BlackBerry®

CYLANCE®

From Zero Trust to Zero Auth with AI

Chris Pittman

Sales Engineer

MSIA Digital Forensics
SEC+, CISSP, CRISC
22 Years in I.T.
17 Years Security
Digital Privacy Advocate

What is Zero Trust?

John Kindervag of Forrester ~ 2010, Still Evolving

Fundamentals

Mobile users are accessing distributed data from multiple devices

The network is always assumed hostile

Threats exist internally & externally

Trust is a vulnerability

Application

Requires unrestricted **visibility** into DAAS

Identity management involves **ALL objects**

Requires **continuous** authentication

Must be proliferated **across environment**

Policies must be **dynamic** & derived from multiple sources of data

The challenge:

Zero Trust

This is what security team wants – nobody gets or keeps access to anything until they prove and continue to prove who they are, that access is authorized, and they are not acting maliciously

Zero Auth

This is what users want – immediate gratification with instant access to anything and everything *they believe they need* to get job done and without hassles of passwords, timeouts, special permissions, 2FA, etc.

A real world example from mobile domain

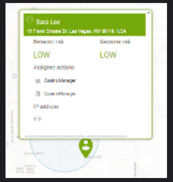
CONSIDER: A typical company device/App policy balancing security and user interference:

- Timeout: 30 minutes
- Fingerprint: allowed, but password required every 72 hours*
- Password: 9 characters, alpha + numeric + special required

Is this policy adequately preventing data loss?

Maybe…? Probably only in specific **CONTEXTS**

How AI can help get from ZT to ZA



Sara Lee

15 Frank Sinatra Dr. Las Vegas, NV 89118, USA

Behavior risk LOW

Geozone risk LOW

Assigned actions

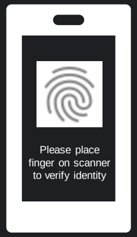
Casino Manager

Casino Manager

IP address

Contextual Auth

AI can help us understand the “**macro” context** and whether the user’s current context fits with trusted behavior and whether we should proceed at all



Please place finger on scanner to verify identity

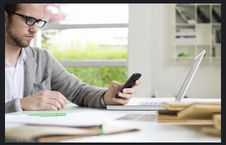
Continuous Auth

AI can help us **CONTINUOUSLY** assess the **“micro” context** of user’s ongoing behavior as it occurs and decide whether we should continue to allow access

Dynamic Policy Adaption

AI can help us dynamically apply policies at the right time and learn when otherwise static policies are either too strict or too lenient

What practical AI techniques apply?

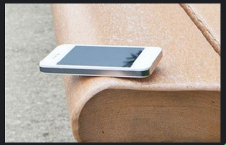


Unsupervised Learning

Learn what is ‘trusted’ and ‘normal’ behavior & locations for individuals, groups, and roles and dynamically apply policy tuned to the user’s **CONTEXT** and ***ACTUAL*** risk profile

Deep Learning

Use passive biometrics & behavioral analytics into ‘n-factor’ authentication of ‘legit’ user and solve practical problems with timeouts, FaceId, and Fingerprints



Anomaly Detection

Exploit patterns almost always vary from normal usage – supervised and unsupervised techniques such as Isolation Forest may be applied

Now, let’s look at those scenarios again…

Contextual Auth

We’ve learned this a trusted location for John and also location that is unique to him. We can relax timeout policy knowing that device loss risk is virtually nil

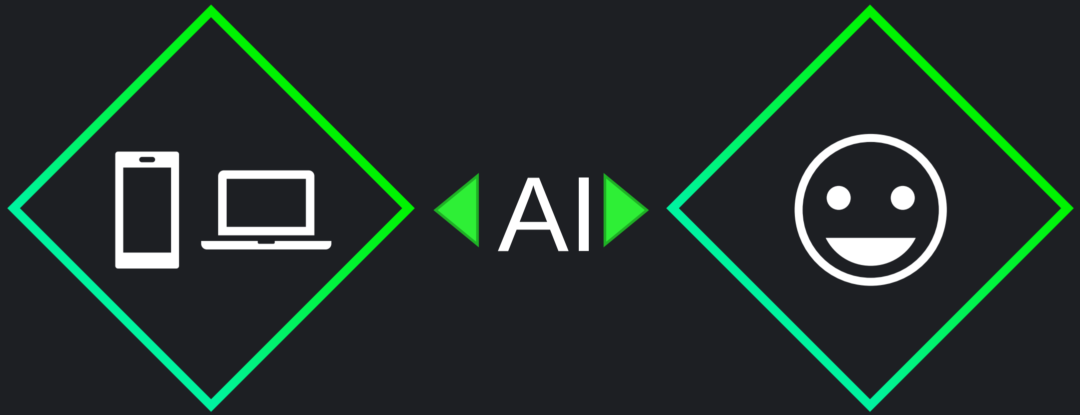
Continuous Auth

We’ve learned this is a trusted location for John and many others. We can relax timeout policy knowing that device loss risk is relatively low, but use Continuous Auth to guard against malicious use

Dynamic Policy Adaption

We know this is not a trusted location for John or anyone else. Timeout was automatically reduced to mitigate against higher probability of loss and can take specific geo-zones and user’s role into account

AI bridges gap from Zero Trust to Zero Auth

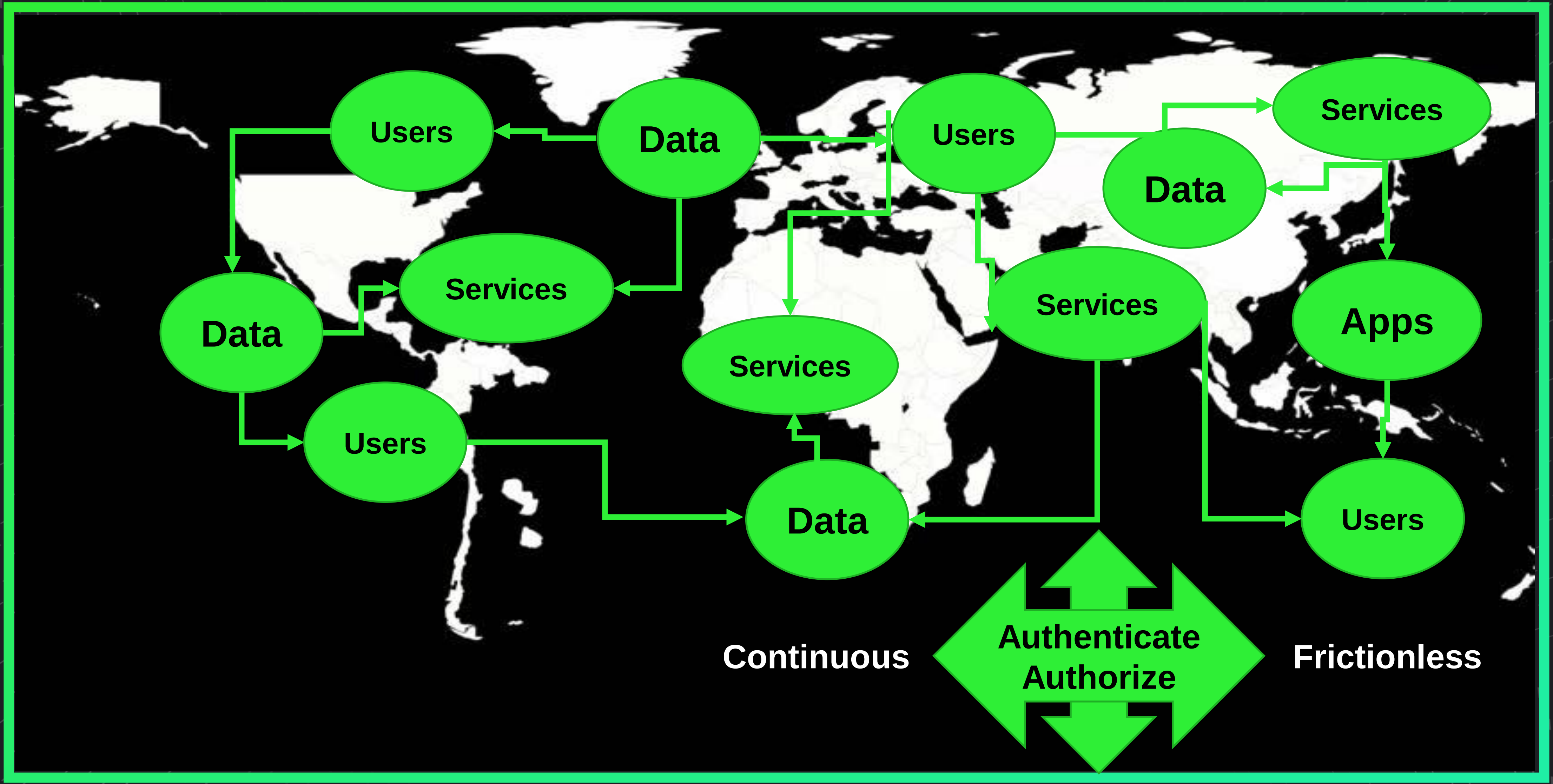


Zero Trust

AI-based Contextual and Continuous authentication enables **“MICRO” and “MACRO” Validation** of user identity and behavior across all devices and environments

Zero Auth

User’s **VALIDATED MOBILE ACTIVITY** provides equivalent of strong second factor for device access when contexts are correlated and known to be high trust; Instantly register changes and dynamically apply controls



Continuous

Frictionless

BlackBerry®

CYLANCE®

THANK YOU!