CISCO SECURE | DUO

CISCO The bridge to possible

Risk-Based Authentication

Risk-Based Authentication

Table of Contents

Introduction to Zero Trust

Secure access used to be simpler. Everyone logged into the same corporate network, on a managed device, with firewalls to protect internal resources from outsiders.

But we live in a hybrid-work world now, with more people working from home, in coffee shops, and while traveling. Each new login attempt from each place and device must be evaluated for risk. Additionally, there needs to be a new model that no longer relied on the corporate network to establish trust and verify access. Zero Trust provides a framework for rethinking trust at each access decision, as employees seek to work from anywhere, on any device.

As Cisco Advisory CISO Wendy Nather summarized Zero Trust, “Trust is neither binary, nor permanent.” In other words, no access attempt is either trusted or not; instead, it is measured on a relative scale to determine if that attempt is in a “high” or “low” trusted situation. It also accounts for change. If an attempt once received “high” trust, it does not automatically qualify for “high” trust later, as trust is constantly being evaluated.

Why Risk-Based Authentication?

One simple solution to reduce the challenge of uncertainty is to make each employee complete frustrating and time-consuming steps at each authentication request. This might guarantee high levels of trust, it would also create a lot of friction for the end users and conflict with business priorities. Organizations want to ensure security, but not at the expense of productivity.

That's where Risk-Based Authentication (RBA) comes into play. Rather than make the end user jump through hoops to login, all the heavy lifting is done in the background. Through a series of signals, RBA can evaluate risk during a login attempt and provide the right level of friction, or additional security measures, based on the corresponding risk level. This enables both security policies and risk signals to work together to create an automated and dynamic experience for the end user. This solves two core challenges for an organization:it allows the end user to quickly and easily gain access, and ensures that access is secure. Tech and security analysts predict enterprises will shift to implementing passwordless authentication for their users to enable this modern digital transformation.

Current Challenges With Risk-Based Authentication

Different versions of Risk-Based Authentication have existed, but with the change in remote and hybrid work, and the increasing noise from new signals, the difficulty of the task has likewise increased. One main challenge of RBA today is its reliance on IP, or Internet Protocol, as an indicator of trust. Historically, IP has been a useful tool because it can communicate a person's location and if the network is safe to use.

When every employee was logging onto a corporate IP, it was a strong signal that trust was high. In today's workforce, remote workers might be logging in from a home office or public Wi-Fi network. IPs can also be masked when a worker uses a Virtual Private Network, or VPN. This does not mean that evaluating IP addresses is a worthless signal; it can and should be evaluated at the point of login. However, if it is the only signal evaluated, it might not provide a full picture of the current level of risk.

Traditional RBA also fails to fully address challenges of employee privacy. No employee wants their workplace to constantly track their location down to whether they moved from the dining room to the office. If employees do not want their user location to be constantly tracked, but employers need to evaluate some signal for a change in risk, this creates an inherent tension that must be resolved.

Finally, Risk-Based Authentication controls have been historically blunt. If there is no risk, a user can log in and if there is risk detected, they are blocked. This solution does not evaluate individual circumstances and adjust the outcome based on the risk level. There is also no option for an end user to self-remediate a potential risk in order to regain account access. This can lead to user frustration, and more work for IT help desks that have to unlock the flagged accounts.

Risk-Based Authentication Solution

In order to work towards fulfilling the ideals of Zero Trust, Risk-Based Authentication solutions must evolve to meet the needs of security teams and the end users. One simple model for conceptualizing risk-based authentications is by breaking up the login process into three moments: the signal, action, and outcome.

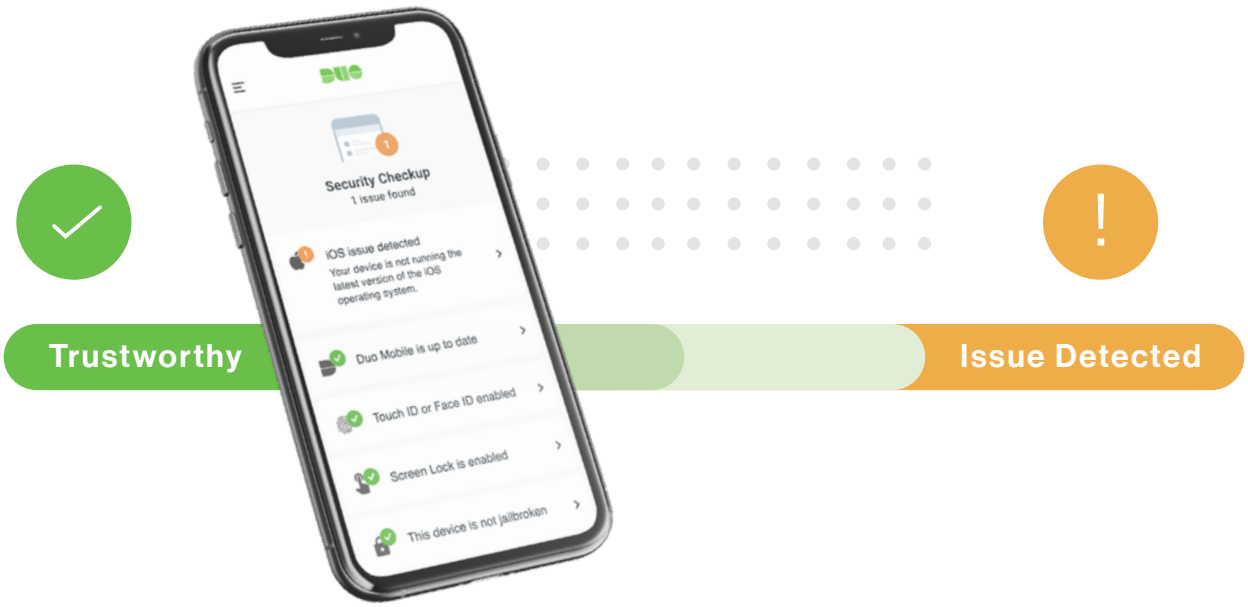
The signal takes in various indicators of risk to assess the trust of the situation. The action is where the decision engine digests those risk signals to evaluate the best mitigation to the assessed risk. Finally, the outcome is what the end user experiences upon login, with the level of friction dependent on the signal and actions. In a holistic risk-based solution, signals, actions, and outcomes can interact dynamically.

As the Risk-Based Authentication solution does the work behind the scenes, your typical end user will most likely not even know that there has been a change in the security posture. If they deviate from their usual schedule, they might feel the impact of RBA, but only through slight nudges to re-establish high trust. The goal of Duo's Risk-Based Authentication is to improve security without burdening users.

Signal: How to Evaluate Risk Responding to Data

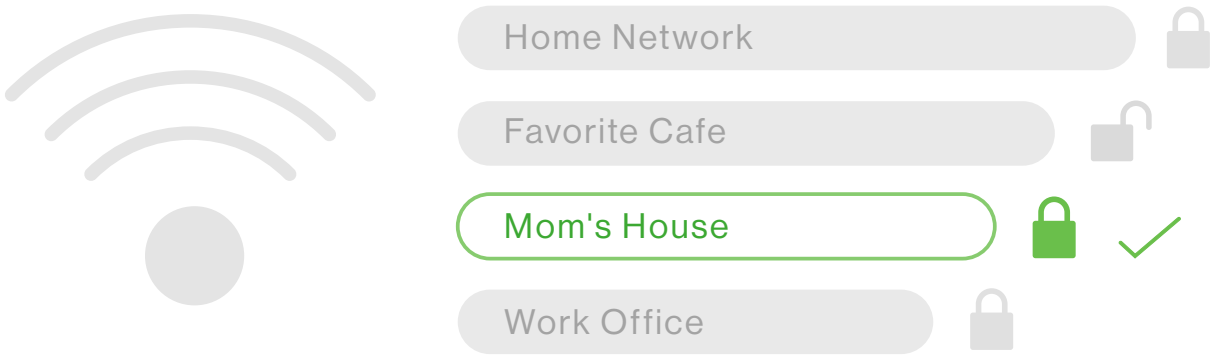
So what signals does Duo use to evaluate risk?
Duo Policy has historically used contextual signals such as

- User location and network from web access requests
- Device attributes such as OS version, browser version, device security settings
- Device management status from Duo Mobile (**iOS**, **Android**) and the Duo **Device Health App** (Windows, MacOS). frustration, and more work for IT help desks that have to unlock the flagged accounts.



For example, a company might have a policy set up where a user cannot access an application if the firewall is turned off. Upon attempting to log in, Duo would block access and inform the user of the next steps: turn the firewall back on in order to proceed with the login attempt.

While Duo's traditional signals provide helpful context to evaluate risk, Duo is expanding those signals to incorporate user Wi-Fi Fingerprint and known attack pattern data. Duo's patent-pending Wi-Fi Fingerprint technology is a new way to evaluate user location while protecting user privacy. The Wi-Fi Fingerprint can evaluate the Wi-Fi Networks that are visible to the access device to determine if the user's location has changed. For example, when you log in to your home Wi-Fi, you might see your neighbors' Wi-Fi network show up on the list of potential networks.



These Wi-Fi networks are typically static and extremely geographically specific. Duo converts the Wi-Fi network information into anonymized data, known as the Wi-FI Fingerprint. When a user attempts to login to a protected application, Duo verifies if the user's current Wi-Fi Fingerprint is the same as past Fingerprints; this determines if the user is in the same location from the last authentication attempt. Duo evaluates this signal without ever knowing exactly where the user is, maintaining that individual's privacy and security.

Responding to Known Attack Patterns

In order to evaluate a user's risk level, Duo also incorporates signals from known threat patterns. These known attack patterns come from authentication data and continuous research. Duo evaluates the following types of security patterns:

- User Marked Fraud: A user receives a second factor authentication attempt, denies the attempt and marks it as fraud
- Call or Push Harassment: A user receives a call or push request repeatedly that is not responded to, marked as fraud, or marked as a mistake
- Push Spray: A single location, identified by IP address, attempts to log in to multiple accounts
- Consecutive Failures: A single IP and user login attempts to log in with multiple, consecutive failures
- Compromised Account: The authentication and access devices appear to be from separate countries

Action: Decision-Making Engine

In Duo's traditional **Adaptive Access Policy**, Security and IT administrators have the power to set policies to influence a group's ability to access specific applications, as well as control the type of **authentication method** (example: only allow Duo Push rather than a one-time passcode).

Duo's new decision-making engine takes the manual work away from Duo administrators and automatically responds to risk. The algorithm evaluates a variety of risk signals to determine where the login attempt exists on the spectrum of trust. For example, if a user logins at their normal time, normal location, and on their corporate device, the decision-engine would label it as "high trust" and would not add extra steps to the login process. However, if at midnight a user receives repeated push notifications in a row, similar to the push harassment attack pattern, Duo would "step up" and ask for only the most secure factors that mitigate that risk. Since the attacker would be unable to fulfill the more secure factor, this would block the attacker's access and end the push harassment.

Duo is able to both ingest and react to these new and traditional signals in real time to protect the organization from risky logins, without adding unnecessary friction for end users. This also takes the burden off Duo administrators as they can rely on a robust engine to react to risk signals without having to manually set them up for individual users or applications.

Outcome: Impact on the End User

In Duo's traditional Adaptive Access Policy, Security and IT administrators have the power to set policies to influence a group's ability to access specific applications, as well as control the type of authentication method (example: only allow Duo Push rather than a one-time passcode).

Duo's new decision-making engine takes the manual work away from Duo administrators and automatically responds to risk. The algorithm evaluates a variety of risk signals to determine where the login attempt exists on the spectrum of trust. For example, if a user logins at their normal time, normal location, and on their corporate device, the decision-engine would label it as "high trust" and would not add extra steps to the login process. However, if at midnight a user receives repeated push notifications in a row, similar to the push harassment attack pattern, Duo would "step up" and ask for only the most secure factors that mitigate that risk. Since the attacker would be unable to fulfill the more secure factor, this would block the attacker's access and end the push harassment.

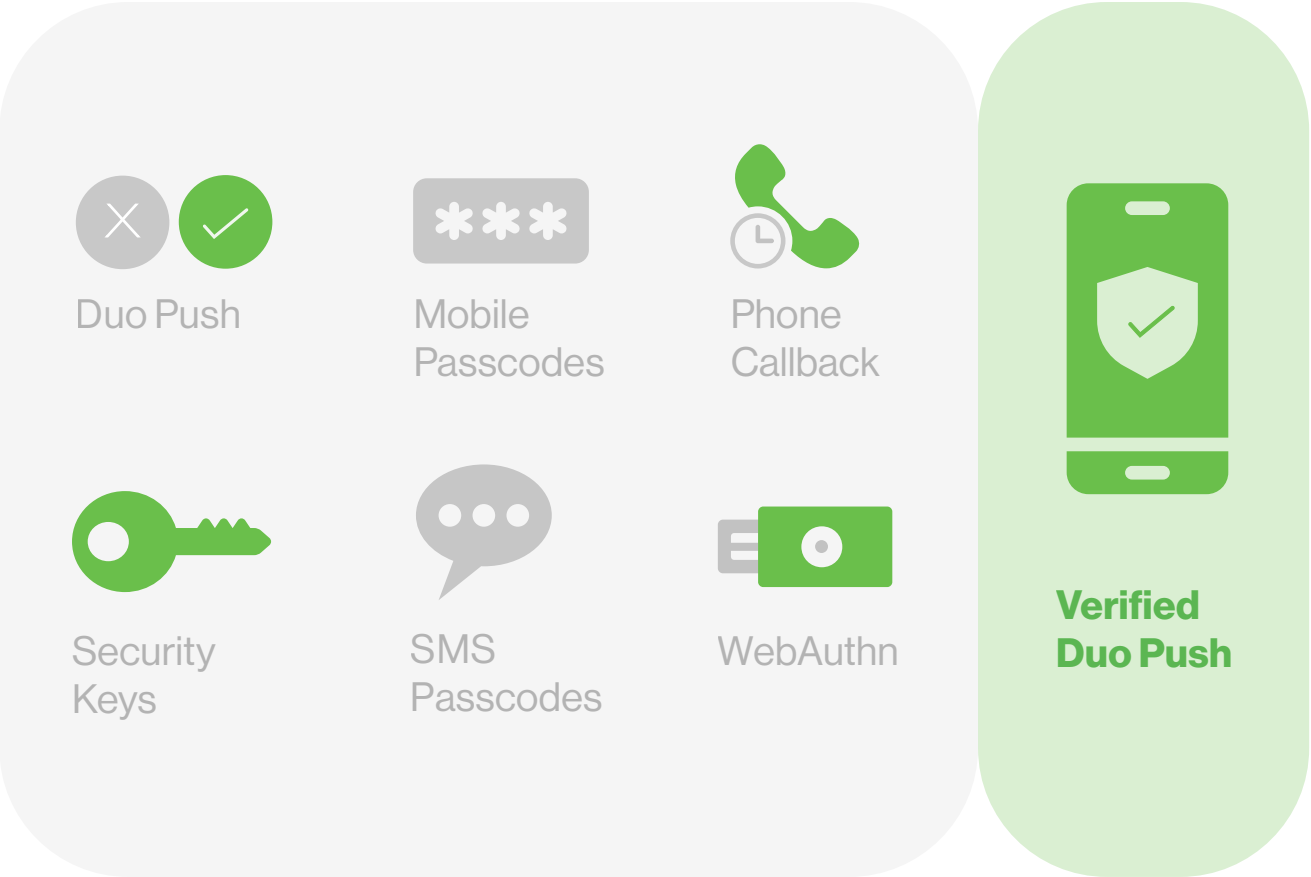
Duo is able to both ingest and react to these new and traditional signals in real time to protect the organization from risky logins, without adding unnecessary friction for end users. This also takes the burden off Duo administrators as they can rely on a robust engine to react to risk signals without having to manually set them up for individual users or applications.

Risk-Based Factor Selection

So what counts as a more secure factor? When it comes to multi-factor authentication, not all factors are created equal. For example, an SMS passcode can be phished, similar to a username and password. While SMS passcodes can be useful if there are no other means of authentication, in general it is best to limit or remove this functionality.

As a more secure factor, Duo supports phishing resistant authentication factors for MFA such as **FIDO2 security keys** and built-in device biometrics, such as TouchID. These authentication factors provide a high level of assurance and minimize friction with the one-tap convenience that customers are used to with Duo. Some organizations may be ready to ditch the passwords and embark on a passwordless journey.

Duo Passwordless also provides phishing resistant authentication using Windows Hello, Touch ID, or security keys by leveraging **WebAuthN** protocols. However, passwordless might not be the ideal solution for all organizations if their users do not currently have access to devices with biometric authentication, or have the budget to invest in security keys.



Therefore, Duo also offers a new, more secure authentication method, Verified Duo Push. Verified Duo Push follows Duo's traditional universal prompt push notification, but rather than just selecting "Approve" or "Deny" to login, the user must also enter a passcode displayed in the user's access device into the Duo Mobile app. This prevents a user from absentmindedly accepting a Duo push when they are not actually trying to login. Similarly, if there is a fraudulent login attempt or a push harassment attack, the unauthorized user would be unable to enter the code in the Duo mobile app, which would prevent access.

While stepping up to Verified Duo Push does temporarily add more friction to the end user, if that user follows the steps and successfully completes a Verified Duo Push, the user will be brought back to the regular factor selection. Then, at the next login attempt, the user will be prompted to follow Duo's traditional push option.

While stepping up to Verified Duo Push does temporarily add more friction to the end user, if that user follows the steps and successfully completes a Verified Duo Push, the user will be brought back to the regular factor selection. Then, at the next login attempt, the user will be prompted to follow Duo's traditional push option.

Why Duo?

User Experience:

The key to strong security is to enact security protocols that all employees will follow. If users are concerned that if they report a fraudulent login attempt they will be locked out of their account, then they won't report it. If users do not have a means to self-remediate, then they might continue to engage in risky behavior.

Risk-Based Authentication through Duo seeks to empower users to quickly and safely gain secure access, without ignoring relevant risk signals. And more importantly, if there are no risk signals, Risk-Based Remembered Devices allows users to go about their business with no interruption. The goal of a good RBA solution is to take all of the burden of evaluating a risky situation away from the end user and put it behind the scenes. This allows users to spend less time authenticating for a smoother, uninterrupted workflow.

Defense In-Depth

In addition to removing burdens from the end user, it is also important that a Risk-Based Authentication solution is a more secure solution. Duo is able to combine both traditional signals, like IP address, along with novel signals, like Wi-Fi Fingerprint, to put together a holistic risk assessment and act in real-time when a user logs in. Through Duo's Trusted Endpoints, Device Health, and Device Remediation policies, along with RBA to help prevent threats in real-time, organizations are well-equipped to work towards a Zero Trust strategy.

Risk-Based Authentication also gives administrators more control over how to remediate potential risks. They no longer have to choose between "block" or "allow," but can instead evaluate where a user falls in the risk spectrum and respond with the equally appropriate friction. With the number of signals and alerts security teams must manage, RBA offers administrators the ability to ensure each login is secure based on individual circumstances, without requiring manual intervention.

Through Duo's solution, users are able to quickly and securely access the data they need to get to work, without compromising security. Ultimately, the goal of Risk-Based Authentication is to create more roadblocks for potential attackers, without disrupting the lives of trusted users.

Explore how Duo can improve your security posture by frustrating attackers, not trusted users.

Start a Free Trial

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo is a trusted partner to more than 25,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more.

Try it for free at duo.com.

cisco SECURE

Cisco Secure delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform.

Learn more at cisco.com/go/secure.