Why Your Multifactor Authentication Platform Should Include Biometrics

WHITE PAPER

BIO-key™

Executive Summary

BIO-key's Chairman & CEO Comment

"Biometrics should not be an afterthought in a comprehensive Identity Access Management (IAM) strategy," said Mike DePasquale, BIO-key CEO. "It should be a core design factor in an IAM platform, for end-user authentication, provisioning and governance. BIO-key offers our customers a comprehensive set of biometric authentication options, both on-device and on-server, to meet the real needs of business users," continued DePasquale.

Cybersecurity has become front of mind for every company and every consumer. Securing online assets, protecting privacy and securing identity are paramount in order to build a sustainable future.

While passwords have traditionally provided the gateway to the web, they now provide open access to hackers and breachers, enabling them to wreak havoc on IT departments and security infrastructures.

Cards, PINs, Tokens and Challenge Response Questions were introduced to add an additional layer of security, but even these time-tested solutions have shown their inherent vulnerabilities.

The objective of this white paper is to provide a deep dive look at fingerprint biometric authentication, a technology that has been around for decades yet is emerging as the most secure and convenient way to address today's cybersecurity challenges. Once considered as a technology that was exclusive to law enforcement, today fingerprint authentication is used across all verticals and use cases and is native to many devices.

There are also two critical and noteworthy occurrences that support the case for organizations to add biometric authentication to their multi-factor authentication platform. An organization known for spearheading security, the FBI, recently issued a Private Industry Notification report that stated adding biometric authentication will help address the vulnerabilities of other MFA methods. Additionally, the world's leading developer of enterprise software, Microsoft, and its CISO stated "use biometrics" at Ignite 2019. Biometric authentication allows organizations to augment the use of passwords and create a "passwordless" security infrastructure.

Let's dive in a bit deeper...

A Follow Up to the FBI Cyber Task Force Report

The September 2019 FBI Private Industry Notification (PIN) report surprised readers by stating that multifactor authentication alone may not be enough to prevent cybercrime. The report's most telling statistic illustrating this fact was that 99% of cyber-attacks rely on a person taking an action such as clicking a link or opening an attachment – and falling for a scam.

During phishing attacks, intruders prey on administrators and hunt below the radar of the organization's IT team, seeking out the most vulnerable paths to much wanted data by tricking the user into submitting their password, and Splash-data reports, "nearly 10% of users selected at least one of the 25 worst passwords for one of their accounts". Therefore, these passwords are not only not strong for security, but easily suspectible to being stolen through phishing attacks.

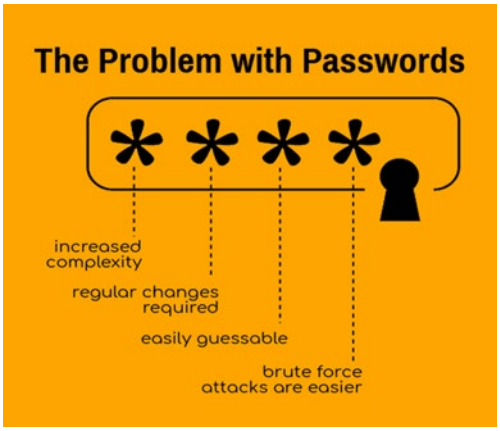
The FBI PIN report recommends the addition of biometric factors and behavioral information checks to multifactor authentication (MFA) approaches, citing known and exploited vulnerabilities of token and phone-based multifactor authentication methods.

As we ask ourselves why the PIN report was released, we must keep in mind that The FBI has one goal, which is the prevention of cybercrime. That makes them a very credible source and the report somewhat eye-opening, especially for leaders in the IT community. Overall, the report hits upon a topic that has a broad foundation and has become a necessity to fight the ramifications of cybercrime. Multifactor authentication is no longer only an option, it's a must have for every organization. Yet, as the PIN report states, "not all multifactor authentication solutions are the same." Although traditional multifactor authentication solutions share the common objective of providing a second form of identification, there are still remaining vulnerabilities and potential risks that can surface after deployment.

This paper will focus on the most widely used biometric form of multifactor authentication, which is fingerprint. It's a technology that has been around for decades and built its reputation in the law enforcement space. From the moment we are born,

our biological print is something that we are identified by and associated with for life.

Certainly, there are many forms of biometric authentication including facial, iris, palm, and even our gait. Yet fingerprint offers the most practical and least invasive form, and according to ABI Research – which predicts the market for biometric hardware will hit $19 billion by 2024 – biometric authentication and verification is continuing to find increasing adoption in the finance, healthcare, government and consumer sectors, with fingerprint recognition continuing to dominate these implementations.



Mitigation Strategies
(According to the FBI report)

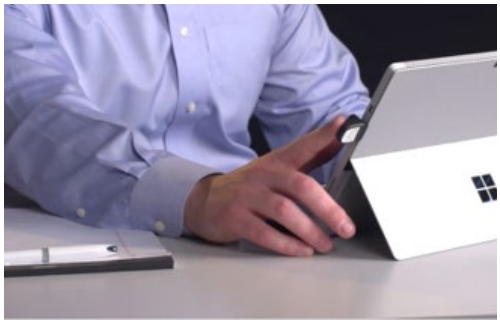
Defending against multifactor authentication attacks requires awareness of the attacks that circumvent the security, and constant vigilance for social engineering attacks.

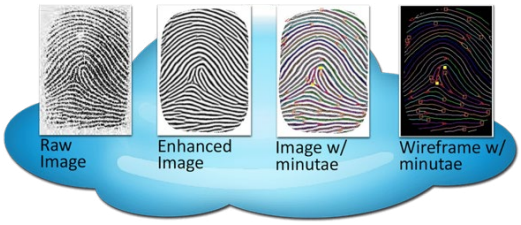
- Educate users and administrators to identify social engineering trickery—how to recognize fake websites, not click on rogue links in e-mail, or block those links entirely— and teach them how to handle common social engineering tactics.
- Consider using additional or more complex forms of multifactor authentication for users and administrators such as biometrics or behavioral authentication methods.

Additional Statistics from the FBI Report

- In 2019, a US banking institution was targeted by a cyber attacker who was able to take advantage of a flaw in the bank's website to circumvent the two-factor authentication implemented to protect accounts
- In 2016, customers of a US banking institution were targeted by a cyberattacker who ported their phone numbers to a phone he owned—an attack called SIM swapping.
- In February 2019, a cybersecurity expert at the RSA Conference in San Francisco demonstrated a large variety of schemes and attacks cyber actors could use to circumvent multifactor authentication.
- At the June 2019 Hack-in-the-Box conference in Amsterdam, cybersecurity experts demonstrated a pair of tools—Muraena and NecroBrowser—which worked in tandem to automate a phishing scheme against users of multifactor authentication.

How Does BIO-key Fingerprint Technology Work?





Fingerprint authentication starts with the enrollment process and having a fingerprint scanner / fingerprint reader. There are two types of fingerprint scanners, swipe and placement. The placement scanner is more accurate and more popular amongst enterprise customers. For customers in highly regulated industries that want to address online security compliance regulations such as those in banking, government and healthcare, a FIPS-compliant fingerprint scanner is required. A FIPS scanner is larger, therefore capturing greater detail and delivering a higher degree of accuracy.

BIO-key's intuitive enrollment interface walks the new user through the process of enrolling their fingerprints.

The software will ask the user to scan their finger three times to capture optimum data. We recommend enrolling two fingers on each hand in case of an injury to your hand or finger.

Once the image of your fingerprint is captured, BIO-key's patented Vector Segment Technology (VST) enhances the image more than 40X (industry average is about 8X). By enhancing the image to such a great degree, we can extract more than 1,500 data points. The newly enhanced image is then converted to a mathematical template using VST. The template is encrypted, time & date stamped and stored on the server. Also, it's important to recognize that fingerprint images are not stored on the device or server. Upon swiping or placing your fingerprint on the scanner it is matching your print versus the stored mathematical template. It is for this reason that prints cannot be reverse engineered.

Moving forward as the user enrolls, they are authenticated if they match the template which is associated with only their biometric. Depending upon the use case, authentication usually takes less than one second. This speed and convenience factor is what makes fingerprint biometric authentication the ideal multifactor authentication solution as it's static free and complements an expeditious workflow.

BIO-key Solutions and How Biometric Authentication Adds Security

Banking is clearly a prime industry for hackers, phishers and other cyber thieves. Banks are faced with multiple security challenges on separate fronts. First, they must secure the house, therefore their internal security platform should include best practices. Part of the challenge of securing internal access is due to the shared workstation – the "roving user" issue. As employees migrate from the drive-thru window to the computer in the lobby there is an inherent risk of compromise and vulnerability. Did the last user log out? Are they sharing passwords or card access? Is serving the customer expeditiously a priority over security? Is it easy for an employee to say, "Just this one time."

Phishing attacks have become somewhat common yet there are some new twists to the attacks themselves. The targets have changed. Initially the IT department was the target as phishers would attempt to gain access to the corporate jewels. But IT departments became wiser over time and phishers saw a diminishing return on their efforts, leading them to phish the more vulnerable staff members such as administrators, sales, customer service and part-time employees. That group is far less suspicious and doesn't have a trained eye to spot the subtleties of a phishing attack.

Subject: Dear Email User
From: John Doe <jdoe@seedschoolmd.org>
Date: 2/9/2016 5:38 PM
To: "admin@notice.org" <admin@notice.org>

Your password will expire in 2 days, Click Here to re-change your password immediately.

Thank you,
IT- Help Desk

Successful phishing attacks all end the same way, with a compromised password or stolen credentials. But what happens if the password is your fingerprint? Similarly to the example above, what if the outside intruder that's trying to gain access to your system asked your employee, "Bob, we are updating our security platform and you'll be receiving a new password. What password are you using currently? - signed Joe from IT." What if you stopped using passwords and started using biometric sign-in? Wouldn't Bob recognize Joe as a fraud from the outset? Wouldn't it make the process invulnerable to phishing attacks?

COVID-19 UPDATE

BIO-key Solutions Match the new Remote Workforce Model

The new remote workforce model being adopted across most industries presents a new range of security and authentication challenges that can be cost-effectively addressed by our solutions. Our online biometric single sign-on (SSO) and enterprise class multi-factor authentication (MFA) solutions operate equally well in on-premise or remote work environments and provide assurance that only the right user can access sensitive systems remotely.

Security and accountability risks increase dramatically in remote work environments. It starts with authenticating the user. In remote environments, using traditional authentication methods, there's no absolute assurance that the person that signed-in is the authorized user.

Remote workers are highly susceptible to phishing attacks as they are more vulnerable to being tricked by an imposter email.

In the case of authenticating the user accurately and dissuading phishing attacks, BIO-key biometric fingerprint technologies address both issues head on.

Why are Traditional Multifactor Authentication Methods Failing Us?

Even though companies worldwide are struggling to protect systems and data from incessant waves of business email compromise attacks—with losses doubling year-on-year to $26 billion—the latest warning from the FBI still comes as a surprise. One of the primary defenses against such cyber-attacks is multifactor authentication (MFA), the use of a secondary token or one-time code to assure the identity of staff. But the FBI has now warned that it "has observed cyber actors circumventing multifactor authentication through common social engineering and technical attacks."

According to the FBI, this use of secondary tokens or one-time codes to back-up usernames and passwords still isn't enough. Unless companies employ "biometrics or behavioral information—such as time of day, geolocation, or IP address," there is a risk that an attack can either trick a user into disclosing a multifactor authentication code or use technical interception to create one for themselves.

It's this accelerating sophistication of employee manipulation—so-called 'social engineering'—that's prompted the warning. In September, Proofpoint offered a stark warning that social engineering is getting out of hand, as criminals exploit "human interaction rather than automated exploits to install malware, initiate fraudulent transactions, steal data, and engage in other malicious activities."

Shared Workstations and Roving Users

In a call center environment where cubicles are closely spaced, how hard is it for an agent to watch their colleague type in their password and memorize it? In a bank, how vulnerable is the teller station that's left unattended or the teller station that's shared? How about as tellers are asked to shift from the drive-thru to the lobby? Could it be possible that someone left their card where someone else could use it? In an environment

using complex passwords, is it possible that the user might write the password down and keep it somewhere near their computer?

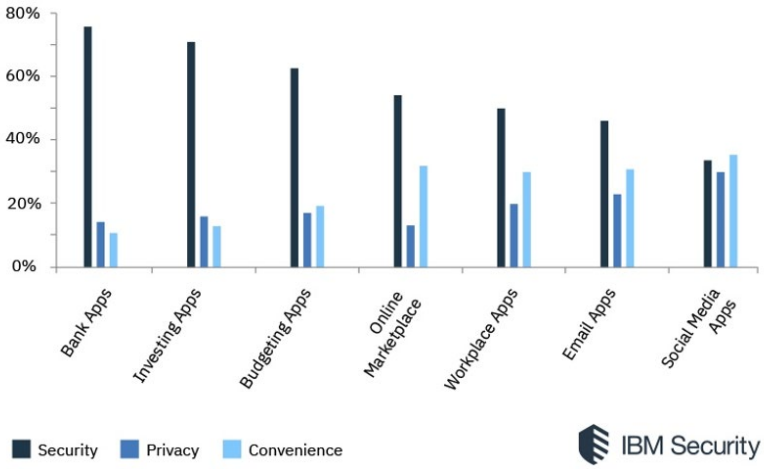
Sharing equipment, sharing resources, and optimizing workspace is commonplace in the enterprise world. But sharing personal authentication methods is criminal and could cause the demise of the security infrastructure, or worse the entire organization.

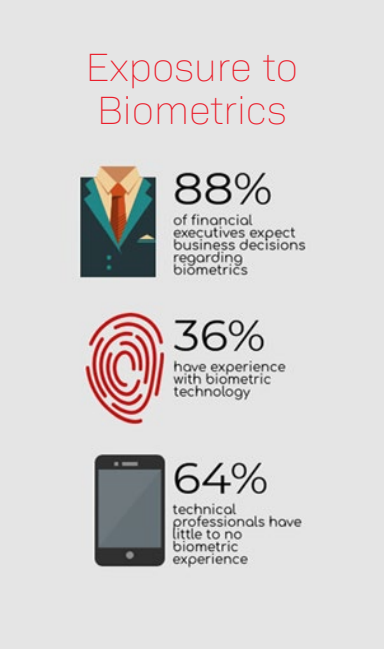
Biometrics can't be lost or forgotten, which may sound like a minor benefit, but when you measure replacement costs of cards and keys and then factor in the disruption to workflow, they certainly aren't minor issues. Biometrics are the absolute most positive form of ID because they are native – inherent and unique to the user. In a cybersecurity world that has seen thieves "copy" passwords, PIN numbers and tokens, you cannot copy biometrics. Even when we look at the closest use case for copying biometrics, "identical twins", we recognize that they have different / unique fingerprints.

But what do end users think about biometrics?

Financial firm Global Data said that 67% of global consumers would be happy to use some form of biometrics to secure their payment details. Specific to the banking and financial industry, consumers treat security above convenience, noting that passwords have always been that 'comfortable' staple as stated from IBM.

And IBM has stated due to the increase of millennial and Generation Z employees entering the workforce, "organizations and businesses can adapt to younger generations' proclivity for new technology by allowing for increased use of mobile devices as the primary authentication factor and integrating approaches that favor biometric methods".





Why Fingerprint versus the other modalities?

Fingerprint wins the test of time competition; it also wins the most use cases competition, making it the most proven form of biometric identification. IBM surveyed 4000 people, with 44% choosing fingerprint as the most secure form of authentication, the highest percentage compared to other biometric forms.

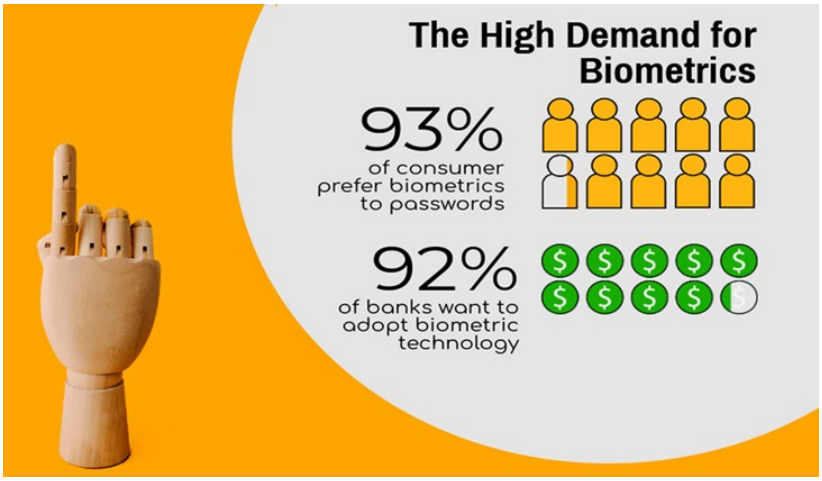
Facial recognition certainly has its purpose and is ideally suited to help vet individuals in large groups or crowds. Facial works well as a surveillance security solution for stadiums and events. Yet reports on facial recognition point to a few distinct flaws in the technology, particularly regarding scenarios when subjects must wear glasses, masks, or are accustomed to wearing makeup. Reports also find that men ages 18-32 who often change hairstyles or grow beards experience difficulties with identification. It brings to the forefront a good point about facial vs. fingerprint, for as our faces change over time our fingerprint remains the same.

Palm authentication, meanwhile, seemed to garner some momentum in the healthcare space but soon encountered some obvious challenges. The cost of the hardware, the lack of a mobile solution and the technique-sensitive requirements halted the popularity of palm ID.

Retina was also considered a biometric option, but studies showed that the retina of a woman can change color during pregnancy, thus creating an inhibitor for retina technology to prolificate.

Voice biometrics are fine for consumer use cases, but obviously lack the security necessary for enterprise use.

Ultimately, it's fingerprint that is most cost effective, most discrete, operates under the most conditions, has the most use cases and offers the longest track record of performance.



Multifactor Authentication Options

Passwords

The most common form of authentication, and certainly served a purpose prior to the days of our devices storing critical data. The most recent effort to improve password security has been to deploy complex 16-character passwords in hopes of making them harder to hack. Yet this causes too much friction for the end user and causes them to write the password down in an area they can easily reference, thus breaking down the security process. Here's the bottom line with passwords: IBM, Microsoft and many other IT leaders have declared the password as dead and urge their customers to find an alternative.

PINs

Easier to use and maintain than passwords, but still offer the lowest level of security. Another issue the organization must consider is overall cost. There are guidelines that recommend that the organization must pay for the employees' phone and service if they are asked to use the device to conduct company business.

OTP

One-Time-Passcodes (OTP) add an extra step into the password/PIN scenario, but it's a small cost for the gains in security and upkeep. Delivered by app, token or SMS message, OTP delivers a time-sensitive, single use code for every login action. Because each code is unique and generated by the system, there is no need to remember or update long strings of characters and they are much more difficult to steal. Modern phishing techniques have decreased the security community's confidence in OTP sent over SMS channels, but the app and token options are considered viable if a bit cumbersome.

Cards

More secure than something you know; a secure smart card is something you have. An MFA system secured with a card is safe from remote hacking and phishing attacks, since it requires an actual physical card to be present at the point of login. With contactless card technology widely available, a simple tap can be all it takes to use this factor for login, but since it is a physical object, it can still be lost, stolen or shared, weakening the assurance that a login is in fact the authorized user associated with the card. Another issue with cards is cost, which tends to sneak up on the organization as replacing cards becomes costly and inconvenient.

Tokens

Tokens, like cards, are something you have. With a small form factor and a wide variety of configurations, tokens can bring multifactor authentication to desktop and mobile channels with ease. A USB token just needs to be plugged into a device, and a wireless token might only need to be in close enough proximity to a device for it to vouch for a user's identity. Just like cards, however, tokens can be lost, stolen and shared, and each compromised object costs a business money, administrative labor and time to replace. Tokens also inhibit workflow and add a layer of friction.

Keys

Keys that store user passwords offer another alternate method for authentication. Users can use their password key on multiple devises. One of the issues with keys is they store all the personal / private passwords on the key itself. If your key gets in the hands of an unauthorized user, they have open access to all your password protected websites, files and applications. Cost also becomes an issue, as replacement costs due to loss or theft compound over time.

Biometric Multifactor Solutions are Here

One Biometric Authentication Engine Supports All Traditional Forms

WEB-key 4.0 is BIO-key's core biometric software engine and delivers biometric authentication to custom applications and websites. WEB-key 4.0 supports all of the traditional forms of authentication making it an ideal platform for your multifactor authentication solution.

With BIO-key's WEB-key, virtually any type of business can benefit from NIST-certified fingerprint recognition, PKI encryption of data in transit, and multi-layer triple encryption on fingerprint modules, protecting the biometric data itself. Perfect for BYOD, remote, and work-from-home scenarios, WEB-key ensures even the most mobilized workplace can easily make the upgrade to MFA.

WEB-key supports the following environments:

- Databases: Oracle, MS SQL, MySQL Enterprise, Sybase, and IBM DB2
- App Servers: Apache TomCat, JBOS, IIS, WebLogic, WebSphere, Cold Fusion, and many more
- Interfaces: .NET, COM, Java
- Browsers: Works with BIO-key Authentication for Active Directory

ID Director for Windows

Supporting Windows 7, Windows 8 and Windows 10 operating systems, BIO-key's ID Director is an advanced authentication software that supports fingerprint biometric authentication for Microsoft Active Directory users. Designed for easy deployment, ID Director does not require you to modify your current Active Directory scheme, and it can be used for both dedicated and shared workstations.

With a high level of customization options, BIO-key's ID Director is an ideal solution for bringing biometric MFA to your enterprise organization, increasing security and productivity while reducing the administrative strain produced by password resets.

SideSwipe

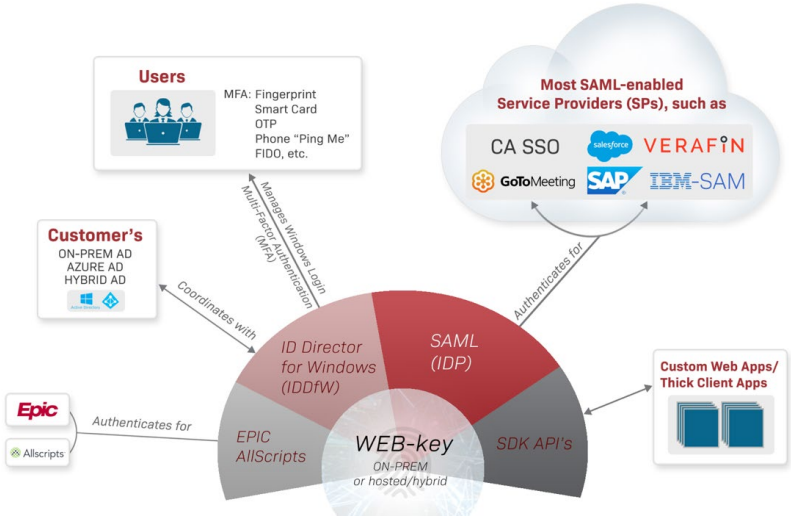
With ID Director you have the power to choose the MFA system best suited for your enterprise:

- Fingerprint
- Fingerprint + PIN
- Fingerprint + Active Directory Password
- Prox Card (RFID)
- Prox Card (RFID) +PIN
- Prox Card + Active Directory Password
- Barcode Cards
- OTP
- PingMe

SideTouch

EcoID

SidePass



Windows Hello for Business

BIO-key was selected by Microsoft as a "Launch Partner" in support of the Windows 10 biometric sign-in options offered by the Windows Hello security platform. Built-in to all Windows 10 devices, Windows Hello enables users and business customers to customize authentication options, and widely available BIO-key solutions make using fingerprint biometrics a natural and secure choice.

BIO-key's plug-and-play fingerprint readers, SideSwipe, SideTouch and EcoID have been tested and qualified by Microsoft as Windows Hello ready. Installation and enrollment is made simple with BIO-key's compact and durable readers, which simply need to be connected to a USB port.

Windows Hello manages the biometric data collected from BIO-key's readers through its Windows Biometric Framework, capturing biometrics, creating templates, storing the data and ensuring it all corresponds to the proper digital ID. With SideSwipe, SideTouch and EcoID, your business can fully do away with PINs and passwords for authentication in supported applications.

SAML 2.0 & SAML Enabled Apps

BIO-key's ID Director can also be used for Single-Sign On (SSO) through the Security Assertion Markup Language (SAML) protocol, which is used for authentication across web applications. SAML allows for one login to authenticate a user across a variety of third-party apps like Gmail for Business, Office 365, Salesforce and more, enabling efficient workflow, uninterrupted by repeated calls for re-assertion of credentials. Of course, with such freedom for the user, it is especially important that the initial authentication be as secure as possible. That's where ID Director for SAML comes in.

SSO is secure and easy with BIO-key's ID Director, which enables multifactor biometric authentication via our compact fingerprint readers – SideSwipe, SideTouch and Eco ID – or any of the 30+ fingerprint scanners integrated with our software.

For many medium and large enterprises, ID Director for SAML can integrate with your current IAM platform as a biometric IDP, thereby enabling fingerprints to be used as a strong authentication factor.

Industry Use Cases

Banking

Our clients in the financial services sector not only need to worry about protecting extremely sensitive customer data, but they must also ensure they comply with a range of stringent regulations. The Payment Card Industry-Data Security Standard (PCI-DSS), for instance, requires financial institutions to ensure access to system information and that operations are governed by strict identity management practices. The user privacy-focused Graham-Leach-Bliley Act (GLBA), meanwhile, requires proactive measures against social engineering fraud such as phishing, which is a major vulnerability for password-based security systems.

The financial services space is regulatorily demanding and high risk. That's why BIO-key offers its banking clients the FIPS-compliant PIV Pro fingerprint sensor together with software tested by the National Institute of Standards and Technology (NIST). By leveraging these technologies in an MFA system to regulate access to shared workstations, financial services providers can reliably monitor exactly who is accessing their assets and when – and keep unauthorized users out. The simplicity of fingerprint scanning means that it can take less time for employees to gain access and can eliminate issues associated with forgotten or lost credentials. Biometrics resist social engineering fraud attacks and enable accurate identity and access records. And at the same time, it all helps to make sure that the bank is in compliance with stringent industry standards.

Healthcare

If there is another industry that is as burdened by government regulations as the banking sector, it's healthcare, and here too our solutions can offer vital assistance. The Health Information

Technology for Economic and Clinical Health (HITECH) Act is motivating a full-scale migration to Electronic Health Records (EHR), and as with everything that makes the jump to digital, identity and access is a crucial consideration. This need is reflected in adjacent health data regulations. To comply with HIPAA (the Health Insurance Portability and Accountability Act), for example, organizations need to ensure sensitive patient data is protected when being transferred between insurance providers.

Major regulatory bodies like the FDA and the National Association of Boards of Pharmacy now recognize biometric authentication as a component of the kind of multifactor authentication required for EPCS, meaning our fingerprint scanning solutions can be used right away to both simplify and strengthen electronic prescriptions. Meanwhile our ID Director for Healthcare software is specifically designed for integration with Electronic Health Records systems. More than almost anyone, doctors need to be able to quickly access the data and tools they need, and our biometric technology is designed to make sure they can.

Manufacturing

In manufacturing plants biometrics are being used to provide lock down security for shared workstations and kiosks. Some manufacturers are replacing the tedious eSignature process with biometric authentication.

The manufacturing sector is one that has prized technological innovation since the Industrial Revolution, with the introduction of automation and robotics being key trends today. And yet it's also an area in which digital security has sometimes lagged, with password-based security still commonplace across a range of facilities. This despite the manufacturing sector being the second-most attacked industry in 2016, attracting bad actors by virtue of the market's expansive nature. With digital threats increasingly turning toward heavy industry and infrastructure, the National Institute for Standards and Technology (NIST) put forward its Cyber Security Manufacturing Profile, encouraging prioritized, flexible, repeatable, performance-based and cost-effective cybersecurity frameworks.

Under this climate of increased cyberthreat and regulation, manufacturing is an area where BIO-key has seen growing interest, particularly with respect to our WEB-key software platform. It's designed to leverage biometric sign-in for custom access to company assets, and it can be used together with more traditional authentication mechanisms like key cards and PINs. And by implementing our extremely cost-effective finger-

print readers at key points on the assembly line and elsewhere in a facility, considerable efficiencies can be found. What's more, WEB-key is offered on a SaaS basis, making it highly scalable and easy to implement.

Elections – Voting Process

The democratic process is at the heart of America, and that's why we need to ensure voting remains, above all, secure and accountable, especially as the specter of electoral fraud looms large in today's increasingly connected world. Government initiatives like the Help America Vote Act (HAVA) Elections Security Grant have emerged to help ensure democracy remains trustworthy by creating a culture of high security in election boards around the country, and that's where MFA authentication solutions from BIO-key come in. Our easy to deploy biometric fingerprint readers and identity management software enable elections boards to reduce risk and increase security where it counts.

After reviewing positive feedback on the Stack Exchange and Spiceworks forums, the Supervisor of Elections (SOE) for Collier County in Florida deployed BIO-key MFA to great effect. The SOE needed a Windows Hello compatible authentication solution, so we worked with the organization to install ID Director for Windows and EcoID and FIPS-compliant PRO-PIV fingerprint readers. The return on investment was clear and immediate. The switch to fingerprint authentication resulted in a massive reduction in password resets, ensuring greater workday efficiency and alleviated administrative strain. ID Director enabled the authentication of remote and mobile workers. And all of this has been accomplished at a lower cost than the Collier County SOE anticipated.

Commenting on the BIO-key upgrade, Jennifer J. Edwards, Collier County SOE's Network Security Specialist, said, "BIO-key provided us with an easy way to implement two factor authentications while maintaining roaming profiles for our users. Setup was smooth and BIO-key worked with us to answer any questions or issues."

Enterprise

Every business is evolving along with our connected mobile culture, and along with that development new modes of work have emerged. Roving and remote workers greatly increase efficiency in the modern workplace, enabling new ways for staff to collaborate, connect and make a living. But with more ways to work comes a broader attack surface for bad

actors, and a greater risk of fraud or human error along with the lost efficiency that comes with it. When multiple users share workstations, the risk of credential sharing increases, muddying access records and removing accountability from an enterprise's identity ecosystem.

BIO-key's line of solutions – including WEB-key, ID Director for Windows and our line of cost-effective and easy to deploy fingerprint readers – allow for employee identity to be as mobile and flexible as modern work demands. BIO-key's one touch authentication is scalable to your business's needs, ensuring that every member of your staff can easily and efficiently comply with best security practices no matter where they're working from. That's the BIO-key promise; that's the power of a touch.

About BIO-key International, Inc.

BIO-key is revolutionizing authentication and identity access management with biometric solutions that enable convenient and secure access to information and high-stakes transactions. We offer software based alternatives to passwords, PINs, tokens, and cards to make it easy for enterprises and consumers to secure their devices as well as information in the cloud. Our premium fingerprint scanning devices offer market-leading quality, performance and price – providing more ways to BIO-key your world!

REFERENCES

https://securityintelligence.com/new-ibm-study-consumers-weigh-in-on-biometrics-authentication-and-the-future-of-identity/

https://findbiometrics.com/biometrics-news-abi-expects-public-security-demands-drive-biometric-hardware-market-120307/