Persistent User Authentication (PUA)

adding the 'always verify' to Zero-Trust security

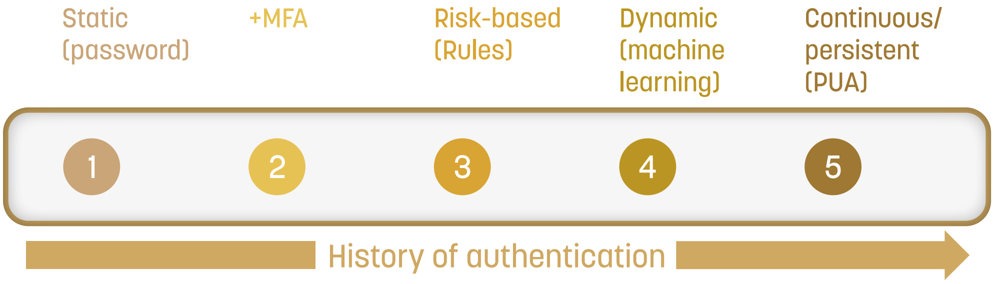
The Whisper Co.

Part 1: The user in the machine: how cybersecurity became an authentication problem

Before discussing how technology intersects with security, it is essential to understand what is happening in the threat landscape. Hacking is no longer about finding programmatic ways into an organization's network and apps. Today, modern cybercriminals understand as much about human behavior as they do about technology. For example, during a login event or transaction, the human in the machine can open the door for cybercriminals to enter the enterprise. Understanding how and why this has come about is critical in finding ways to close that door.

A short history of authentication

The humble password is something that we all understand. It is a linguistic method of controlling access to something. But the password is a static object; even if rotated, it still maintains its state and is a potential weakness in a system. Passwords or key phrases, however, continue to dominate sign-in to apps, devices, and other IT resources. However, to counteract this weakness, evolution in the industry occurred. Evolution comes about by a process of natural selection. The selective factors in the development of authentication are usability, security, and ease-of-implementation.


Static (password)
+MFA
Risk-based (Rules)
Dynamic (machine learning)
Continuous/ persistent (PUA)
1
2
3
4
5
History of authentication

1 Passwords

Easy for users to understand and developers to implement. However, passwords come with inherent issues.

Problem: passwords are usable but insecure. Social engineering tricks, data breaches, and phishing are used to steal passwords. Credential stuffing, automated bots are used to inject stolen usernames and passwords are behind 193 billion cyber-attacks in 2020.[1]

2 2FA/MFA

Two-factor or multi-factor authentication uses additional mechanisms to augment passwords; for example, an SMS text code and a password are required to log in.

Problem: multi-factor authentication methods such as SMS text codes can now be circumvented by cybercriminals. In 2FA phishing attacks, cybercriminals create fake webpages that collect a 2FA during its generation by a legitimate site; using the short window open to use the code, the cybercriminals then login to the actual site.[2]

3 Risk-based authentication (RBA) (also known as adaptive authentication)

Rules can be applied to a login event to determine the level of authentication needed for a transaction. These rules-driven systems augment the static nature of password-based systems, as policies enforce a more robust level of authentication.

Problem: RBA is still dependent on a password; it uplifts the password to a higher level of security by checking certain other factors, such as the location of the user, IP address, etc. Making sure the rules do not impact usability requires careful testing and ongoing updates for changes.

4 Dynamic or behavioral biometric authentication

Behavioral biometrics uses behavioral patterns, typically micro-movements when using a device, that offers a unique user fingerprint to add a level of assurance to a logon event.

Problem: users may feel this technology is intrusive and have privacy concerns. It can cause false positives and prevent ease of use..

Persistent User Authentication (PUA) adding the 'always verify' to Zero–Trust security

5 Persistent User Authentication (PUA)

All the above still exist, but each has security and/or usability weaknesses. The next generation of authentication, called **Persistent User Authentication (PUA)**, is the evolutionary step needed for always-on security. PUA uses risk-based and dynamic authentication traits to provide a 360-degree view of a user to assure identity during a login event or transaction. These security and usability issues have helped inform this innovative design in user authentication.

The cybersecurity landscape and human factors

The cybersecurity landscape pivots upon the user and how that user accesses an account or performs a transaction. Statistics gathered from industry research and surveys show cybercriminals successfully target the 'human in the machine'. Below is a compilation of data that builds a picture of the cybersecurity threats impacting all industry sectors across the world.

Accounts, passwords, and other problem areas

Account takeover (ATO): cybercriminals target accounts to harvest sensitive data and financial information., including reward points. The volume of ATO attacks increased by 307% between 2019 and 2021, and almost one-quarter of fraud in the US is associated with ATO attacks.[3] [4]

Social engineering: Around 70-90% of breaches have a social engineering component. Social engineering manipulates human behavior to trick a person into performing an act on behalf of a cybercriminal. to trick a person into performing an act on behalf of a cybercriminal. Social engineering often involves methods used to steal login credentials or personal data that can lead to access control vulnerabilities.[5]

Remote malware: malware like Redline Stealer, can steal passwords in browsers. A recent example even bypassed VPN protection, as the username and password to the VPN were stored in the user's browser.[6]

Bot attacks: almost 28% of online traffic is from bad bots. These automated programs can be used for brute force attacks and credential stuffing.[7]

Data breaches and malware

The result of breached accounts and transaction fraud are cyber-attacks:

Cyber-attacks and tactics: Symantec researchers found that 96% of data breaches start with a phishing email to steal credentials or other identifying data.[8]

Credential theft a critical entry point: The DBIR identifies credential theft as one of the top four methods used to breach data.[9]

Ransomware out of control: Credential theft can lead to a ransomware infection. CyberEdge Group says that 71% of companies suffered from a ransomware attack in 2021.[10]

Ransomware leads to data theft: CrowdStrike found data leaks associated with ransomware grew by 82% in 2021.[11]

The human in the machine

Human beings are increasingly targeted by cybercriminals who see the user as the entry point into a network.

Human element: The 2022 Verizon Data Breach Investigations Report (DBIR) found that 82% of data breaches involve a human element.[12]

Human error: Stanford University researchers found that 88% of security breaches can be traced to a human error event.[13]

Careless staff: Kaspersky identified "careless or uninformed staff" as the second most likely cause of a security breach.[14]

Credential reuse and misuse: A Google survey shows that 62% of people reuse passwords and 52% reuse those passwords across multiple accounts[15]. A SurveyMonkey report found that 34% of employees share passwords with their coworkers.[16]

Password exploits: A 2022 Spycloud report shows that cybercriminals exploited 1.7 billion credentials in 2021. Worryingly, 64% of passwords exposed in 2021 were reused, and 70% of previously compromised passwords are still in use.[17]

Costly data breaches: credential theft leads to data breaches. Ponemon calculated that the cost of credential theft had increased 65% from $2.79 million in 2020 to $4.6 million in 2021/2022.[18]

What about password managers and MFA?

Password managers and MFA are solutions addressing better usability and improved security. However, this is not being seen in the real world where:

Insecure MFA: Cybercriminals are working out ways to circumvent MFA.[19]

MFA low adoption rates: the adoption rate of MFA by enterprises and consumers is low. Microsoft says that only 22% of enterprise users add 2FA to AD.[20]

Password manager low adoption rate: Google Password managers also have a poor uptake, with only 24% of people using a password manager.[21]

Part 2: how authentication affects different sectors

How a person identifies themselves during a transaction, including a login event, is crucial in the fight against cyber-attacks and fraud. The war of attrition is centered around authentication and plays out in various sectors. Below are some of the issues in four industries. These issues center on the human operator and how they access enterprise apps, data, and the network.

FinTech

The financial sector is one of the most heavily regulated and fraud-targeted industries. The banking industry, for example, had a 1,318% increase in ransomware attacks during the year.[22] In 2021, losses due to fraud increased by 79% to $24 billion, despite improved methods of transactional authentication and anti-fraud tools. Fraudsters continue to push the boundaries of cybercrime by exploiting accounts. Consequently, ATO-associated losses increased by 109%, with one in twenty Americans being victims of fraud in 2021.[23] As much cybercrime is finically motivated, the financial sector is at the coalface of cybercrime; phishing and credential stuffing attacks lead to ATO. Even MFA can be circumvented.

Robust authentication is a critical point of action for any FinTech developer to incorporate into banking or financial apps. It is no longer enough to use MFA, a more persistent authentication system such as PUA is needed for this targeted industry and its customers.

HealthTech

The National Health Care Anti-Fraud Association (NHCAA) estimates that the financial losses caused by healthcare fraud are tens of billions of dollars yearly.[24] This is not surprising as the healthcare industry is a data-rich sector managing many sensitive data sets. With the advent of open health data, this is becoming even more critical to ensure that access to these data is at a high level of assurance. As well as data theft, fraud is blighting the industry, too: the 2018 National Money Laundering Risk Assessment NMLRA) shows that healthcare fraud is the largest source of illicit funds in the US, losing $110 billion each year.[25]

Open health data creates an expanded attack surface with end users, system administrators, and the like, requiring a more robust and persistent approach to authentication.

LegalTech

Legal firms deal with highly sensitive data and govern high-value transactions. This places law firms at high-risk. The American Bar Association (ABA) 2021 survey on technology use and cybersecurity evidence this finding 29% of law firms experiencing a cyber-attack.[26]

Both data access and transactions need to be secured using persistent and intelligent identification of law firm employees and clients.

Government

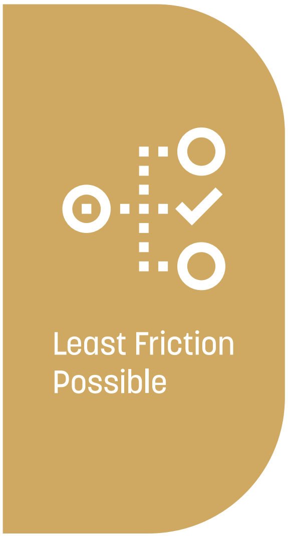
Governments are uniquely positioned in terms of technology use cases; digital government services must provide technology solutions for a broad demographic of users, including citizens. Balancing security vs. usability is critical in this sector. Unfortunately, the government is also a target for fraud and cybercrime. Governments must supply usable but secure identity-centric services. Persistent, usable, secure authentication is a critical component of citizen identity. Coupled with this are the massive supply chains used by the government. Supply Chain Attacks often begin with a spear-phishing email that steals and circumvents poor authentication measures.

Persistent user authentication (PUA) offers a usable, secure, and more easily implemented solution to the authentication problem in all of the above sectors; the next section explains how.

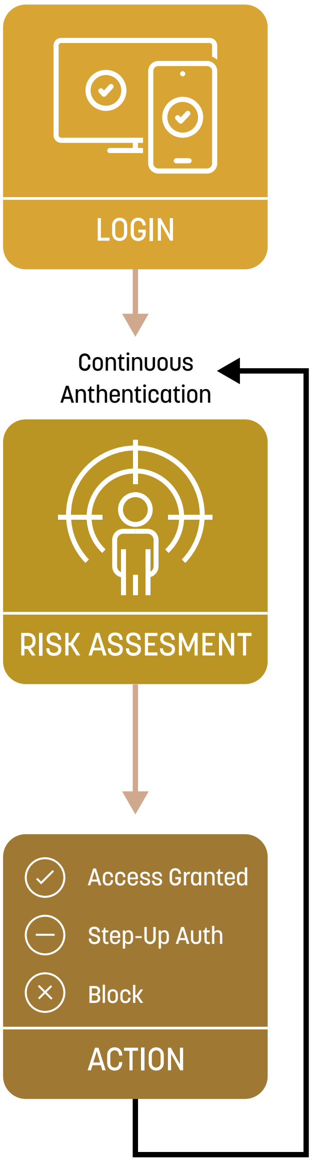
Part 3: How Persistent User Authentication (PUA) solves the authentication problem

Without always-on security, gaps can open that facilitate data leaks; this is the fundamental idea behind a Zero Trust approach to securing data and other IT assets. Often explained by the phrase 'always verify, never trust,' PUA translates perfectly to a framework that requires always-on checks to authenticate access.

- The right people
- Have the right level of access
- To the right resources
- In the right context
- That is assessed continuously


Least Friction Possible

Persistent User Authentication (PUA) adding the 'always verify' to Zero–Trust security



Zero Trust eXtended (ZTX) ecosystem framework was introduced by the analyst firm Forrester in 2017. ZTX assumes that there is no implicit trust. Using this principle, security and risk (S&R) professionals must retain visibility and control across the entire digital business ecosystem, regardless of location, device, user population, or hosting model. For such a system to work, it must:

- **Satisfy the CIA triad (Confidentiality, Immutability, Availability)**
- **Be embedded with the data (encrypted)**
- **Validate in-situ in a scalable fashion**
- **Be part of a standard so any developer can implement PUA consistently**

Current solutions fail short of covering all four requirements. However, PUA is a 'Zero Trust by design' (ZTbD) solution, encompassing all four conditions.

Persistent User Authentication or PUA uses ongoing facial recognition (and other biometrics, as required) to ensure that the person performing a transaction or logging in is authorized. This authentication persistence removes security gaps, provides an always-on security layer, and applies instantaneous response to an authorized users if they move away from their device.

Persistent User Authentication (PUA) adding the 'always verify' to Zero-Trust security

PATENTED PERSISTENT USER AUTHENTICATION

Standard MFA **VS** Patented PUA

	Authorized		Shoulder Surfer	No one	Unauthorized
	The Authorized user is in front of their device		A shoulder surfer comes in the picture	The authorized user leaves the field of view	The unauthorized user comes by in front of the screen
Standard MFA	✓	MFA security is only upon entry. No session security. In all three scenarios, valuable and sensitive information is at risk.	✗	✗	✗
Patented PUA	✓	With patented PUA, the user in front of the device is persistently checked, protecting from all three scenarios. The instant (s)he is not there or another face appears, the screen is obfuscated and the information is protected.	✓	✓	✓

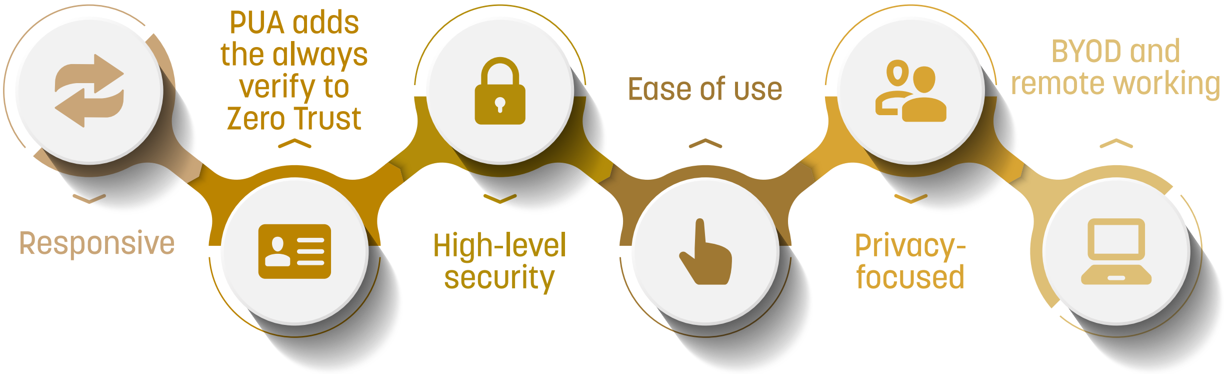
PUA removes the security flaws caused by:

Phishing: phishing relies on tricking users into providing data and/or credentials. PUA is spoof-proof as it is instantly responsive and depends on the user being at the device during a transaction or login event.

MFA: Even multiple factors can now be circumvented, making MFA no longer fit for purpose. PUA is always-on responsive authentication that cannot be spoofed by attacks that steal or bypass MFA.

Shoulder surfing: if a user moves away from their device, even momentarily, a fraudster can take advantage and take over a user's logged-in session. PUA prevents this from happening by instantaneously closing a session if a person moves away from their device. A 3M study found that 'visual hackers' obtained sensitive information in 88% of attempts.[27]

Six key benefits of Persistent User Authentication (PUA)



PUA uses biometric authentication as part of a process rather than a single event. Authentication then becomes persistent, always-on verification. This creates a 360-degree trust experience that fills the always verify criteria of a Zero Trust environment.

This combination of always-on verification and a highly responsive authentication process is the critical differentiator between persistent authentication and more traditional methods, including behavioral and dynamic systems: the user must be visible to the device to authenticate to a given session.

Persistent User Authentication (PUA) has several key features that set it apart from other forms of authentication, including continuous and behavioral-based authentication:

Responsive: PUA is supremely responsive. Continuous verification checks are performed during a session, responding rapidly to changing circumstances. In addition, PUA allows Developers to add ongoing use of biometrics to apps. This guarantees that if the authorized user is no longer focused on the app (or device), or an unauthorized user is using the app, or another user is “shoulder-surfing,” the app will pause and obfuscate the screen. This process prevents any sensitive information from being not visible to shoulder-surfers or leaked.

Persistent User Authentication (PUA) adding the 'always verify' to Zero–Trust security

PUA adds the always verify to Zero Trust: Zero Trust networks are built upon the ethos of "always verify, never trust." So, PUA fits naturally into a Zero Trust environment to ensure that authentication events and transactions are always verified and continuous.

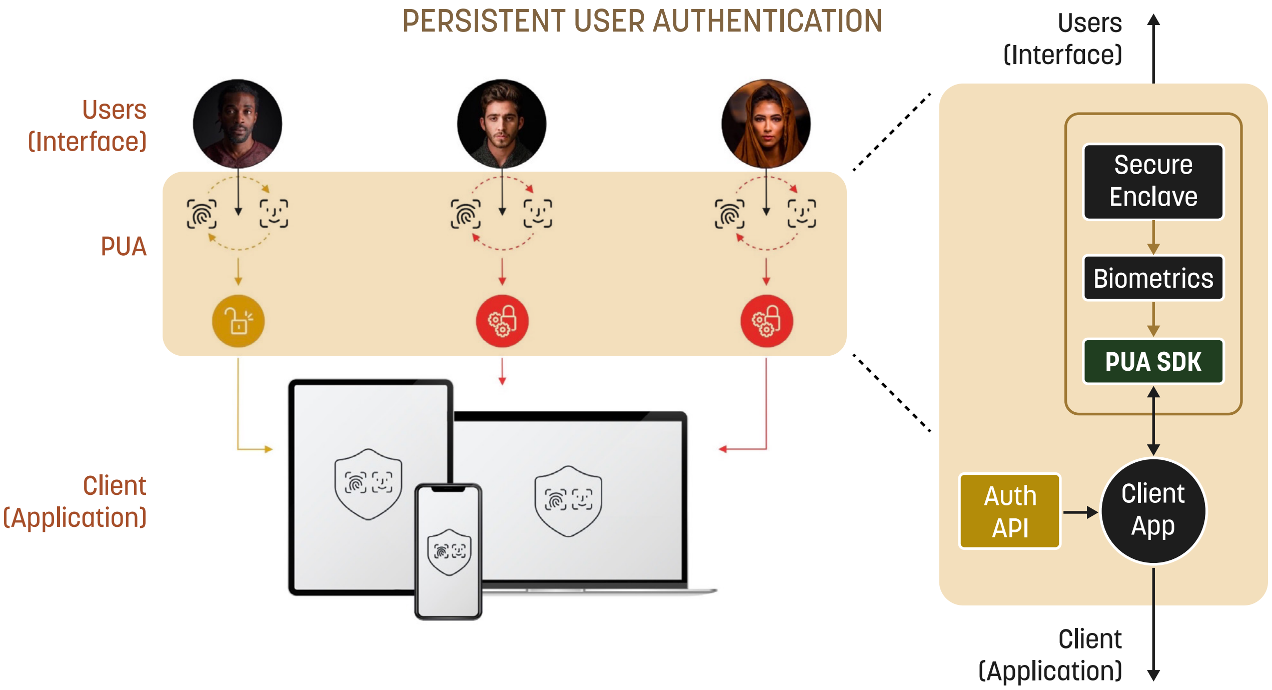
High-level security: a 'For Your Eyes Only (FYEO) environment is integral to how PUA works. This automatically ensures that privileged access rights are verified and enforced.

Ease of use: unlike other authentication methods, PUA provides a frictionless experience for end users. This helps to improve productivity.

Privacy-focused: enforces data privacy by ensuring only those who need to know can have access to sensitive data. PUA prevents data leaks by stopping unauthorized users from stealing or misusing data by accessing an open session. PUA is designed with privacy in mind and contributes to a Privacy by Design approach, ensuring compliance with privacy regulations.

BYOD and remote working: the introduction of any new technology into the workplace changes the organizations' risk profile.[28] BYOD policies are ubiquitous, with around 96% of devices connecting to a network being personnel.[29] BYOD allows a boost productivity and morale. However, BYOD also expands the enterprise "perimeter" or "attack surface," providing more potential for cyber-attacks or data leaks.

Persistent User Authentication (PUA) adding the 'always verify' to Zero-Trust security



The Whisper Company and PUA

PUA is a user-centric approach to meet the usability needs of authentication while ensuring the highest levels of security are met. A company can build a Zero Trust environment by applying persistent user authentication. The Whisper Company provides a PUA API that performs the following functions:

- **Authenticates:** detects an authorized face and initiates a session
- **Tracks:** identifies an authorized face within a frame.
- **Secure pause** if an authorized face leaves the field of view a session is suspended. The session will automatically resume once the user comes back to the device.
- **Shoulder surf prevention:** detects when another face is detected and ends the session.
- **Gaze tracking:** records when a user is not looking at the screen

Persistent User Authentication (PUA) adding the 'always verify' to Zero–Trust security

Whisper PUA provides the always-on verification needed for a private and secure high-trust environment solution.

Whisper PUA makes authentication a process, not a one-off event

The Whisper PUA API allows a developer to build an app or device that continuously captures biometrics to authenticate that the user is the authorized user of the app or device. After an initial authentication and authorization using biometrics (or any other method implemented by the developer), the Whisper PUA uses the device camera to continually authenticate the user as a process, not a one-off event.

The Whisper Company provides an SDK/Framework/ Library/API for iOS and Android, enabling app developers to embed an end-point (mobile or desktop platform's interface) continuous user authorization tool.

A comparison of static, continuous, and persistent authentication

	Static	Continuous (risk-based/ biometric)	Persistent (PUA)
Credential sharing	Password sharing is a serious issue that can cause security gaps to appear Extra factors (MFA) can help prevent security issues, but are still not protection against a cyber-attack	Password sharing can still occur but the extra factors such as behavioral and rules-based increase of factors required to log in can help improve security	**Stops the security gaps inherent in credential sharing. PUA is user-centric authentication that prevents 'second-face' use of a logged-on session.**
Workflow and productivity	Causes friction when logging into multiple apps. Causes users to reuse passwords, even compromised passwords. Impacts productivity. Single Sign On (SSO) can help but this creates a central point of attack.	Still some friction but risk based SSO can help alleviate friction.	**Friction-free, facial biometric (or other biometric) can be used to seamlessly login and stay logged in until the authorized user moves away from the device.**
User change in session (e.g., device/session left open)	Anyone can jump into an open session if left open	If already open, the session can by used unless a rule is set to spot certain behaviors (not all risk-based/behavioral systems can do this)	**Automatically responds to user moving away from a device and closes the session.**
Implementation by developers		Varies, often provide an API and /or SDK	**API and SDK for both iOS and Android**
Usability	Users need to remember multiple passwords unless using a password manager.	Typically, still requires passwords to be remembered at some point.	**Seamless to the user**
Dynamic rules for uplift of security	Not based on rules that adjust the behavior of the authentication	Rules can uplift the factors required to access a device, app, etc.	**Inherently dynamic in nature, rules close session when authorized person not detected.**

Why behavioral authentication is not fit for purpose

Why has the evolution of authentication continued beyond behavioral authentication? While behavioral authentication meets the security gaps inherent in static authentication systems, it still does not meet the remit of modern consumer needs. Issues with current behavioral authentication continue to hold it back from being a 360-degree solution to the requirements of modern access control and rapid transactional models of human-computer interactions. Issues include:

Privacy and creepy tech issues: consumers and employees are educated on privacy issues. A consumer and Internet Society survey found that 63% of people find smart devices' creepy' by collecting data on behavior.

Bias: bias can be a stumbling block when biometric data is used to determine an outcome, such as OK (or not) access. Behavioral authentication is still inherently biased in the design of its algorithms. Racial bias is a well-known issue, for example. The industry is attempting to overcome this using 'Multimodal Biometric Authentication (MBA) – however, this approach may make these systems even more 'creepy' and privacy disrespectful.

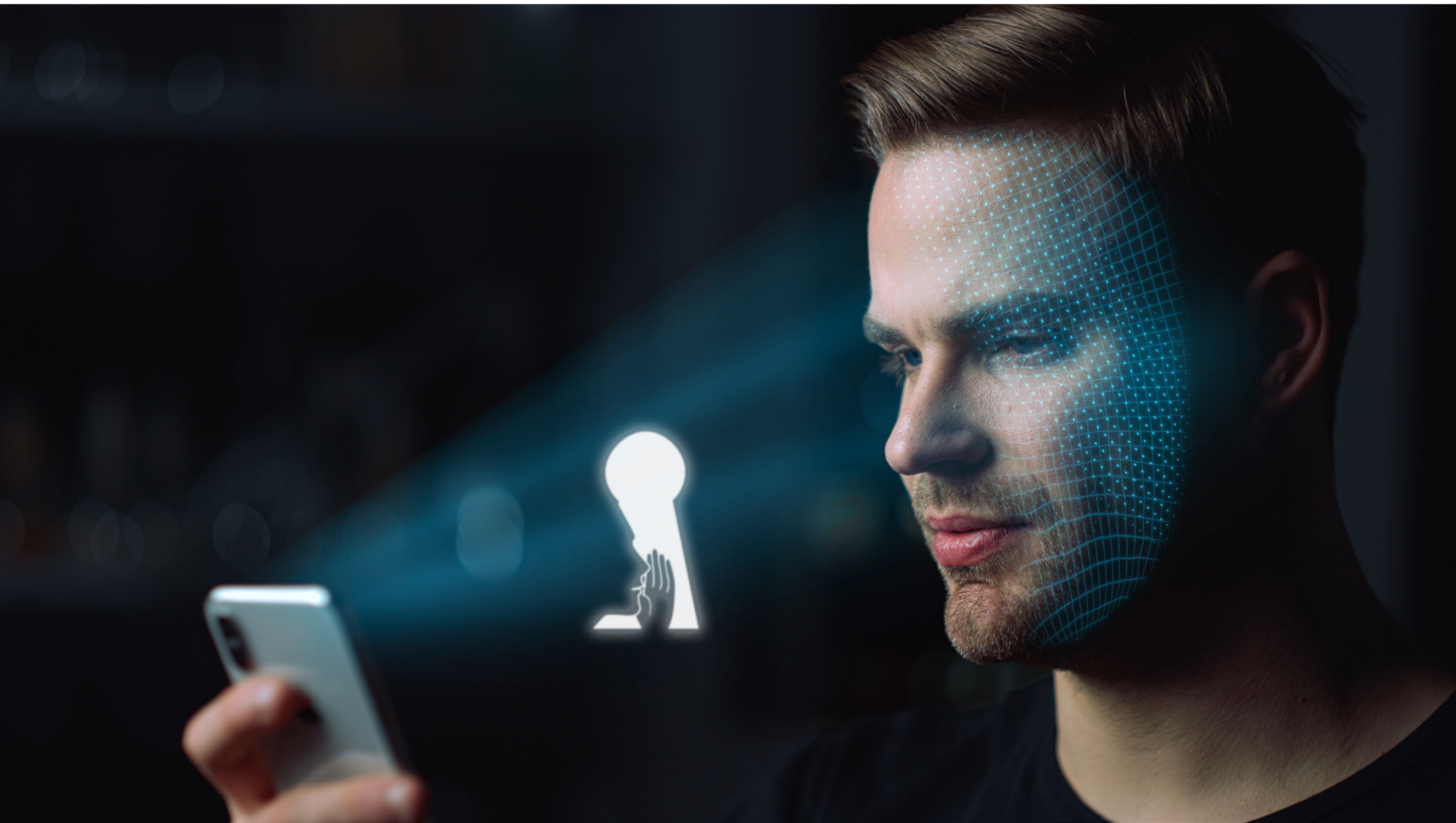
High workload for developer integration: dev and commercial teams are under pressure to get the product into production. Behavioral biometric systems can have an increased workload for developers to integrate, test, and maintain.

Accuracy: the behavioral analytics behind this method requires a multimodal blend of behavioral and physiological data points. False alarms can prevent accurate authentication and impact user experience negatively. Training can take time, and accuracy over time should be questioned.

PUA: Always on verification for persistent security

User authentication that is usable and enforces security has always been a thorn in the side of User authentication that is usable and enforces security has always been a thorn in the side of system and app designers. If the system is usable, like static systems, it is inherently insecure; if security improves, such as multimodal behavioral systems, it becomes creepy, and users reject it. Finding the security-usability balance has not been easy. However, PUA enforces the "always verify" of a Zero Trust approach to security. The ZTbD nature of persistent user authentication crosses the chasm of usability, security, and ease of implementation.

This vanguard in user authentication gives developers and CXOs, alike the confidence to get the best possible product into production and ensure an exceptional total experience for all types of users.



Footnotes

[1] https://www.akamai.com/blog/trends/keeping-up-with-the-botnets
[2] https://securitytoday.com/articles/2019/03/25/2fa-immune-phishing-attacks-are-on-the-rise.aspx
[3] https://resources.sift.com/ebook/q3-2021-digital-trust-safety-index-battling-new-breed-account-takeover/
[4] https://risk.lexisnexis.com/about-us/press-room/press-release/20220106-annual-true-cost-of-fraud-study
[5] https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks
[6] https://www.komando.com/security-privacy/redline-stealer-malware-exposes-passwords/821033/
[7] https://www.imperva.com/resources/resource-library/reports/bad-bot-report/
[8] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-q1-2020
[9] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
[10] https://cyber-edge.com/cdr/
[11] https://go.crowdstrike.com/global-threat-report-2022.html
[12] https://www.verizon.com/business/resources/reports/dbir/
[13] https://cisomag.eccouncil.org/psychology-of-human-error-could-help-businesses-prevent-security-breaches/
[14] https://www.kaspersky.com/blog/the-human-factor-in-it-security/
[15] https://services.google.com/fh/files/blogs/google_security_infographic.pdf
[16] https://www.surveymonkey.com/curiosity/why-people-share-passwords-with-coworkers/
[17] https://spycloud.com/thank-you-2022-annual-identity-exposure-report/
[18] https://hub.novipro.com/en/2022-ponemon-cost-of-insider-threats-global-report?
[19] https://securitytoday.com/articles/2019/03/25/2fa-immune-phishing-attacks-are-on-the-rise.aspx
[20] https://therecord.media/microsoft-says-mfa-adoption-remains-low-only-22-among-enterprise-customers/
[21] https://services.google.com/fh/files/blogs/google_security_infographic.pdf
[22] https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats
[23] https://javelinstrategy.com/press-release/identity-fraud-losses-total-52-billion-2021-impacting-42-million-us-adults
[24] https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/
[25] https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf
[26] https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/
[27] https://www.3m.co.uk/3M/en_GB/privacy-protection-UK/expertise/visual-hacking-experiment/
[28] https://www.wallix.com/blog/privileged-account-management-and-byod/
[29] https://www.comparitech.com/blog/information-security/byod-statistics/