ZIGHRA

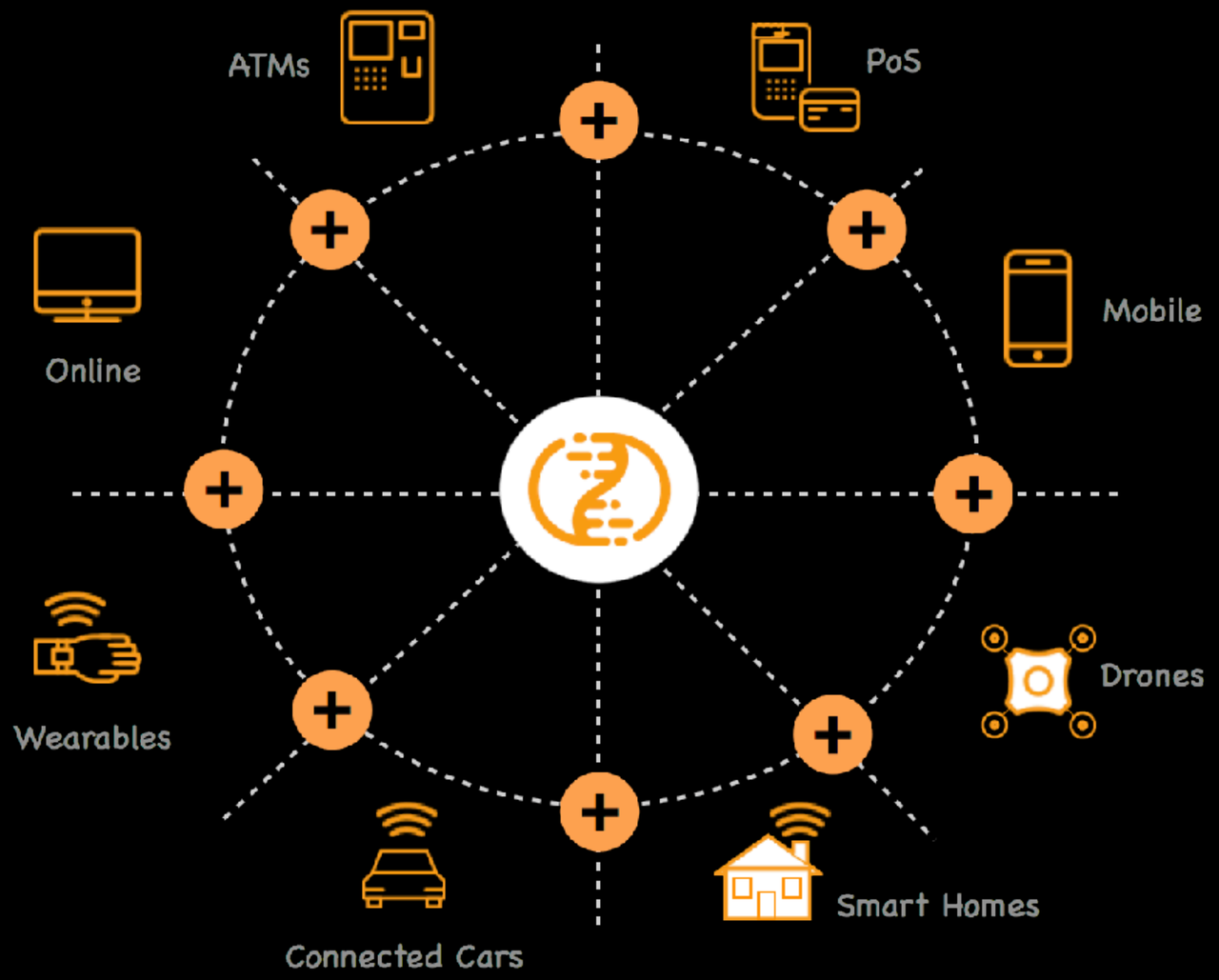
Smart Identity Defense

INFO DECK

AI-powered Continuous Authentication

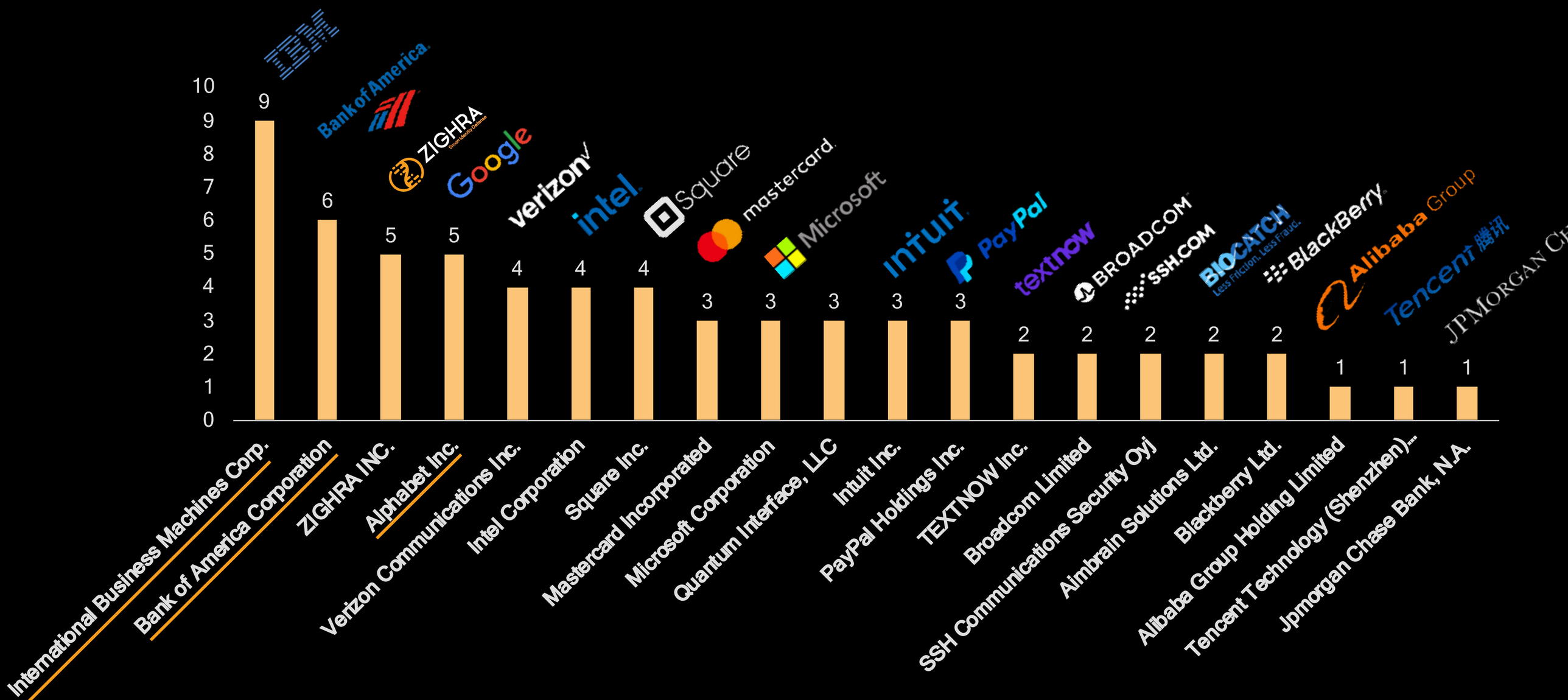
Continuous Authentication for a Connected World

Zighra offers a decentralized, AI-powered authentication and behavioural awareness platform. Providing a suite of intelligent analytics to create highly personalized models to authenticate the user in a transaction based on their natural interaction patterns. Zighra's solution is accessible across connected devices.



100+ Forward Citations

The following section highlights company's representative assets that cite Zighra patents:



Continuous Authentication

Problem

Current authentication systems are **Centralized** and **1-Dimensional** resulting in serious cybersecurity breaches:

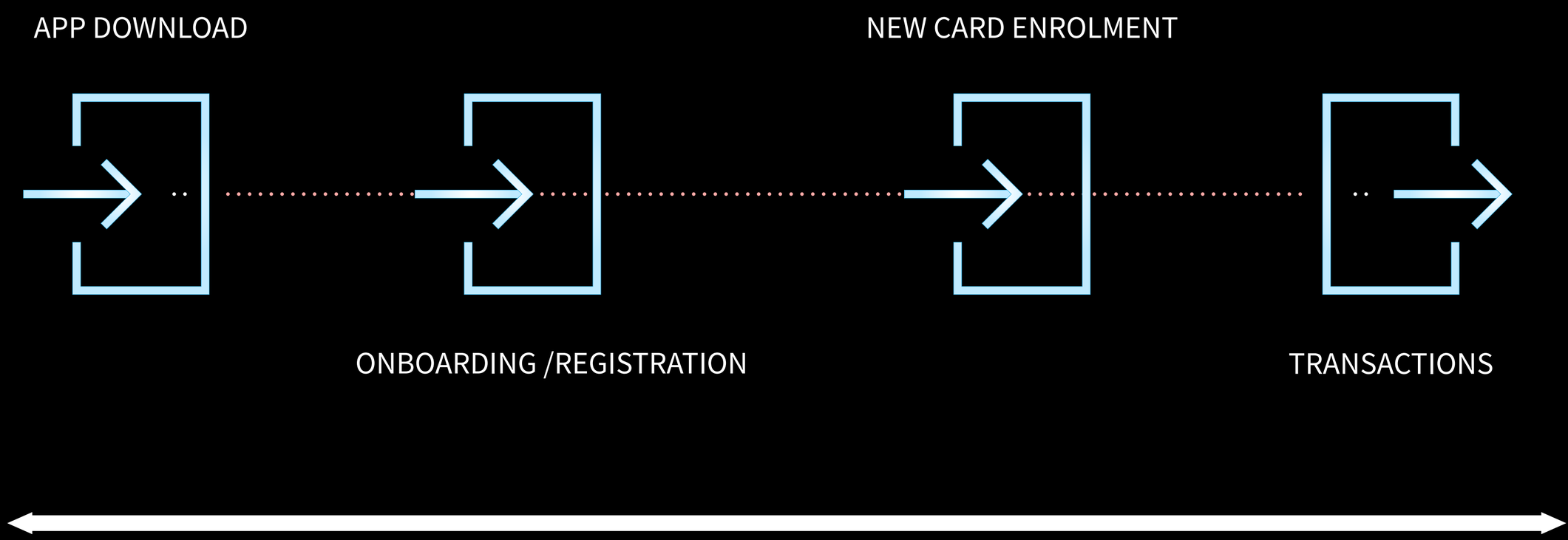
Cyberattacks happen every **39** seconds.

347% increase in account-takeover fraud.

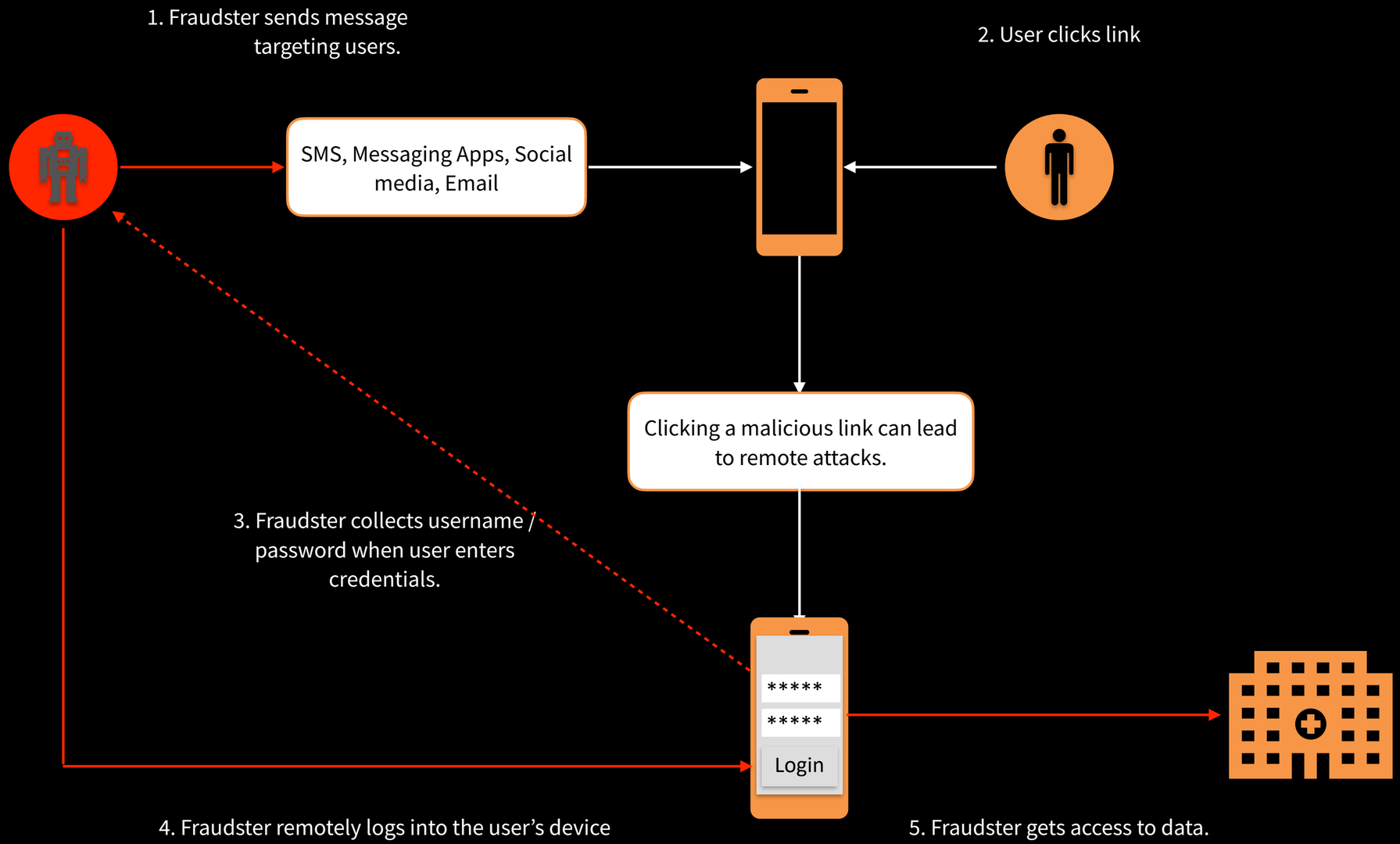
60% of digital fraud now originating from mobile channels.

93% of total mobile transaction in 20 countries were blocked as fraudulent.

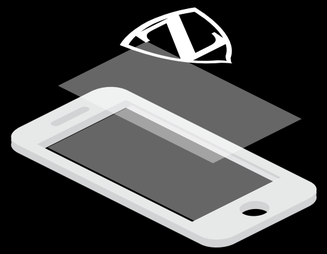
Fraud identified at every stage of the user journey



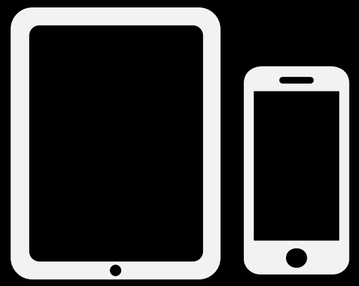
Use Case - ATO (Account Take Over), Remote Attacks



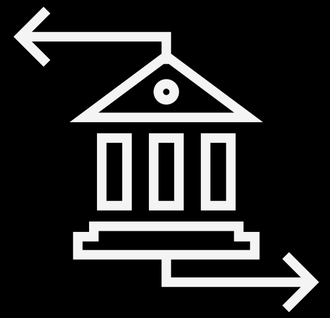
Technology



Zighra SDK



Apps

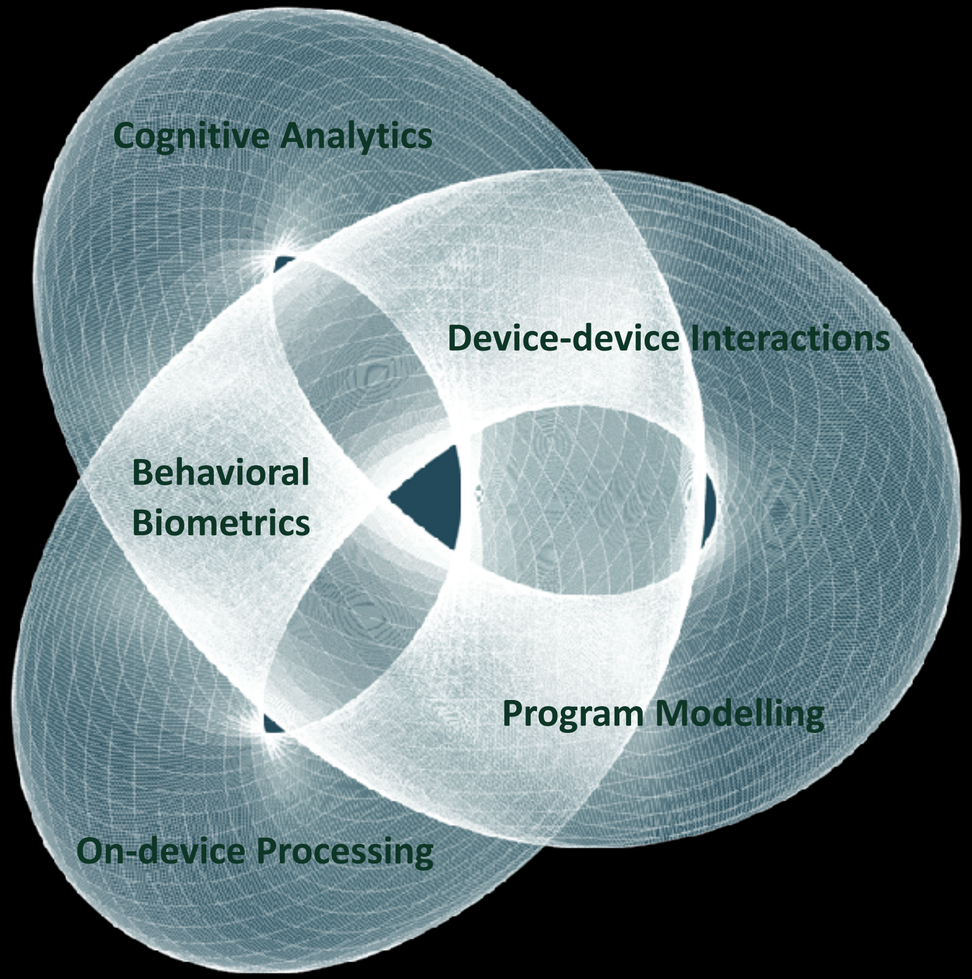


User Interactions

AI-Powered Assured Identity

* 10 Granted US Patents

Priority 2012



Verifiers - A behavioural authentication algorithm that provides CMFA with evidence of user identity.

Context - Trusted factors from the local environment whose presence can extend the lifetime of evidence received from a verifier.

Trust Levels - The level of confidence that is provided by the verifiers as well as the context currently seen by the system.

One platform multiple use cases

Workforce Authentication - Enterprise

Enterprise Workforce Authentication

As enterprises move more towards remote work, the attack surface gets larger while phishing attacks, credential reuse, and password reset costs get higher.

81% of all data breaches involve exploitation of compromised credentials.

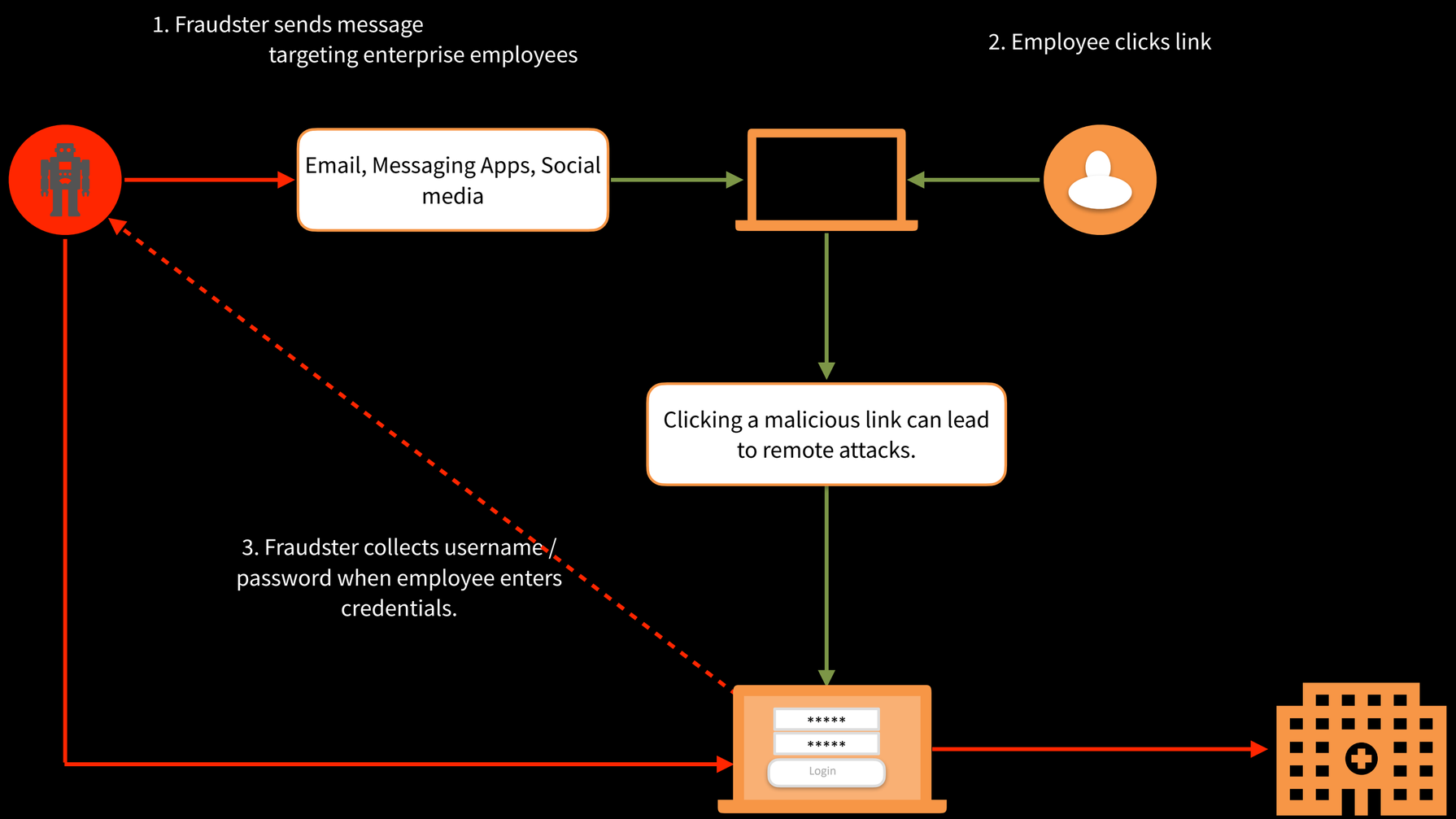
Shared secrets are the #1 cause of enterprise breaches, fraud and phishing attacks.

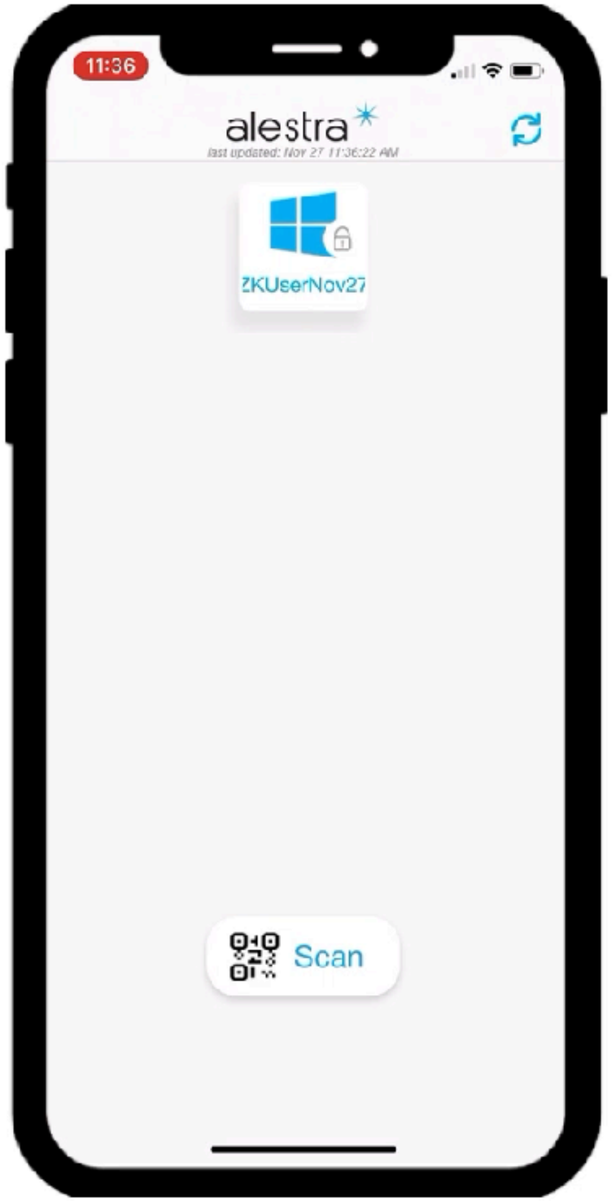
20% of support costs for enterprise IT related to forgotten passwords.

30%-50% of all Help Desk tickets are now related to password resets and account lockouts

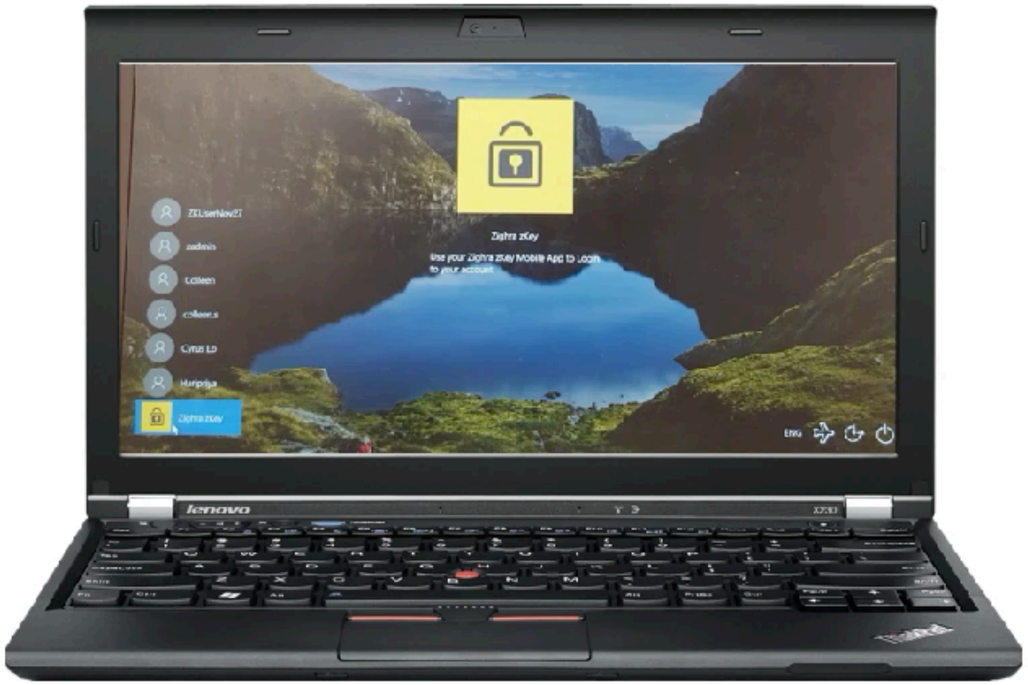
Use Case - Workstations and Applications

700% growth of RDP attacks over the last 12 months.

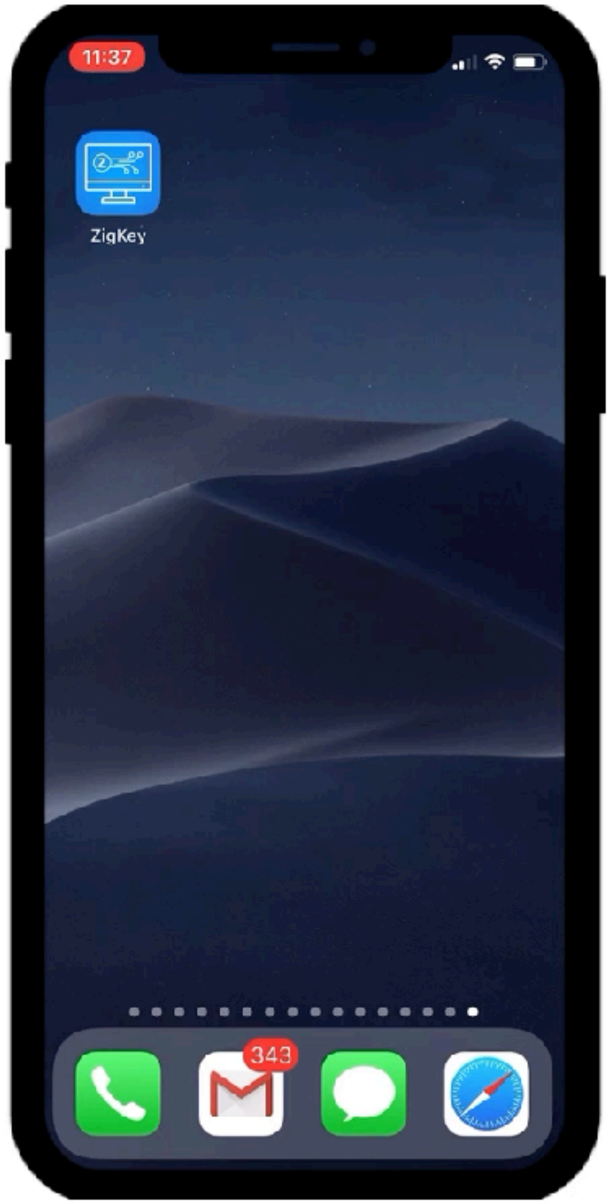




World’s first **FIDO certified** Behavioral Authentication



Demo of desktop/laptop Access



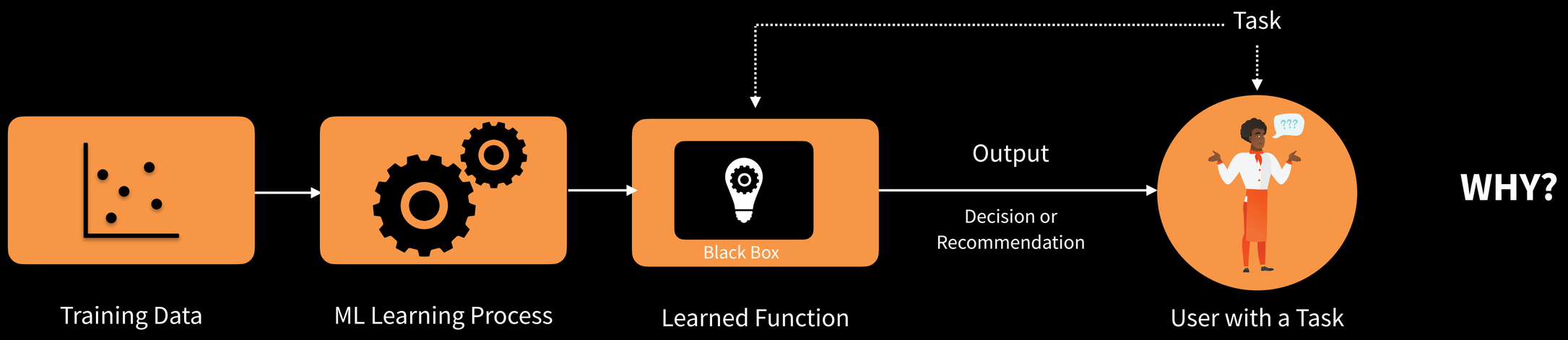
Continuous Multi Factor Authentication **(CMFA)**

Demo of Behavioural Anomaly Detection and Remote Lock

DeepSense - Explainable AI at the Tactical Edge

Traditional AI/ML

Only 18% organizations extensively adopt AI in their offerings. This gap indicates a very real usability problem when it comes to AI — primarily because of trust issues that lie at the core.



The effectiveness of current systems is limited by the machine’s inability to explain its thoughts and actions to human users.

Why Explainable AI/ML in Cybersecurity

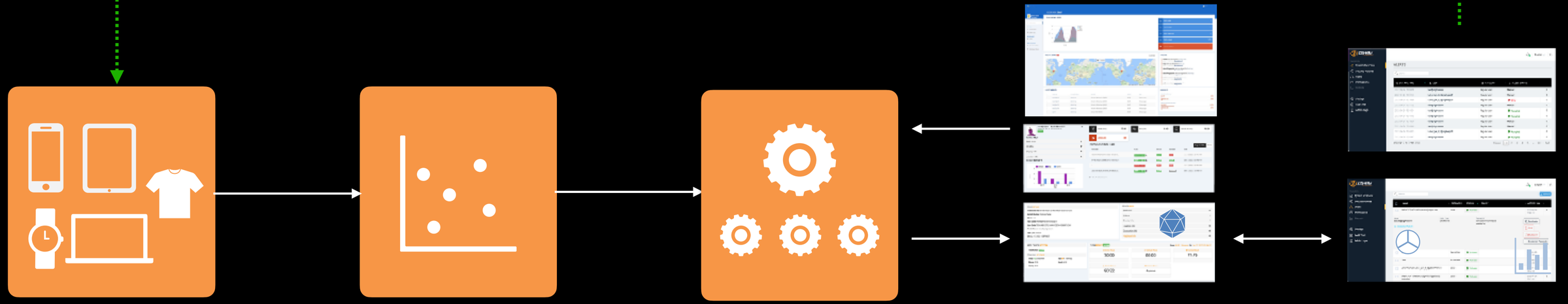
- Operators must come to trust the outputs of AI systems.
- Commanders/leaders must come to trust the legal, ethical and moral foundations of AI.
- Citizens must come to trust the values their Government has integrated into every application.

Zighra Technology Platform

Shutdown Endpoint(s)

Remediation Action: lock

Policies: strict, acceptable, lenient



Sensor Data Collectors

Sensor Data Processing

ML Learning Process

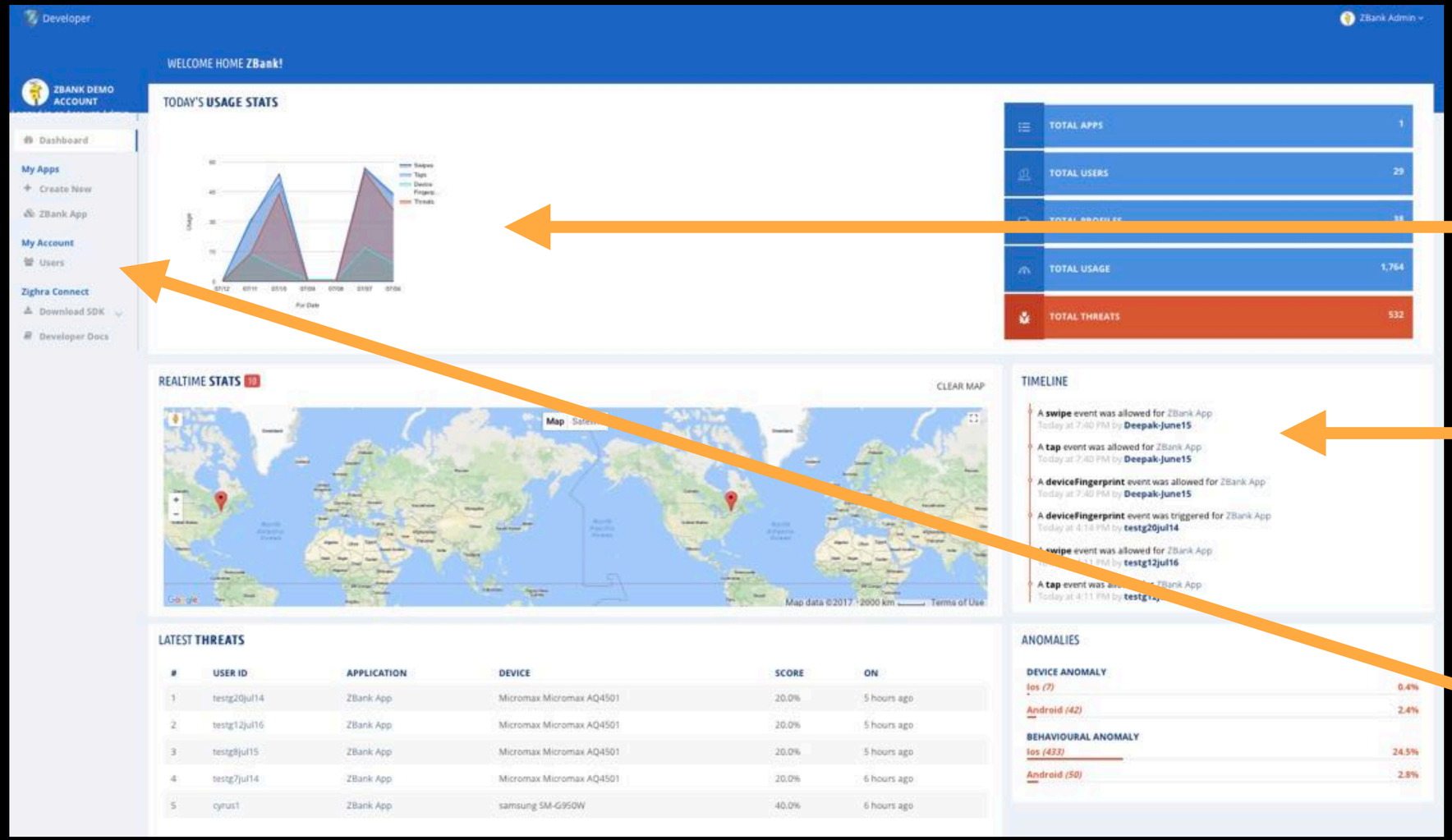
Explainable Interface

Administration Portal

1. I know when you succeed.
2. I know when you fail.
3. I know when to trust you.
4. I know there is no bias.
5. I understand why/why not.

ADMIN

Zighra's explainable AI interface enables users to understand, appropriately trust, and effectively manage an emerging generation of AI capabilities.



Real-time Cognitive Intelligence

Explainable AI/ML Analytics

Control Center

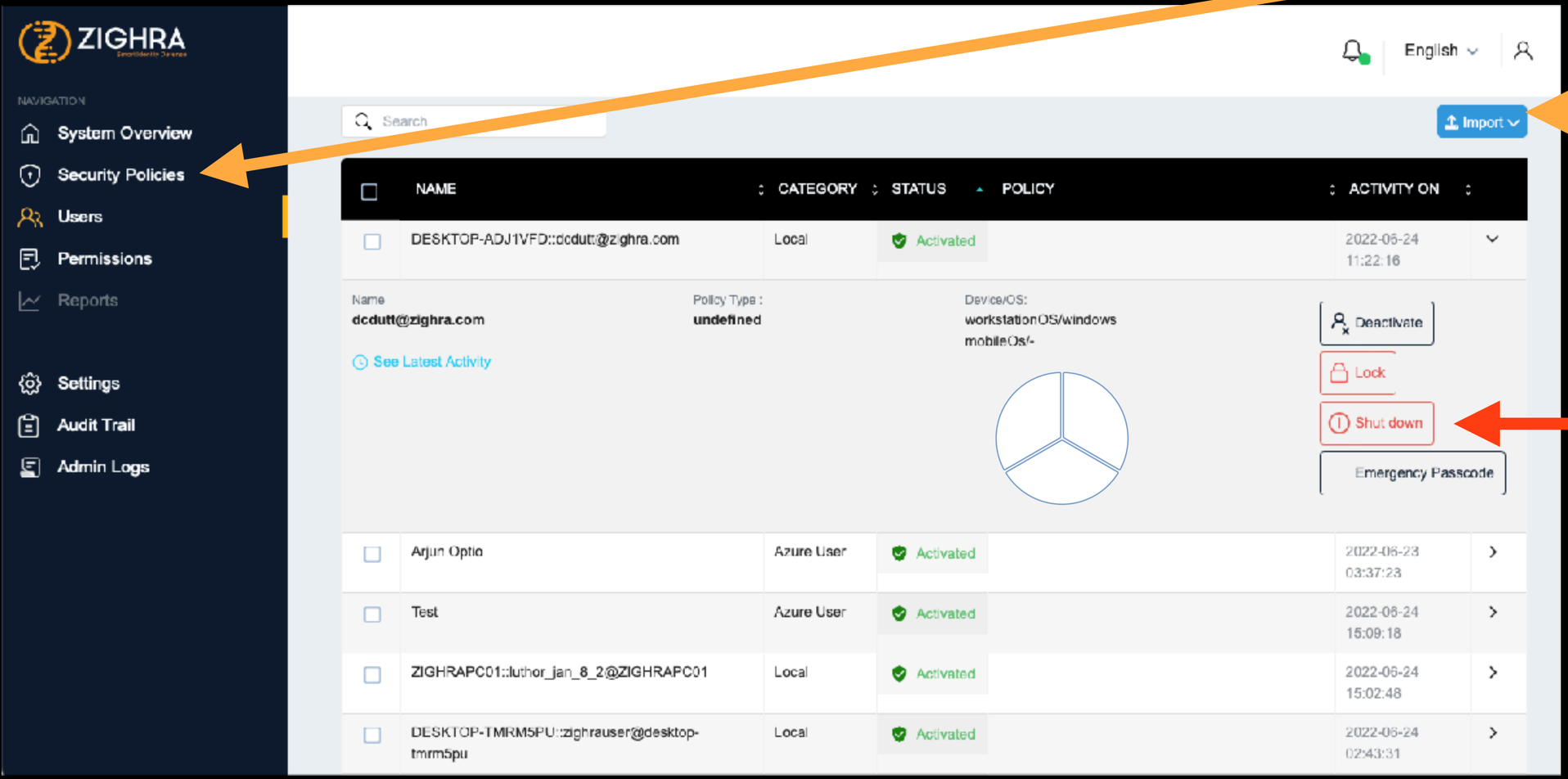
Remote management and remediation

Control Center

Security Policies

Integrate with existing Identity Systems

Remote SHUTDOWN



Benefits

Harmonize CyberSecurity and UX

- Continuously protect users and device identities and reduce fatigue/friction.
- Save thousands of hours in employee productivity.

Reduce Analyst Fatigue

- Provide actionable and situational awareness for analysts.
- Reduce false alerts and improved incident awareness and analysis.

Reduce Costs

- Save **millions of dollars** in password reset costs.
- Cross-Cloud, Cross-Platform solution.

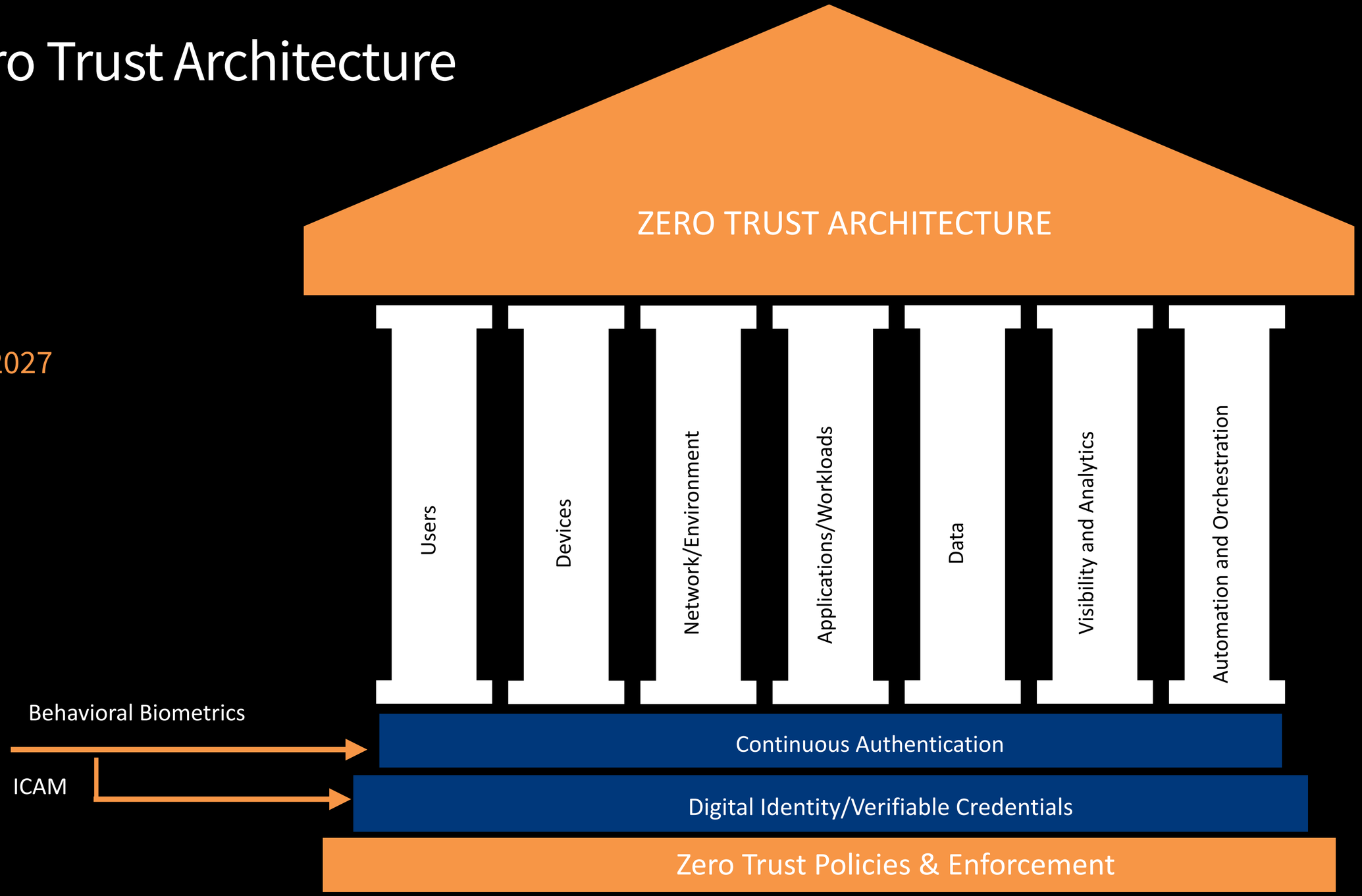
Enhance Trust in AI Systems

- Understand, appropriately trust, and effectively manage an emerging generation of cognitive machines.
- No special AI-chips or hardware is required.

CMFA - Zero Trust/ICAM framework

US DoD Zero Trust Architecture

* In Production by 2027

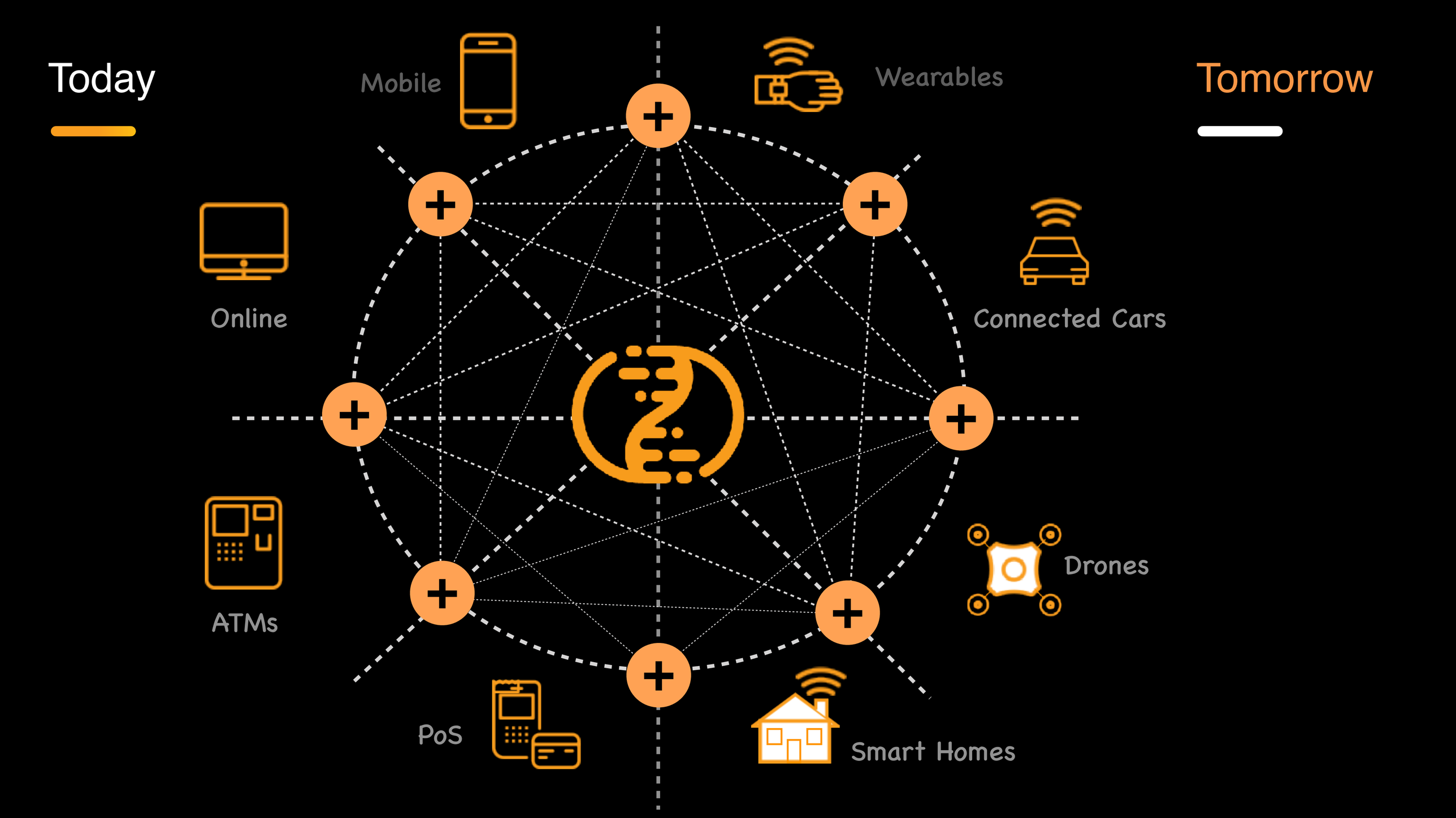


Government of Canada

Shared Services Canada

Royal Canadian Navy

Canadian Coast Guard


Today
Mobile
Wearables
Tomorrow
Online
Connected Cars
ATMs
Drones
PoS
Smart Homes

ZIGHRA

Smart Identity Defense

Deepak Dutt

613-799-1479

deepak@zighra.com

@dcdutt

Buzz

WSJ

CNBC

2018 OFFICIAL MEMBER Forbes | Technology Council

48 HOURS IN THE VALLEY

FROST & SULLIVAN 2019 BEST PRACTICES AWARD CONTINUOUS AUTHENTICATION AND THREAT DETECTION NEW PRODUCT INNOVATION AWARD

THE HILL