Technology Currents...

December 14, 2020

J.Gold Associates, LLC. 6 Valentine Road, Northborough, MA 01532 USA
www.jgoldassociates.com +1-508-393-5294
Research, Analysis, Strategy, Insight

Device Security Needs to Get Personal

A Publication of
J.Gold Associates

The traditional and still prevalent user/password credential to log in to most organizations' devices and data processing systems is both insecure and subject to exploitation. Indeed, the number one mechanism used to breach corporate and personal systems is a stolen or otherwise compromised user name and password credentials. Biometrics, such as fingerprint readers, is a step forward, but in many cases unreliable, and if not done correctly, subject to hacking of the central database of biometric signatures. Current schemas are also specific to single devices if they use biometrics or similar logins, so multi-device users have an increased exposure level.

What's needed is a uniquely user-centric schema that can determine that it's a specific user no matter what devices, and without the need to store confidential information about the user that can easily be discovered and/or corrupted. AI driven continuous identity management creates an opportunity to take device security to the next level. It not only helps with logins, but can be extended to understand the policies each user is entitled to, such as network access, file manipulation, app availability, etc., and can be a strong addition to an organization's compliance policy

> *"…the notion of an AI-based continuous authorization program like Persona being able to understand that it's a specific user from usage patterns is a much more secure method of creating logins, access rules, and compliance monitoring than the current user name and password, and is far superior in mitigating stolen credential threats than current systems......"*

Continuous authorization and behavior analysis

Stolen credentials, the number one security breach mechanism in organizations, is also the hardest to stop with traditional security systems like anti-malware or even cloud based login brokers and Single Sign On (SSO) systems, since systems assume once a user is verified, all is normal and available to the user. To move to the next level of security, what's needed is not a onetime up front access determination as with login password and user name, but rather a way of determining that the user is actually who they claim to be, and to do so on a continuous basis while that user is logged in and accessing apps and data. This can only be accomplished by monitoring the actual operations of the user, and assessing, by the user's behavior, the likelihood that it really is the specified user. The process should create a "score" that can be assessed and if it falls below a certain value, used to initiate specific operations like data limitation, app exclusion or even fully denying access. It should not be a onetime activity at the start of the session, but rather must be the result of continuously monitoring and acting on that basis throughout the duration of user access.

What can it prevent?

The ultimate goal of any security system is to prevent data breaches and malicious behaviors. A knowledge-based continuous monitoring and authorization system can be effective at mitigating:

- *Stolen credentials*- Unusual access to data, running of unusual apps, and/or suspicious network connectivity could indicate that the credentials have been stolen, and will initiative a shutdown or severe restrictions on the account
- *Insider malicious behavior* – If user behavior changes to include access to unusual data or anomalous use of applications during a connected session, the system will score that as a threat and shut down access until the potential threat can be verified.
- *Physical device compromise* – if a malicious actor gains access to a device that is already logged in, the system will recognize the ambiguity between the credential of that user and the operations being performed by the operator, and rescind the access.

One such AI-based continuous authorization product currently available is BlackBerry Persona. Instead of identifying a person by a user name and password, its AI based system monitors and "learns" the specifics of the user's digital life, by learning how s/he types, what sites may be accessed, how any data is used, etc., and builds a "quality rating" to assess whether or not it's really that person using the device. This "score" can then be used by system admins to set score-specific policies and limitations, and/or used to verify compliance – something highly valuable particularly in regulated industries. Even if a user were to acquire stolen credentials, but not meet the specific characteristics of the credentialed user, the machine would know that it wasn't the real user and initiate, based on the preset policies, actions such as restrictions, logouts and/or reporting for further investigations. In conjunction with a Unified Endpoint Management (UEM) component, this can automatically limit or eliminate access, as well as force management changes to the end user device, based on the most expeditious methodology for remediation of the threat. This is a major step towards a full blown Unified Endpoint Security (UES) solution that is far more secure than traditional credentials approaches.

The downside is that it does take some time for the AI program to learn about each user. It learns by monitoring the "user" activities for perhaps 2 weeks or so, in order to build out a knowledge base. And this is not 100% transferrable as a user shifts to a new device, since the characteristics of "user" might be changed if s/he gets a new machine, adds a new keyboard or external peripherals, etc. That would require retraining of the AI program to gain new knowledge about "user". Persona is currently available for mobile devices for BlackBerry UEM customers, while Persona for desktops doesn't require the use of BlackBerry UEM.

Bottom Line: Even with its current limits, the notion of an AI-based continuous authorization program like Persona being able to understand that it's a specific user from usage patterns is a much more secure method of creating logins, access rules, and compliance monitoring than the current user name and password, and is far superior in mitigating stolen credential threats than current systems. We expect that within the next 2-3 years, such AI powered knowledge based security and compliance capability will be a defacto component of highly secure and compliant access management infrastructure, starting with enterprise uses but eventually moving on to consumer devices as well.

"…We expect that within the next 2-3 years, such AI powered knowledge based security and compliance capability will be a defacto component of highly secure and compliant access management infrastructure, starting with enterprise uses but eventually moving on to consumer devices as well…."

J.Gold Associates

J.Gold Associates, LLC.
6 Valentine Road
Northborough, MA 01532 USA

Phone:
+1-508-393-5294

Web:
www.jgoldassociates.com

Research, Analysis, Strategy, Insight