RSA

WHITE PAPER

A New Paradigm for Identity Assurance

The criminals, hacktivists, and others trying to breach corporate cybersecurity are just like anyone else: they want to accomplish their missionas efficiently as possible. So why focus on compromising an organization's access device or infrastructure? That's not where the action is.

Advanced threats today target what is on either side of those systems: the user sitting at the keyboard, and the corporate data he or she has access to as part of the job. The goal for the attacker is to compromise identities, impersonate legitimate users to glide past security controls, find valuable data, and glide back out undetected.

Grasping the concept of a threat is one thing. Grasping the implications for cybersecurity—the wholesale change in thinking among practitioners, and in implementing the appropriate controls and processes for corporations—is quite another.

Start with the baseline cybersecurity strategies that most organizations have employed: firewalls to keep intruders out; layers of security that legitimate users must penetrate; authentication challenges where users must prove they are who they claim to be. All of this is predicated on the idea that users assume the burden of proving their identity so they can access data.

That approach hasn't done well in the real world. Password requirements have become more complicated, and password challenges have become more frequent. This often leads to employees and increasingly third-parties, exhausted from password fatigue, using Post-It notes slapped onto computers with passwords written on them. Even without the Post-It notes, the very idea of current methods of authentication carry a risk: if you ask people to identify themselves, you give outsiders the opportunity to breach your security via impersonation.

As the age of social media expands, that ability to breach security via impersonation has become easier. When targeting high-value users, hackers might glean personal information (birthdays, car colors, high school mascots) from one place and use it to circumvent identity controls that rely on this static data. Once an identity is compromised, a cybersecurity system based on authentication performed by the user falls apart.

From authentication to assurance

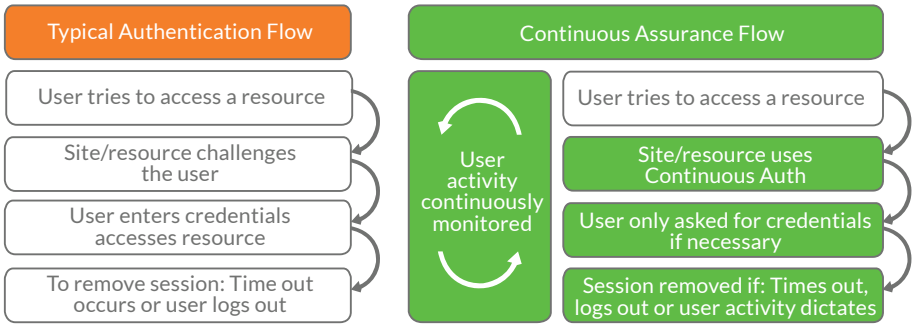
Go back to the earlier, now outdated, metaphor of cybersecurity as a wall to keep intruders out. The reality today is more fluid and dynamic: people moving around from one wi-fi network to another (in the office, at home, on the road, or, at a local coffee shop); working on various devices that the company may or may not own; using applications provided by third-party vendors; manipulating data stored in the cloud. What's more, all of that has to happen with relative ease—because if the IT department does not allow it to happen easily, the user will just find his or her own solution. And, that's what leads to shadow IT.

In this new dynamic environment, what's needed are a series of observation and listening posts, so the cybersecurity team can understand which user activity is normal, and which is abnormal – all in real time. That knowledge enables the IT security function to quickly identify bad actors. This knowledge enables identity controls to automatically take actions based on behavior patterns, in order to provide better security. For example, if a given user attempts to access a resource using a device they've never used before and from a foreign country, the IT security system would require a stronger form of authentication than if the user was accessing it from a company-owned computer on the company network. The additional context that these "listening posts" provide enables more effective, context-aware security decisions.

Additionally, with the advent of new authentication capabilities, organizations can offer users more convenience in proving their identity and in some instances a frictionless, risk-based authentication that does not require any user action. These new capabilities can help organizations deploy an authentication approach that is more flexible and policy based. An important element of this strategy will be the cybersecurity teams' ability to assign a priority level to applications and resources. Once this occurs, authentication policies can be implemented that take application/resource sensitivity, along with device capabilities into account. That way, as new authentication methods become available (e.g., with new biometric authentication methods on mobile phones), it is easy for the organization to leverage a diverse range of methods that are determined based on the priority of the application/resource and user convenience.

In contrast to traditional authentication, which would prompt a user for the same credentials during every login attempt, identity assurance determines the risk associated with the action the user is about to take, based on context gathered over time, continuously, from various posts, then combines that with what it knows about the user, their device and their current environment, to make dynamic decisions on how best to authenticate them.

Authentication -> Continuous Assurance



Key to the success of identity assurance is gathering contextual information about the user and the users peers, before, during and after the login process. Such context can be derived from various entities. For example, consider network security detection services. If such a service notices odd behavior coming from a specific device or IP address, it can act as a context-provider for the identity assurance service: Access attempts from such a device can now be either blocked or require a higher level of assurance.

That shift from identity authentication to identity assurance brings numerous benefits. First, it reduces the chance for outsiders to use compromised identity as an attack vector, since the guiding philosophy is no longer to authenticate once and then grant free movement through the rest of the IT system: Ongoing, behind-the-scenes context processing helps reevaluate the users identity at each and every post, and over time; which reduces the identity threat vector.

Second, it eases the burden on the user, while increasing security; that, in turn, reduces the likelihood that he or she might turn to "home grown solutions" (such as post-it notes for complex passwords). If the user is a customer, it reduces the chance that he or she might turn to a competitor who offers more convenient, user-friendly security.

More broadly however, identity assurance simply respects the reality of modern IT and how people use it in their daily lives. Cloud computing and data storage are here to stay. The IT options available to users will only grow more numerous. Personal, mobile devices are permanent fixtures of work and home. This creates a new challenge for the IT security function because the combinations of devices and networks a user might try to access enterprise infrastructure are logically unlimited. Businesses must work within the confines of that reality, and that means the paramount concern is proper use of company data, at all times. So long as the data and the person using it are properly governed, identity assurance can present the user with device-and-network-appropriate options.

For example, the identity assurance flow for a user accessing company resources from a known, company owned device or from a known location would be different than that of a similar assurance flow for an unknown device or a new location. And, when non-employees or contractors access data, there are additional controls and policies for their access needs. Device, identity and network context help drive identity assurance.

That's the concept, at least. As usual, the implementation gets much trickier.

Putting identity assurance into practice

The challenge with implementing identity assurance as a foundation for cybersecurity is that it requires input, cooperation, and support from areas well outside traditional IT security domains. Successful identity assurance hinges on policies and procedures as much as it does on technology. In this world, training is more important than a strong password, and the CISO supports other parts of the organization as they help impose cybersecurity—not the CISO and his or her team.

Take the example of access privileges. The idea of giving users access only to the data they need is not complicated, but tracking what those privileges should be over time might require coordination among HR, IT, business units, or other departments within the company. As users move within an organization, how they're authenticated would need to change accordingly. As their roles change, the sensitivity associated with the actions they can take shifts, and so would the assurance levels needed when authenticating them. Additionally, gleaning at the behavior of other members of the user's peer group within the organization can help determine if the new user's activity is deemed as "normal" or "abnormal." This, in part, helps determine the risk associated with the users activity, which helps dynamically adjust the proper identity assurance process for this user.

At its heart, what's accomplished here is identity assurance that is in lock step with the business decisions made by the organization: The user's business role, and the business services which they access drive their identity assurance.

How have CISOs been faring in this journey to identity assurance so far? Results from one recent survey of 335 IT security professionals, done by the Enterprise Strategy Group (ESG), paint a telling picture. Sixty-eight percent of respondents said the rise of cloud computing and mobile devices has made identity and access management more difficult; 56 percent say they have an identity governance project underway at their organizations, but only half of that group also say they have support from business-unit leaders.

The challenge for most large organizations will be to map their users and workflow processes to the data they have. Only then can they implement security controls, and build other Identity and Access Management (IAM) analytics tools to monitor users' behavior. According to the ESG study, 35 percent of organizations plan to monitor user activity more thoroughly in coming years; others are considering multi-factor authentication, identity standards that could connect to third parties, and similar new ideas.

Identity assurance: Essential piece of the modern IAM puzzle

The list of ideas in the ESG study, from monitoring users to identity standards for third parties, suggests how successful IAM will work in the future. Identity assurance will require a collection of efforts: smarter policies about user access to various data, applications and other resources, classification of applications' requirements for user assurance, better enforcement of those policies; better communication among IT security and other parts of the organization—and, yes, strong passwords, security tokens, and other "traditional" IT security controls. Recall the metaphor we used earlier of an open field with various observation posts to let the CISO understand who is moving around. Your collection of IAM efforts, like a series of observation posts, must all work together to achieve the goal of more effective data security.

Obviously that collective, organization-wide effort needs support from the CEO and the board to succeed. Thankfully, IAM puts concrete substance behind the idea that "cybersecurity is a process." Good cybersecurity is a process, yes; but saying so doesn't help an organization understand precisely what the company should do. IAM illuminates what the steps in that process can be. In the boardroom, it frames the conversation and helps board directors have more productive discussion with management.

Beyond that executive support, however, IAM only succeeds based on how well all senior executives below the CEO work together—how effectively they articulate risks and workflow processes, and then cooperate with the CISO to ensure security efforts align with those risks. Little surprise, then, that when the ESG survey asked respondents what is most important for identity governance programs to succeed, "strong relationships among IT, security, and business managers" placed first at 31 percent. CISOs will only be able to implement the assurance protocols that work for your company if the rest of the business clearly defines the identities and habits of users, as well as the sensitivity of their application resources.

As a vision for a more secure future that respects the reality of modern business, IT, and human behavior, identity assurance works. As always, the human element will be crucial—we just need the people involved to work together, too.

Takeaway points:

- As a cybersecurity protocol, authentication carries its own risk within itself: the risk that an intruder can impersonate a user, circumvent an authentication check, and gain access to data..
- Identity assurance works as a series of measures to continuously monitor user behavior, reducing a company's reliance on static authentication, and expanding the range of misconduct the company can detect.
- In contrast to identity authentication, which would prompt a user for the same credentials and offer the same methods of authentication during each and every login attempt, identity assurance determines the risk associated with the action the user is about to take, based on context gathered over time, continuously, from various posts, then combines that with what it knows about

the user, their device, their peers, and their current environment, to make dynamic decisions on how best to authenticate the user.

- Identity assurance offers a new approach to effective authentication, and as an integral part of an overall IAM solution, it not only significantly improves overall security, but also improves the user's experience as well.
- Successful identity assurance hinges on cooperation among IT, the CISO, business units, HR, and other key functions to define what a "normal" user does, and finally aligning security to the risks that user poses.