Plurilock

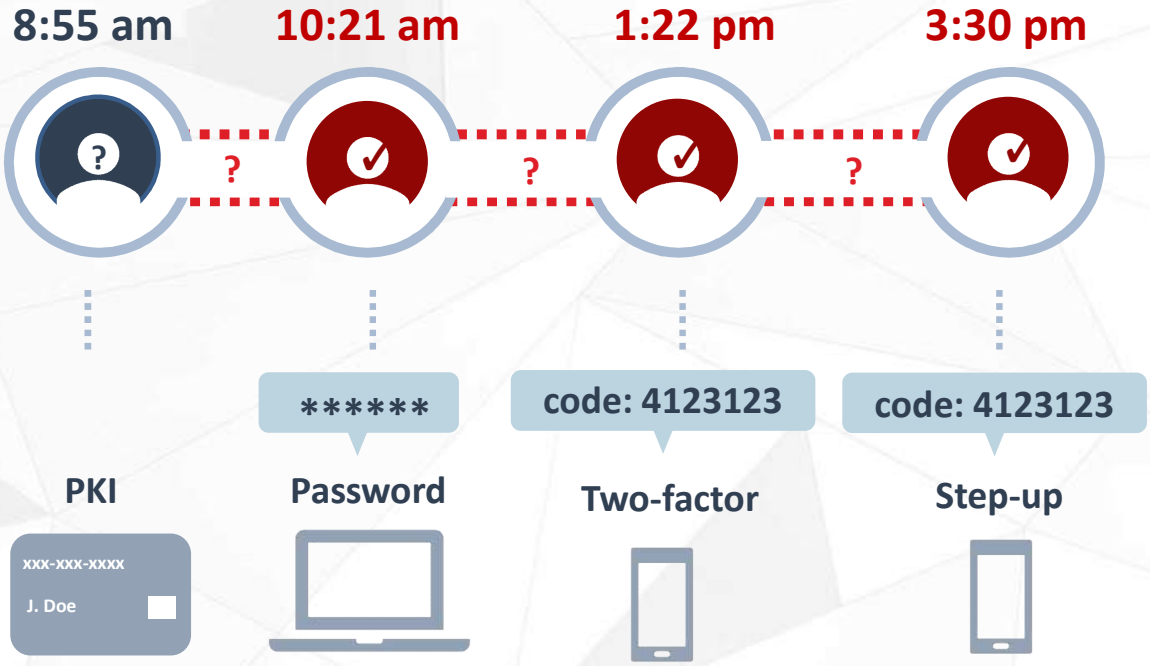
Using keystrokes and mouse behavior to protect your workstation

Ehab Samy

Vice President, Product Management

Plurilock

Authentication during the workday



"4 / 5 data breaches used weak or stolen passwords "
Verizon Data Breaches Investigation report 2017

99% of Work Day Unprotected

- **4 – 6 identity checks** throughout the day
- **Work interruptions** and **frustration**
- Users are assumed to be the right person with little verification

Plurilock

How Plurilock works

User interacts with their workstation as normal

Requires no additional hardware

Automatic enrollment in a little as 15 minutes

A lightweight Plurilock Endpoint Agent collects keystroke and mouse data, combines with user information and unique contextual identifiers, and creates an encrypted package

Package sent to server every 3-5 seconds

Plurilock server examines package and compares to the user's biometric profile

If the biometric patterns match, user is validated

When suspicious behavior is detected, policy-specific workflows can autonomously challenge the user, log the event, or notify security team in real time.

Plurilock

Use Case: Reducing Authentication Friction

FRUSTRATING **POLICIES**

Replace/reduce policies with continuous authentication compensating control

******

Password Rotation | Password Complexity | Inactivity Timeouts

---

Eliminate step-up workflows using Plurilock 'FastPass' - invisibly check identity score with BioTracker APIs

ANNOYING **TWO FACTOR (2FA)**

Plurilock

Use Case: Identity Assurance of Privileged Users

Privileged users

- Bank employees
- Power plant operators
- DOD network administrators

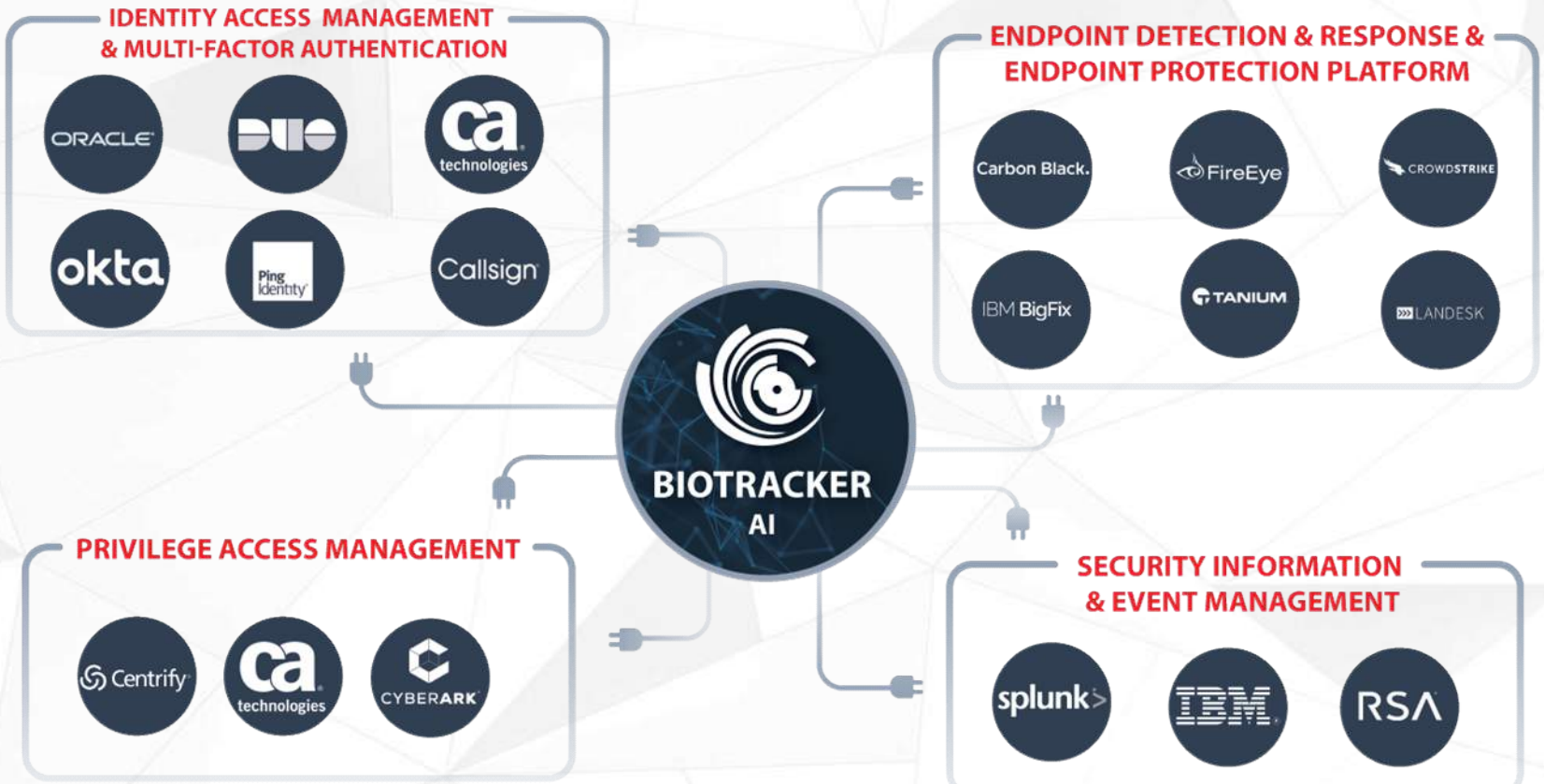
Offshore / remote access considerations

- Citrix/Dell/VDI

Add continuous layer of protection for privileged users in the form of behavioral biometrics

Plurilock

Works With Other Technologies



Plurilock

Common vulnerabilities. **Uncommon protection.**

Stolen credentials
Every active user is known—and their actual identity is assured.

Password sharing
Only intended users have access, password or no.

User substitution
Outsourced work is done by the users you know—no one else.

Insider threats
Inadvertent or malicious privilege elevations don't give access.

Invasive trojans
Activity by unknown users or agents is detected and blocked.

USB and scripting attacks
Automated attacks are quickly and easily spotted and stopped.

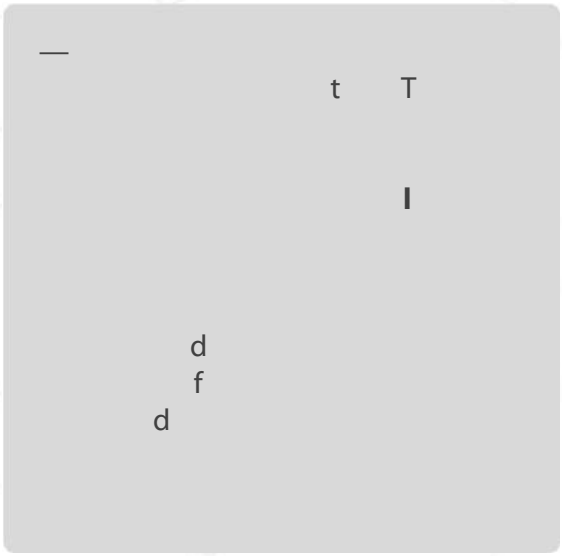
Phishing attacks
Distant phishers are unable to use accounts, even if compromised.

Unclear attribution
Bad behavior can be definitively traced to those that engaged in it.

User carelessness
Forgetful step-aways with no logout are no longer a risk.

License violations
Illicit sharing no longer leads to licensure liability and cost.

External identity fraud
End-users and customers can be profiled and authenticated, too.



Plurilock

Ehab Samy
ehab.samy@plurilock.com

www.plurilock.com

Plurilock