Catching up to the New Normal with Zero Trust

Novel forms of secure and frictionless remote access

1.888.776.9234
sales@plurilock.com
www.plurilock.com

Plurilock

WHITEPAPER

Catching up to the New Normal with Zero Trust

Up until recently, remote access was almost unheard of among sensitive or high-security workforces.

Following the COVID-19 pandemic, remote work has become the new normal, and organizations are struggling to address the technical challenges this presents for network security.

Plurilock's cutting edge solutions establish a new framework that:

- Provides continuous authentication for end users in a way that reduces friction
- Scans for a person's unique identity signature throughout the workday, invisibly
- Runs with existing hardware, eliminating the need for costly new equipment

Introduction

Cyber attacks are increasing and organizations must respond

Cyberattacks are on the rise, with data breaches exposing 36 billion records in the first half of 2020 alone.[1] Government agencies and supply chains have been some of the hardest hit by these attacks, with the compromise of SolarWinds' Orion platform, the Colonial Pipeline and JBS Meats attacks, and a cyber attack that has targeted more than 150 government agencies, think tanks, and related organizations.[2] In today's environment, keeping networks, devices, and assets secure is more critical than ever.

Where we work has also seen a significant shift during the COVID-19 pandemic, as organizations navigate the new normal of employees working away from the office in remote and hybrid situations in more significant numbers.

As attackers become more sophisticated with their attacks, organizations must respond with cybersecurity solutions that protect critical systems in new and novel ways. This is an obvious need—but the need to sustain productivity by minimizing the burdens and interruptions faced by remote users due to existing authentication paradigms is just as critical.

The alarm has been sounded at the highest levels due to these recent attacks and the response is palpable. President Biden's administration has issued a groundbreaking executive order that lays the foundation for a new generation of cybersecurity best practices, including increased communication between the government and private sector and new standards for handling breaches.

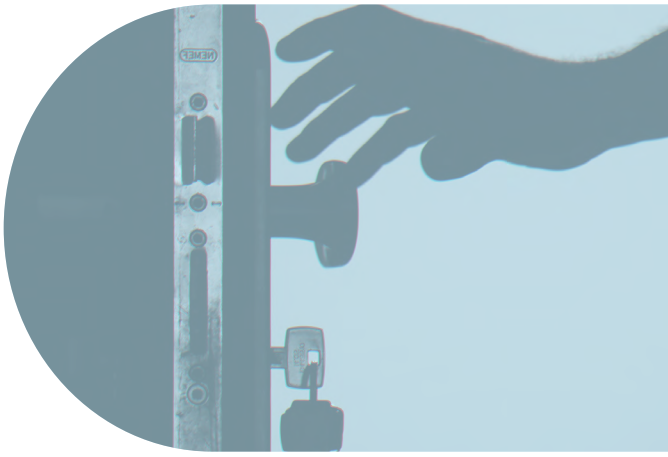
Also foundational to this executive order is the Administration's allocation of significant funding to support more effective and robust authentication solutions, finally ushering in the long-awaited era of the Zero Trust Architecture (ZTA).

How will organizations address this growing problem?

Assessing the existing framework

Current solutions fail to provide true identity detection and continuous authentication

When securing devices and systems, passwords have long been the default, lowest-common-denominator standard for establishing identity. Over time, attackers have become better at compromising credentials, with phishing and brute-force attacks now in widespread use. Password requirements have been strengthened and many organizations have added multi-factor authentication (MFA) to their login workflows, but while these credentials build a more substantial front door for attackers to break through, once they're through that door they have complete access to critical files and systems. MFA and 2FA also slow down and frustrate the workforce with additional friction.



1 https://purplesec.us/cyber-security-trends-2021/
2 https://www.cnn.com/2021/05/28/tech/microsoft-solarwinds-russia-hack-intl-hnk/index.html

1.888.776.9234
sales@plurilock.com
www.plurilock.com

Plurilock

WHITEPAPER

Catching up to the New Normal with Zero Trust

Recent breaches have demonstrated that no login workflow, no matter how robust, can guarantee that a new computing session is being used by the intended, authorized person—even when valid credentials are provided. This underscores the need to establish a ZTA environment, in which your system continuously assesses and authenticates users, based on their behavioral biometrics, *in real time,* as opposed to traditional biometrics like fingerprints and facial scanning that can be duplicated for malicious purposes.

With the government workforce still predominately working remotely, agencies face an additional challenge: to provide remote access to government systems and data securely. These systems hold critical data concerning citizens, sensitive material, and many forms of personally identifiable information. This data must be protected, yet must also be accessible to off-site users, to enable them to deliver critical services to their stakeholders, users, and staff.

But there's a challenge that organizations face when considering options for continuous authentication—how do they constantly challenge and authenticate users without causing so much **friction** that they use unauthorized workarounds, software, and applications?

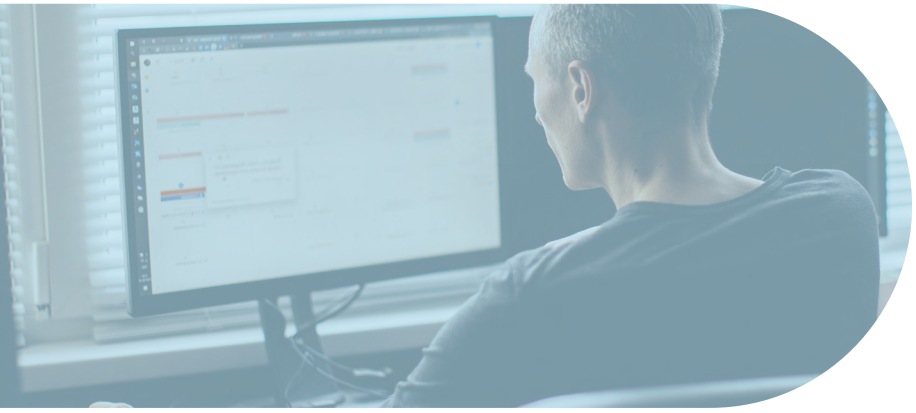
Systems currently used by government agencies for authentication impose so many strict internal controls and obstacles that users frequently opt for workarounds instead. In blunt terms, this means that communication about projects often happens on personal messaging platforms; sensitive or classified conversations often happen at coffee shops instead of through appropriate platforms.

Identifying a solution

Using cutting edge tools that address today and tomorrow's cybersecurity challenges

Current frameworks have seen incremental improvements in securing the "front door"—in securing login workflows—but with the ongoing cyberattacks and vulnerabilities throughout large-scale environments by which attackers can gain entry, there needs to be a significant shift in approach to protect assets moving forward.

Government agencies and organizations need to use proven, but cutting-edge technologies belonging to a new cybersecurity paradigm—one that provides users with remote access to data while authenticating a user continuously and without additional friction.



Considerations when assessing an existing framework for authentication and secure access:

Legacy systems cannot support modern authentication methods

For organizations running legacy systems, using many of the modern authentication methods is not possible as they're often not supported. These systems have largely relied on more antiquated MFA methods, leaving organizations vulnerable.

Challenges with user adoption, impact on users

Organizations must balance security needs with the roadblocks that cybersecurity tools impose that negatively impact employee productivity. For example, current identity authentication frameworks require users to complete additional steps—passcodes, email confirmations, mobile authenticators. These create significant friction for the end user, often multiple times a day!

Does not account for ongoing authentication

Current frameworks authenticate a person's identity and credentials only during the initial login. This strategy attempts to provide the system with verification that the correct user is accessing systems during the initial interaction, but it leaves systems vulnerable throughout the day if another individual has access to the device or hijacks the session.

Cannot truly confirm an individual's identity

Passwords, fingerprints, facial scanning, and multiple layers of authentication are methods to prevent unwanted access, but they ultimately cannot truly confirm a person's identity. Passwords are now considered to be insecure; fingerprint and face scans have been compromised using relatively low-tech methods, and OTP systems are vulnerable to social engineering, peer-over-partition, and other kinds of attacks.

1.888.776.9234
sales@plurilock.com
www.plurilock.com

Plurilock

Catching up to the New Normal with Zero Trust

How can this be done?

The future of authentication

As an identity-centric cybersecurity solutions provider with behavioral biometrics and machine learning in its DNA, Plurilock is the answer to this question. We provide enhanced login security and continuous authentication, all while minimizing user friction.

Plurilock's proprietary technology is fundamentally different from other authentication solutions. Our solutions give you true identity detection, enabling organizations to let people in or keep people out—not just credentials or scans of body parts. Plurilock's software is with the user invisibly, every step of the way–starting with initial logon and then continuously throughout the day, even detecting the moment when the authorized user walks away from their device and unauthorized user steps in.

Plurilock does this by using behavioral biometrics to observe micro-patterns in user keystroke and pointer behavior, along with other identifying factors, all analyzed using machine learning techniques that generate a unique and evolving identity signature for each user.

As a characteristic set of movement patterns over time, this behavioral biometric identity profile is virtually impossible to recreate or reply. Plurilock observes, evaluates, learns, and makes an identity decision every 3-5 seconds, all day long, to spot unauthorized users in real-time. This decision data can be digested by security information and event management (SIEM) systems to create a continuous human risk score, enabling a true ZTA environment. This enables accelerated incident management should an attacker appear in—much less attempt to move laterally within—a network.

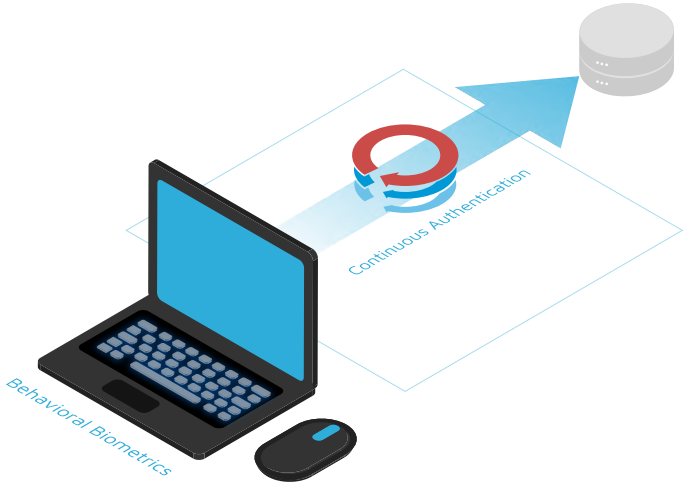
Plurilock enables organizations to protect their environments from credential compromise and attacks using continuous identity authentication while eliminating the obstacles and friction that make it difficult for end-users to complete their missions.

Our solutions are compatible with existing hardware, including standard keyboards and pointing devices, offering agencies a high level of security without additional equipment purchase expenditures.

Our technology solutions offer a compensating control to accommodate today's changes in physical security and enable business continuity, ensuring that users can continue to provide services regardless of location or situation.

Access additional Plurilock resources:

- https://www.plurilock.com/what-is-behavioral-biometrics/
- https://www.plurilock.com/glossary-of-terms/
- https://www.plurilock.com/frequently-asked-questions/



Every organization needs security especially now with expanding remote access needs.

Get ahead of the mandates in President Biden's executive order that require a ZTA security model.

Plurilock is ready to serve your organization's continuous authentication and identity assurance needs. Contact us today for a demo of Plurilock's cutting-edge technology solutions and see how your organization can leverage Plurilock to protect sensitive data and support your critical mission.

1.888.776.9234 • sales@plurilock.com • www.plurilock.com

1.888.776.9234
sales@plurilock.com
www.plurilock.com

Plurilock