2019 Buyer's Guide to the Employee Authentication Galaxy

TRUSONA

A tool from your friends, the Trusonauts.

www.trusona.com

Welcome

Hey, rock star. Good to see you.

Whether you're implementing a second-factor authentication solution for the first time (congratulations!) or replacing an existing authentication solution (good for you!), dig into the details that will help you find the best fit for your employees while protecting your organization and, of course, your bottom line.

Use these tables to deconstruct and compare the **security, user experience, cost and deployment** of different 2FA solutions. We're throwing our hat into the ring, hoping to be helpful in your search.

Now, let's get straight to business. We hope you learn great things.

Security

While requiring a second factor of authentication is a no-brainer, there are a few other security concepts seldom discussed. Bad guys can (and do) steal static credentials around the clock. And you know all about the dangers of shared, weak passwords. You've seen them written on sticky notes on your employees' displays. To ensure the solution you choose isn't built on a shaky foundation, hunt for the real — often elusive — truly password-less 2FA.

Starter questions	*Trusona*	*Vendor A*	*Vendor B*
Dynamic auth Does this solution eliminate vulnerable, static credentials for good?	✓ Doesn't create usernames or passwords.		
Anti-replay tech Does this solution protect against session replay attacks?	✓ Patent-pending anti-replay ensures every login is unique.		
Truly password-less Does this solution eliminate passwords (not hiding them behind biometrics)?	✓ No passwords. Period.		
Adaptable auth Can I start with two factors and add additional ones as I see fit?	✓ Add more/different auth factors and/or ID proofing.		
FIDO-compliant Does this solution meet FIDO UAF requirements?	✓ Meets and exceeds FIDO UAF requirements.		
Other	Contact us to find out.		

The bottom line is: avoid the use of static credentials like usernames and passwords. They are so 1964! Also, stay clear of solutions that hide passwords behind biometrics or, worse, behind other names. Talking to you, Mr. Passcode.

User experience

Have you heard that security that isn't usable isn't secure? Usable security is security your employees won't work around. Look for tested, intuitive 2FA designed around the way people live and work. Learn the right questions to ask in search of legitimate user-friendly solutions. In a world of "frictionless" products and "better UX" empty promises, these chops will come handy.

Starter questions	*Trusona*	*Vendor A*	*Vendor B*
No extra hardware Does this solution eliminate extra hardware tokens to keep track of?	✓ Use tokens your employees already have.		
Not memory-based Does this solution eliminate my employees' need to memorize and manage credentials, or their cousins, knowledge-based answers (KBAs)?	✓ We all know, your employees have better things to think about.		
No typing Does this solution eliminate the pain of typing credentials or one-time passwords (OTP)?	✓ No typing for fewer slips and mistakes and less frustration.		
Third-party tested Has this solution been scientifically proven to be preferred by end-users?	✓ 7/10 people prefer Trusona's password-less 2FA over passwords.		
Other	Reach out to us. We love talking shop.		

Look for solutions that work across channels, including VPN, SSO and web apps. No passwords, no usernames and no typing equal a secure, elegant user experience for your employees.

There's an authentication world with no more hoops to jump through and no superfluous hardware. A world far more secure with happier employees who breeze into their accounts as easily as they would stroll into the office. Can you see it? You can make it happen.

Cost

How much should you pay for the security you deserve? Protecting your organization is paramount. Removing hurdles for your employees to work efficiently is a must. And it shouldn't break the bank.

Let's talk cost. Dough. Dinero. While you shop for 2FA for your employees, keep in mind not only MSRPs, but also latent fees like purchasing and reissuing hardware tokens, resetting passwords and the toll that managing on-premise solutions takes on your IT team.

Starter questions	*Trusona*	*Vendor A*	*Vendor B*
Upfront TOC Is the price of this solution free of added/hidden fees?	✓ Unlimited logins. No extra fees.		
IT help desk Does this solution eliminate time-sucking passwords that need to be managed, changed and reset?	✓ No time wasted on password reset calls, so your team can focus on what really matters.		
Existing hardware Does this solution rely on hardware tokens already in your possession?	✓ Trusona uses mobile devices. No extra hardware tokens.		
Maintenance Is this solution free of hardware maintenance, storage, distribution and disposal costs?	✓ No time or effort spent on managing extra hardware tokens.		
Other	Ping us. We'd be happy to chat.		

Give brownie points to 2FA that requires no extra hardware tokens so 1) you don't spend money on unnecessary tech and 2) your IT team isn't bogged down managing and supporting it.

When comparing price tags, don't forget to factor in the cost of doing nothing AKA the risk of sticking with usernames and passwords: unruly help desk call volume, never-ending IT tickets, and sneaky productivity losses. Not to mention the real possibility of an expensive cybersecurity snafu.

Deployment

Solutions that are easy for your employees to use are only half the story. During the shopping process, it's important to ask what kind of resources will be required of you. Prevent any unnecessary IT headaches by landing on a robust solution that's both easy to implement and manage.

Starter questions	*Trusona*	*Vendor A*	*Vendor B*
Cloud-based Is this service cloud-based?	✓ No hardware or software installation.		
Self-provisioning Can I forget about provisioning each employee?	✓ Forget time-consuming training and manual tokens.		
Easy onboarding Can my employees enroll themselves?	✓ No hand-holding required.		
Quick deployment Can my org be up and running quickly and with minimum effort?	✓ Spend less time in implementation and more time securing your org.		
Pilot program Can I try the tech with my employees in my environment before I buy?	✓ Pilots available for you to test functionality, integrations and receive user feedback.		
Other?	Glad you ask. Contact us to find out.		

To make life easier for your security administrators, select a vendor that supplies built-in integrations for major cloud apps, VPNs and SSOs so you can have a functioning solution out of the box without any unnecessary hassle.

Look for authentication that supports common protocols like Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) so you can integrate it across all your systems and have a standard for exchanging authentication data.

Wrap-up

In a sea of "no passwords" 2FA solutions, it's taxing to distinguish the real ones from the phonies — or the overly optimistic. When choosing 2FA vendors make sure to consider all the factors that affect that decision, including:

Security

Your organization's particular security needs, use cases and existing systems.

User experience

Your employees' user experience throughout the authentication journey (starting with onboarding) and the effect it has on security.

Cost

The total cost of ownership, including purchasing and maintaining hardware tokens or other latent charges.

Deployment

The time and effort required from your team to deploy and maintain the solution.

We understand choosing an employee authentication solution is no easy task. We'll be in touch to learn about your organization's needs and if/how we can help.

We look forward to hearing your thoughts.