Plurilock

NEXT-GENERATION AUTHENTICATION

Device-free authentication for zero trust.

Reduce friction. Recognize actual people. Achieve zero trust.

Plurilock provides strong multi-factor authentication for web applications and enterprise environments without the need for additional devices. By combining behavioral, environmental, and contextual identity signals with machine learning technology, Plurilock recognizes real human beings—not merely credentials, devices, or secrets.

With traditional MFA, users carry or know something that—in theory—nobody else carries or knows. But in the real world, anything one person can carry or know can be carried or known by anyone else. Other tools rely on fingerprints or face scans for authentication—but these are bad for privacy, add steps, and are surprisingly easy to fool. Not Plurilock.

No Phones Needed

Get the benefits of MFA without issuing phones or controlling apps.

No New Hardware

Sidestep the need for fingerprint readers, USB fobs, or other hardware.

No Codes or Tokens

Eliminate the need to deliver, receive, or enter one-time codes or tokens.

User-Transparent

Deploy MFA rapidly without affecting user logins or workflows.

Strong Security

Achieve security levels not matched by traditional MFA technologies.

Plurilock

Invisible MFA

AT LOGIN PROMPTS

Plurilock ADAPT authenticates invisibly.

Rather than relying on any one identity factor, Plurilock ADAPT combines a variety of real-world identity signals to recognize legitimate users. At the top of the stack, Plurilock relies on patented behavioral-biometric algorithms, analyzing micro-patterns in input behavior that are as unique as fingerprints, yet privacy-friendly and impossible to forge. These are augmented with geolocation and location history, device fingerprinting, network context, and other ambient signals to provide strong authentication invisibly, in the background.

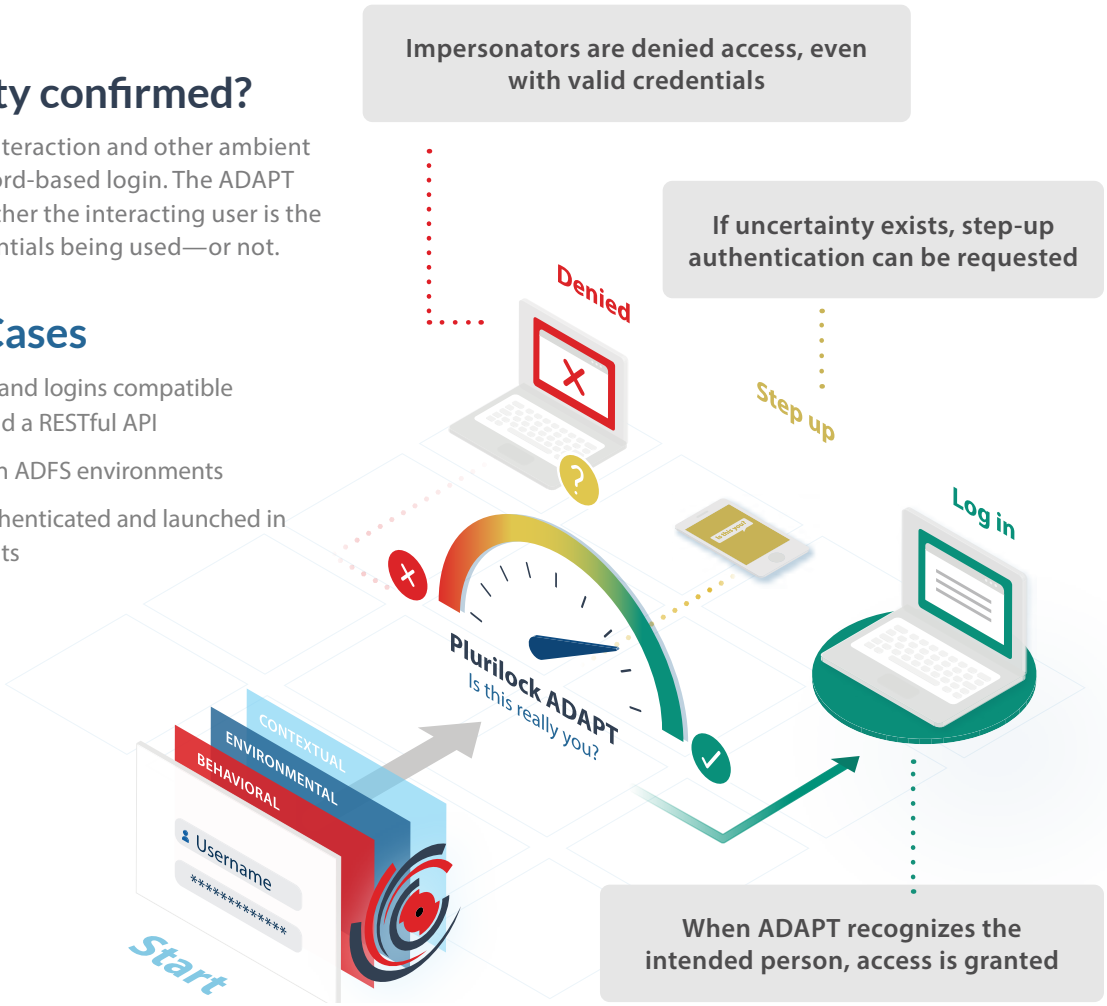
Every company would prefer to add multi-factor authentication without compromising productivity. Traditional solutions add steps, frustration, and support overhead, yet are user-agnostic—they know only that someone has provided the right password, device, or token, not whether that someone is the right someone. By combining machine learning with multiple observable identity signals, Plurilock can authenticate users by simply recognizing them.

How is identity confirmed?

ADAPT observes user interaction and other ambient signals during a password-based login. The ADAPT API then indicates whether the interacting user is the real owner of the credentials being used—or not.

ADAPT Use Cases

- Web applications and logins compatible with JavaScript and a RESTful API
- Login workflows in ADFS environments
- Citrix sessions authenticated and launched in ADFS environments



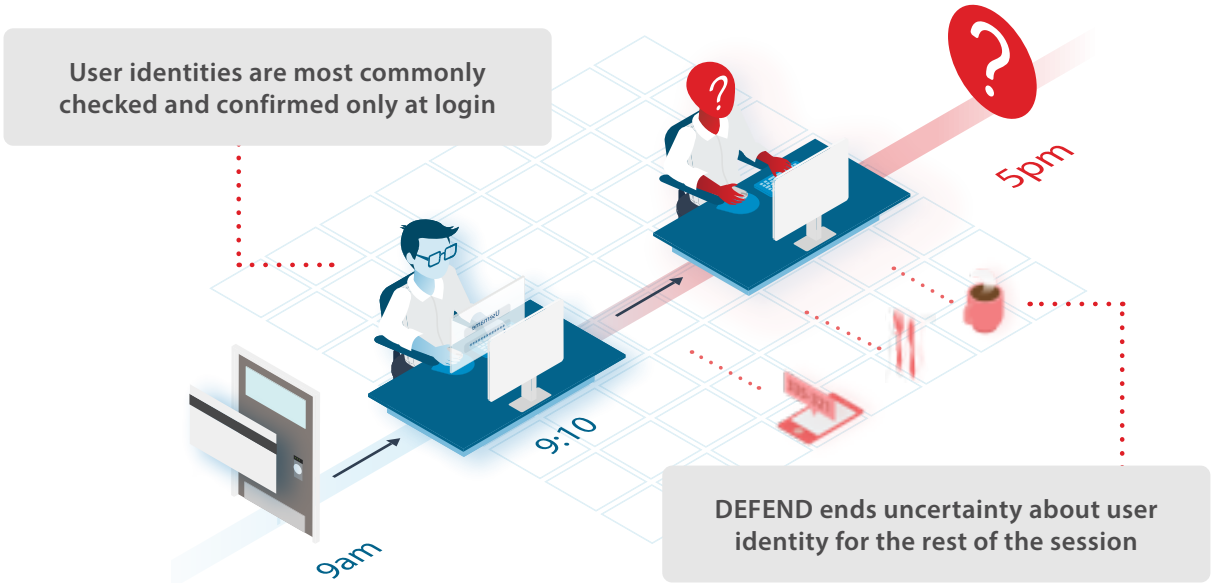
Plurilock

Continuous Authentication

IN THE BACKGROUND

Plurilock DEFEND authenticates all day long.

Rather than checking identity only at login, Plurilock DEFEND analyzes imperceptible micro-patterns in keyboard and pointer interaction to invisibly authenticate users every 3-5 seconds, nonstop—minutes, hours, or even days after login. The moment a stranger appears, DEFEND knows and springs into action.



How is identity confirmed?

DEFEND observes user interaction in the background as work happens, throughout the workday. If at any time the user of a session is found not to be the rightful owner of the credentials used to log in, DEFEND immediately ends the session or alerts your SIEM.

DEFEND Use Cases

- Windows endpoints and workstations in enterprise environments
- Mac OS endpoints and workstations in enterprise environments

True continuous authentication is a **must** for zero trust.

NIST SP 800-207 outlines the criteria for a true zero trust environment, including the requirement for "continuous monitoring and re-authentication...throughout the user interaction." Only DEFEND has it.

Plurilock

Zero Trust Readiness

FOR FULL-WORKDAY IDENTITY

The NIST 800-207 Standard

In recent years, "Zero Trust" has increasingly become a cybersecurity best practice. The term refers to a cybersecurity posture in which the network is assumed to be hostile, with no differentiation between internal and external hosts and systems. All users, both internal and external, are assumed to be threatening interlopers until proven otherwise.

For this reason, US National Institute for Standards and Technology (NIST) recently issued Draft Special Publication 800-207, which seeks to outline and codify requirements for the successful implementation of a "Zero Trust Architecture."

Plurilock and Zero Trust

Because Plurilock products are based on advanced anomaly detection technology, both ADAPT and DEFEND enable key forms of compliance with NIST SP 800-207.

Plurilock ADAPT provides adaptive authentication using behavioral, environmental, and contextual factors. Plurilock DEFEND provides continuous, real-time authentication using multiple behavioral factors. Both are driven by machine learning and provide NIST-compliant identity confirmation to support Zero Trust computing.

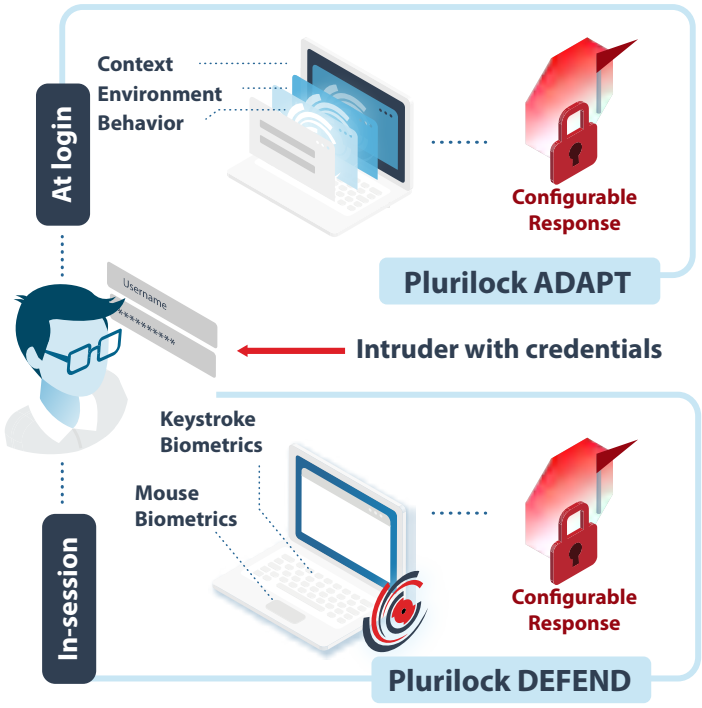


Figure 1

Plurilock analyzes the behavioral, environmental, and contextual data that users generate as they compute. When these don't match past profiles or exhibit anomalous characteristics, users are denied access, reported to security teams, or locked out. ADAPT protects particular login and cloud workflows while DEFEND provides continuous, full-session endpoint protection.

Plurilock

ZERO TRUST READINESS

Plurilock and NIST 800-207

Section	NIST advice or concern	What Plurilock does	Related product
§ 2.1 item 4	**Access to Resources** Must be determined in part by "network location, previously observed behavior…automated user analytics, device analytics, and deviations from observed usage patterns."	**Authenticate users with a combination of:** ✔ Network location ■ ✔ Previous location history ■ ✔ Current location analysis ■ ✔ Device properties ■ ● ✔ Previous behavior profile ■ ● ✔ Current behavior analysis ■ ●	■ Plurilock ADAPT ● Plurilock DEFEND
§ 2.1 item 6	**User Authentication** Must occur through "a constant cycle of access, scanning and assessing threats, adapting, and continuously authenticating" in which "[c]ontinuous monitoring and re-authentication occur throughout the user interaction" to "achieve a balance of security, availability, usability, and cost-efficiency."	**Continuously observe user behavior in order to:** ✔ Assess threats ● ✔ Adapt user profile data ● ✔ Confirm user identity every 3-5 seconds ● ✔ Authenticate invisibly for maximum usability ●	■ Plurilock ADAPT ● Plurilock DEFEND
§ 3.2	**Trust Algorithm** Must incorporate multiple identity inputs and automate responses to ongoing use and new access requests. Inputs may include behavioral data, biometric data, time data, and geolocation data.	**Capture and act on behavioral- biometric and other identity data:** ✔ Typing rhythm ■ ● ✔ Pointer interaction ● ✔ Geolocation ■ ✔ Computing context ■ **Act in order to:** ✔ Deny requested access ■ ✔ Terminate ongoing access ■ ●	■ Plurilock ADAPT ● Plurilock DEFEND
§ 5.3	**Insider Threat** Must reduce the risk of insider attack and access from compromised accounts. Systems should be able to "detect access patterns that are out of normal behavior and deny…access to sensitive resources."	**Deny access, even with valid credentials, in cases of user-specific:** ✔ Anomalous keyboard behavior ■ ● ✔ Anomalous pointer behavior ● ✔ Anomalous device properties ■ ✔ Anomalous locational behavior ■ ✔ Anomalous network context ■	■ Plurilock ADAPT ● Plurilock DEFEND

Plurilock

Quick Summary

Plurilock's advanced MFA is flexible and can invisibly protect both point in time applications (logins) and continuously secure endpoint and web sessions.

Device-free

Authenticate with factors already at work. Behavioral and contextual signals authenticate users at login and throughout the day.

Invisible

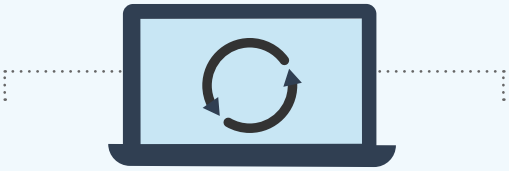
Many MFA solutions require fobs or phones. By authenticating silently, the user is only interrupted when suspicious behavior is detected, not when completing their daily work.

Continuous

Most MFA handles the "point in time" use case, where Plurilock can protect the entire session. Protect against insider threat and data getting into the wrong hands.

Secure

Passwords simply aren't sufficient to protect critical data,but users can rebel against MFA hassle. Plurilock secures with machine learning and micro-patterns, drawing on many factors -- not just something you have or know.



DEFEND
Continuous Authentication

- Endpoint
- Web Sessions

ADAPT
Login MFA

- Multi-factor authentication
- Multi-factor authentication Full-day, real-time protection for Citrix XenDesk

Unlike traditional device-based MFA solutions, Plurilock uses micro-patterns from many factors to create and compare a digital profile.

CUSTOMERS

- Enterprises
- MSP MSSP
- Citrix Providers
- High Security Organizations
- Resellers

INDUSTRIES

- Banking Finance
- Government/ Infrastructure
- Critical Infrastructure
- Health
- SaaS

Plurilock

Case Study

A top New York hedge fund turns to Plurilock when YubiKey falls short.

Quantitative Hedge Fund (QHF)* is a global top-10 algorithmic trading fund with over $50 billion in assets under management—and a universe of proprietary data and trading algorithms that are the closely-held secret to the success and market position that QHF enjoys.

If these core assets were ever to be stolen or compromised, it would mark the end of QHF's dominance, so QHF protects them jealously—while needing also to continuously maintain and optimize them. This careful protection, development, and moment-by-moment tuning of data and algorithms is the secret key to QHF's performance and competitive edge.

Highlights

- **A top-10 hedge fund needed strong MFA and non-repudiation logs to protect proprietary, industry-leading data and algorithms**
- **Existing YubiKeys couldn't provide proof of identity in non-repudiation logs, yet caused costly delays and frustration**
- **The fund deployed Plurilock's ADAPT technology as an MFA solution**
- **Plurilock enabled a 94% reduction in YubiKey events plus compliance-ready non-repudiation logs with confirmed identities**

YubiKeys do not guarantee anything about the identity of the individual holding them during an authentication event.

For these reasons, QHF is meticulous in requiring strong multi-factor authentication to access or update these assets. It also works to achieve the most robust possible set of "non-repudiation" logs—records that outline not just which account, but ideally which person inside the organization accessed which critical data or code assets—and when.

Conventional Best Practices Weren't Up To the Job

In an attempt to protect these assets and generate authoritative non-repudiation logs, QHF initially deployed YubiKey hardware authentication tokens—a popular, market-leading solution—and required their use whenever sensitive data access or update events were to occur.

Unfortunately, though QHF's YubiKey solution did provide some measure of added security, significant problems and risks remained.

While YubiKey-driven non-repudiation logs could show which YubiKey was responsible for a particular request, they didn't offer definitive proof that a particular person was responsible in each case. This is because by design, YubiKeys do not guarantee anything about the identity of the individual holding them during an authentication event. In fact, YubiKeys offer no protection against theft, illicit use in quick take-then-return actions, or other insider threats.

As a result, individuals whose YubiKeys were represented in non-repudiation logs could still claim ignorance and disclaim responsibility when critical data issues arose—simply by asserting that someone else must have temporarily been in possession of their YubiKey. This was not an acceptable compromise for QHF.

Plurilock

At the same time, key employees at QHF also found the YubiKey solution to be cumbersome and irritating. For example, access to critical data or changes to tune important algorithms required the approval of managers, who first had to authenticate with their own YubiKeys in order for approval to take place.

These managers often found themselves needing to approve a request at one location only to realize that their YubiKey was at another—on a different floor, for example, or in a different building altogether. This caused unacceptable delays in live operations in an industry in which microsecond-precise timing is everything, with negative consequences for competitiveness.

Still other managers took to leaving their YubiKeys permanently inserted at their desks to minimize misplacement issues, even though this was against policy, thereby creating a security risk that defeated the purpose for which YubiKeys had been deployed in the first place.

QHF Turns to Plurilock's Behavioral-Biometric Technology

What Quantitative Hedge Fund needed was a new authentication solution—a solution able to:

- **Definitively recognize and log the identities of actual people, not just hardware authenticators that anyone might find, steal, or carry**
- **Do this wherever these people happened to be working at a given moment, without delays caused by the need to find or retrieve small, easily-misplaced devices**

To meet these requirements, QHF turned to Plurilock and Plurilock's ADAPT technology, which provides invisible, person-centric authentication in the background—without requiring extra devices such as phones, USB fobs, or scanners.

Instead, Plurilock ADAPT uses behavioral biometrics and machine learning to recognize people by the tiny patterns and variations that emerge in the cadence of their everyday typing—characteristic patterns and variations that are as unique as fingerprints.

Plurilock's solution was particularly attractive to QHF because it was able to authoritatively confirm the identity of the person at the keyboard during sensitive data access events—rather than merely the presence of a particular YubiKey device.

And since Plurilock's solution didn't depend on extra hardware, it also promised fewer costly delays caused by things like YubiKey misplacements—or instances in which YubiKeys were inadvertently left behind, keeping their owners from performing urgent tasks at another location.

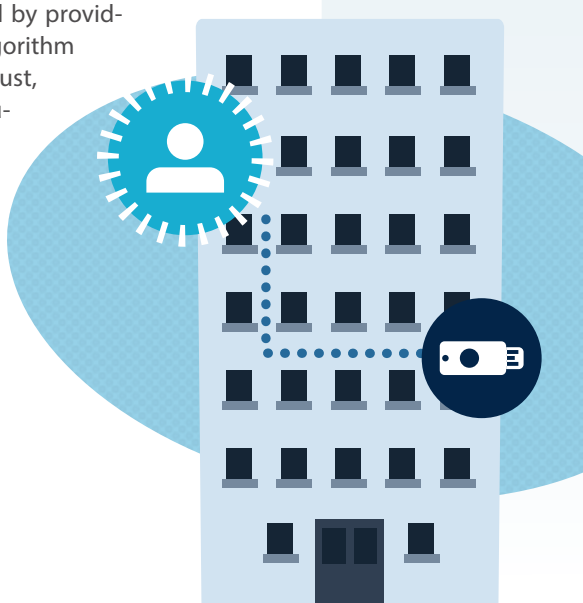
Plurilock's Solution Reduces YubiKey Events by 94 Percent

Plurilock configured QHF's authentication stack to rely on ADAPT first during authentication events, and to prompt for a YubiKey only when behavioral-biometric certainty fell below a context-appropriate threshold.

At Plurilock's recommended threshold, the number of YubiKey insertions on affected QHF teams was reduced by 94 percent. Key team members and managers were thrilled not to have to carefully manage and track YubiKey authenticators any longer—or risk imposing costly delays in data or algorithm updates at a multibillion-dollar algorithmic fund.

At the same time, risk and compliance stakeholders were relieved to finally have a solution in place that enabled true non-repudiation logs—**logs able to state with authority which individual was responsible for a sensitive data event, rather than merely which YubiKey was associated with it.**

Plurilock's solution is accomplishing what QHF's fleet of YubiKeys couldn't. ADAPT is enabling a global top-10 algorithmic fund to maintain its edge and position at the top of the market—all by providing delay-free data and algorithm security along with robust, person-centric non-repudiation logs for risk and compliance management. ■

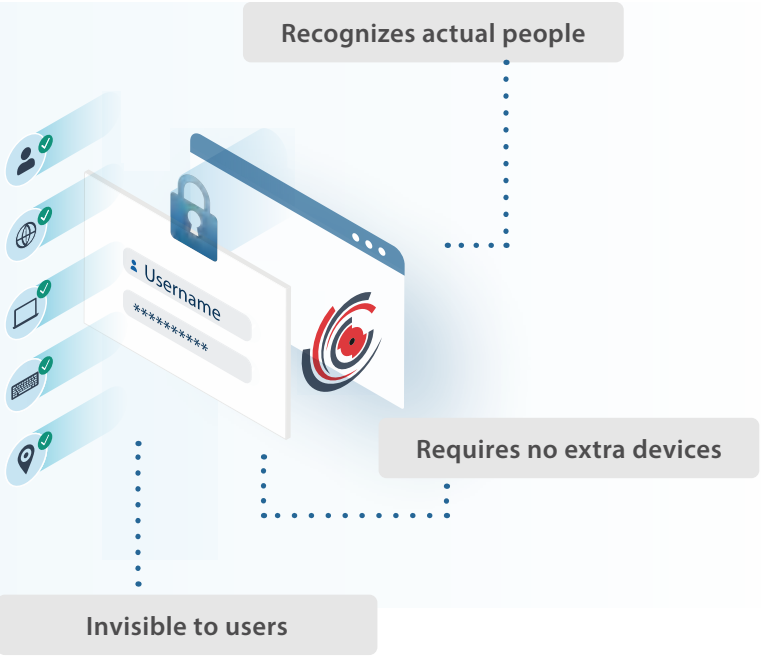


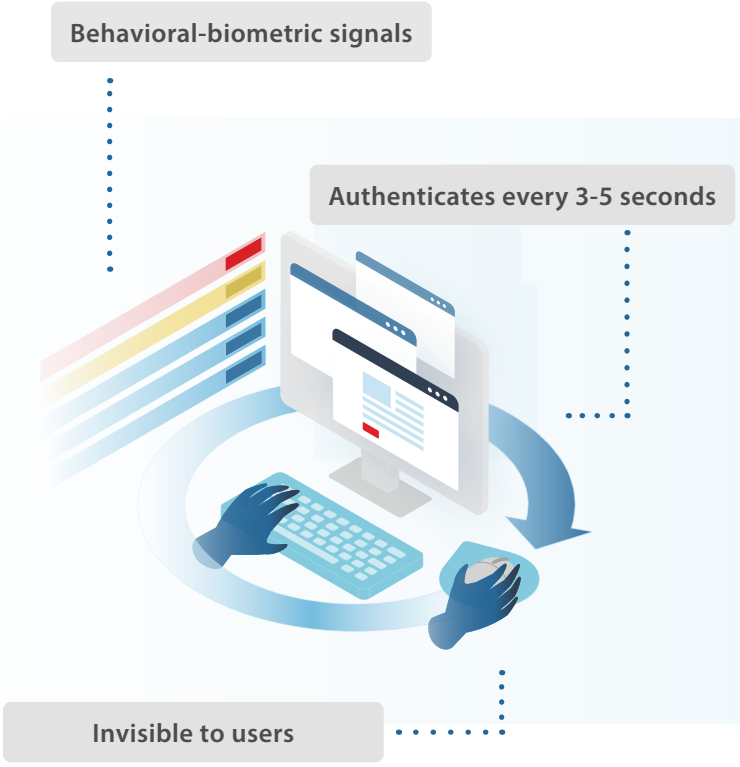
Products

Plurilock ADAPT

Invisible MFA

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





Plurilock DEFEND

Continuous Authentication

- ✓ Continuous, full-day authentication
- ✓ Enterprise endpoint and workstation protection with identity assurance

Plurilock

Plurilock ADAPT

Data Sheet

Use For

- Invisible, adaptive MFA for logins and workflows
- Cloud/JS applications
- ADFS environments
- Citrix sessions in ADFS environments

Includes

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

JavaScript Client Compatibility

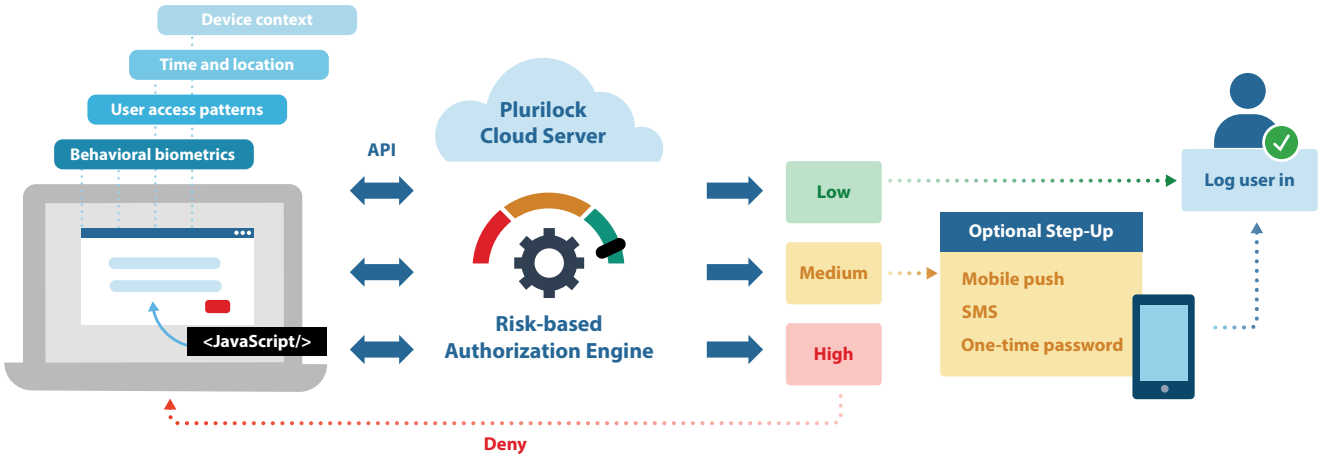
- Microsoft Edge
- Mozilla Firefox
- Apple Safari
- Google Chrome

Server Instance Specifications

- Amazon AWS
- CentOS 7

Plurilock API Reference Implementation

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



ADAPT provides invisible, adaptive, biometric MFA for your workflows and apps—no phones, fobs, or new hardware required.

Plurilock

Plurilock DEFEND

Data Sheet

Use For

- Continuous, real-time authentication
- Citrix ADFS environments
- Enterprise Windows endpoints
- Enterprise Mac OS endpoints
- Endpoint detection and response
- SIEM-ready event and identity data

Includes

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

** On-premises server also offered. Contact Plurilock for specifications and availability.*

Compatibility

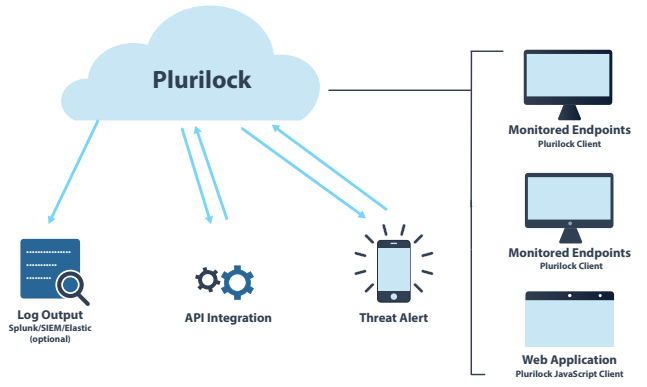
- Windows 7, 8, 10
- Windows Server 2008, 2012, 2016, 2019
- Mac OS Yosemite, El Capitan, Sierra, High Sierra, Mojave

Server Instance Specifications

- Amazon AWS
- CentOS 7

Footprint

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



DEFEND authenticates users invisibly and continuously, every 3-5 seconds, as they work—ensuring smooth access for the right users and no access for anyone else.

Plurilock

Let’s talk

www.plurilock.com | info@plurilock.com

Plurilock