So, You Want To Use ZoOm…

We Have *5* Important Questions Before We Get Started!

Over the years we have learned to pose a few important questions to organizations before they jump into the world of biometric security. It's a complex marketplace made even more confusing by irresponsible vendors that self-servingly ignore the need for transparency and 3rd-party testing. The following questions may appear to have obvious answers, but sincerely addressing them will save you (and us) time, money, frustration, and quite possibly your brand's reputation.

#1. Do you *need* better security? Or just *want* it?

Whether you realize it now, or not, changing the way you secure your attack surface is going to be scary to the people in your organization who resist change. We have spent years building ZoOm with relentless internal testing and 3rd-party evaluations, and we are here to ensure that your efforts will result in far better attack surface security and user convenience, and are well worth your time.

In the real world, ZoOm works: we have *never* had a single customer take ZoOm out of a production app. Users find it intuitive, and the security it provides is proven to be very real. We can offer plenty of social proof, but until your organization is on the other side of a successful implementation, some people in your organization are still very likely have anxiety about adopting something new.

So again we ask, do you really *need* better security? If yes, you can't afford *not* to integrate ZoOm immediately, and we are here to help you get that done. But if your business simply treats fraud as a write-off and your organization doesn't change until it's forced by government regulation, then now is probably not the best time for you to be dabbling in biometric authentication.

If that sounds like your group, please come back when you are really serious about implementation. There are tens-of-thousands of organizations that *need* ZoOm face authentication to survive and we want to focus our time with them right now.

#2. Do you think, "Facial Recognition (1:N) is picking 1 face out of a million-face database, so 1:1 must be a million times easier"?

You might very well fully understand facial recognition for 1:N matching in surveillance scenarios, but don't conflate 1:N Facial Recognition with 1:1 Face Authentication. 1:1 Face Authentication isn't easier because it's "only one person to check against." If Face Authentication was that easy, there would already be mass deployments everywhere and passwords would be a thing of the past.

That's obviously not the case, so please believe us when we say that 99.9% of the people in this industry who think they know a lot about Face Authentication still have *a lot* to learn. (Google

Dunning–Kruger effect) We say this with confidence because biometrics conference participants, most of the media, and even our "competitors" are uninformed, under informed or ill informed about Presentation Attack Detection, 3D Depth vs. Liveness, Conflating PAD & Matching, Continuous Learning, Complicit User Fraud, Biometric Phishing, Concurrent Liveness & Unique Human Traits, Diverse Training Sets, On-Device Frame Selection & Processing, and so on...

So who should be listened to on these topics? Our opinion is that only organizations with recent and relevant certifications should be pontificating about these topics, the rest of the industry who haven't gotten to that level of mastery simply do not know how deep these rabbit holes go and they should keep their naive views to themselves.

We've built and patented the only solution to have ever passed the iBeta/NIST/ISO 30107-3 Level 1&2 PAD Tests, and you won't find any of the typical unchecked biometrics industry hype here. We are confident, but not overconfident, and we will tell you the bad news along with the good. We really do have this figured this out, and unlike most biometric "solutions" the more you learn about ZoOm, the more you will like it, there's no gotchas, no "other shoe" waiting to drop. But we don't expect you to take our word for it, or even the word of a NIST-certified testing lab; if you've read this far, and really do need internal due diligence to appease the powers that be, we will happily address that in question 4.

#3. Are you willing to learn from us (and pay us to teach you)?

We all tend to frame things through our past experiences, and we know from the outside looking in that Facial Identification and Face Authentication look extremely similar. But we assure you, using a face identification algorithm-based system for face authentication is a serious mistake that your organization will come to regret.

Today, 2D Face Matching Algorithms are a commodity, and not even relevant outside surveillance scenarios. In 1:1 Face Authentication scenarios where the user interacts with the camera, they simply can't perform in the real world. In Face Authentication, **if it's not using a 3D FaceMap, it's not relevant.**

Our team has over 130 collective years in biometrics, has literally made history with the world's first sanctioned Anti-Spoofing test certification, and has unique knowledge and valuable experience to share. We are working with customers all over the world at all hours of the day and night, and there are unending demands on our time, so it's not feasible for us to spend a lot of time with you for free.

#4. Do you trust 3rd-party experts, or do you need focus groups and internal testing?

We're happy to help you get what you need either way. Obviously we *love* 3rd-party testing when it's done right by professionals. Problems quickly arise, though, when first-time internal testing teams don't know how to test scientifically, don't know how to use controls, and often don't even know how to measure success or failure within their own testing.

We have world-leading 3rd-party security test results and plenty of social proof that ZoOm is intuitive and well-liked by users around the world. However, organizations still often tell us that - even with their limited expertise - they need to conduct their own internal usability and security tests to ease internal concerns. We consistently find that successful internal tests uncover nothing new, and unsuccessful tests result from flaws in testing methodologies. Mistagged, unrecorded, or unanticipated variables can create false-negative results and skew opinions. To help, we've written the following guidance to benefit teams who want to conduct internal testing:

https://www.zoomlogin.com/ZoOm-Customer-Internal-Testing-Guidance.pdf
and https://www.zoomlogin.com/FaceTec_Liveness_Testing_Methodology.pdf

#5. What ZoOm configuration do you need?

You can add the Device SDKs to your apps and web pages, and connect to the FaceTec Managed API. Or, you can host your own Server SDK and provide your own API. We've made ZoOm flexible and have solutions that meet the needs of the smallest start-ups to the largest banks in the world.

ZoOm Configuration Options PDF: https://www.zoomlogin.com/ZoOm-Configuration-Options.pdf

To sign-up for a Developer Account: https://dev.zoomlogin.com/zoomsdk/#/

For pricing information, please visit: https://quote.zoomlogin.com/#/

Once you've answered these 5 questions for your organization, you are well on your way to better biometric security.

We look forward to working with you!

- The FaceTec Team