identity assurance solution "as a service." Easily offer a range of advanced mobile authentication options to your users, including push notification and biometrics.
- **Achieve convenience and security without sacrifice:** Provide invisible yet effective continuous authentication. Leverage identity analytics to request step-up authentication when needed and allow users to authenticate with the methods that are most convenient for them and most secure for the business.
- **Apply risk-based, contextual access policies:** Efficiently configure access based on risks associated with the areas users operate in, their physical location, application sensitivity, session and network information, and device type.
- **Enable the business to grow:** Speed user access to applications and data with a frictionless user experience, enabling the business to get more done.
- **Regain control of user access:** Bridge islands of identity with a centralized, consistent approach to managing user access to corporate resources from any device location inside or outside the network.
- **Provide continuous assurance:** Risky or unlikely access scenarios automatically trigger additional authentication or controls, adhering to rigorous security and compliance requirements.

RSA SECURID ACCESS ENABLES CONVENIENT, SECURE ACCESS

RSA SecurID Access provides the most trusted, resilient and flexible forms of strong authentication on the market today. Over 25,000 customers use it to protect more than 60 million end users worldwide.

RSA continues to evolve the RSA SecurID Access solution to help organizations provide convenient and secure access for today's modern workforce. With advanced risk-based identity assurance; a range of mobile-optimized authentication methods; and the ability to protect the broadest range of cloud, web and traditional client/server applications on premises and in the cloud, RSA SecurID Access is the most complete multifactor authentication solution on the market today.

RSA SecurID Access enables dynamic user populations to access exactly what they need, how they need to access it, from anywhere, at any time.

ABOUT RSA

RSA offers Business-Driven Security™ solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90% of Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to **rsa.com/reimagine**.