

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 can't be forged. These are augmented with geolocation and location history, device fingerprinting, network context, and other ambient signals to provide strong authentication invisibly, in the background.

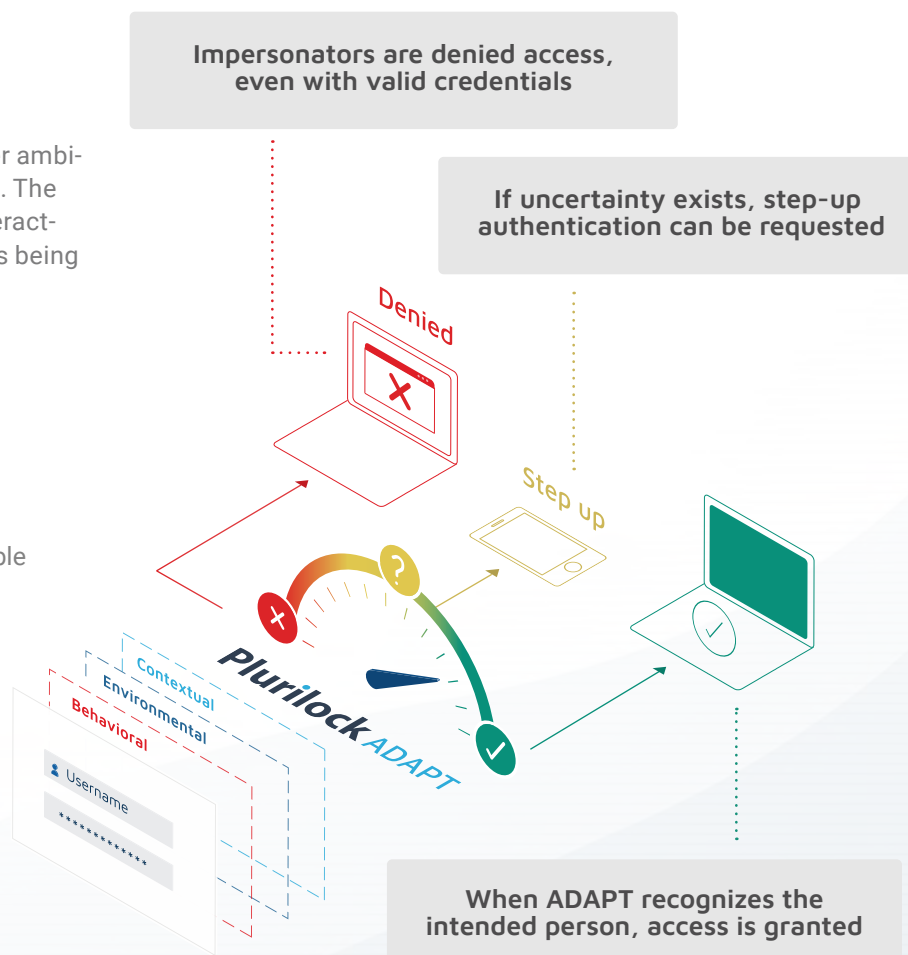
Every company would prefer to add multi-factor authentication without compromising productivity. Traditional solutions add steps, frustration, and support overhead, yet are user-agnostic—they know only that someone has provided the right password, device, or token, not whether that someone is the right 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

- SSO environments supporting SAML or OpenID
- Web applications and logins compatible with JavaScript and a RESTful API
- Citrix sessions authenticated and launched in ADFS environments

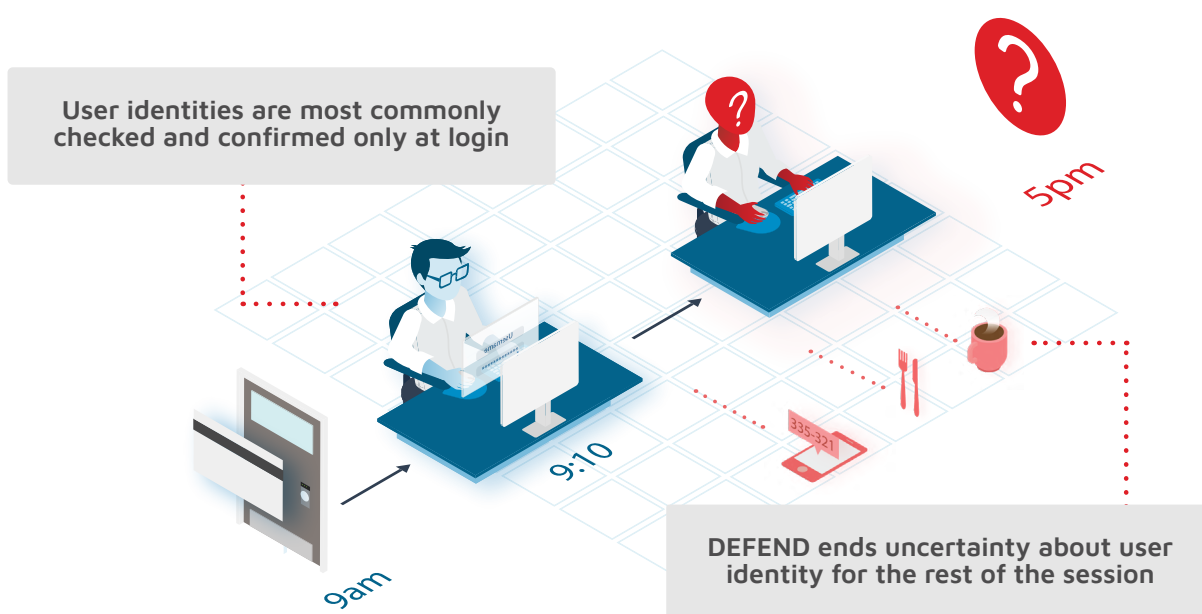


Continuous Authentication

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.

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.

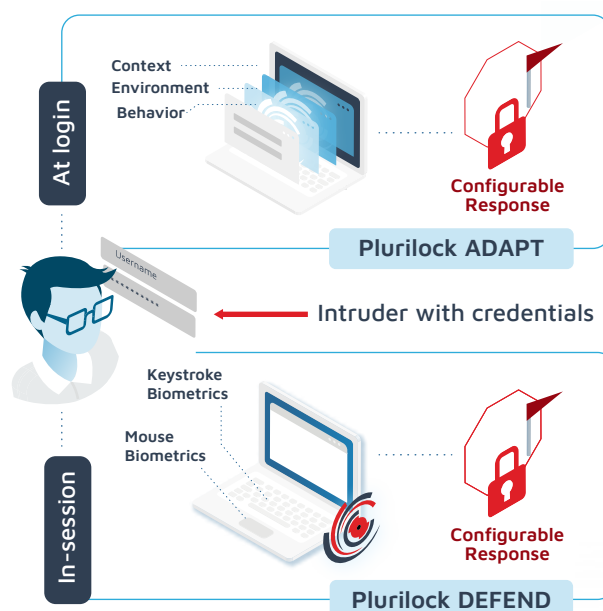


Figure 1

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 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: <ul style="list-style-type: none"> ✓ 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: <ul style="list-style-type: none"> ✓ Assess threats ● ✓ Adapt user profile data ● ✓ Confirm identity ever 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: <ul style="list-style-type: none"> ✓ Typing rhythm ■ ● ✓ Pointer interaction ● ✓ Geolocation ■ ✓ Computing context ■ Act in order to: <ul style="list-style-type: none"> ✓ 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: <ul style="list-style-type: none"> ✓ Anomalous keyboard behavior ■ ● ✓ Anomalous pointer behavior ● ✓ Anomalous device properties ■ ✓ Anomalous locational behavior ■ ✓ Anomalous network context ■ 	■ Plurilock ADAPT ● Plurilock DEFEND

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

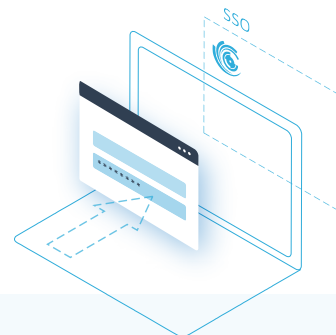
Passwords simply aren't sufficient to protect critical data, but users can rebel against MFA hassle. Plurilock secures with machine learning and micro-patterns, drawing on many factors—not just something you have or know.



Plurilock DEFEND

Continuous Authentication

- Endpoint
- Web Sessions



Plurilock ADAPT

Login MFA

- Risk-based login authentication
- Out-of-band multi-factor authentication

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

SOLUTIONS FOR



Enterprises



MSP / MSSP



Citrix*
Providers



High Security
Organizations



Resellers

INDUSTRIES



Banking
Finance



Government/
Military



Critical
Infrastructure



Health



Education



SaaS

Products



Plurilock ADAPT

Invisible MFA

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



Recognizes actual people

Requires no extra devices

Invisible to users

Behavioral-biometric signals

Authenticates every 3-5 seconds



Invisible to users



Plurilock DEFEND

Continuous Authentication

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

Use For

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

Includes

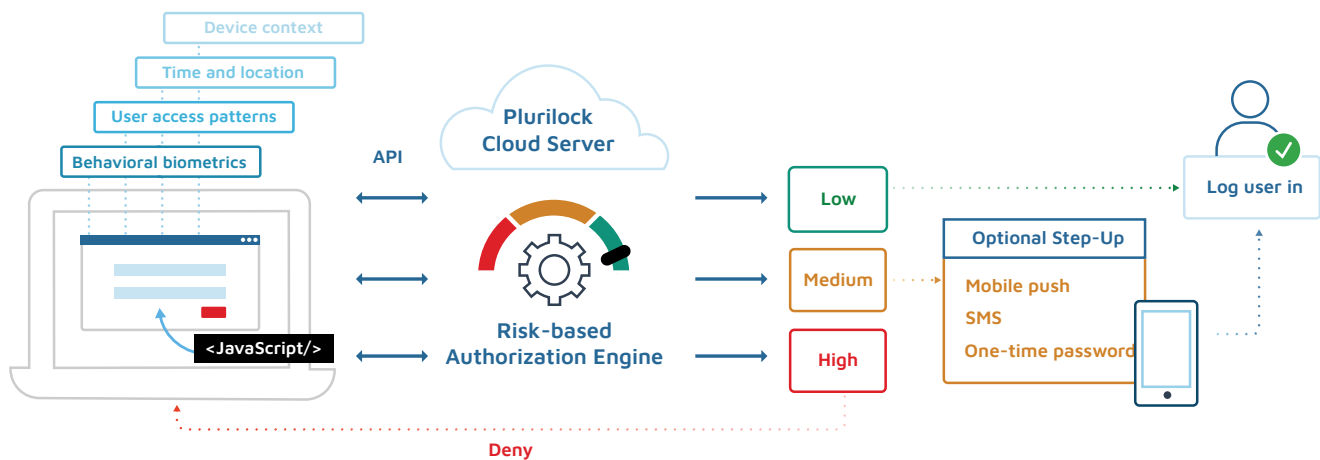
- Plurilock ADAPT JavaScript agent
- Plurilock ADAPT RESTful API access
- Plurilock cloud server instance

JavaScript Client Compatibility

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

Plurilock API Reference Implementation

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



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



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

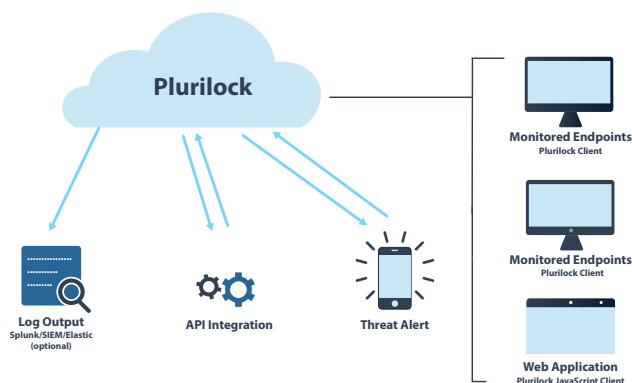
** On-premises server also offered. Contact Plurilock for specifications and availability.*

Compatibility

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


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.





Let's talk

1.888.776.9234 | www.plurilock.com | sales@plurilock.com

