BEYOND IDENTITY

Authentication Metrics to Track and Why They Matter

Why track authentication metrics?

Metrics matter because what you can measure, you can improve. Metrics provide visibility into what is and is not working for a business, enabling the company to improve processes or make strategic investments to maximize efficiency and revenue.

Authentication is a vital component of the user experience. In fact, many of a user's most important—and potentially most frustrating—interactions with a company's website involve the authentication system, including:

- **Account Creation:** Account creation is a potential customer's first interaction with a business and the company's first chance at providing a positive user experience. If the account creation process is painful, a customer may give up and abandon their cart or seek out a competitor.
- **Account Login:** Users will most likely need to log into their accounts every time they visit a company's website or attempt to take a privileged action, such as changing account information. If the user has forgotten their password or the process is inconvenient—such as needing access to a phone for 2FA—the user may leave the site rather than authenticating.
- **Password Resets:** Knowledge-based authentication systems, such as passwords, run the risk that the user will forget their password. Password reset systems are designed to fix this problem but are often time-consuming and frustrating. Plus, often the process is escalated to customer support teams to resolve.
- **Data Breaches:** Data breaches have become a near-daily occurrence and often involve the loss of a customer's authentication data, such as saved username and password data, or worse personally identifiable information (PII) attached to their account. No customer wants to receive an email or see a news story about how a company was breached and lost their data.

Authentication must provide security, efficiency, and a positive customer experience. However, determining whether an organization's existing systems achieve these goals requires a means of measuring these properties, making authentication metrics essential to a company's success and profitability.

Measuring the authentication experience

Making authentication as seamless and painless as possible is vital to optimizing the user experience and maximizing revenue.

Companies can measure the effects of authentication on the user experience via: user conversions, usage of various authentication methods, and failed authentication attempts.

User conversions through the authentication lifecycle

Users will need to authenticate at various times ways, including:

- **Registration:** percentage of failed, incomplete, and successful registration completions
- **Login:** percentage of failed, incomplete, and successful logins
- **Recovery:** percentage of failed, incomplete, and successful recovery completions, percentage of users who required help from customer support
- **Checkout:** percentage of users who choose guest checkout, percentage of users who drop off after being prompted to create an account

A painful authentication experience is a common cause of cart abandonment and lost sales. By measuring conversion rates when users are performing authentication actions, a company can determine if a time-consuming or high-friction authentication experience is driving losses in sales and revenue.

Authentication latency

Speed in seconds or milliseconds is also an indicator of authentication health. If authentication is too slow, the user will be more likely to drop off.

Typically engineering teams have tools in place to measure the time it takes for each step during an authentication request, challenge, and response. This is not only a helpful measurement for troubleshooting, it can help identify areas of improvement to accelerate the authentication flow.

Usage of authentication mechanisms

Most companies have a variety of different authentication mechanisms available to users. At a minimum, most web pages offer password-based logins as well as single sign-on (SSO) using social media accounts (Google, Facebook, Apple, etc.). Users may also have enabled multi-factor authentication (MFA) with various factors, such as SMS-based one-time passwords, authenticator apps, or biometrics.

The percentage of customers using each available authentication mechanism can provide valuable insight into whether an authentication mechanism is working for customers. If most users are opting for social logins over passwords or avoid SMS-based one-time passcodes (OTP), this is an indication that passwords and SMS-based OTP are providing a poor user experience.

Failed out-of-band authentication

Most of the user authentication experience is performed on the company website. However, some authentication experiences—such as password resets and MFA—involve out-of-band (OOB) communications using SMS, email, or mobile apps.

These OOB communications are a common source of UX friction and abandoned sessions. If an SMS or email takes too long to arrive or a user needs to grab their smartphone to get a one-time password, they might abandon the session. Measuring the success and failure rates of password resets, MFA, and similar communications can provide insight into whether these processes are resulting in lost customers and sales.

Securing the authentication experience

The purpose of authentication mechanisms and processes is to verify a customer's identity. If the authentication process can be bypassed or exploited, the attacker gains illegitimate access to the user's account and their sensitive data.

Account takeover attacks are a common threat to businesses and their customers. If an attacker can guess or steal a user's authentication information (password, MFA codes, etc.), they can perform fraud using the customer's accounts.

By measuring its vulnerability to account takeover attacks, a business can determine the strength of its authentication system and its potential exposure to fraud. Some key account takeover metrics include:

- **Number of Attempted Attacks:** Cybercriminals commonly automate account takeover attacks, trying many potential passwords and looking for a match. By analyzing login traffic for suspicious factors—location, IP address, rate of requests, user agent strings, etc.—an organization can estimate the number of attacks that it is experiencing.
- **Authenticated-Related Complaints**: A successful account takeover attack will likely result in a user complaint or other customer support request. Or customers may report phishing attempts.
- **Exposed and Breached Credentials:** If an attacker learns a customers' login credentials, they will likely use them to access the user's account or sell the

data on the Dark Web. Monitoring for successful suspicious login attempts, fraudulent activity, and passwords leaked on the Dark Web can help to detect breaches and evaluate the security of a company's authentication system.

- **Insecure User Accounts:** Users commonly use weak, reused, and breached passwords for online accounts. If a company offers password-based authentication, testing a sample of user credentials against known weak, common, and breached credentials can help to determine if user behavior is placing the company and its customers at risk.
- **Cost of Fraud Per Breached Account:** Suspicious activity on user accounts may leave a merchant footing the bill for fraudulent transactions. Calculating the average cost of fraud per breached user account provides an estimate of the price of weak user authentication.

Successful account takeover attacks hurt both customers and the business. Securing the authentication process can improve profitability, enhance the user experience, and simplify compliance with data protection regulations.

Improving operational efficiency of user authentication

The user authentication process can follow one of two potential paths. A successful authentication provides the user with immediate access to their account. A failed attempt, on the other hand, can force a user to start over or follow a time-consuming and painful account recovery process.

Optimizing the authentication experience requires metrics for both of these paths. On the positive path, a company should measure the latency or speed of authentication. If the authentication process takes too long, it could result in lost customers and consume a company's IT resources.

The path of account recovery can create significant costs for an organization as resources are diverted to support password resets or other account recovery actions. Some key recovery metrics to track include:

- **Requests Requiring Customer Support:** Ideally, a user will be able to complete the account recovery process independently without contacting support. Tracking the percentage of recovery requests that require customer support enables an organization to measure the effectiveness of automated recovery processes and systems.
- **Authentication-Related Support Calls:** Customer support is responsible for meeting a variety of customer needs. Determining the percentage of support calls that deal with password resets and similar issues helps to measure the resources consumed by authentication issues.

- **Support Session Time:** An authentication-related customer support call requires verification of the caller's identity, which can take significant time. Measuring the duration of the average authentication-related support call helps with estimating the impact on the customer and on the business.

All of these metrics show the cost of password resets and other authentication-related support calls. This can help a business to determine the return on investment of transitioning to a passwordless authentication system that eliminates these issues.

Streamlining and securing the authentication experience

Companies have various options for authentication mechanisms. However, some are better than others. For example, many of the user experience, security, and operational efficiency issues that companies face are specific to password-based authentication systems. Attempts to bolster the security of these systems with MFA provides limited benefits, especially with weak authentication factors and low consumer adoption.

Companies looking to improve the user experience and decrease costs to the business should consider making a switch to passwordless authentication. Passwordless authentication is easier for customers to use, offers stronger security than passwords, and eliminates the need for painful, expensive, and high-friction password reset processes. Additionally, passwordless authentication reduces costs and improves profitability for businesses by decreasing their risk of data breaches and eliminating authentication-related customer support calls.

By making authentication secure and easy, you can not only drive revenue forward but also reduce operational costs for your internal teams. Learn more about making the switch to passwordless today with Beyond Identity.

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.