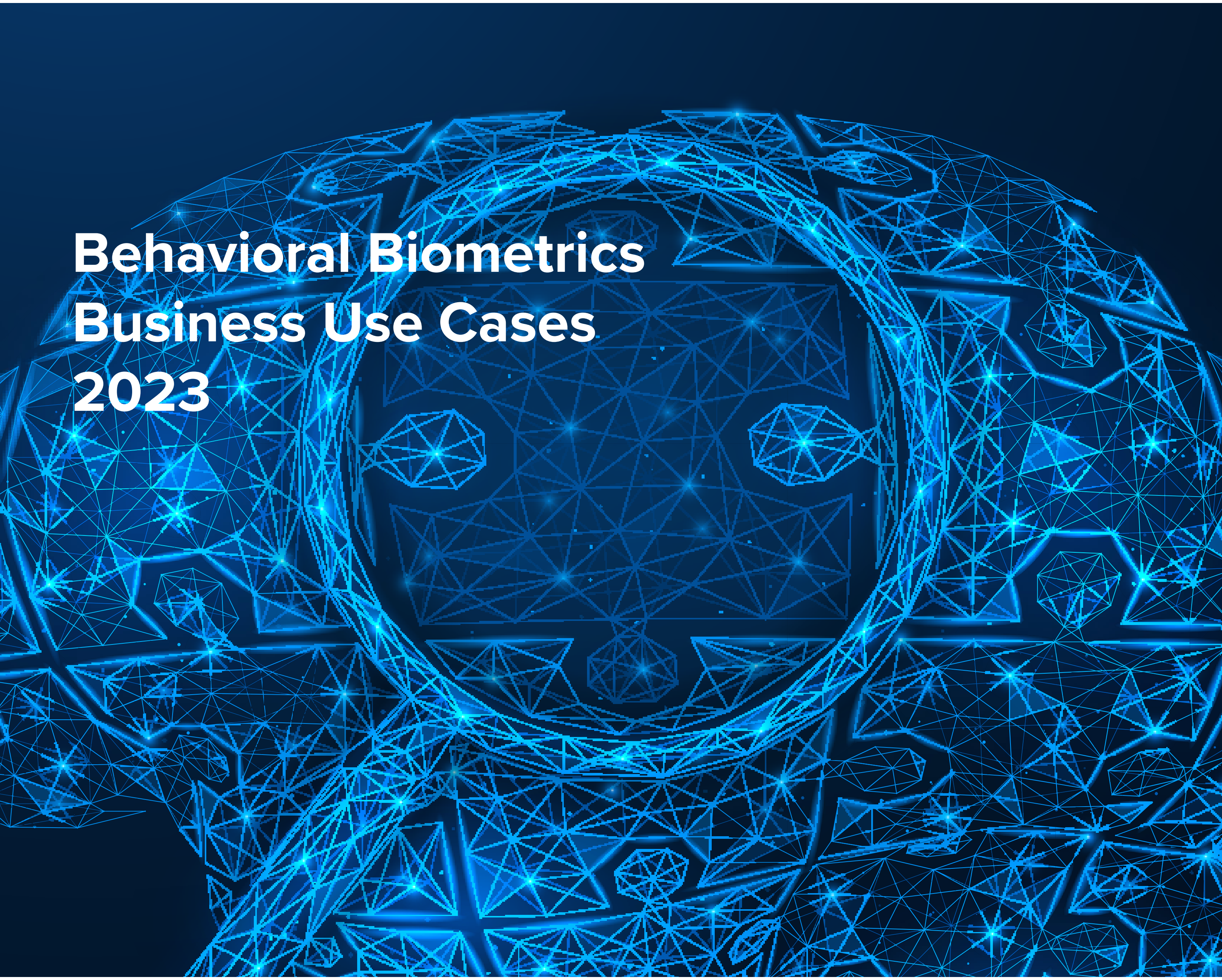
BSI Biometric Signature ID



Behavioral Biometrics Business Use Cases 2023

biosig-id.com

Beyond unique digital identity credentials.

Digital credentials are a ubiquitous part of most critical or essential business processes and operations. They are used to control and manage digital and physical assets alike. This is why both the digital credentials and the activities and assets that they guard must be carefully managed and protected.

Multi-Factor authentication (MFA) is the new normal when it comes to the use of digital identity credentials based security. Several factors related to "something I am, something I know, or something I have" are combined to prove the identity of the user going through the process of authentication.

In the authentication process, these multiple factors are usually provided by separate and distinct technologies that require the use of special, and expensive, equipment.

When it comes to the use of biometric based factors, physical biometrics meet the "something I am" requirement. Some behavioral based technologies can meet the "something I am" and/or "something I know".

Even so, most biometric and other technologies prove only that the correct credentials are being used to satisfy the digital challenge.

That said - can they prove that:

1. **The creator of the credentials is present?**
2. **The person seeking to satisfy the security challenge is "present of mind"?**

BSI Continuous Vector Lines (CVL) based behavioral biometrics do just that, and with certainty that exceeds 192 Billion to one odds.

The most interesting part of CVL technology is not even the fact that it requires no special hardware, training, or that it satisfies all three elements of Multi-Factor Authentication (MFA) in one single activity.

Because the user who created the behavioral biometric credentials is the only human that can recreate the authorization credentials sequence; the human has to be present, and completely focused in order to pass.

This means that:

1. **Computer based ML/AI "bots" can't recreate the credentials in a reasonable time to defeat the security system.**
2. **The user has to be of "clear mind" (not inebriated, drugged, under duress) in order to authenticate.**

These two little gems make BSI credentials unique, well beyond the "neat" and robust patented math algorithms. It allows to link with irrefutable attribution the credentials to the person that can use them, and to the fact that they had to know what they were doing when they tried.

Let's explore some of the unique problem use cases that behavioral biometric CVL technology can solve.

USE CASE #1

Protecting complex machinery and human life.

Problem manifestation(s)

- An highly technically trained employee needs to operate complex machinery, but has had a few too many drinks during the lunch hour.
- An unqualified (not yet certified) employee attempts to operate complex machinery in a critical operation that requires substantial training and proficiency.
- An employee who is well trained, certified, and current on their credentials shows to work and intends to operate complex machinery, but is sleepy because of lack of rest, or use of medication.

The unsolved problems

- A fingerprint reader can't tell if the person authenticating is drunk or otherwise impaired.
- A proficient operator can enter a password, have a validation device, and pass a retinal, fingerprint, palm, or any other form of scan; even with 2 hrs of sleep.
- Credentials and passwords can be shared. One person can "turn on" the equipment and then leave a non-qualified operator to use the equipment. When an accident takes place, there is no way to hold either or both parties accountable.
- One operator can vouch for another in order to by-pass observance of mandatory rest periods.

How does CVL behavioral biometrics solve the problem?

The root causes for these problems are not solved by forcing the use of correct credentials.

They are solved by persistent verification of presence and validation of the correct (or the absence of a negative) state of mind.

Recreating a "drawn" or written password requires focus, practice and concentration; just like when it was generated.

Even in the worst case scenario, and presuming that a user authenticates and then has someone else operate the complex machinery, 1:1 attribution is established - so the operators can be held to account in a court of law.

Examples

- A lathe or band-saw operator about to work in a manufacturing plant.
- A commercial airline pilot about to preflight an Airbus or Boeing airframe.
- A farmer about to use a John Deere combine out in the field.
- A top-drive drilling system operator about to come "on watch" in an offshore oil drilling rig like the Transocean Horizon.
- An NYCTA train conductor who has been sick for three days and has been re-called to work.
- A nuclear power plant worker about to perform maintenance on the primary loop or nuclear instruments.

Possible financial impact

- The cost of human and hardware loss in an airline accident is hundreds of millions of dollars.
- Failed maintenance at Plant Vogel in GA could bring a $30BN dollar project to an end.
- The Transocean Horizon accident cost $60BN dollars.
- A combine can cost $500K. Loss of a single unit can cost a farmer, or its insurer hundreds of thousands of dollars.
- 4,600 fatal accidents claim the lives of freight drivers each year.

USE CASE #2

Defending against automatic “bots”.

Problem Manifestation(s)

- An online gateway portal is attacked for penetration by a persistent automatic technology seeking access to a LAN.
- A critical and protected portion of a LAN is attacked for penetration through an automated script that seeks gaining control of sensitive data therein.
- An attachment to an email or chat carries a sleeper script that worms itself into other machines for activation in the future.

The unsolved problems

- Automated scripts can simulate one or more factors in the MFA challenge.
  - ◊ They can sequentially guess ASCII based passwords.
  - ◊ They can perfectly emulate a FINAL STATE drawing.
- Automated scripts can repeatedly and quickly submit variations of credentials and challenge elements, overwhelming the system by trial and error over a long period of time, so as to remain undetected.
- Credentials can be shared and repeated between users.

How does CVL behavioral biometrics solve the problem?

The root causes for these problems are not solved by forcing the use of correct credentials.

They are solved by persistent verification that a human is seeking access.

Physical biometric hashes, passwords, and other authentication devices can be stolen or shared. Every written password has irregularities that have to be exactly replicated both in order, and time sequence.

When “drawn” credentials are used, the permutations of the codes generated far exceed 192BN:1 permutations - which requires substantial time and financial resources to defeat the security protocols associated with the process of authentication. It’s not about the final image, but how it was created.

Examples

- An online application portal for where one application is sent to several community colleges for registration.
- An online portal for financial aid, where one registrant can apply to several colleges and financial aid institutions at once.
- A malware application that quietly and persistently tries to borrow into the corporate PAM.
- A crafty employee that develops a “macro” like script to automate functions that should be controlled.

Possible financial impact

- Federal tuition financial aid programs in Texas and California have suffered losses estimated in excess of $15BN per year since 2021.
- UBER had their PAM recently compromised, when an ML script was used to break into their LAN and protected portions of the network. The loss linked to the event is estimated in the millions of dollars.
- IP data losses are estimated at $200BN per year.

USE CASE #3

Unsupervised controlled substances release.

Problem Manifestation(s)

- In bars and similar venues, bartenders must validate the age of a consumer by using an easily falsified form of ID.
- At pharmacies, a licensed pharmacist has to dispense scheduled substances to patients, taking them away from providing valuable consults to other patients seeking advice.
- In both cases, human supervision is required in a one-to-many scenario, forcing wait times on one end, and errors linked to haste on the other.
- Over prescription by a physician is hard to prove if the prescription itself is not tightly controlled between office and pharmacy.

The unsolved problems

- A physical biometric readers can't tell if the person authenticating is drunk.
- A fingerprint can't tell if you understood the instructions.
- A child can get the credentials of a parent to gain access to an automatic dispensary, but that does not guarantee that the warnings associated with the substance use will get to the patient (parent).
- Paper or digital prescription slips can be altered in flight, and received by anyone who has access to the email / receipt account.

How does CVL behavioral biometrics solve the problem?

The root causes for these problems are not solved by forcing the use of correct credentials.

They are solved by persistent verification of presence and validation of the correct (or the absence of a negative) state of mind.

Behavioral biometrics can prove that the person receiving the controlled substance (or prescription, for example) is in fact the person to whom they can be released and, that they are of clear mind when they receive them. Meaning that the receiver was aware of what they got and the instructions and conditions on how to properly use them.

Examples

- CVS "pharmacy kiosks" can't be currently used to dispensed scheduled substances.
- "Pour Tap Room" bars have chips that are linked to the user "of age", but the chip is not smart enough to tell if the user is inebriated. The system relies on human intervention or rudimentary rules of thumb to "guess" if the user should be "cut off".
- A digital prescription book from a physician may be compromised for a prolonged period of time before discovery.

Possible financial impact

- Bars serving beyond the reasonable are liable for consequential damages stemming from over serving.
- A pharmacist on staff may see 33% of their time lost to clerical interaction and activity that does not require their intervention (not consults).
- Hundreds of millions of dollars are processed each year in malpractice claims associated with patients not understanding the warnings associated with their medications.
- The above is true as well for pharmacist who fail to conflict potentially competing medications for patients.

USE CASE #4

Execution of legally binding documents.

Problem Manifestation(s)

- Last and Living wills are sometimes altered under questionable circumstances that make their execution fraught.
- Documents requiring notarization are sometimes certified with Notary Publics with expired, or out of jurisdiction credentials.
- Financial instruments of "material" size require wet signatures to prove the executor was "present", which means that transactions may be delayed to allow for travel for "in person" execution.

The unsolved problems

- A physical biometrics and other technologies can't tell if the person authenticating is drunk, under duress or being impacted by an illness like dementia or Alzheimer's
- A clever forger may copy the "image" of a signature, and have access to the correct credentials of the subject, thus gaining the ability to certify a document in front of a Notary Public.
- The images of digital signatures created outside of biometric parameters can be copied.
- With the correct disguise, even when challenged face to face, a human with access to correct digital credentials can impersonate another.

How does CVL behavioral biometrics solve the problem?

The root causes for these problems are not solved by forcing the use of correct credentials.

They are solved by persistent identity verification and validation of the correct (or the absence of a negative) state of mind.

Because not even a "twin" can replicate CVL biometric credentials, the threat of impersonation is removed, therefore a signature obtained through the credentials is as good as a "wet signature".

Because a "clear mind" is needed to pass the authentication challenge, no one suffering from dementia or Alzheimer's can pass the challenge, protecting estates from predatory practices.

Examples

- An elderly parent modifying their Last Will and Testament when they are not of clear mind and judgment. Sometimes coerced by predator family or relatives.
- Permission to remove a patient from life support.
- An complex or substantial investment transaction.
- Registration or transfer of a new / existing banking account online.
- Execution of an affidavit via phone or at a kiosk.
- Notarizing documents at a self serve kiosk.

Possible financial impact

- $40 trillion dollars exchanged hand in the US over real estate transactions in 2022. Assuming 0.5% (usually 2%) in cost associated with legal transaction costs - this could tap a niche in the realm of $200BN/year
- Consumers lost $5.8BN to fraud, including last will and stolen inheritances in 2022.

BSI

BSI Biometric Signature ID

Patented behavioral biometric technology for Multi Factor Authentication (MFA).

	“I am”	“I know”	“I have”	“I can do”
Behavioral Refers to unique behavioral patters of the user. These are PII free.	Awareness	Code / Password	Device	Written gesture BSI
Physical Refers to unique physical features of the user’s body. By definition, they are all PII.	Facial scan Facial Recognition DNA Speech pattern Palm geometry Palm scan Fingerprint Voice recognition Iris scan Retinal scan Vein patterns			
Other Tech. Other authentication technologies outside of the realm of biometrics.		Code / Password	UBI Key	

BSI’s behavioral biometrics meet MFA requirements in a single step, without the need of additional hardware.

In addition, the written gesture (like your signature, or writing a symbol) generates a set of credentials that can’t be shared, stolen, or reproduced by another person or technology.

What is more, the person using the credentials can’t be under duress or inebriated when authenticating their intentions.

Sample Available Solutions

BioSig-ID™

A patented biometric identity authentication solution that controls access to files and information through MFA in one product. It works on all devices using HTML5.

- Requires no hardware or software downloads and authenticates users with a four-character password.
- Blends amazing biometric technology with the password format users are comfortable with.
- Provides real-time warning of potential data crimes in progress.

BioTect-ID™

Prevents unauthorized access to Windows workstations, tablets, laptops, and the information and files within, by replacing the device's native lock screen.

- Grants access to devices after a successful authentication.
- Identity credentials can be stored locally, to allow temporary use offline.
- Protects workstations and blocks access to unauthorized users like RDP attacks.
- Allows administrators to monitor and change device access ability, reset passwords, and audit illicit access attempts.

BioProof-ID™

Used for the initial ID verification of an individual.

- Analyzes the person's government issued documents and checks the front and back to determine legitimacy of the OCR codes.
- Stores a user approved "selfie" of the user, used to compare with photo in the government ID.
- Provides both, verification AND authentication of identity.

BioSight-ID™

Used for automatic proctoring of online training and continued education programs.

- Does not collect any biometric markers and protects the privacy of the user by blurring all images
- Works seamlessly with the world’s leading learning management systems (LMSs)
- Provides complete class and course analytics and guides instructors to find suspicious activity by the student.

BioName-ID™

Transforms signatures into digital identity.

- Prevents use of PNG/JPEG forgeries
- Eliminates the need for “wet ink” to attribute the signature to a human.
- Authenticates signatures through tamper-proof MFA in a single application.

BioSafe-ID™

Secures online transactions.

- Prevents “card not present” fraud
- Ensures that the transaction is executed by the human owns the credit card, not the “entity” that may have the digital credentials.