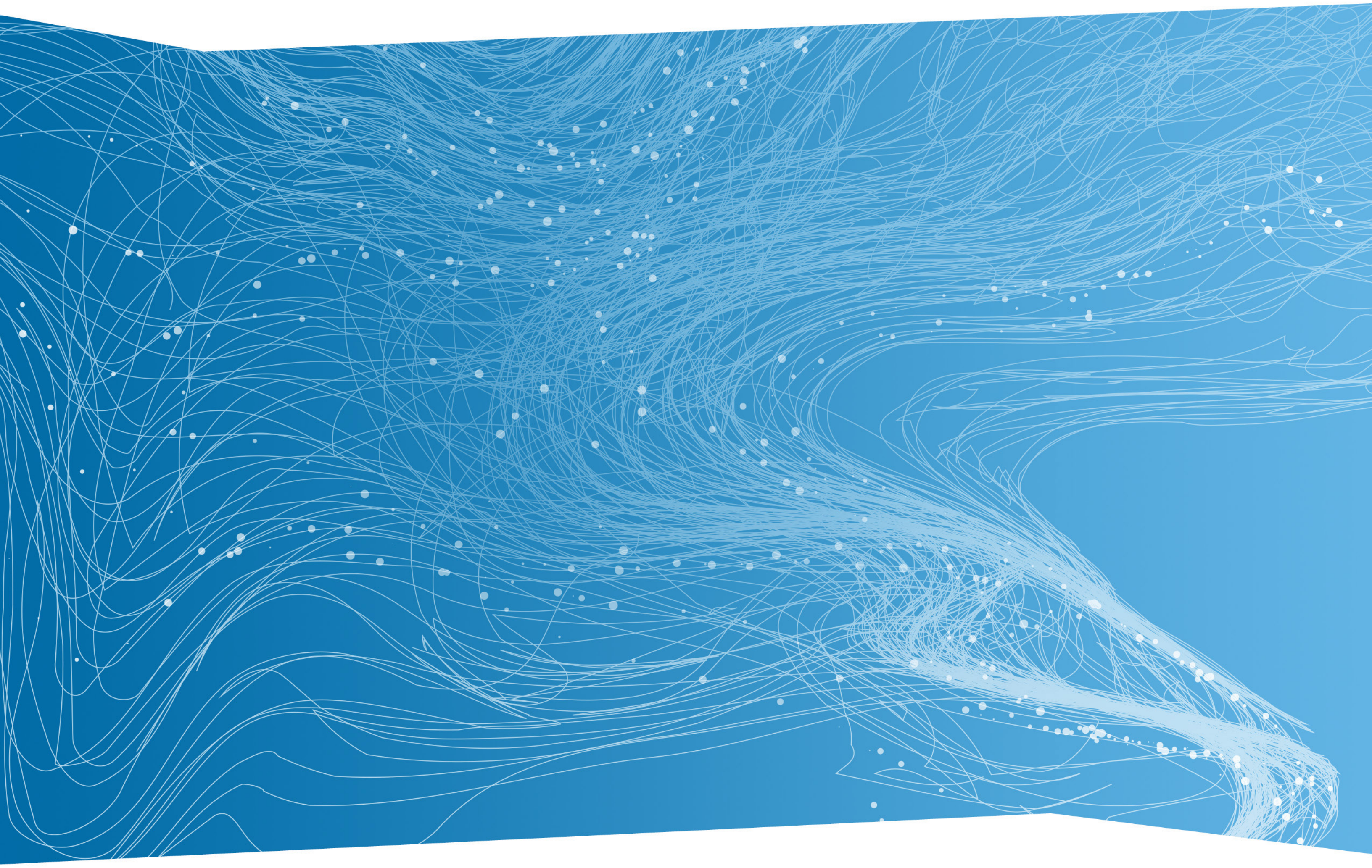
WHITE PAPER

6 KEYS TO SUCCESSFUL IDENTITY ASSURANCE

DELIVERING ACCESS THAT'S BOTH CONVENIENT & SECURE



Now that so many applications have moved to the cloud, and so many users have embraced mobility, organizations continue to work toward being able to fully embrace the opportunities this new world without boundaries presents—and also manage the risk that comes with such unprecedented openness. Traditional authentication solutions require a trade-off between secure access to resources and convenient, usable access tools, which are often deployed with a "one-size-fits-most" mentality. Today's organizations need to shift their thinking away from authentication as being a static one-time event, to one where they can continuously assess users, based on the context that surrounds them and the associated risks of granting access to a particular application or data set.

Intelligence-driven identity assurance can result in 90% fewer interactive authentications while maintaining MFA-level protection.

By applying a risk-based approach to identity assurance, organizations can go beyond a simple yes/no decision or step-up authentication process and add intelligence that provides broader context about the user and the situation in which they are requesting access.

Identity assurance helps to quantify:

- How confident am I a user is who they claim to be?
- How sure do I need to be based on the information they are accessing?

There are six key elements to consider when creating an effective identity assurance strategy:

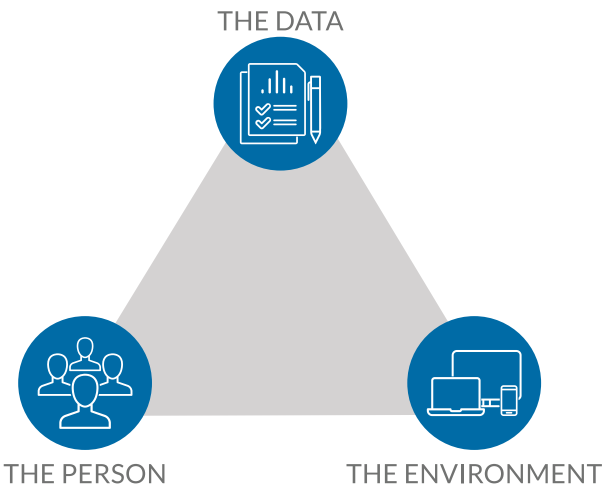
1. Business context
2. Anomaly detection
3. Machine learning
4. Broader ecosystem
5. Consistent experience
6. Flexible authentication

This paper explains how to employ these key elements to increase information security while simultaneously optimizing the end user's experience. We will explore each element individually and also look at how, together, they enable access that meets the security needs of organizations and the convenience that users demand—putting an end to the tug-of-war that exists between IT and end users.

#1 BUSINESS CONTEXT: WHAT, WHO AND WHERE

Business context is the information we can seamlessly gather to help form baseline assumptions about an access request. A good way to look at context is to break it down into three fundamental pieces:

- The data
- The person
- The environment



Business Context: *The information used to form baseline assumptions about each access request.*

THE DATA: WHAT IS BEING ACCESSED

Traditionally, when multi-factor (or two-factor) authentication solutions have been put in place, it's been to protect data that sits behind a company's firewall. However, due to the explosion of enterprise SaaS applications and hosted data centers, more and more sensitive data is stored in the cloud, outside of IT's control, instead of in a corporate data center.

Unfortunately, authentication has been slow to keep pace with the cloud and the ability to ensure that the most sensitive data is protected appropriately no matter where it resides. As a result, companies are left with a multitude of applications, each containing a set of user identities, and each having different, disjointed authentication requirements. All too often these authentication requirements don't align to the sensitive nature of the information they are trying to protect.

Regardless of where the data lives, the fundamental question is, "How sensitive is the data being accessed and what risk does it pose to the organization?" Is it confidential intellectual property or the company holiday calendar? It's important to consider this context, since without it we run the risk of not imposing enough protections on company secrets or of running users through a security gauntlet just to see what's for lunch. When data is treated appropriately, based on its sensitivity, it becomes possible to achieve both security and convenience.

THE PERSON: WHO IS REQUESTING ACCESS TO THE DATA?

Equally important as the data is the level of access a specific user has within a particular application. Is this user an IT administrator with nearly limitless access or is this person an end user with limited access? We need to view these users specific to their different levels of assurance to gain access. We have information available about the user in potentially multiple identity repositories. We must be able to leverage the available data from all of these sources to adequately ensure the appropriate security is applied.

THE ENVIRONMENT: WHAT IS THE SESSION CONTEXT OF THE REQUEST?

The third piece of business context to consider is the environment in which data is being accessed. What do you know about the device the user is requesting access from? Is it a personal device, or one owned and managed by the company? Beyond device, other session context attributes include trusted networks, trusted locations, blacklisted locations and IP addresses. Taken separately or together, these types of attributes provide broader visibility into risk and make it possible to dynamically protect access based on real-time session data.

PUTTING IT ALL TOGETHER

Taken together, these three business context fundamentals (data, person and environment) form a foundation for building policies to ensure the authentication required is appropriate for each access request. When evaluating multi-factor authentication solutions for identity assurance, it's important to choose a solution that fully leverages business context to create granular policies. It's also important for these components to be easily configurable so an administrator can have confidence in who they are allowing access and what authentication will be required.

Anomaly Detection:
Watching behavior to determine what's normal and what's not.

#2 ANOMALY DETECTION: BUSINESS AS USUAL—OR NOT?

While business context is one key to a successful identity assurance strategy, it's also important to look beyond what can be done with static rules. A dynamic view of your users may allow you to spot suspicious behaviors that might signal fraudulent activity.

In granting access to users, understanding their behavior can go a long way towards providing frictionless, secure access experience. Monitoring user behavior to benchmark what is normal and what is not enables customized authentication polices that deliver an optimal experience for each user or group.

IDENTIFYING ABNORMAL ACCESS REQUESTS

Let's start by taking a look at what makes an access request appear abnormal. There's a simple question that can be asked to recognize an abnormal request: Is this access request unlikely to be legitimate? Answering this question fully may require information from multiple sources. However, a modern multi-factor authentication solution should have capabilities to perform a basic level of anomaly detection. Here's a look at some of these capabilities.

1. **Isolate bad IP addresses.** When known bad IP addresses are used in access attempts, they should simply be blocked.
2. **Recognize velocity anomalies.** When a user's location is known, a correlation can be made between this access request and other recent

requests. For example, is it possible for a user to log in from Colorado and ten minutes later log in from Moscow? No; that would constitute a ground speed violence. Better get more proof the user is who they claim to be—or maybe just deny that access request.

3. **Flag locations as untrusted.** If a geolocation for an access request is coming from a strange or known blacklisted location, you may want to simply deny this request. It's also possible to require additional authentication for a location, such as a specific country.

When capabilities like these are built into the identity system, policies can leverage the information they provide to properly deny access or require additional authentication. A later section of this paper will discuss how to gain broader awareness into enterprise risk by leveraging intelligence that comes from outside a strong authentication solution.

RECOGNIZING NORMAL BEHAVIORAL PATTERNS

In addition to recognizing abnormal behavior, it's essential to look at the inverse, and define what constitutes normal behavior and how it can impact identity assurance. Everything starts with the context attributes discussed earlier—but in this case, trust is not pre-determined through static rules alone. Rather, the user and their attributes (device, location, network, time of day, access patterns) can be evaluated to determine whether there's been a common pattern of "known good" authentication attempts where these attributes are consistent.

A consistent access pattern can provide assurance of who this user is without having to challenge them with step-up authentication. Introducing behavioral intelligence into access decisions makes it possible to invoke real-time policy decisions for a higher level of security and convenience.

Machine Learning: *Continuous authentication that immediately recognizes changes in how the user interacts with the device.*

#3 MACHINE LEARNING: GETTING TO KNOW USERS

While applying business context and anomaly detection is effective, it also generates large amounts of data. Therefore, it's important that a modern authentication solution has the ability to not only automatically comb through data, but also interpret the results and learn from them over time, in order to continuously improve its decision making, so that it can assess complex access scenarios without the need for human intervention.

BIG DATA MACHINE LEARNING

Machine learning has been around for a long time and is widely used for fraud detection by organizations monitoring financial transactions, such as credit card processors. These machine learning tools look at broad user populations and report back on fraudulent activity, which helps tune the model for everyone. Financial services companies generally have reliable out-of-band feedback systems to capture fraud (such as unauthorized access or forged charges), which further improves this type of data model.

MACHINE LEARNING FOR SMALLER POPULATIONS

The big data approach doesn't work as well for monitoring enterprise access to business applications. User feedback is far less likely given that people who interact with the organization are likely unaware of, and therefore cannot report on, unauthorized access events. Therefore, a different model is required for business-related access—a model in which the focus shifts from fraud detection towards identity assurance.

To put it another way, how confident can you be that a user is who they claim to be based on previously successful authentications? This confidence comes from learning from the data available in users' past authentication attempts. Some examples of this data include:

- Location/network
- Time of day
- Device fingerprint
- Pattern of access
- Keystroke dynamics

Much of this data is either the same as or similar to data discussed in the section of this paper covering business context. The difference is in how it is applied. Instead of evaluating static rules, organizations look at those attributes to learn what is normal for each user. Rather than declaring a network address is trusted or not trusted, for example, one can analyze user activity and determine if the user has provided a high level of authentication from an IP address multiple times.

That insight provides one piece of data to consider when determining confidence in the user's identity. Pairing it with many other data points creates high confidence across multiple attributes, so that it becomes possible to make an intelligent determination as to whether more authentication is needed for the access request or not.

DON'T FORGET TO FORGET

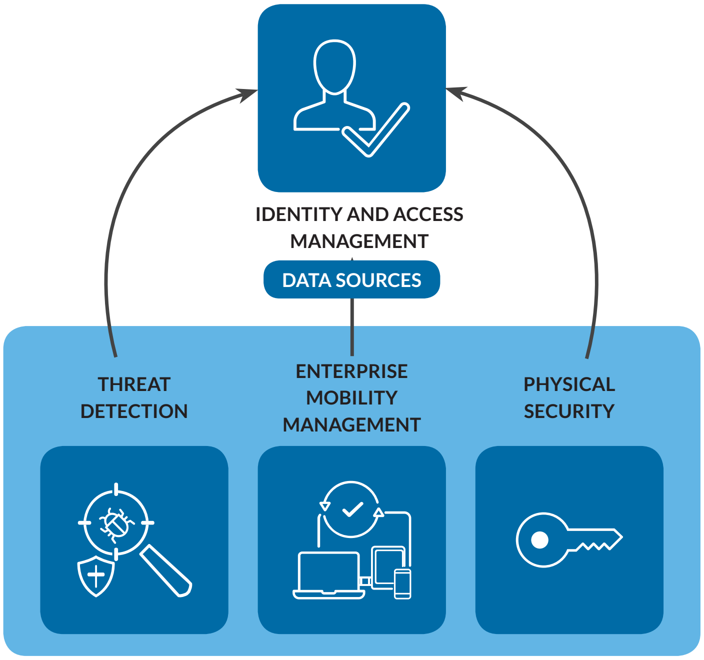
To take this to the next level, it's also necessary to forget behaviors when they are no longer relevant due to changing circumstances. If a user moves or gets a new computer, the old details should be phased out in favor of a new set of benchmarks. In time, the earlier circumstances are forgotten and the new ones become more relevant. Remembering to forget is as important as initial behavioral learning.

Applying machine learning techniques for enterprise security is still in its early stages. The ability to decipher many other, even more personal, behaviors is emerging to make authentication more secure while creating less friction for users. And although machine learning is relatively new in the identity space, modern authentication solutions must have the ability to automatically comb through data, interpret the results, and learn from them over time, so that they can provide a high level of security and convenience without the need for human intervention.

A Broader Ecosystem:
Capturing the most information to inform access decisions.

#4 BROADER ECOSYSTEM: INPUT FROM EVERYWHERE

It's important that access systems have a broad view of what's happening around them. Security takes a village, and systems need to be able to not only mine their own data, but also leverage intelligence from other sources such as threat detection solutions, enterprise mobility management (EMM) tools and physical security systems. These and other sources all have intelligence that can inform an identity assurance system and impact access policies. Here are some examples of how it works.


IDENTITY AND ACCESS MANAGEMENT
DATA SOURCES
THREAT DETECTION
ENTERPRISE MOBILITY MANAGEMENT
PHYSICAL SECURITY

THREAT DETECTION

Security information and event management (SIEM) and cloud access security broker (CASB) solutions are among the threat detection systems that may be part of the IT environment. Within that ecosystem, threat detection and identity assurance should work hand-in-hand. Identity assurance systems have log information that should feed threat detection solutions. Sharing failed and successful logins and locked-out accounts can assist in identifying potential threats. But the idea is even more compelling if the data flow also works in reverse, going from threat detection solutions to identity systems. When the threat detection system receives an alert, the identity system should be able to react in real-time. Here are a couple of examples to consider:

1. **Threat alert for a user.** When an alert is raised for a specific user, flagging them as high-risk, identity assurance should adjust to either require multi-factor authentication for all access for this user or, if the threat is significant enough, block access for the user until this alert is cleared.

2. **Threat alert for a resource.** For alerts on a resource, anyone attempting access to that resource should be blocked from access until the alert is cleared and the resource is deemed trustworthy.

Regardless of the specific use case, the key is that the identity assurance solution should be able to not only share log information with other security analytics systems but also ingest threat intelligence from them and be able to adjust access policies on-the-fly, based on the level of risk shared.

ENTERPRISE MOBILITY MANAGEMENT (EMM)

EMM, the successor to mobile device management (MDM), usually involves some combination of MDM, and mobile application and information management. These systems collect data about mobile devices, their applications and the information stored on them. Data, such as whether a device is personally or company owned, can then be used for additional context when making identity assurance decisions.

PHYSICAL SECURITY SYSTEMS

Physical security systems such as door-access badges can also be tied into a secure access solution to help provide added confidence that users are who they claim to be when logging into systems and applications. If an employee just badged into an office in San Francisco, and soon after is attempting a login from London, that's a red flag event and something that should be protected against at the access control point. Conversely, if someone just swiped into their local office, that information can be considered in determining if step-up authentication is required to access their Office 365 account.

Threat detection, EMM and physical security systems are not the only systems that can help feed threat intelligence, behavioral data and static policy results to the secure access solution. You most likely have a "security village" you can tap into that will provide increased visibility into enterprise risk and a more orchestrated approach to secure access.

#5 CONSISTENT EXPERIENCE: WHAT'S GOOD FOR THE USER

While so far we've primarily focused on ways to collect and use information to better assess risk, we must also be sure to consider what users want. We know, as users ourselves, that we want predictability and consistency when interacting with our applications and devices.

Today, users require access to both on-premises and cloud-based resources including internal web pages, SaaS apps, VPNs and mobile apps. They access these resources from multiple corporate, personal and shared devices. With all that variety, how is it possible to deliver a consistent authentication experience across all user access points? That's an important question because delivering a consistent experience can reduce helpdesk calls, increase user productivity and improve user satisfaction. Embracing what's often the weakest link (users) will go a long way in creating a successful identity assurance strategy.

Consistent Experience: *Generating a user experience that is intuitive, predictable and easy.*

THE ROLE OF SINGLE SIGN-ON (SSO)

The rise of software-as-a-service (SaaS) has tempted many an organization with the promise of much needed scalability, business agility and, in many cases, lower operating costs. Yet each of these thousands of applications requires their own access, creating islands of identities that become increasingly complex to manage—as users struggle to remember many usernames and passwords, while grappling with varying access policies and procedures. Enter SSO.

SSO provides users with a consistent authentication experience across their applications. And while it can increase employee satisfaction and reduce help desk costs, SSO by its inherent nature can create a large single point of failure for organizations. With one "master key" to unlock all applications, having a high level of assurance that the user is who they say they are is vital.

WHAT ABOUT APPS THAT AREN'T INTEGRATED WITH SSO?

When considering an identity assurance strategy, it's important to think beyond applications protected by SSO. While many organizations have an SSO solution, they may also have additional applications that are not integrated with their SSO. There are several reasons for this:

- The SSO solution is optimized for cloud applications, which leaves out on-premises applications.
- The SSO solution may be a legacy web access management (WAM) solution, in which case all the cloud solutions may not be integrated, or users may need to log into the VPN first to access the WAM.
- VPNs, thick client apps, etc. are often not included in SSO.

In reality, there are always going to be critical resources that are not part of an SSO deployment. Just because these applications are excluded from SSO does not mean they should be excluded from the identity assurance program. The user authentication experience should remain consistent for these apps as well.

The more resources are protected by the same user authentication experience, the lower the cost and the better the user experience the organization can provide. Users don't care if it's a RADIUS client, some type of agent or a SAML integration. They don't care whether the application they're accessing is in the cloud or in a datacenter. These are problems for IT and solution providers. It's the job of the identity assurance/authentication solution, and those administering it, to ensure that regardless of the back-end technology, the user experience is simple and consistent while maintaining right level of security.

Flexible Authentication:
Offer choice of authenticator method for a diverse set of users and use cases.

#6 FLEXIBLE AUTHENTICATION: TO EACH THEIR OWN

You've collected data, automated its use through a self-learning engine, integrated third-party threat intelligence for broader visibility and provided a consistent user experience. However, if you don't make the experience easy and convenient for users, then you've failed to end the tug-of-war between security and convenience.

When thinking of flexibility for administrators, it's easy to focus on the authentication methods available based on data sensitivity, user context and associated risk. But the question administrators ought to be asking is, "What authentication methods *should* I make available?" The answer depends on the specifics of both the security requirements and the user population.

- **Security requirements.** Let's start with the basic concept of authentication being something you know, something you have or something you are. In determining what methods to offer a user, it's important to first determine whether one of those is enough (possession of a registered device, e.g., a phone or token), or if combining them would be preferable (possession of a registered phone, plus a fingerprint). There are other security factors to consider as well. Is an SMS one-time password (OTP) sent to a user's cell phone less secure than a push notification using a mobile app? The industry has different opinions, but it's important to identify where your organization stands on these issues. The U.S. National Institute of Standards and Technology (NIST) has a broad set of identity guidelines that provide a good reference.
- **User population.** If an organization's IT administrators are already using hardware tokens, it may be desirable for them to continue to have that option while also having biometrics for some users. For users who have been authenticating with only passwords, something more mobile-friendly or potentially more universally available, such as a voice or an SMS-delivered OTP, may be preferable to hardware tokens.

The administrator should strive to give users choice, but they must also insist on authentication methods that provide the required security based on context, risk and the user population.

GIVE USERS A CHOICE OF AUTHENTICATORS WHEN POSSIBLE

A range of secure authentication options can equate to needed flexibility for end users: "Is an SMS-delivered token better for you, or would you prefer a simple push to approve using a mobile authentication app?" Giving users a choice also makes it possible to adapt to the specifics of their situation. For example, think about a user who typically uses a push notification but also needs a biometric such as a fingerprint or eyeprint. What if they're accessing resources from a plane? Their laptop may be connected to the internet, but the phone may not be. That user should be able to select a method such as an OTP protected by a fingerprint that will work in airplane mode.

Here are four tips to keep in mind when considering flexibility for end users:

1. Give the user a choice in what methods are most convenient.
2. Offer methods that cover situations where an option may not be available (in a place where there is no cell service, for example). Don't get stranded like this Tesla owner.
3. Remember the favorite method to limit user friction for their most common scenarios.
4. Create a consistent experience across methods whenever possible (for example, push notification and OTPs delivered from the same mobile application).

Administrators need flexibility in deploying methods and users need flexibility in using them. An identity assurance solution that ensures both will keep these two groups happy with high levels of security and convenience.

THE ROAD TO IDENTITY ASSURANCE – PUTTING IT ALL TOGETHER

Business context, anomaly detection, machine learning, a broader ecosystem, a consistent experience and flexible authentication are all characteristics fundamental to an organization's ability to be confident that users are who they say they are. With this identity assurance, access is both convenient and secure, requiring as little effort as possible on the part of the user while providing the highest level of security for the organization. Traditional strong authentication solutions tend to favor one at the expense of the other—sacrificing security for the sake of user convenience, or vice-versa—but solutions based on these six identity assurance keys will strike the right balance for IT, users and their respective organizations.

ABOUT RSA SECURID® ACCESS

RSA SecurID Access uses risk-based analytics and context-aware user insights to provide seamless authentication, using a variety of authentication methods that don't impede work. You can give your organization the confidence that people are who they say they are, while providing a consumer-simple experience for your users.

RSA SecurID Access:

- Offers industry-leading authentication technology that can be deployed quickly as a service, speeding deployment while alleviating IT of the operating requirements associated with deploying and maintaining software and related infrastructure.
- Incorporates a broad range of authentication choices—from push notification to biometrics, FIDO to hardware and software tokens—depending on the level of risk identified and assurance level required.
- Delivers innovative identity assurance by considering risk-based analytics and real-time context attributes. This makes authentication not only stronger but seamless to the user, without having to sacrifice on convenience or security.

RSA SecurID Access provides the most trusted, resilient and flexible forms of identity assurance on the market today. Our solutions are trusted by 25,000 customers and protect more than 60 million end users worldwide. RSA invented the secure access market more than 30 years ago and continues to invest in and evolve the RSA SecurID Access solution to help organizations provide convenient and secure access across on-premises, cloud and mobile environments.

RSA can serve as your strategic authentication advisor and work with you to incorporate best-of-breed, third-party and RSA solutions to support a futureproof security solutions—one that enables secure and convenient access for any user, from anywhere to anything.

Learn more at rsa.com/authentication.

RESOURCES

Learn more about identity assurance in these resources from RSA:

Video: Rethinking Your Identity Strategy with Identity Assurance

White Paper: A New Paradigm for Identity Assurance

Webinar: Innovations in IAM: Moving from Simple Authentication to Identity Assurance

Webinar: Enabling Access for the Modern Enterprise with RSA SecurID Access

Demo: SecurID Access Mobile Authentication

Dell Inc. or its subsidiaries believe the information in this document is accurate as of its publication date. The information is subject to change without notice.