The Case For Passwordless Authentication

thumbsignin

The Case For Passwordless Authentication

The password as a means of authentication has outlived it usefulness. It is now widely accepted that not only are passwords difficult to use and manage for the organizations as well as their users. However, more ominously, it is at the root of many serious and costly problems due to their inherent security flaws as evidenced by the recent high profile breaches at Yahoo, LinkedIn, Target and the DNC. As organizations require the passwords to be more complex and changed more often, their usability has taken a nosedive that has led to poor user security practices such as using the same password for multiple applications as well as increased IT support costs as users forget their passwords more often.

As biometrics technologies become more mature and go mainstream, they are emerging as an increasingly desirable authentication mechanism for users as well as organizations alike. They provide authentication that is simpler and stronger with compelling ROI. The rest of this white paper discusses the benefits of adopting passwordless authentication within your organization.

Benefits

#1 Time Savings and Productivity Gains

Logging in using passwords is a time consuming process if you consider the time taken to type, retype, remember, change, create passwords. While these actions may individually seem miniscule, they are performed multiple times a day and can easily add up to three minutes per day for every user.

It is easy to see how eliminating passwords can result in substantial productivity gains and cost savings for the organization -

Time saved per year per employee

= 3 min/day x 240 working days / year

= approx 12 hours / year

Cost saved per employee per year (assuming average employee cost of $40 per hour)

= 12 hours / year x $40 / hour

= $480

Cost saved for an organization of 1000 people

= $480,000 per year

#2 Ease of Use

Transitioning to passwordless authentication means upgrading your users' authentication experience - they don't have a password to remember, change, enter repeatedly, or worry about being stolen. This makes authentication an enjoyable experience and and improves important metrics like user engagement and retention.

#3 Reduced Support Costs

According to the Gartner Group, between 20% to 50% of all help desk calls are for password resets. Forrester Research states that the average help desk labor cost for a single password reset is about $70. If that seems like a high number, consider that this includes not just the time of the support staff but also that of the user requesting the password reset and the time he/she has lost being locked out of his account until the password has been reset.

Eliminating passwords means eliminating password reset calls saving time for both the user and the IT support staff. The ROI due to such reduced costs is straightforward. In our example of the organization with 1000 users, assume conservatively that each user makes two password reset call per year. If each call costs $70, the organization spends **$140,000 per year on password reset calls**. This can be easily reduced to a small fraction by deploying passwordless authentication solutions.

#4 Perception of Security

From a user perspective, the fact that they are using a biometric to authenticate with a system gives them a sense of comfort and security. They intuitively understand that their fingerprint / retina scan is unique, personal and cannot be stolen - unlike passwords. This increases user confidence in the system.

Choosing the Right Vendor

With the move away from passwords towards biometrics being inevitable, we expect a large number of organizations to transition their existing enterprise or consumer apps to passwordless authentication. Such organizations should consider using a vendor who offers a products certified to the FIDO UAF (for passwordless experience) and U2F (for second factor experience) standards. Other factors to look out for are the availability of web APIs, mobile app SDKs, prebuilt authentication widgets, customizability of the solutions, flexibility to adapt to your specific use cases, existing

feature roadmap, plans to support the evolving standards, out of box integration with enterprise applications and the ability to provide ongoing technical support.

ThumbSignIn provides a platform for organizations to easily integrate passwordless authentication mechanisms into their applications.

For more information and to test drive Thumbsignin for free visit www.thumbsignin.com