Daon

The Complete Guide to **Identity Continuity**

The Complete Guide to **Identity Continuity**

The Complete Guide to **Identity Continuity**

Introduction

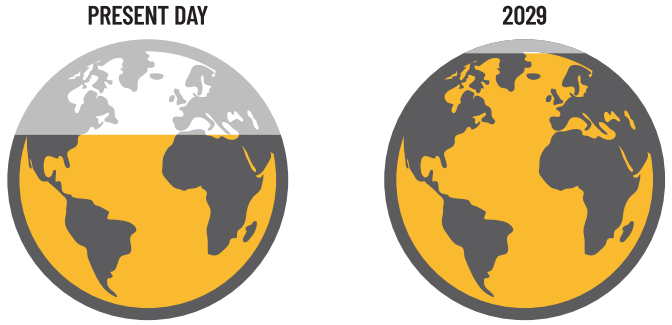
Modern daily life is a unique blend of digital and physical experiences that often intertwine to offer us convenience and insight. You can now scan your palm to check out at a grocery store or tap your phone to fuel your car with gas. According to Statista, the number of Internet users globally currently stands at 5.35 billion people but will reach 7.9 billion by 2029. In 2024, two-thirds of the world's adults use digital payments. That number is sure to increase, as is the complexity of our hybrid digital and physical lives.

For businesses, this paradigm shift is rife with both opportunity and complication. The Identity Theft Resource Center reports that publicly reported data compromises have hit an all-time high, with 353,027,892 individuals impacted last year—representing a 78% increase from the previous year. The average cost of a data breach is $4.5 million, not accounting for damaged brand reputation and lost consumer trust.

Generative AI technology has unleashed an onslaught of deepfakes, synthetic identities, voice cloning, hyper-convincing forged documents, and more. A fraudster can now blend real and fake information to create identity replicas that pass the scrutiny of traditional identity assurance tools and unlock consumers' most sensitive accounts and data.

Identity Continuity presents a novel, future-forward solution that balances consumers' desire for better, faster digital experiences with the highest levels of security. Identity Continuity cultivates a consumer's identity profile as a single, centralized entity and tracks it holistically across every transaction, in every channel (mobile, desktop, contact center, in person), and across time. It delivers insights cross-departmentally to allow for well-crafted, highly responsive user experiences.

Identity Continuity is built on a foundation of biometric factors—unique characteristics of who you are that cannot be stolen or replicated. That foundation sets the stage for adaptable, tailored technologies to fortify identity data. Importantly, Identity Continuity streamlines an otherwise clunky user experience in which consumers must remember and reset passwords. Instead, it reassures any company's customers that the timeless cornerstones of good business—security and trust—stand firmly in place, even as their needs and technology evolve.



The number of Internet users globally currently stands at **5.35 billion** people but will reach **7.9 billion** by 2029.

The Complete Guide to **Identity Continuity**

What Is Identity Continuity?

Identity Continuity is an answer to a set of challenges posed by the identity assurance market. AI has reset the security arms race; digitization promises to overtake manual processes; and legacy security solutions have lost potency. Modern users call for technology that offers maximum flexibility and security paired with minimal user effort, or friction.

A solution unique to Daon, Identity Continuity is a strategic security framework that removes siloed customer credentials. With a singular, centralized identity profile in place for each customer, Identity Continuity leverages AI-driven technologies across the three main processes of each customer's identity journey, streamlining the user experience.

Identity verification ensures that each customer is who they claim to be by linking their identity claims to verifiable proof, such as government documents. During identity verification, each customer establishes a biometric profile, or a data set of unique, unchanging biological characteristics like facial scans, fingerprints, or voice recordings.

Identity authentication activates during each successive customer interaction. It validates known users quickly, minimizing inconvenience, frustration, or distrust. Here, biometrics seamlessly confirm consumers' identities throughout their lifetime of interactions with a service provider. Customers can also update their records at any time, registering additional factors to expand authentication options and cross-channel capabilities.

Identity Continuity re-envisions the **account recovery** process, because users are empowered to maintain account access or update account information without passwords, PINS, or security questions.

With the synergy of these processes, Identity Continuity establishes the principle of "one customer, one record." Because each user has a single identity profile that follows them throughout their journey with an organization, relying parties can gain insights into customer experience. Customer information is shared across departments, which enables personalized service that's not possible under siloed systems. A customer's habits and preferences—as well as the barriers they encounter—are easily viewable, allowing service providers to tailor user experiences and eliminate inefficiencies. Companies can place customers and transactions into categories such as high- and low-risk, making sure services match needs at every turn.

Identity Continuity offers organizations the opportunity to improve customer satisfaction while reducing costs—all while futureproofing against fraudsters' increasingly advanced tactics.

The Complete Guide to **Identity Continuity**

Identity Verification 101

According to TransUnion, 13.5% of new account creations are suspected to be fraud attacks, and sophisticated synthetic identities threaten to amplify that threat. Deloitte cites synthetic identity fraud as "the fastest growing financial crime in the United States" and expects associated losses to topple $23 billion by 2030.

Under an Identity Continuity framework, identity verification establishes, confirms, and secures a user's identity claim. To onboard with a service provider, a user simply scans an ID document or other verifiable credential and snaps a selfie. The two are instantly linked and authenticated using patented, AI-driven technology.

This includes examining special features (watermarks, holograms, foils, textures, stamps) for evidence of tampering. Documents can be automatically checked against fraud watchlists to flag potential bad actors. AI algorithms assign risk scores to individuals based on completed data analysis, flagging suspicious activity or those requiring additional verification.

Such precision-based features place a company securely in line with Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance standards.

But ease and efficiency are more than a competitive edge in the identity verification process; they reflect an unflinching market demand. The average U.S. consumer abandoned purchases and services 4.76 times per day in 2023 due to the inability to remember a password, according to Sapio Research. The failure to meet consumers' mandate for simplified, secure service translates directly to lost revenue, and Experian reports that one-third of consumers will abandon an online shopping cart if a transaction exceeds 30 minutes.

*Deloitte cites synthetic identity fraud as **"the fastest growing financial crime in the United States"** and expects associated losses to topple **$23 billion by 2030.***

With Identity Continuity, AI ensures that verification is rapid and mostly invisible once selfies and documents are provided. Customers can add both biometric and non-biometric factors to their identity record at any time after the initial verification. These additions allow customers to adjust their authentication options over time as their needs and preferences evolve.

The Benefits of Biometrics

Biometrics refers to unique biological traits that verify and authenticate individuals, forming the central pillar of Identity Continuity. Biometric factors such as fingerprints, facial features, voice patterns, or even typing rhythm are far more resistant to replication and theft, making them by far the safest identity verification and authentication factors.

Most users are familiar with biometrics on some level, having scanned their faces or fingerprints to unlock phones and tablets. According to NordVPN, half of U.S. consumers use at least one biometric factor daily. Use rates increase for those 42 and younger, an indication the future holds greater biometrics usage in store.

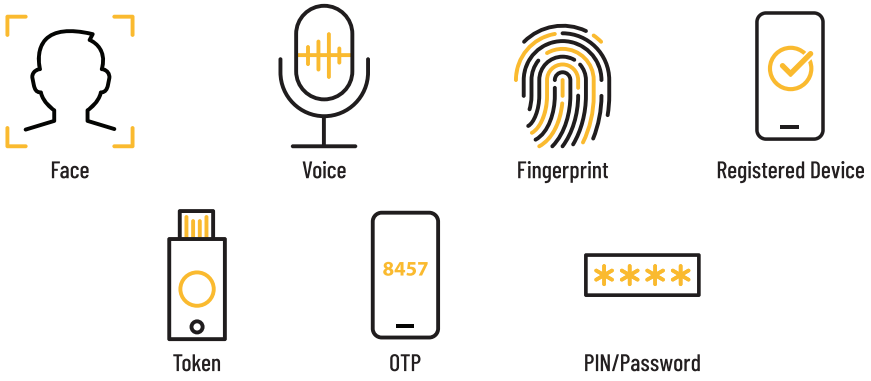
Biometrics can be divided into two categories: physical and behavioral biometrics. Physical biometrics rely on physical traits inherent to an individual, such as your fingerprints, facial features, the patterns in your iris, and the arrangement of veins in your hand.

Behavioral biometrics derive from your actions and interactions, but they are no less distinctive. Gait analysis, keystroke dynamics, and even the way you hold and manipulate a mobile device provide a blueprint of your identity that can serve as a critical key to accessing information and services. AI extracts and analyzes patterns in behavior that create measurable data.

Voice biometrics relies on distinct sound variations, including accent, rhythm, vocabulary, and intonation, to differentiate individuals. Customers provide upfront samples, called "voice prints," that can be used to authenticate identity quickly and accurately.

All of this creates a digital package of who you are that is distinct and secure, ensuring that you, and only you, can access your information and services.

Authentication 101



A customer's central identity record can be accessed through a variety of authentication factors. These can include knowledge-based factors (passwords, PINs), possession-based factors (mobile devices, security tokens), and inherence-based factors (biometric authentication like facial, voice, or fingerprint scans). Biometric factors can be combined, known as multi-modal biometric security, to add fraud-proof layers of protection. Organizations can pair biometric and non-biometric factors (such as a registered device and a facial scan) for multi-factor authentication, another highly secure option.

Biometric data is passwordless and immune to user error or cyber hygiene. Physical and behavioral data collected upfront during verification can be matched to a live customer in seconds. Behavioral monitoring, when real-time actions are compared to behavioral data, allows users to simply perform their usual activities without disruption. Users can be continuously authenticated in the background of a web, contact center, or mobile session, reducing opportunities for criminals to take over legitimate transactions.

Voice biometrics can identify someone according to distinct and recurring sound variations in their speech that can be captured and analyzed. Voice recognition can be text-dependent, meaning a user repeats a particular phrase to verify and authenticate their identity, or text-independent. For text-independent systems, a person can be identified based on voice characteristics regardless of what they say. Customers can simply begin talking to a call center agent without any security prelude; in the background, their live voice is compared to samples collected during onboarding to ensure frictionless, secure interactions.

With Identity Continuity, organizations can craft authentication processes adjusted for industry, transaction, and user categories. Customers can self-select and even adjust their choice of authentication factors, further ensuring accessible and inclusive practices.

Further, authentication via Identity Continuity can be cross-channel, allowing customers and service providers to use the most convenient, secure methods of securing particular transactions. For example, a call agent who receives a request for a high-risk action—like granting a second user account access—could allow a caller to provide a facial scan via a company app, utilizing both voice and digital channels.

Account Recovery 101

Passwords have dominated as the primary method of digital identity authentication for decades. Their ease of implementation has established them as the historic standard for account access across virtual platforms.

Increasing digitization, however, has confounded a legacy solution. According to NordPass, the average user juggles 255 passwords between personal and business accounts. It's no wonder, then, that the ideal of "strong" passwords falls by the wayside in practice. The most used password in 2024 is 123456, despite enhanced password requirements across platforms such as minimum length and special-character inclusion. Of the top twenty most common passwords, eighteen are variations on the numbers 1-9 or the word "password."

From a business lens, passwords are a costly primary tool, requiring dedicated resources for resets and recovery. Gartner estimates that 40% of all support calls are for password resets, and Yubico reports that associated lost productivity costs the average company $5.2 million per year. The account recovery process is also at high risk for security breaches, opening the door for fraudsters who claim the need for a password reset as means to take over a legitimate account.

Identity Continuity eliminates the need for password resets—and the associated risk. When a user needs to recover their account, they can verify their identity using their stored biometric data. For example, they might simply take a new selfie that the system compares to their stored biometric template. Once verified, the user can update authentication factors without ever having to call for support, reducing costs and ensuring a smooth customer experience where the user remains in control.

The average user juggles

255 passwords

between personal and business accounts

The most used password in 2024 is

123456

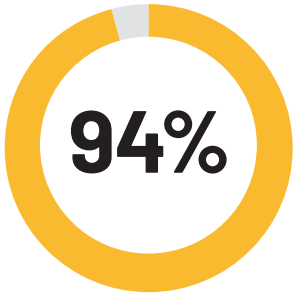
The Complete Guide to **Identity Continuity**

Unlimited Benefits for an Unlimited Future

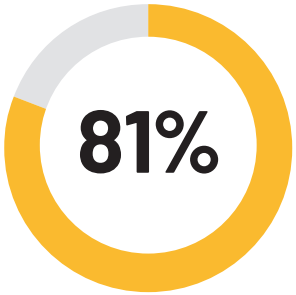
Security concerns are pressing and timely: nearly a quarter of businesses now see managing and securing digital identities as their number one security priority, up from 17% in 2023, according to The Identity Defined Security Alliance. Identity Continuity offers a robust solution to contemporary security challenges facing businesses today.

Identity Continuity is not merely a security measure; it's the foundation upon which organizations can build enduring trust with their customer base and navigate the evolving landscape of digital identity verification, authentication, and account recovery. These capabilities rest on AI-based technologies that are both responsive to the current challenges and poised to evolve alongside future innovations. The sense that AI represents the path forward for identity assurance is nearly unanimous. Among identity and security professionals, 96% see AI as key to addressing identity-related challenges, and 81% see passwordless authentication as a solution to identity issues.

AMONG IDENTITY AND SECURITY PROFESSIONALS



see AI as key to addressing identity-related challenges



see passwordless authentication as a solution to identity issues

Tech Deep-Dive: The Power of Identity Continuity

Facial Biometrics

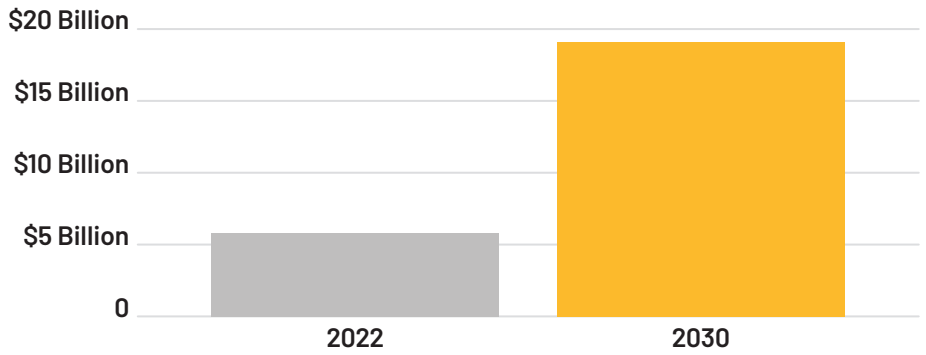
Using any particular characteristic for authentication depends on having a device that can accurately "read" and capture biometric factors. With facial biometric capabilities built into most modern mobile phones and tablets, facial scanning might accurately be described as a household technology.

According to Statista, nearly 70% of the world's population owns smartphones, which means that most people are prepared for facial biometrics. Almost every smartphone with a camera released since 2010 has built-in facial biometric capabilities. Research and Markets expects the facial recognition market to grow from $5.8 billion in 2022 to $19.1 billion by 2030, nearly quadrupling in under a decade. However, the technology is not new: facial biometrics find their origins in facial recognition technology first used in the mid-1960s.

Facial biometrics, also known as facial recognition, refers to a technology that identifies key features on a person's face in the form of mathematical data. Captured data remain consistent and accurate over time, designed to account for appearance changes and the effects of aging.

Powered by AI that can detect a level of detail invisible to the naked eye, facial biometrics allow users to securely authenticate themselves with a simple selfie, in seconds. First, advanced image technology precisely identifies human faces in still photos or video. Then, it compares facial images against an individual user's stored data record, such as matching an image from an ID document to a real-time selfie, as well as against larger user databases to root out fraudsters or existing duplicative user records.

Research and Markets expects the facial recognition market to grow from **$5.8 billion** in 2022 to **$19.1 billion** by 2030



These capabilities make facial biometrics one of the most secure forms of identity authentication in existence, particularly when used as part of a multi-factor authentication (MFA) strategy. The simplicity of facial recognition—and its reliance on widely available technology—may remove access barriers that users experience with other authentication tools, making it inclusive and accessible.

A Template, Not a Face

Facial biometrics falls squarely in the "who you are" category of authentication factors, also known as inherence factors. These factors cannot be lost, shared, or stolen, which is why they are the most impenetrable authentication option.

Facial biometrics does not store or use image-based representations of your face. During a facial scan, AI-powered biometric algorithms analyze and record mathematical representations of distinguishing facial landmarks, storing only the data that is necessary for authentication. Characteristics such as cheekbone shape, the distance between the eyes, lip contour, eye socket depth, and distance from forehead to chin are compiled into what becomes a unique data set, or facial template, one that can recognize you as you age and change your appearance over time.

Because facial templates are algorithm-encrypted snapshots of select facial features, they are impervious to reverse engineering and immune to phishing. In a hacker's hands, even if they were to decrypt the data, facial biometric information is a meaningless mathematical data set that cannot be translated into any image or likeness.

Daon's market-leading biometric algorithms are assessed by the U.S. National Institute of Standards and Technology (NIST), which utilizes its Facial Recognition Vendor Test (FRVT) to evaluate technological benchmarks. In the U.K., Daon's biometric algorithms have been reviewed by the National Physical Laboratory.

Liveness Detection

Liveness detection is a technology deployed to guard against presentation attacks. During facial and voice biometric checks, criminals may use masks, photos, videos, deepfakes, image injection techniques, voice recordings, or synthetically generated voices to co-opt another person's identity and masquerade as a genuine customer. Liveness detection uses AI-based algorithms to differentiate between a real human and a fabricated representation.

Two types of liveness detection exist: active and passive. Active liveness detection requires users to perform a specified action, such as saying a particular phrase or moving their heads. For example, a user may be asked to hold their ID up to a smartphone camera. In an instant, detection technology tracks a person's pupil movements as they glance at their ID, move their hand, and look toward the camera. Or they may be asked to repeat a phrase that is compared against a recording gathered during onboarding, such as, "This is José, and this is my voice. Authenticate me."

However, Daon's passive liveness detection operates discreetly by verifying liveness while a user performs their normal tasks. Passive liveness analyzes the content of a user's facial or voice biometric input via AI neural networks that assess elements like shadows, colors, audio artifacts, and textures of the user's skin or the pitch, tone, and cadence of the user's voice, respectively. An identity thief is less likely to recognize when authentication or verification processes occur, making it immeasurably more difficult to "spoof."

Because passive liveness checks are invisible to genuine customers, too, they increase trust and minimize frustrations that trigger abandoned transactions.

Document Verification

The practice of forgery is as old as written communication itself. However, AI has revolutionized criminals' ability to craft documents that elude security checks by cannibalizing publicly available information—or breached information on the dark web. Document verification processes now require increasingly advanced, multi-layered processes to outpace fraudulent attacks.

Document verification generally begins during customer onboarding, as customers provide initial documents to prove their identity. It can also occur when either customers or organizations elect to bolster existing user profiles with additional documents and authentication options. Many industries require document verification as part of KYC and AML regulations, and violations can translate to hefty fines. Digital document verification ensures iron-clad compliance with regulations, including eKYC or remote requirements.

Through Identity Continuity, document verification is immune from human error, as it begins with image analysis that validates photos contained within identity documents (most typically a driver's license or passport). The verification guarantees the document contains all fields necessary.

Checks performed on the document, which could number in the hundreds but take place in mere seconds, may include analyzing special features (watermarks, holograms, foils, textures, stamps), document completion, and checking for evidence of tampering (including image replacement and colorspace, which refers to the lighting, color, shadow, texture, etc. present in a document). As with liveness detection, these checks protect against photocopies, pictures, or videos that criminals may attempt to substitute for real documents.

An increasing number of documents, such as ePassports, contain near-field communication (NFC) capabilities. In these cases, identity data contained within a document, such as within a passport chip, can be shared through contactless transmission.

Once the document is validated, the system extracts its data and matches it with personally identifiable information (PII) the user provided during onboarding or a previous interaction. Information collected—such as name, date of birth, address, email address, phone number, and identification number—can also be compared instantaneously against identity fraud watchlists, government ID databases, and information stored within document barcodes. This step guarantees that printed information and stored data within the document itself do not contain discrepancies, and that all provided information matches a real, genuine person. If an inconsistency appears, an organization can reject a user's account-creation request or require further information.

Daon's document verification solutions process over 12,000 different types of identity documents from nearly every sovereign entity in the world, promising a customer-centric experience no matter where you do business or where your customer is located.

MFA (Multi-Factor Authentication)

Most users are familiar with some form of multi-factor authentication (MFA), including anyone who has swiped a bank card that also requires PIN entry via a keypad. By requiring a combination of factors (in this case, the card and the PIN), companies create layers of security that catch potential gaps and resist threats. The result is stronger, synergistic security that prioritizes frictionless user experience. Infosecurity Magazine reports that the use of MFA alone could prevent as much as 90% of cyber-attacks, according to the U.S. National Security Cyber Chief.

For online interactions, the most common example of MFA is a password with a secondary prompt that could range from OTPs (one-time passwords) delivered by SMS (text message) to an authentication code generated by an app, or, in some cases, to a registered device. While some of these security features are visible to users, such as OTPs, registered devices are an example of "invisible MFA" factors. A customer may not realize their registered device is actively confirming security until they attempt to log on from a different device, prompting an email warning or an additional authentication step.

Under Identity Continuity, multi-factor authentication can be tailored to the needs of a specific company, transaction category, or user type. As a guiding principle, blending a variety of authentication factors increases overall security. Common authentication types include something the user knows (a password or security question), something the user has (a registered device), and something the user is (biometric factors). Because biometric factors cannot be lost, replicated, or stolen, they represent the most powerful tool in a company's authentication arsenal. Biometric factors can be visible or invisible, but as a whole they require the least amount of user effort, making them the optimum solution to minimize friction in user interactions.

User experience stands at the core of any MFA strategy with Identity Continuity. Customers move seamlessly between channels, and Daon's MFA solutions provide a range of factor options that follow across these channels.

Identity Continuity prioritizes convenience alongside security because service providers can offer customers choices that meet their needs without sacrificing ease—fostering brand reputation and trust. For example, if a primary MFA factor isn't available, (i.e., a client doesn't have their phone), individuals can successfully access data through alternative security methods.

Multi-factor authentication is suitable for any risk level and provides an opportunity to grow with your customers and your company. As organizations in all industries and sectors collect more data, MFA provides a scalable way to protect that information.

Identity Continuity: Futureproof, Frictionless, and User-Friendly

At Daon, Identity Continuity places your relationship with your customers at the crux of technological innovation.

Identity Continuity means you are building a security foundation that isn't tied to a single technology, a particular device, or a moment in time. Instead, Identity Continuity builds solutions that treat each person as an individual with a distinct, centralized profile. That profile learns how your users interact, what they prefer, and what problems they encounter, and then makes that information transparent across your company. Instead of a series of discrete interactions, Identity Continuity envisions the customer lifecycle as a journey that endures. Within every customer's journey, you can adapt to meet changing needs, eliminate flagged barriers, and transform experiences to align with whatever appears on the technological horizon.

Futureproof

A staggering 90% of businesses reported an identity-related incident in 2023, according to The Identity Defined Security Alliance. It should therefore come as no surprise that nearly all businesses—99%—plan to deepen their investment in security outcomes within the next 12 months.

The future of security is a future built on biometrics, which are sure to adapt and evolve. Identity Continuity was crafted with flexibility and technological innovation at its heart. Biometric innovation means that the ways we collect and read data are already changing. Identity Continuity was built to accommodate innovations we anticipate (and those we can't) through a flexible platform that can be scaled up or down.

Frictionless

Identity Continuity strikes a powerful balance between security and convenience with frictionless technology. This represents more than a competitive edge: from a consumer perspective, it's a non-negotiable demand. According to Deloitte, one-quarter of adults in the UK will abandon account opening processes due to cumbersome identity checks. The rates at which U.S. customers abandon purchases because of password fatigue rose 28% between 2022 and 2023, reports a study by Sapio Research.

Biometric tools continuously authenticate in the background of a user session. These AI-based systems learn about users over time, analyzing dynamic information that constantly refines security measures. With the highest security in place, your customers can do what they want to do most: use your services.

Frictionless technology benefits both you and your users. As a provider, you have access to data and insights in a single, central location where you can easily view customer journeys and edit them via customization. As a user, biometric tools protect against security threats without interrupting digital experiences, ensuring your data and information are protected without sacrificing ease of use.

User-Friendly

With the population of digital users nearing 8 billion by the decade's end, one-size-fits-all approaches fall short. Customers demand choice, and companies must meet the moment through adaptability, offering a range of security options across multiple channels and platforms.

Consumers themselves readily reveal the solutions they'd like to see in place of passwords and security questions. Sapio Research found that biometrics is the most popular method of signing in to an account or service via a global survey. JP Morgan expects biometric payments to reach $5.8 trillion and 3 billion global users by 2026.

Because Identity Continuity is fueled by biometrics, it allows you to place, and keep, your finger on the pulse of user-friendly, digital-first customer relationships. As a standard function on near-ubiquitous technology, biometric security both prioritizes accessibility offer and customers choices in how they interact. These inherence factors, based on unique biological traits, can't be lost, stolen, or forgotten, making them both seamless to use and highly secure. They eliminate the need for password resets and account recovery calls and place power back in the hands of customers, who can add factors or modify authentication methods over time.

The Complete Guide to **Identity Continuity**

Why Identity Continuity? Why Now?

Identity Continuity serves as a central vision under which companies can align security measures and strategic goals. Powered by AI, Identity Continuity re-envisions digital identity verification, authentication, and account recovery as smooth, swift, and user-driven. And it tackles the digital threat landscape head-on with security technology poised to evolve as rapidly as the world's technology.

Identity Continuity is built so that you can start anywhere and expand everywhere. Whether you begin with onboarding, authentication, or recovery, you can seamlessly integrate Identity Continuity into your current system. Imagine you already use some level of biometric authentication within your app. For instance, customers log in by scanning their fingerprint. With Identity Continuity, you can expand this secure, frictionless experience to include robust identity verification for new customers, building towards a more comprehensive identity journey. Daon serves as a strategic partner throughout your business evolution to make certain that Identity Continuity is a smooth process, with minimal friction, allowing your customers to interact confidently and securely with your brand at any time.

Daon is the Old Irish word for human, an expression of our human-first approach to technological innovation. We craft processes that envision the humans who use and administer our tools holistically. We anticipate and solve for your problems, offer solutions to meet you where you are, and create with inclusivity and accessibility at the forefront. We anticipate what's to come, taking the guesswork out of living and working in a digitally driven world. That way, you can focus on what's always mattered most: reaching people and building customer relationships that endure.

External Sources

1. New Study Reveals 90% of Organizations Experienced an Identity-Related Incident in the Last Year, 84% Reported a Direct Business Impact
   Source Title: PR Newswire, report from Identity Defined Security Alliance
2. Using biometrics to fight back against rising synthetic identity fraud
   Source Title: Deloitte
3. The Password Plague: Consumers Are Abandoning Purchases Out Of Frustration by Ray Schultz , Columnist, October 16, 2023
   Source Title: Sapio Research
4. New Account Creation Fraud and How to Combat It
   Source Title: TransUnion
5. Internet Usage Statistics In 2024; Digital Payments - Worldwide; Digital Payments Statistics in 2024 (Latest U.S. & Global Data)
   Source Title: Statista
6. Identity Fraud Cost Americans $43 Billion in 2023
   Source Title: AARP
7. Facts + Statistics: Identity theft and cybercrime
   Source Title: Identity Theft Research Center
8. 2023 Data Breach Report by the Identity Theft Resource Center
   Source Title: Identity Theft Research Center
9. Cost of a Data Breach Report 2023
   Source Title: IBM
10. Global smartphone penetration rate as share of population from 2016 to 2023
    Source Title: Statista
11. NordVPN survey: Half of the US uses biometric authentication daily
    Source Title: NordVPN
12. Juggling security: How many passwords does the average person have in 2024?
    Source Title: Nordpass
13. Global Facial Recognition Market 2023: Market to Grow to $19.1 Billion by 2030 from $5.8 Billion in 2022 - Safety, Security, and Expansive Applications Driving Growth - ResearchAndMarkets.com
    Source: Research and Markets
14. Tech CEOs: Multi-Factor Authentication Can Prevent 90% of Attacks
    Source: Infosecurity Magazine
15. J.P. Morgan to pilot biometrics-based payments for merchants
    Source: JP Morgan
16. The Benefits of Passwordless Authentication
    Source: Yubico
17. Resetting Passwords (and Saving Time and Money) at the IT Help Desk
    Source: Gartner

daon.com/identitycontinuity

Daon®

The
Digital Identity Trust
Company