Risk-Based Authentication

Duo's solution helps organizations respond to risk and step-up security measures to frustrate attackers, not trusted users.

The Challenge

Keep logins easy while responding to risk

In the world of hybrid work, employees access corporate resources from almost anywhere. Working from different locations, devices, and networks gives users greater flexibility and productivity, but can make it difficult for organizations to evaluate the risk level of each login attempt and protect their data and other resources. One way to ensure secure access is to force users to go through time-consuming authentication measures, and to authenticate frequently. While this solution would guarantee high levels of trust, it would also create a lot of friction for the end users and conflict with business priorities. Organizations that are attempting to fulfill a zero trust security strategy need to find new ways to adapt and respond to evolving risk signals.

Another challenge with current security tools is the lack of visibility and reliance on IP (internet protocol) address as the main risk signal. While IP addresses can be a helpful indicator, the move away from the corporate network, as well as the use of VPNs (virtual private networks) that can obfuscate location, have weakened this signal. This creates tension for businesses that want to responsibly track unusual activity, but also want to respect employee privacy.

Finally, traditional controls at the time of authentication have been historically inflexible and blunt. Rather than offer the opportunity for the user to reestablish trust or self-remediate, the typical controls are to allow or block the user. These extreme outcomes run the risk of stopping an honest login attempt. while accidentally granting access to a fraudulent user.

There needs to be a new solution that respects user privacy, evaluates appropriate signals, and adjusts outcomes to avoid adding unnecessary burdens to the end user.

The Solution

Dynamically assess risk behind the scenes

01 Enhanced Visibility

Duo Policy has historically used contextual signals such as user location and network from web access requests, as well as device attributes and status from Duo Mobile (**iOS**, **Android**) and Duo Desktop.

Duo is now expanding those signals to include patent-pending Wi-Fi Fingerprint technology. Wi-Fi Fingerprint enables Duo to convert Wi-Fi network information into anonymized data to know if the user has changed locations, without ever tracking that user's location.

Duo also incorporates data from known attack patterns. For example, Duo can intervene in a scenario in which a user is experiencing a push harassment attack, or when a user receives multiple fraudulent push attempts. These new signals allow Duo to adjust the security requirements in real time to help secure access.

02 Security Resilience

Rather than simply block or allow access, Duo's solution offers more granular controls at the point of login. Administrators can respond to risky situations by increasing friction through new authentication methods, including **passwordless** or Verified Duo Push.

Verified Duo Push steps up the traditional Duo Mobile Push by requiring the user to enter a code displayed on their login screen. This prevents a user from absentmindedly accepting a Duo Push when they are not actually trying to login. Once the user enters the code, and reestablishes trust, they will be able to return to the regular **Duo Push**, without the additional friction.

The purpose of these new authentication tools is to step up the security measures when the risk signals warrant extra caution, and remove them when trust has been established.

03 Improved User Experience

For a typical user that is following their regular routine, they will be unaware that Risk-Based Authentication has been activated. They can easily gain access, with no disruption to their day. Duo's Risk-Based Remembered Devices enables this functionality to allow for a quick and secure authentication experience.

However, if a user's circumstances do change by logging into a public Wi-Fi network from an unusual location, for example, that would adjust the user's verification requirements. Duo would automatically evaluate that change in risk and might ask the user to complete a Verified Duo Push to reestablish trust.

This requires no additional work for the IT Administrator or security teams, as Duo's risk-based policies go into effect in real-time, at the point of login.

Cisco Duo protects against breaches with a leading access management suite that provides strong multi-layered defenses and innovative capabilities that allow legitimate users in and keep bad actors out. As a trusted partner, Duo quickly enables strong security while also improving user productivity.

Try it for free at **duo.com**.