Plurilock DEFEND™

Identity Assurance for Amazon WorkSpaces

Continuous zero trust identity confirmation in an Amazon WorkSpaces virtual environment

With remote workforces and BYOD environments increasingly becoming the norm, zero trust identity solutions are more critical than ever. Amazon WorkSpaces' virtualization helps organizations to deploy, scale, and manage infrastructure and workforces faster than traditional desktop environments can.

But this virtualization carries risks. More than ever, workforces connect to work remotely, leaving Amazon WorkSpaces environments vulnerable to a variety of identity-driven attacks and MFA bypass exploits. With cybercrime on the rise, organizations need a new level of identity security designed for virtual desktops.

Security Threats in Amazon WorkSpaces environments

Continuous identity assurance

Organizations can no longer rely on physical security to augment their cybersecurity infrastructure. In a virtual environment, devices are vulnerable to stolen credentials, session theft and takeovers, and step-ins and snatch and grabs.

Imposter interviewers

In a standard VDI session, organizations can't be sure that the person that interviewed for a role is the one that is completing the work from day to day, posing a significant security risk or potential for a data breach.

Hourly employees faking activity

In a virtual environment, organizations can't be sure if the activity on an employee's device is legitimate or through the use of "mouse jigglers" and other devices that mimic activity to extend their workday.

Compliance challenges

For industries with compliance requirements that can lead to costly fines or interruption to business operations, having assurance that the authorized employee is the user in a virtual session is critical.

View our 5-minute demo

How Plurilock DEFEND works

1. The DEFEND agent gathers input metadata (key stroke timing, pointer movements, and other similar data) every 3 to 5 seconds in real time, invisibly as users work in an Amazon WorkSpaces virtual session.

2. The DEFEND cloud server continuously analyzes this input metadata using Plurilock's patented AI and machine learning techniques to create a unique digital signature that recognizes and confirms identity based on the user's typical keyboard and pointer movement speed and cadence, and to spot kinetic anomalies.

3. When patterns in the input metadata don't match the user's typical keyboard or pointer movement, DEFEND recognizes the presence of an unauthorized user—even if credentials and session identifiers are valid—and terminates access to the virtual session.

Safeguard Amazon WorkSpaces with cutting-edge passive biometrics

Plurilock DEFEND uses behavioral biometrics to invisibly prevent credential compromise and identity-driven attacks in Amazon WorkSpaces environments. DEFEND provides a robust and more resilient protection than credentials or SSO tokens alone, without adding end user friction.

1.888.776.9234
sales@plurilock.com
www.plurilock.com

Plurilock