The Authentication Factor

2FA, MFA, and Zero Trust are supposed to protect us from the skyrocketing breach rate. If they're giving you migraines, you're not alone—but there is a solution.

In an information economy, data and the systems that manage it are wealth. The risks and liabilities that accrue if these fall into the wrong hands are daunting, to say the least.

Traditional password protection is simply no longer up to the task. For some time now, two-factor authentication (2FA) and multi-factor authentication (MFA) have been the order of the day.

Yet now it's becoming clear that both 2FA and MFA also fall short of the mark. Adoption continues to rise—yet so do rates of system compromise and critical data theft.

Those who work in cybersecurity know that authentication is becoming a larger and larger factor in cybersecurity concerns and strategies—even as it's more and more obviously broken.

Can it be fixed?

THE SECURITY PROBLEM

In our world of cloud systems, software-as-a-service (SaaS) applications, and computational companies, the breach rate continues to increase exponentially.

Data and data systems are falling more and more frequently into the wrong hands, with disastrous results. Failing authentication strategies are largely to blame.

Today, the vast majority of breaches result not from sophisticated, highly technical attacks, but from a very basic problem: compromised login credentials. In fact, over the last several years this has been true in four out of every five cases.

Organizations of every size are at risk. More than two-thirds of the attacks in 2018 were against small and medium-sized companies—not massive, high-value corporations or government agencies with top-secret data.[1]

Global cybercrime damage is predicted to reach a total of more than $6 trillion by 2021[2]—twelve times the size of the global drug trade and thirteen times the size of the GDP of Singapore, one of Asia's largest and most central trading economies.

All of this has happened as companies scramble to retrofit existing systems for tighter security and try to balance risk and liability, compliance requirements, and costs.

This is why passwords are now harder to use and remember, why login flows are now harder to navigate, why companies are spending more on authentication services—and why all of these seem ad-hoc and dysfunctional.

Everyone Is At Risk

- **4 in 5** — The proportion of breaches that result from compromised login credentials[3]
- **80%** — The proportion of breaches that could have been prevented with better use of MFA[4]
- **2 in 3** — The proportion of small- and medium-sized businesses that experienced cyberattacks in 2018[5]

PASSWORDS

Early on, shared secrets (now commonly known as passwords) were the most common method for establishing identity.

This venerable strategy, which predates written language, is simple: decide on a secret word, phrase, idea, sign, or symbol that is to be known only to the right person. Exclude anyone that can't produce it upon request.

The problem with this strategy—as virtually any child knows—is that secrets are difficult to keep. As humans, we have a tendency to share them, whether intentionally or accidentally, for a variety of reasons.

In today's terms, this means that passwords can be phished. They can be snooped when typed or when written down. They can be shared casually in ways that mistakenly seemed sensible or practical at the time. And, sadly, all of these now happen frequently.

This makes shared secrets a weak proof of identity. Anyone that has a shared secret can use it—so in an information economy, it was inevitable that the illicit use of shared secrets and passwords would eventually become rampant.

Yes, strategies exist to make passwords more secure. Unfortunately, they're only partially effective and are often counterproductive.

2FA AND MFA

Most experts now agree that shared secret represent only one of three fundamental "factors" that, when taken together, prove an identity.

Things that you **know** are the first factor, and include things like passwords and shared secrets.

Things that you **have** are the second factor. Your mobile phone is a classic modern example—it is yours and has distinct serial and International Mobile Equipment Identity (IMEI) numbers that belong to no other device.

Things that you **are** constitute the third factor. In cybersecurity today, this means things like fingerprints and facial structure, since they can be used to confirm the presence of your body—though as we'll see, this is often a misguided assumption.

For authentication, many organizations now rely not just on a single instance of the first factor—a password, in other words—but instead on evidence representing at least two of these identity factors.

These strategies are known as two-factor authentication (2FA) or multi-factor authentication (MFA) strategies, and have become common in recent years as organizations continue to battle the rising breach rate.

Simple passwords are easily cracked, but complex passwords get written down—and then stolen.

Password Strategies

As a form of "shared secret" authentication, passwords will always be somewhat insecure. In the best cases, they're paired with policies that make them memorable, so that users don't write them down, as well as long and unpredictable, so that they're hard to guess.

- **15 characters** — Require passwords of at least this length to prevent "brute force" attacks in which malicious tools guess passwords by simply trying every possible combination of characters
- **Passphrase-based** — Encourage passwords composed of multiple, unrelated words in a user's native language, rather than random strings of letters and numbers that are difficult to remember without writing down and difficult to enter without mistakes
- **Stable** — Avoid requiring users to periodically change their passwords, since users forced to frequently change passwords often resort to writing passwords down or to selecting easy-to-guess passwords, in the interest of remembering them
- **No character rules** — Avoid requiring the use of punctuation characters or numbers in passwords, as users tend to forget these—leading once again to password writing or simplification

2FA and MFA Strategies

Because passwords tend to be vulnerable to loss, theft, or guesswork no matter how complex they are, many organizations now use additional identity "factors" for authentication. These "2FA" or "MFA" methods for establishing identity tend to rely on common technologies.

- **SMS** — Requires the user to enter a "one time code" sent via SMS to their phone to log in
- **Authenticator apps** — Require the user to enter a "one time code" provided by a mobile phone app or to perform a particular task in a dedicated mobile phone app in order to log in
- **Hardware tokens** — Require the user to plug a dedicated piece of "identity hardware" (such as a special USB key) into their computer or to provide the code displayed on a dedicated piece of "identity hardware" in order to log in
- **Biometric scans** — Require the user to provide the correct fingerprint or to present the **correct face to a scanning device in order to log in**
- **Additional secret questions** — Require the user to demonstrate accurate knowledge of a series of personal or biographical details in order to log in

THE RELATED IDENTITY PROBLEM

Authentication is the key to cybersecurity because the best way to protect data and systems is to ensure that only trusted, trained, and properly vetted individuals can access them.

This "only the right people" approach is fundamentally about identity, and identity is what authentication is designed to recognize and guarantee.

That's why authentication strategies—both in relation to passwords and in relation to 2FA or MFA—continue to become more complex with every passing day.

Where does "Zero Trust" fit in all of this?

Zero trust is a philosophy—not a cybersecurity technology. In theory, a "zero trust" organization tries to ensure the security of its data and systems by refusing to ever "trust" users, under any circumstances.

This is supposed to mean that systems are configured to act as though everyone is a potential attacker all of the time—both inside and outside the organizational environment. In practice, zero trust has come to mean simply requiring more and more frequent authentication (usually through login prompts), during which more and more identity factors are provided.

Though this sounds secure, it still requires "trusting" whatever authentication factors are in use—not to mention trusting users during the times in between each authentication event.

Too often, multi-factor authentication and zero trust mean that users are forced to constantly fumble with complex login workflows and phones or other that can be easily stolen anyway.

INSECURE SECURITY

For the reasons we've discussed, organizations ought to pursue better security and a "zero trust" culture. Unfortunately, however, all of the identity factors and methods in common use are inherently insecure in some way.

Things You Know

These factors have to balance strength of authentication against the limits of human memory.

Shorter, simpler passwords are easier to remember, but also easier to crack using so-called "dictionary" and "brute force" attacks.

Longer, more complex passwords are less easily attacked using automated tools, but are far more difficult to remember, meaning that users often adopt practical but insecure strategies to aid in recall—passwords and secrets are also typically entered using keyboards, which can be monitored by malicious "keylogging" software for password theft.

Once stolen or discovered, passwords and secrets can be used by anyone—whether or not they're the intended user. This insecurity is inherent to the shared secret model.

An average password can be brute-forced in the background in the time it takes to listen to a couple of songs.

Dictionary and Brute Force Attacks

Dictionary and **brute force** attacks are two of the most common ways for hackers to gain access to password-protected accounts.

In a dictionary attack, automated software tries to access an account by endlessly trying to log in using common words, phrases, names, and combinations of these. It may take thousands of attempts, but that's no problem for an automated attack script.

In a brute force attack, attacks try every possible combination of letters, numbers, symbols, and password length. This may sound impossible, but modern home computer systems can brute force an 8-character password in just a few hours.

How vulnerable are passwords?

How long does it take to discover a typical password using automated "brute force" methods? With a modern home computer system, cracking times are surprisingly short:

Six-character password	Less than one second
Seven-character password	Less than ten minutes
Eight-character password	Less than four hours
Nine-character password	About four days

These figures apply to cracking truly random sequences of characters that are difficult to remember. For passwords that contain patterns—words, names, or dates for example—attack times are often exponentially shorter.

How vulnerable are 2FA and MFA tools?

Most of the common tools for 2FA and MFA security that are in use today are also vulnerable. Here are the problems with each of them.

SMS code via mobile phone	Phones are easily stolen
App via mobile phone	Phones are easily stolen
Hardware token	Hardware tokens are easily stolen
Fingerprint scanner	Can be fooled in minutes with a print sample
Face ID	Can be fooled in hours with commodity tools

Even when these are used in combination—for example, a code delivered via an app to a mobile phone that is fingerprint-protected—the vulnerabilities at each step ultimately mean that a skilled attacker can gain illicit access with relative ease.

Things You Have

As physical objects that live in the world, these factors are even easier to steal than passwords.

The most common of these are things like mobile phones (for receiving SMS codes) or housekey-sized hardware "fobs" that display rotating security codes on tiny screens. Ask yourself how often you've mislaid your phone or your keys—or how hard it would be for a determined thief to steal them from you—and you can see the security problem here.

Yes, some of these devices like mobile phones, have protections of their own to prevent users from accessing them. Most, however, do not—and even devices that have their own protections may be vulnerable.

For example, lock screen PINs on mobile phones are merely something known once again—and are easy enough to steal by carefully watching someone as they unlock their phone.

Worse, security measures on these heavily-used devices are often inconvenient, leading users to frequently bypass or minimize them in device settings.

Once an attacker has control of a phone, hardware token, or other physical object, they are able to use it to identify themselves as the intended user. This, again, is insecure.

Things You Are

In recent years, many organizations have turned to biometrics as an apparent cure-all for security issues.

Because they're used in forensics and require computing power to analyze, fingerprints and faces are often presumed to be highly secure identifying technologies.

In fact, anyone with five minutes' access to your workspace or home can probably obtain a clear copy of your fingerprint. Unless you wear a mask at all times, your face is always visible, public, and easily recorded.

With these resources in hand, a motivated hacker has everything needed to fool a fingerprint or face scanner. Fingerprint security is particularly easy to fool, and many amateur hackers have posted YouTube videos showing them quickly circumventing fingerprint scanners using a fingerprint and household items.

Face scans require more effort to crack because of the infrared heat signatures involved, but researchers have demonstrated high success rates at fooling face scanners using tools that are within any hobbyist's budget.

In short, measurements or images of your body may be unique to you, yes. But in the real world, they're not actually **you**—and the measurements or images are all that is needed to unlock fingerprint- or face-based authentication prompts.

ZERO TRUST

With the adoption of "zero trust" policies, users are more frequently asked to frequently required to re-enter login credentials or re-assert their identities.

This boost in frequency provides the illusion of more security. Users are being forced to "prove" their identities more often, after all. In most cases, however, this strategy provides only that—an illusory increase in security.

If the methods being used to authenticate are vulnerable to begin with, as we've seen, then entering them more often reduces productivity without providing any more certainty about a user's identity.

Worse, all of these strategies try to establish identity only for a moment—they're temporary interruptions in otherwise unprotected work.

Once a user provides the correct password, code, or fingerprint, they are given unfettered "access" to work until the next check, whenever that may be.

In practice, there's nothing to prevent a rogue employee from logging in, then simply handing their workstation off to a malicious "someone else."

There's also nothing to protect a system when the right user simply forgets to log out before stepping away—and the wrong user steps in and continues to compute without facing any checks whatsoever.

Why Zero Trust Login Policies are Often Too Trusting

No matter how frequently users are asked to prove their identities, the gaps remain **unprotected.**

Even if policy forces a user to re-authenticate every fifteen minutes—at 8:15, then at 8:30, then at 8:45, and so on—the time in between authentication events remains **trusted** time, during which the identity of the user isn't guaranteed.

ALL THE COSTS, NONE OF THE BENEFITS

In the real world, today's most common 2FA and MFA tools are neither a strong nor a durable answer to the rising breach rate.

Most impose a variety of additional costs. More hardware or software is usually required, along with specialists to operate and over-

see them. More support staff are needed to troubleshoot user problems.

Worse still, they tend to harm productivity and morale.

Users' workflows are interrupted. Mornings are lost waiting on hold to talk to support teams after inappropriate lockouts.

Complicated, multi-step login workflows frustrate users quickly, and ways to bypass or short-circuit them become a bigger part of company culture as any "zero trust" initiative.

Worst of all, "zero trust" companies that use 2FA or MFA often develop a false confidence about security—while still trusting almost everyone almost all of the time, and verifying identity with weak tools the rest of the time.

The Worrying Big Picture

- Passwords are easy to crack
- Today's most common 2FA and MFA methods are easily compromised
- Zero trust is often anything but
- Adopting these strategies is costly, in dollars and in productivity loss
- The more of these that companies adopt, the more morale and productivity fall, and the more frequently insecure workarounds are found and employed by users

In short—new authentication tools and strategies are needed, because **authentication** is rapidly becoming the central front in the global cybersecurity battle.

IN A PERFECT WORLD

What would a more secure authentication universe look like? Using the discussions about shortcomings that we've just had as a guide, we can outline some basic criteria.

A more secure, practical, and cost-effective authentication strategy would:

- Enable rather than limit productivity, imposing no net increase in support overhead, training costs, or lost work time
- Make users feel secure without making them feel frustrated, hamstrung, interrupted, or impeded as they work
- Grant access only to the right people, rather than to anyone that acquires the right information, credentials, bodily measurements, or devices
- Be capable of verifying identity continuously, at all times, as users work, rather than checking it only periodically
- Be cost effective, both in dollar terms and in labor and productivity terms

This is the kind of list that makes pessimists laugh. It's an impressive set of requirements, and when considered alongside traditional authentication strategies, it seems impossible to achieve. Just a decade ago, it would have been—but happily, today isn't a decade ago. Today is now.

FINDING A SOLUTION

In 2016, a small and relatively obscure team of researchers at the University of Victoria developed a breakthrough technique for biometrically identifying individuals.

Their technique was different from traditional biometrics in one key way—it didn't rely on measurements of the shapes and sizes of body parts like fingertips, fingerprint ridges, chins, or cheekbones.

Instead, it used the new science of machine learning to identify users based on tiny and entirely individual patterns in their movements.

This breakthrough provided distinctive, radical benefits over traditional biometric technologies.

The result was a form of biometric identity checking that is essentially unbreakable, yet at the same time also continuous. It's able to establish identity in the background with certainty as people go about other, productive activities.

The researchers involved in the project applied this science, called "behavioral biometrics," to the bodily movements involved in typing and screen pointing to create a new, nearly ideal avenue for authentication in computing systems.

Patents were applied for and awarded, and the team went on to take the product to market as Plurilock—the same company that produced the article you're reading right now.

Dr. Youssef Nakkabi, Plurilock's innovation director, is part of the team that's revolutionizing authentication.

FROM BEHAVIORAL BIOMETRICS TO ADVANCED AUTHENTICATION

It was clear early on that behavioral biometrics enabled a new kind of authentication, but more was needed. Why? Because human beings aren't robots—they always behave at least somewhat unpredictably.

On a given day, any person may be tired after a late night, or have sore hands from moving their piano upstairs, or be wearing a bandaid on a cut finger, or be recovering from a seasonal cold. All of these things can slightly affect their movements.

This creates a key question—how stringent should behavioral checks be? A skilled impersonator may be able to meet a less stringent, piano-friendly behavioral check. On the other hand, a highly strict behavioral check might

wrongly exclude a legitimate user whose movements have been affected by everyday life circumstances.

The Plurilock team developed two strategies to address this tension. First, they made the strictness of behavioral checks configurable, so that security administrators can tune authentication requirements for the security needs of their own organization.

Next, they added additional forms of observable user data to the machine learning input. These include things like location and recent travel, browser and hardware fingerprinting, network topology and context, and additional nearby sensor data.

The result is what Plurilock calls advanced authentication—invisible, incredibly strong, AI-driven, continuous-capable, and resistant to false positives and false negatives.

IMPROVED UX AND REDUCED OVERHEAD

The security benefits of advanced authentication are significant, but some of the knock-on effects have been at least as impressive—if not moreso.

Advanced authentication puts a stop to the forward march in unwanted login complexity that's happened in recent years.

Users are exhausted by the endless arrival of ever-more complex login workflows—and organizations are tired of implementing, maintaining, and supporting them.

Because advanced authentication is invisible and operates in the background, it adds no new steps to everyday login attempts. In fact, already deployed 2FA and MFA steps can often be eliminated, returning users to the days of simple username and password logins without losing the protection of a strong form of multi-factor authentication.

This ease of use and transparency means far less time and money spent on technical support teams, whose jobs have recently become ever more a matter of simply helping users to log in.

User morale, satisfaction, and compliance grow, while the overhead that results from high support loads and lost productivity is reduced—or eliminated.

The Two Key Benefits of Behavioral Biometrics

It's impersonation-proof.

Behavioral-biometric data can't be stolen and re-used. While it's easy to create a perfect copy of a fingerprint and re-use it, it's prohibitively difficult to steal the micro-cadences and variations in their bodily movements, and virtually impossible for anyone other than the person in question to exhibit them.

It happens in the background.

Behavioral-biometric tools take biometric measurements in an entirely new way. No longer a focused, one-time "scan" that must occur before work begins or before access is granted, this type of biometrics is instead an ongoing "observation and analysis" that happens during a user's movement—as other, regular work is happening.

Why Authentication UX Matters

When login workflows are overly complex, users tend to:

- Find **insecure** work-arounds like credential storage or various bypass strategies
- Avoid logging in, which means the **postponement or neglect** of critical privilege-escalated tasks
- Suffer from **decreased morale,** job satisfaction, and **productivity**
- **Share credentials** with other users that are unable to log in
- Use significantly increased amounts of **support time**
- See cybersecurity as a **hindrance** to be avoided, rather than as an important protective strategy

ADVANCED AUTHENTICATION IN THE WILD

Where is advanced authentication in use today? In a wide variety of roles and environments.

In the defense industry. Plurilock provides the most cutting-edge versions of its technology to key national defense agencies in both the United States and Canada.

In the finance industry. Plurilock provides security for a number of major banks and financial services companies, with billions of dollars at stake.

In healthcare and education systems. Highly regulated organizations require solutions that guarantee high levels of security and high levels of privacy on systems that may involve hundreds or thousands of user touches, making advanced authentication an ideal solution.

In SaaS applications. Plurilock's sells to SaaS organizations in the financial technology ("fintech"), health technology ("healthtech"), educational technology ("edutech"), and business operations verticals, all of whom must protect a growing store of cloud data without driving away paying end-users that resent increased app "friction."

In the cybersecurity industry. Plurilock's cybersecurity partners include both B2B and B2C providers, all of whom are keen to

Renewing the Promise of Authentication in Cybersecurity

Because of its ability to recognize individual human beings, regardless of credentials, and its ability to operate invisibly and continuously, **advanced authentication** significantly expands the list of protections that strong authentication can provide.

What kinds of attacks is **advanced authentication** well-positioned to reduce or prevent?

- Advanced persistent threats
- Remote Access Trojans, botnets, backdoor attacks, and ransomware
- Social engineering attacks
- Illicit privilege escalations
- User access control bypasses, abuse of escalated privileges
- Impersonation, phishing, brute forcing, theft cracks, authentication factor interception, and replay attacks
- Logon scripting, remote logins, remote file copying
- Cross-site scripting attacks

enhance the security profile of their offerings and services to clients—and to reduce the levels of risk and liability that they bear as cybersecurity providers.

GETTING BACK TO WORK

It's been a long time since authentication flows were a simple afterthought in the typical workday, rather than a series of repetitive tasks that consume time and dollars.

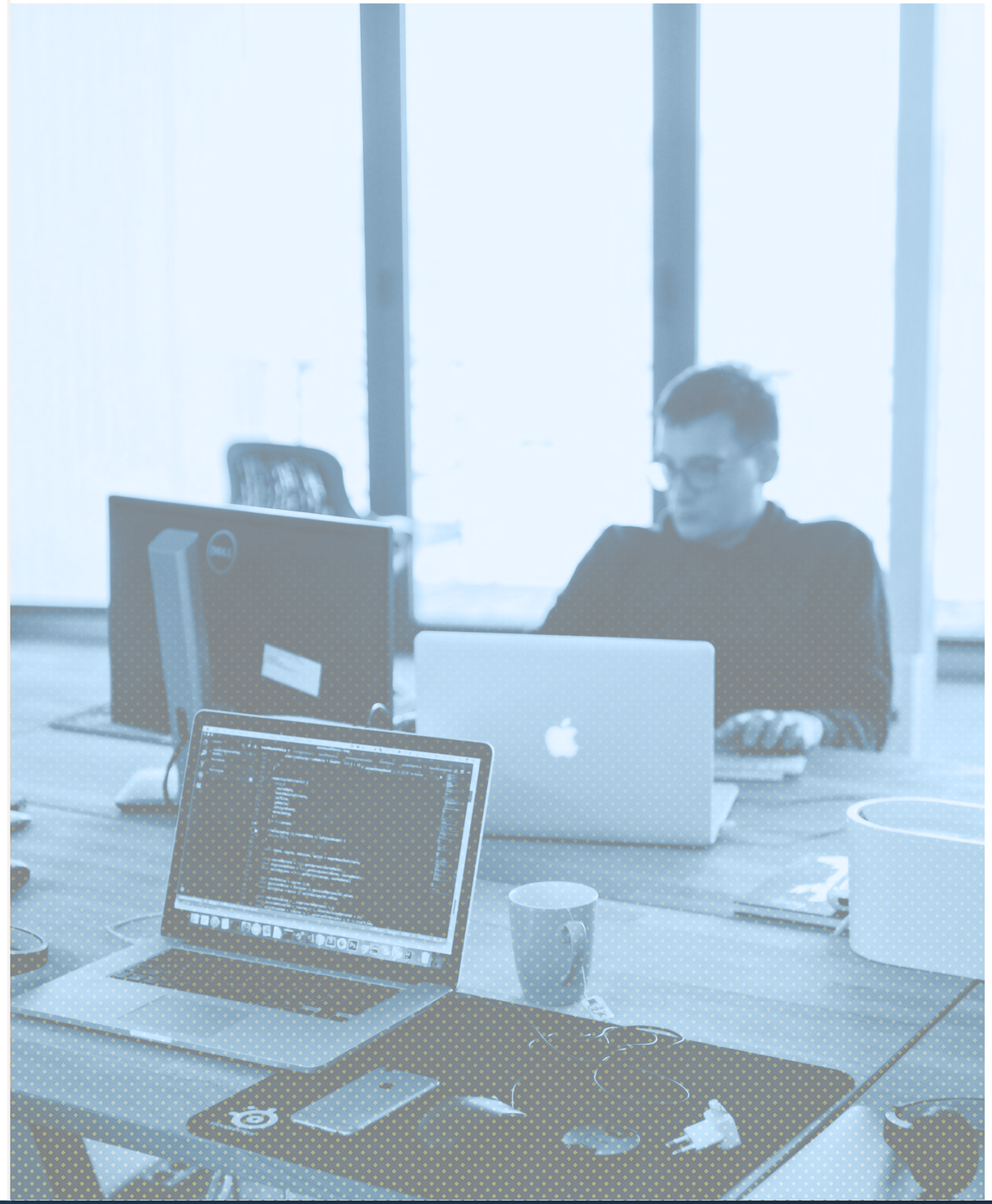
Today, behavioral-biometric security and advanced authentication flows are becoming commonplace.

Plurilock solutions are available in desktop-native and cloud-based versions supporting enterprise endpoints, and SaaS applications.

The list of potential applications is now endless—and a sea change in the way that organizations handle authentication is well underway.

Authentication can be—and has been—fixed. The migraines can stop.

Years after it became clear that password security represented a threat to the cyber economy, users at organizations of all kinds can finally get safely back to work. ■



APPENDIX — PLURILOCK SOLUTIONS

Plurilock ADAPT
Adaptive MFA

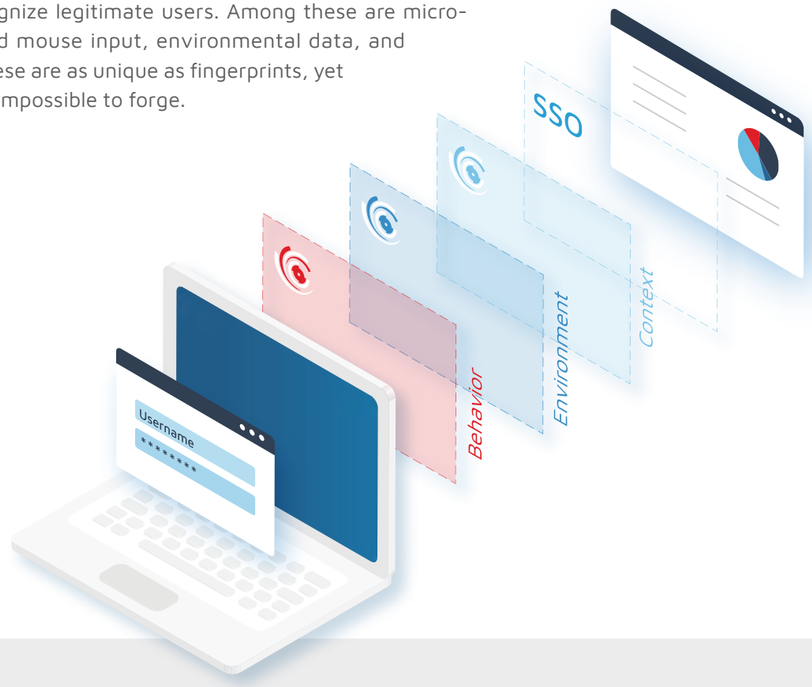
- ✓ Risk-based, adaptive authentication
- ✓ Behavioral, environmental, and contextual factors

Plurilock DEFEND
Continuous MFA

- ✓ Continuous authentication
- ✓ Risk-based, adaptive authentication
- ✓ Behavioral, environmental, and contextual factors
- ✓ Enterprise endpoint and device protection

With traditional MFA, users carry or know something that—in theory—nobody else carries knows. Yet in the real world, anything one person can carry or know can be carried or known by anyone else, too. More recent tools rely on the shapes of bodies—fingerprints, iris scans, or faces. But these are rough on privacy and easily fooled.

Rather than relying on any one factor, Plurilock adaptively uses a variety of available factors to recognize legitimate users. Among these are micro-patterns in keyboard and mouse input, environmental data, and contextual metadata. These are as unique as fingerprints, yet are privacy-friendly and impossible to forge.



Plurilock ADAPT

Use For

- Adaptive, risk-based authentication
- MFA in Cloud/JS applications
- MFA in Citrix environments
- SSO MFA in SAML, OIDC, or ADFS environments

Includes

- Plurilock ADAPT JavaScript client
- Plurilock ADAPT API access
- Plurilock cloud server instance

JavaScript Client Compatibility

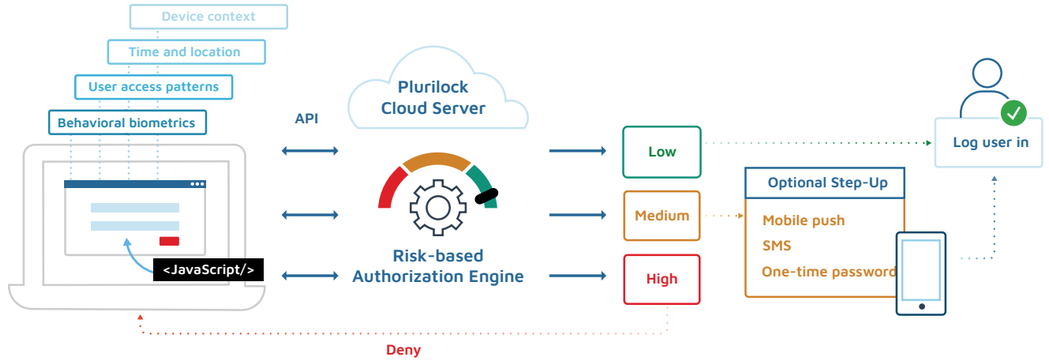
- Microsoft Edge
- Mozilla Firefox
- Apple Safari
- Google Chrome

Server Instance Specifications

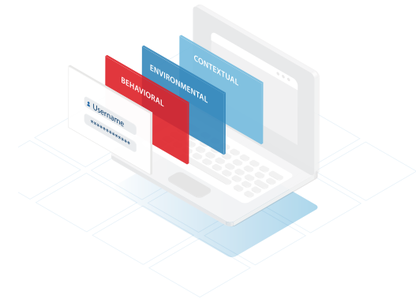
- Amazon AWS
- CentOS 7

Plurilock API Reference Implementation

- Python 2.7 + Django 1.11
- Javascript + HTML/CSS (Bootstrap)



Plurilock ADAPT provides adaptive, biometric MFA for your workflows and apps—no phones, fobs, or other hardware required



Plurilock DEFEND

Use For

- Adaptive, risk-based authentication
- Continuous authentication
- Cloud/JS apps
- Citrix ADFS environments
- Enterprise endpoints
- Endpoint detection and response
- SIEM-friendly data streams

Includes

- Plurilock DEFEND endpoint/EDR agent
- Plurilock ADAPT JavaScript client
- Plurilock ADAPT API access
- Plurilock cloud server instance *
- Online admin console

* On-premise server available. Contact Plurilock for specifications and availability.

Endpoint/ Agent Specifications

Compatibility

- Windows 7, 8, 10
- Windows Server 2008, 2012, 2016, 2019
- Mac OS Yosemite, El Capitan, Sierra, High Sierra, Mojave

Footprint

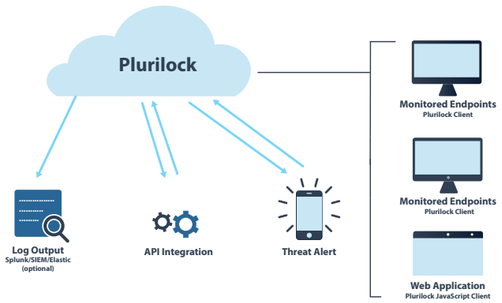
- 2MB installer
- 3MB installed
- <1% CPU, memory, network usage

Javascript Client Compatibility

- Microsoft Edge
- Mozilla Firefox
- Apple Safari
- Google Chrome

Plurilock API Reference Implementation

- Python 2.7 + Django 1.11
- Javascript + HTML/CSS (Bootstrap)



Plurilock DEFEND authenticates users invisibly, 800 times a day—providing smooth access for the right users and no access for anyone else.

Protects against

Stolen Credentials

Whether due to phishing attacks, data theft, user carelessness, or other breaches, once attackers obtain legitimate credentials, they can cause limitless harm and be almost impossible to detect. With Plurilock, every authorized user is can be continuously matched against a known behavioral and environmental profile. Strangers are recognized in seconds—no matter which credentials are used.

Password / Account Sharing

When users secretly share licenses, logins, or passwords, they create security risks and licensing issues. Plurilock recognizes only the authorized individual—not a set of credentials—so that only intended users have access to key resources.

User Substitution

Outsourcing organizations have a nasty habit of substituting one user for another without the client's knowledge or consent, putting systems and data at risk. With Plurilock, outsourced work is done only by the users you're paying for—and no one else.

Insider Threat

Internal bad actors often use other employees' credentials or workstations for criminal activity, making them difficult to detect and identify. Because Plurilock recognizes actual human beings and not just accounts, inadvertent or malicious privilege elevations no longer provide the access necessary to carry out harmful acts.

External Identity Fraud

Organizations that serve online clients or members of the general public are faced with the daunting task of protecting against data theft and account compromises. With Plurilock, online users can be profiled and authenticated using the same advanced MFA stack.

User Carelessness

Even the most conscientious users sometimes walk away before logging out, leaving workstations and sessions open and enabling bad actors to step in unnoticed to wreak havoc. Plurilock immediately detects user changes like these—so that moments of forgetfulness no longer lead to months or years of consequences.

Frequently Asked Questions

Does Plurilock know what I'm typing?

No. Plurilock analyzes the way that you type—characteristic times and patterns between and during keystrokes—rather than what you are typing. The data is numeric, yet highly individualistic, and it is this data Plurilock's tools analyze—not the content of your typing.

Does Plurilock know what I'm clicking on, or what websites I visit?

No. Plurilock analyzes the way you use your mouse—characteristic patterns in speed, acceleration, and actuation timings—not what you do with your mouse.

Can someone record my keystrokes and trick Plurilock into thinking it's me?

No. Recorded movements do not have the same micro-variations over time that real humans generate. Recorded movements are not recognized as being authentic input from the intended user.

How resource-hungry is the Plurilock?

Plurilock's authentication technology is incredibly lightweight, using far less than 1% of any system resource, including memory or CPU cycles, on any modern endpoint or computing device.

How is my profile stored, and is it secure?

Profile data is encrypted for transmission and for storage in a secure database. A key Plurilock advantage is that even if somehow lost to the wild, stolen profile data cannot be used to reconstruct a user's real-world identity.

What happens if a user's hand is injured or they're sick?

When behavior patterns change, Plurilock takes action, and authentication failures result. As administrators mark these failures as false alarms, however, Plurilock's machine learning algorithms come to recognize the user's "new" interaction style—and update the user's profile accordingly. At any time, security personnel can also instruct Plurilock to re-learn about a user's behavior from scratch.

REFERENCES

1. Verizon Data Breach Investigations Report 2018
2. Cybersecurity Ventures 2017 Cybercrime Report
3. Verizon Data Breach Investigations Report 2017
4. Verizon Data Breach Investigations Report 2017
5. Verizon Data Breach Investigations Report 2018

Let's talk

1.888.776.9234 | www.plurilock.com

Plurilock