Today’s rapidly changing technology landscape is transforming the face of business—and IT. Mobile computing, for instance, has freed employees and consumers from the tethers of their traditional PCs and has placed significant computing power directly in their hands.

While increased information access and availability have tremendous benefits for businesses and their users, many enterprises are challenged by the security and policy implications of these emerging technologies, which introduce diverse users, additional access points—and predictably, new threats.

IT organizations, as a result, must find innovative ways to make information available and accessible anywhere, anytime and from any device—while protecting against aggressive and sophisticated attacks in these new channels.

This white paper offers insight on how a risk-based approach to authentication can help organizations meet end-user demands for convenience—and enforce the information security controls necessary to prevent unauthorized and fraudulent access to their sensitive information resources. In addition, we provide an overview of how RSA’s distinctive approach to risk-based authentication enables organizations to balance the priority of information security with user privacy.

Risk – It’s a Matter of Context

When evaluating risk, context is everything. The potential for loss associated with risk varies greatly—and depends on the specific action and its related circumstances.

The amount of risk associated with granting a user access to protected information, for instance, depends on the conditions surrounding that user’s login attempt:

– Are the circumstances (e.g., location, device, time) normal for this user?
– Are the circumstances (e.g., location, device, time) normal for similar users?
– Does this login attempt resemble other recent login attempts?

It is important, therefore, to understand first what is “normal” for a user—and for similar users within the same group. “Normal” can include login patterns, user behaviors, and the devices that are used. By establishing a baseline of typical login behavior, it becomes easier to spot anomalies of a login attempt that may be associated with malicious activity.

To gain a better understanding of how a risk-based approach to authentication can be used effectively in this example to evaluate the context of the user’s login attempt and prevent unauthorized access to sensitive data, we must first take a closer look at how risk-based authentication works.
Risk-Based Authentication – Under the Hood

Risk-based authentication is a system that measures – behind-the-scenes and in real time – a series of authentication characteristics (risk indicators) to establish trust between a protected resource and the user.

At the core of risk-based authentication technology is a risk engine, a powerful self-learning analytics tool that tracks and evaluates multiple data points – including user login behaviors, device, and IP geo-location – compares them to previous valid authentication attempts, and assigns risk based on measured similarities and differences to previous attempts. The greater the difference, the higher the risk level presented, and the greater the likelihood that an identity or action is fraudulent.

If the risk engine determines the authentication request to be above the acceptable policy, then risk-based authentication prompts – in real time – a request for additional proof of identity. In this scenario, a user may be asked to answer a few challenge questions or submit an authorization code delivered to a phone via SMS (text) message or email to complete the authentication.

Because the risk analysis occurs behind the scenes, legitimate users engaging in typical login behavior will have a transparent authentication experience. It is only during a high-risk login attempt that a user will be challenged to provide additional information.

Device Profiling: Something the User Has

Device profiling enables the majority of users to authenticate to protected resources transparently. During the device profiling process, the risk engine analyzes the physical mobile or PC device from which the user is attempting to authenticate. Based on this analysis, the risk engine then determines if the device is trusted – in other words, is known to be associated with the user.

Device profiling includes the following key components:

**Unique device identification** assists in identifying a user by embedding two main elements on the user’s device: secure first-party cookies and Flash Shared Objects, also referred to as Flash cookies. Secure first-party cookies are placed on the user’s machine to serve as unique cryptographic identifiers, and they typically are the initial factor used to identify a user. Flash cookies are used in conjunction with first-party cookies to provide a double layer of reliability. Much like first-party cookies, Flash cookies tag a user’s machine and store cryptographic information for retrieval at a later time. The advantage of using Flash cookies is that they are not deleted as often as first-party cookies because most users are not aware that they exist. Even users who are aware of them are not always certain how to remove them. Together, first-party cookies and Flash Shared Objects enable the risk engine to recognize a user’s device during an authentication attempt.

**Device fingerprinting** refers to the process of analyzing the characteristics unique to a specific device. The device fingerprint is used to associate a specific user statistically with his or her unique device. This analysis generally is used as an alternative method of device recognition during situations in which unique cryptographic identifiers (the first-party cookies or Flash cookies described previously) are missing or the organization chooses to prohibit the use of cookies.

Some of the data points captured by the device fingerprint include data collected from HTTP headers and via Java™ script, including: operating system version, operating system patch levels, system display settings, browser version, browser plug-ins, browser language, system language settings, time zone settings, installed objects, and IP address.
Behavioral profiling is used to assess the contextual risk associated with a login attempt to determine – based on a user’s known typical behavior – the likelihood that the user attempting to access the protected resources is the authorized user.

During behavioral profiling, the risk engine looks for potentially high-risk activities associated with a login attempt. Parameters that the risk engine analyzes include: recent authentication activity, IP address information, user location, comparison of IP address with previous login attempts, and recent account changes.

The Risk Assessment

After analyzing hundreds of data points (risk indicators) collected from the device and user behavior profiles, the risk engine calculates an assurance level. A policy can then be applied to the assurance level to achieve the desired outcome that balances security for the organization with convenience for the end user.

The steps required for a user to complete an authentication attempt are dependent upon the risk associated with that attempt. Organizations can customize the policies that risk-based authentication enforces based on specific risk thresholds (see Step-Up Authentication).

There is nothing for the end user to manage since risk-based authentication is performed behind-the-scenes, which makes these solutions easy-to-use and convenient for all types of users – both internal and external to the organization's environment. A user will be challenged to provide additional proof of identity only in the case of a high-risk login attempt.

Step-Up Authentication

The organization can customize the security policies that are enforced by risk-based authentication. When a risk score is higher than the organization’s acceptable threshold, these security policies require a user to provide additional proof of identification before being permitted to complete the authentication.

This identity verification process, known as “step-up authentication,” requires the user to authenticate using an additional factor of identity that the user either knows or has. Additional factors of identity include one-time passwords sent out-of-band to the true user, the correct answers to a series of static challenge questions, or correct answers to a series of dynamic knowledge-based authentication questions.

During a high-risk login attempt, a user is able to access protected resources only after passing the step-up authentication challenge successfully. If the user is unable to pass this challenge, the authentication attempt fails and the user is denied access to the protected resources.

Balancing Information Security and User Privacy

In today’s threat environment, organizations often are forced to make tradeoffs between information security and user privacy. The appropriate balance requires a great deal of consideration.

In risk-based authentication, the profiling of the user behavior and device in particular may be perceived as affecting the sensitive balance of security and privacy. The profiling activities associated specifically with RSA risk-based authentication, though, enable organizations to place security as the priority – without infringement on user privacy.
Data Tracking  The RSA risk engine, in order to enable accurate device and behavior profiling, tracks device characteristics, user authentication behaviors, and geographic locations associated with a user’s login attempts over time. RSA risk-based authentication technology does not track any other type of behavior or personally identifiable information (PII) that can be traced back to a specific user.

Data Monitoring  RSA risk-based authentication technology creates an accurate behavioral profile by monitoring behaviors associated with a user’s authentication activities. RSA technology does not track any user activities other those related to the authentication attempt itself.

Cookies  Key components of a user’s device profile are the cryptographic identifiers stored in the form of first-party cookies and Flash Shared Objects. RSA cookies are static objects that contain data useful for authentication, and as such, they have no tracking capabilities.

Summary

Risk-based authentication enables organizations to extend secure remote access privileges to a diverse user base and access points – both internal and external to the organization’s environment – without having to compromise on user convenience or user privacy.

Whether IT administrators are concerned about maintaining a secure and seamless customer experience or they simply are worried that users will seek workarounds to more demanding processes, risk-based authentication can provide the information security organizations require with a transparency and convenience that users demand.

The profiling components of RSA risk-based authentication technology provide the data points necessary for strong security without infringing on user privacy. The security policies associated with RSA risk-based authentication technology can be customized and continuously fine-tuned by the organization in order to address the patterns of a changing – and increasingly aggressive – threat landscape.