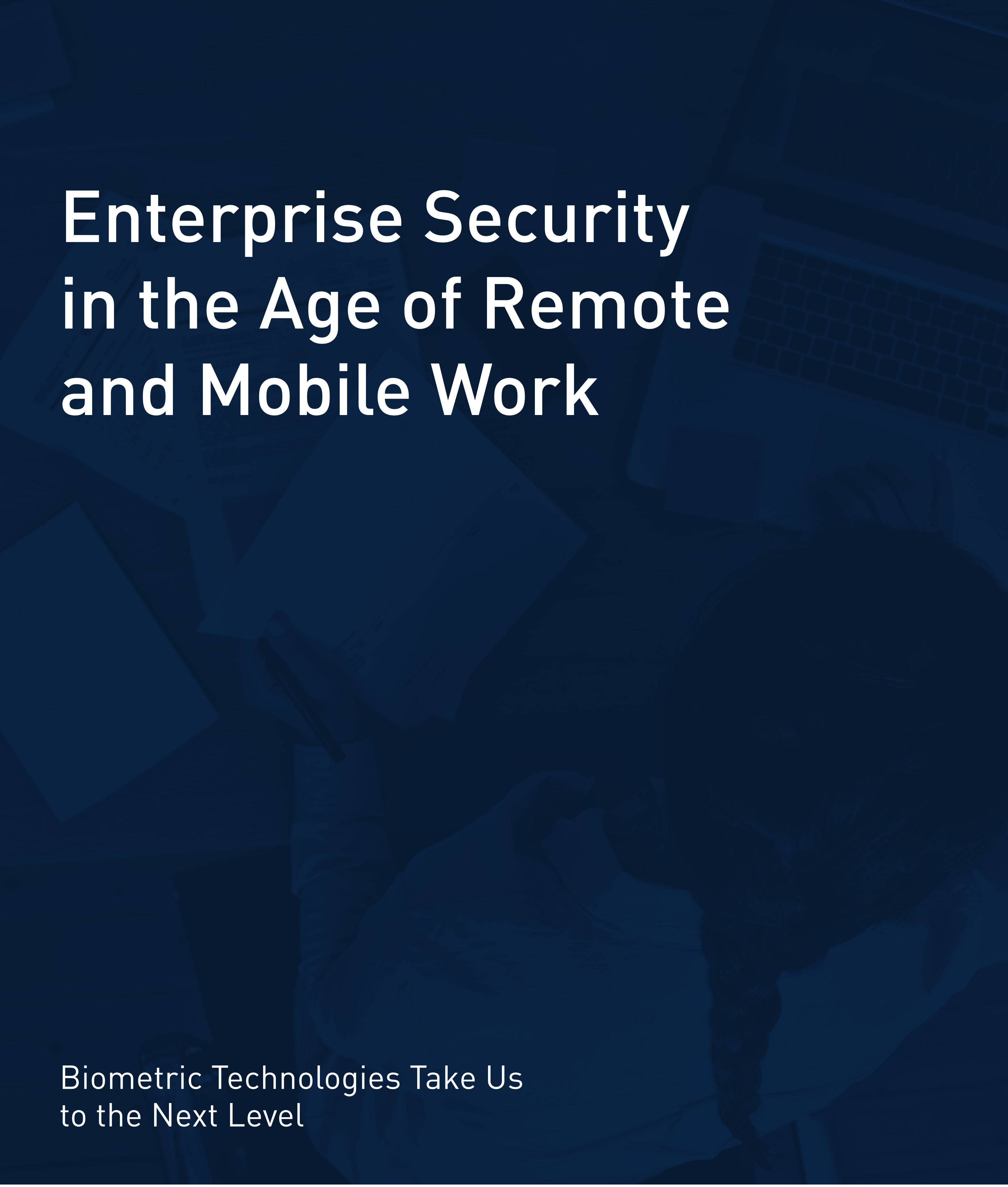


# Enterprise Security in the Age of Remote and Mobile Work

Biometric Technologies Take Us to the Next Level

AWARE

# New Work Means New Security Challenges

**Work has changed.** Advances in mobility and connectivity have accelerated the evolution of the modern business, allowing new types of enterprises to emerge. Thanks to the ubiquity of smartphones, tablets, and other connected devices, the classic nine-to-five workday confined to the cubicles of an office space is no longer the norm.

The new challenges of today's mobile-enabled workplace stem from an identity crisis.

Today's work environments are as unique as the people powering them, from the entry level up to the corner office. Wireless technology enables remote workers and mobile offices, keeping businesses on the move and allowing them to span the world. In today's "gig" economy, new, disruptive mobile apps empower independent workers to integrate their work into their life in a way that's best for them, turning their cars into taxis and their spare bedrooms into miniature hotels.

All the while, the rapid rate at which business culture is evolving, coupled with new economic and cultural pressures, has resulted in a renaissance of freelancing. In short: connected mobile technology has allowed us to adapt our work to fit our modern lives. And while this new kind of work opens up innovative new opportunities, it also brings with it new security challenges, specifically in regard to access management and fraud prevention.

The new challenges of today's mobile-enabled workplace stem from an identity crisis. With so many different access points to a business, it is more important than ever to have assurance that persons granted permission onto an enterprise's network are who they claim to be, regardless of the passwords they know or the security keys they have.

The consequences of this workplace identity crisis are plastered across today's headlines, with industry giants like Yahoo, Equifax, TimeHop, and Uber each reporting massive data breaches

affecting customers and employees, and paying heavily for it. The numbers of users impacted are staggering: the Uber breach leaked data belonging to approximately 25 million people[1]; approximately 21 million[2] were affected by TimeHop's blunder; 143 million users[3] had personally identifiable information compromised in the Equifax breach; and the Yahoo hack affected every single one of its 3 billion users. In addition to hefty fines and lawsuits, each company's reputation was tarnished. Given the value of personally identifiable information (PII), customers and clients are losing faith in businesses to safeguard their data.

In a Vanson Bourne survey[4] of 10,500 consumers from around the world, 66 percent of respondents indicated they are unlikely to do business with a company that suffered a data breach involving the compromise of PII. What's more, 67 percent of 18-24 year olds would pursue legal action in the wake of a data breach. But perhaps the most important result shed light on where consumers cast the burden of responsibility; not with the hacker who breached their data, but with the company that failed to protect it. Ninety-three percent of all polled would blame businesses for any data breaches they suffered.

Identity lies at the heart of security, and so strong identity technologies have emerged in lockstep with the rise in connected mobility. They enable enterprises to better safeguard the sensitive assets upon which they rely to be competitive. At the forefront of these technologies is mobile biometric authentication. Flexible, secure, and intuitive... done right, biometrics can solve the identity crisis of today's mobile workplace, enhancing security, efficiency, and convenience.

It's time for the mobile empowered enterprise to address its challenges. It's time to deploy biometrics.

[1] Chappell, Bill. "Uber Pays $148 Million Over Yearlong Cover-Up Of Data Breach," NPR, September 27, 2018, https://www.npr.org/2018/09/27/652119109/uber-pays-148-million-over-year-long-cover-up-of-data-breach

[2] "Timehop Security Incident, July 4th. 2018," TimeHop, Updated July 11, 2018, https://www.timehop.com/security

[3] "The Equifax Data Breach," Federal Trade Commission, accessed April 30, 2019, https://www.ftc.gov/equifax-data-breach

[4] "Data Breaches and Customer Loyalty Report 2018," Vanson Bourne, May 12, 2018, https://www.vansonbourne.com/client-research/15021801tc

# Biometric Authentication in the New Workplace

**Authentication is the process of proving** to a system that you are who you say you are.  Traditionally, this has been done with passwords and usernames. Passwords may have been sufficient before the advent of networks that allow for remote access to databases, but time has proven they are no longer sufficient for enterprise security. Of the four massive data breaches listed in the previous section, three were the result of compromised password credentials that impostors used to authenticate.

Biometrics technology makes use of measurements of a user's unique behaviors and physical traits. Your fingerprint, your face, your iris, the sound of your voice, even the way you type – these are all aspects of your biological identity that no one else has.

The inadequacy of the password in the age of mobility is easy to understand. Because a password is a piece of information, presenting it to authenticate only proves one thing: you know the password. A password system doesn't protect against stolen passwords, guessed passwords, or phished passwords. And what's more, they are inconvenient for the demands of connected culture. Mobile keyboards are optimized for fast communication, making the input of long incomprehensible codes incredibly inconvenient, and given the number of private accounts an individual user needs to protect, the best practice of having a unique password for every login screen has become unrealistic.

Biometrics technology makes use of measurements of a user's unique behaviors and physical traits. Your fingerprint, your face, your iris, the sound of your voice, even the way you type – these are all aspects of your biological identity that no one else has. Biometric technology essentially leverages these traits as a digital proxy of identity to prove you are who you claim to be to an information system. This makes biometrics ideal for authentication.

In an authentication scenario, biometrics can fully replace passwords. To login to a workstation  or gain access to an account, a user simply scans their biometric – by taking a selfie or touching a fingerprint sensor, for example – and the measurements from the scan are compared to a biometric template associated with the authorized user. If the biometric submitted matches the information in the template, and is proven to be from a live person, access is granted. If not, it's denied. The proposition is simple, secure and convenient. An "out of band" authentication mechanism can also be employed, where upon entry of a username on a desktop prompts the user to biometrically authenticate on their device.

The benefits of biometric authentication in the workplace are myriad. From a security standpoint, biometrics are largely immune to the pitfalls of passwords. This is because biometrics are not secrets, and so they can't be shared, lost, or phished. Their security is based upon their difficulty to reproduce.

Beyond increased security, however, biometric authentication also brings greater convenience and efficiency to the next generation enterprise. With biometrics, workers never lose or forget their credentials, completely eliminating time-consuming password resets and credential reissuance. Once a user is on boarded in the hiring process, submitting to a one-time biometric enrollment, they are set for easy access with no risk of demanding more work from administrators. When an employee or contractor leaves a company for any reason, it is just as simple to revoke their access, resecuring company assets without having to worry about changing passwords.

Workers can rest assured too, since biometrics are a more intuitive authentication method for the mobile channel. Biometric software can take advantage of built-in sensors on mobile devices, like the microphone or front-facing camera, making authentication for work as easy as taking a selfie, or speaking a phrase.

While biometric authentication is intuitive and simple in practice, there are key considerations that need to be taken into account when considering how to deploy the technology:

## Presentation Attack Detection

To protect against fraudulent attacks targeting the biometric security features, biometric authentication mechanisms include functions to perform liveness detection and spoof detection.  Without them, fraudsters might be able to use photos, videos, or recordings of a potential victim to spoof the algorithm by impersonating them.  There are several techniques used to do this, ranging from "active" methods that challenge the user to demonstrate they are showing a live image, to "passive" methods that use algorithms to detect suspicious artifacts in the biometric data.

Thanks to the rapid advancement of machine learning algorithms, biometric modalities such as face and voice are now ideal for bringing biometric authentication to a mobile-enabled enterprise.

## Mobile App versus Native Sensor

Many high-end smartphones now include some form of native biometric security, with dedicated sensors and integrated software. They are designed to be used for password-free access to the device and to mobile apps for using features requiring security, such as financial transactions. But for some applications such as enterprise security, native biometrics are not seen as optimal. This is in part because they operate as somewhat of a "black box", offering no clear view of how they perform, let alone any control over how they operate.

Biometric software can be incorporated into the mobile app and use universal device sensors such as camera, microphone, and keyboard. This permits optimization of the security features and user experience for their particular requirements, and avoids dependency on any single device or supplier, as well as functionality differences across the various devices owned by their user base. It's a more secure and desirable alternative for the average CISO..

## Multimodal Biometrics

The benefits of app-based biometrics also include multimodality – the capability of using multiple biometric types for authentication. The ability to offer face and voice authentication through a single biometric software solution enables greater convenience and the option to scale up security as the situation calls for it. Not all access is created equal, so while gaining access to a personal email might only require a biometric selfie, the permission to view a company's financial data might require facial biometrics supplemented with a spoken one-time password used for voice recognition.

Multimodal biometric solutions also enable enterprises to deploy the best biometric for any given situation. In a ride-sharing business, in which employees are operating vehicles, hands free voice biometrics are the more intuitive choice. But in situations in which speaking out loud would be problematic – in a shared office space, for example – contactless and secure face biometrics can work.

## FIDO® Certified versus Centralized Authentication

There are two main architectural paradigms in biometric authentication: device-centric and server-centric. A server-based approach offers a few advantages that might be important for some use cases. It allows collection of biometric data that can be used to improve algorithm performance and attack detection and monitoring. It also allows the biometric data to be used for other purposes, such as watch list searches.

A device-centric method can adhere to specifications from the FIDO Alliance, an industry consortium dedicated to developing standards for authentication with the aim of replacing passwords. The FIDO method keeps biometric templates and matching on the end user device, meaning no personal information is ever transmitted over networks. The advantages of a FIDO-based approach include scalability, prevention of large-scale breaches of biometric data, and a standards-based approach that affords lots of flexibility and vendor alternatives.

While there are a number of choices to make when picking the right biometrics for your business, it’s important to know that authentication is only one aspect of the workplace identity crisis that biometrics can solve.

# Identity Proofing with Biometrics

**Authentication is only truly effective** if the person enrolled in the system is known to be who they claim to be in the first place. Employers typically verify a new-hire's claimed identity as accurate in a process called "identity proofing," an essential first step in securing a business against fraud and insider threats.

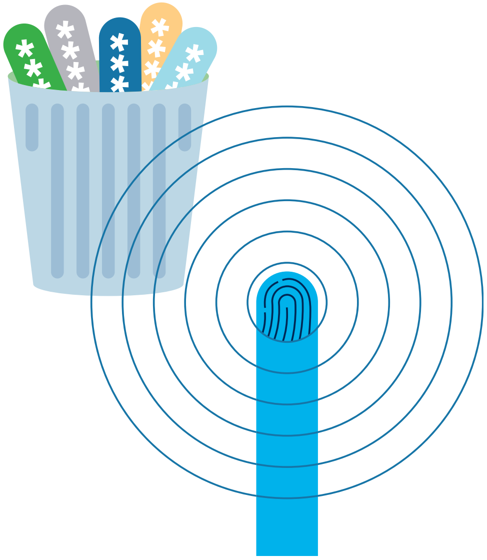
Ensuring biometrics are part of the identity proofing process seals the modern enterprise from the hiring stage through to day-to-day operations.

Traditionally, identity proofing is done using biographical data and identity documents, which are cross-referenced with identity databases, such as those operated by private data providers or government entities. While the use of biographics-based identity proofing is potentially vulnerable to falsified documents and well-known identity theft methods, a mobile-enabled workplace amplifies these challenges. Remote workers may have a much easier time getting onboarded with a false or stolen identity, simply by virtue of not being present for the onboarding process. Meanwhile, the massive workforce numbers and high employee turnover associated with the gig and sharing economies necessitates so many identity proofing events that the administrative burden can tend to open the door to bad actors, fraudsters, and criminal liabilities.

Biometrics, once again, solve this identity problem with great efficiency. In the identity proofing process, the applicant submits biometric data such as their fingerprints and face along with the normally requisite biographical data. The biometrics add a higher level of assurance to the subsequent identity checks. When compared to watch lists, criminal records, or an internal biometric database, any match with a record associated with another person will be flagged. Biometrics are unique to every individual, so a fraudster assuming a fake identity with stolen documents takes on a very high risk of discovery during identity proofing.

Unlike biometric authentication, which matches a single biometric to another, biometric identity proofing involves a process of "identification"; a one-to-many search. For instance, the FBI's Next

Generation Identification database contains multiple biometric modalities. A biometric background check for a job applicant performed as part of the identity proofing process will compare that person's biometric data to the millions of records in the data set, only producing exact matches. Hits uncover previous enrollments that can enlighten the prospective employer to an attempt on the part of their candidate to misrepresent their identity.



There was a time when procurement and deployment of such biometric identification capability was daunting and expensive, reserved only for the largest corporations and government institutions. But today, the broad adoption of cloud computing technology and software as a service (SaaS) makes biometric enrollment and identity proofing available on a SaaS subscription basis. “Biometrics as a Service” allows even small organizations to take advantage of powerful biometric matching technology in a low-risk, cost-effective, “pay-as-you-grow” manner, while ensuring the very latest advancements in AI, machine learning and liveness detection are being leveraged. Just as with SaaS, biometrics as a service enables use of software as an operational expense instead of a capital expense.

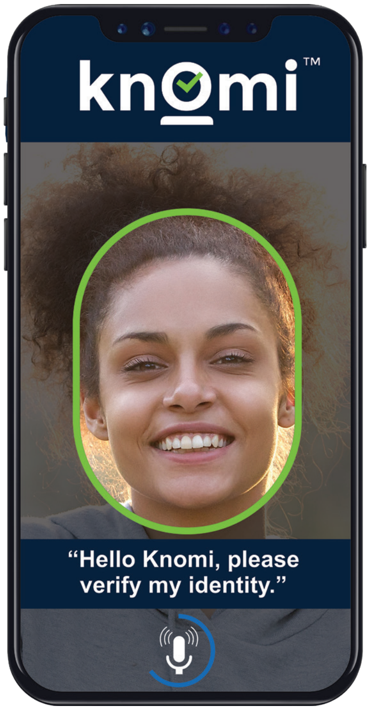
Ensuring biometrics are part of the identity proofing process seals the modern enterprise from the hiring stage through to day-to-day operations. Enrolling an employee with a biometrically-verified identity into your next-generation identification system means that people with access to company assets are exactly who they claim to be.

The combination of biometric identity proofing and biometric authentication is everything it takes to have a trusted, secure, and efficient workplace that's ready to adapt with the rapidly evolving mobile-enabled enterprise landscape.

# Implementing Biometrics in Your Workplace

**Biometric authentication** supported by biometric identity proofing can empower enterprises to adapt to advances in mobility and connectivity without opening themselves up to the myriad cyberthreats plaguing today's businesses.

Aware, Inc. offers biometric software solutions for every step of the process, with a flexible product line that can meet all your company's specific identity needs.



## Knomi

Knomi™ is a mobile biometric authentication solution comprised of a family of biometric matching and attack detection algorithms that use face and voice to enable secure and convenient multifactor authentication without passwords. Any government agency or commercial enterprise can deploy Knomi to enhance their password-based authentication mechanisms, making login to their systems more secure and convenient.

Knomi can also be used for identity proofing as part of a mobile onboarding solution, with advanced security checks that authenticate driver's licenses and passports, and spoof-resistant biometric facial matching between the live and printed images.

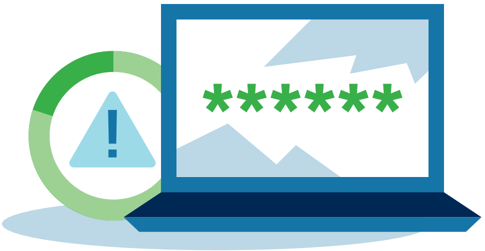
Knomi's advanced presentation attack detection algorithms detect not only authentication spoofs, but also false non-match spoofs that impact the ability to use the facial images for other biometric identity proofing functions such as watch list checks and duplicate prevention.

Knomi software components can be used in different combinations and configurations to enable either a server-centric architecture or a device-centric, FIDO Certified implementation.

## Indigo

Indigo™ is Aware's turnkey biometric solution, available through a traditional software license or as a cloud-based software-as-a-service (SaaS).  Indigo solutions are designed to deliver useful functionality and powerful biometric matching performance out-of-the-box, without requiring integration and configuration. They are built upon Aware's time-tested, market-leading software components for biometric enrollment, analysis, and matching. Indigo is ideal for biometric identity proofing when onboarding new employees.

# Tomorrow's Business is Built on a Foundation of Biometrics



**Work will continue to change,** but identity will always remain a fundamental element of enterprise security. As innovations in mobile technology and wireless connectivity spur evolution in our culture and redefine how we do business, trust founded on the basis of verified identity is crucial. Biometric software enables that trust to be practiced at a foundational level, ensuring that while your business grows, your security challenges don't. Integrate biometrics into your business and get ready for the next stage of the mobile-enabled enterprise.

**About Aware, Inc.**

Aware is a leading global provider of biometrics software products and solutions used to collect, manage, process, and match biometric images and data for identification and authentication.

Our products include complete biometric software solutions as well as the modular components used to build them: SDKs and applications for enrollment; fingerprint, face, iris, and voice matching algorithms; mobile biometric capture and authentication software; a biometric workflow and middleware platform, and a biometrics-as-a-service platform.

These products fulfill critical biometric functionality for applications in financial services, enterprise security, healthcare, human resources, citizen ID, border management, law enforcement, defense, and intelligence. Aware is a publicly-held company (NASDAQ: AWRE) based in Bedford, Massachusetts.