USE CASE - REMOTE WORKFORCE CONTINUOUS AUTHENTICATION

ZIGHRA
Smart Identity Defense

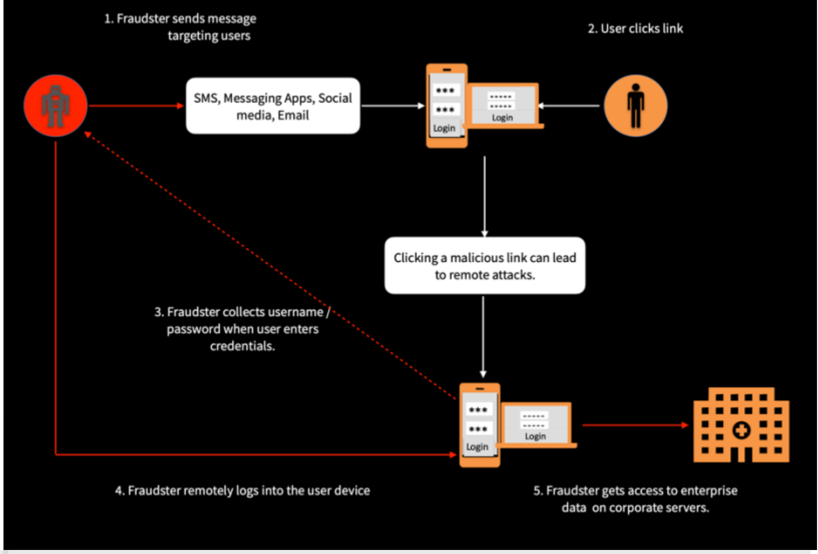
Since March 2020, cyber threats and attacks have increased by 71%. Recent breaches have armed attackers with stolen credentials enabling successful remote attacks, credential stuffing and password spraying. As their places of work transform into distributed organizations overnight. Security teams urgently need to look at new solutions that help continuously protect users and customers against increased cyber threats and online scams.

CONTINUOUSLY AUTHENTICATE YOUR WORKFORCE

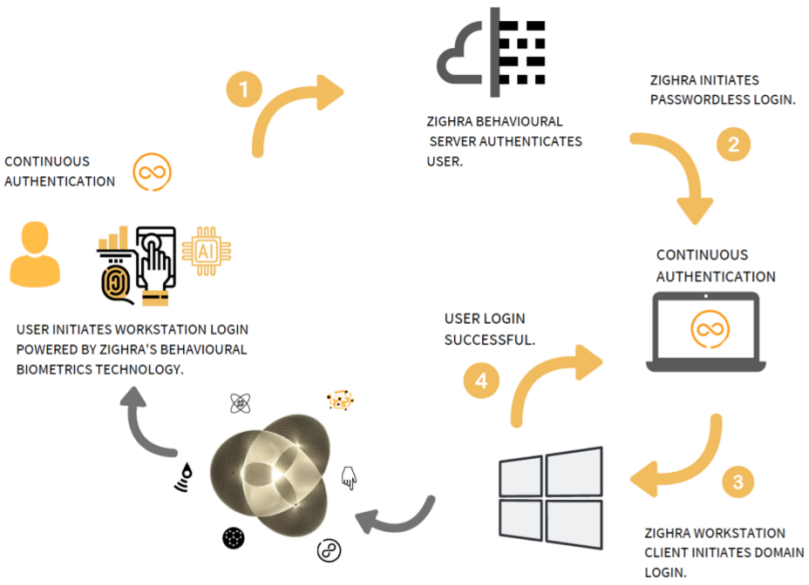
Zighra's patented technology delivers real-time behavioral intelligence and powerful security controls to continuously ascertain the identity of the user, without the slightest disruption to user experience.

With Zighra, you know exactly when you are interacting with your user and when you are not, down to the very second and help secure the organization and users against remote attacks, phishing attacks, and other credential threat vectors. Businesses can eliminate credentials-based vulnerabilities and keep users secure and productive, wherever they work.

REMOTE ATTACKS ARE ON THE RISE


1. Fraudster sends message targeting users
2. User clicks link
SMS, Messaging Apps, Social media, Email
Login
Login
Clicking a malicious link can lead to remote attacks.
3. Fraudster collects username / password when user enters credentials.
Login
Login
4. Fraudster remotely logs into the user device
5. Fraudster gets access to enterprise data on corporate servers.

CONTINUOUS PASSWORDLESS AUTHENTICATION


1
ZIGHRA BEHAVIOURAL SERVER AUTHENTICATES USER.
ZIGHRA INITIATES PASSWORDLESS LOGIN.
2
CONTINUOUS AUTHENTICATION
CONTINUOUS AUTHENTICATION
USER INITIATES WORKSTATION LOGIN POWERED BY ZIGHRA'S BEHAVIOURAL BIOMETRICS TECHNOLOGY.
AI
USER LOGIN SUCCESSFUL.
4
3
ZIGHRA WORKSTATION CLIENT INITIATES DOMAIN LOGIN.

KEY BENEFITS

- Continuously protect your organization against remote attacks, credential stuffing and credential reuse.
- Enable a password-less experience and let your users' login into their workstation securely.
- Reduce millions in IT costs by eliminating password resets and other login issues.
- Fine grained behavioral controls allow request-based actions including blocking or accepting requests.
- Flexible deployment for on-premise, cloud or on-device. Support for iOS, Android, Windows AND Mac OS.
- Offline mode ensures you can login from anywhere.

BEHAVIORAL INDICATORS

Behavioral Biometrics | Device /Sensor DNA | User Activity Signatures | App Interactions | Advanced telemetry | Step-up Authentication

✉ info@zighra.com

☎ +1 613-663-9090

www.zighra.com