

Identity Access Management

How and Why we got here and
What you need to know

Mike D'Arezzo
Director of Security Services

© 2019 ePlus inc. Confidential and Proprietary.

Agenda

- What is a Mike D'Arezzo?
- How and Why did we get here?
- Evolution of Identity
- What do I need to know now?



Mike D'Arezzo



- 20+ year career in Information Technology and Security
- SLAIT Consulting/ ePlus as Director of Security Services
- General Electric (GE) as Software Governance Leader and Third Party Risk Compliance
- AMF Bowling/ Bowlmor – PCI Compliance and POS Analyst
- MICROS Systems Inc/ Oracle
- Bachelor's degree in IT Management/ Security from the University of Richmond
- (ISC)² CISSP & ISACA CISA

Level set: What is Identity Access Management?

- A framework of processes to allow the identification of users, processes, or machines in an accepted role
- A “broker” that is accepted within a construct to manage access
- An uphill battle of legendary proportions!

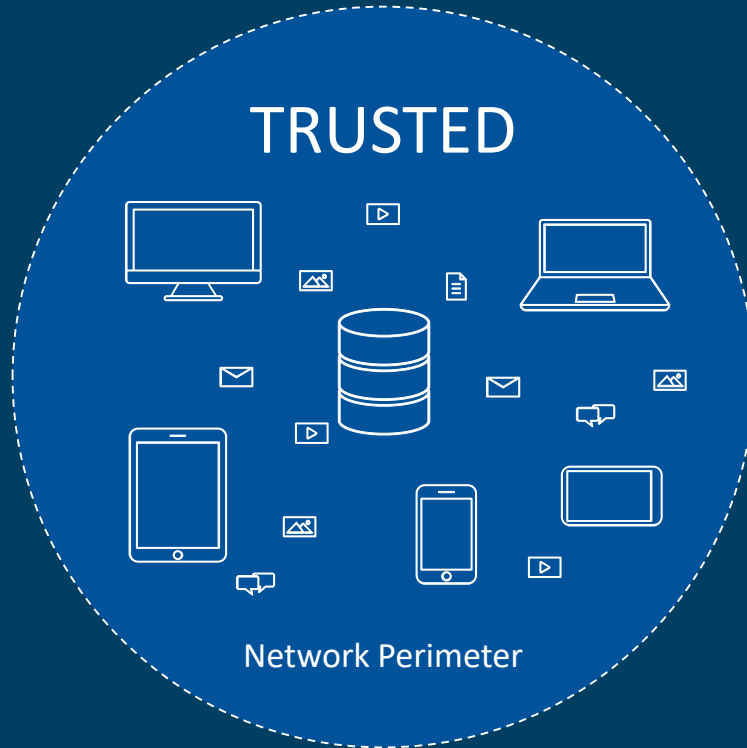
Heroes are remembered but Legends never die!

How and Why Did we get Here?

Role Based Access Controls and Active Directory/ Samba

- Web based applications
- Building to the “edge” of your Network
- The Cloud and multi-network/ multi-tenants

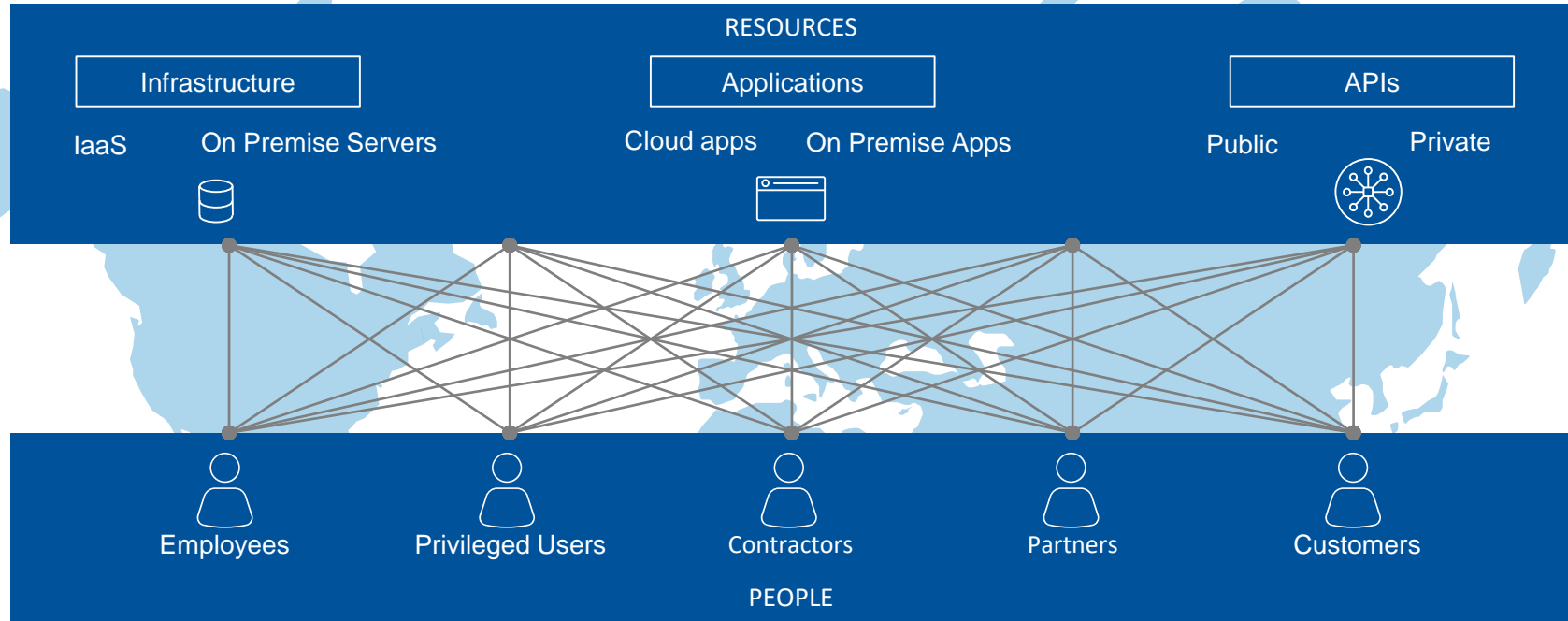
The Old Approach to Security Relies on the Network Perimeter



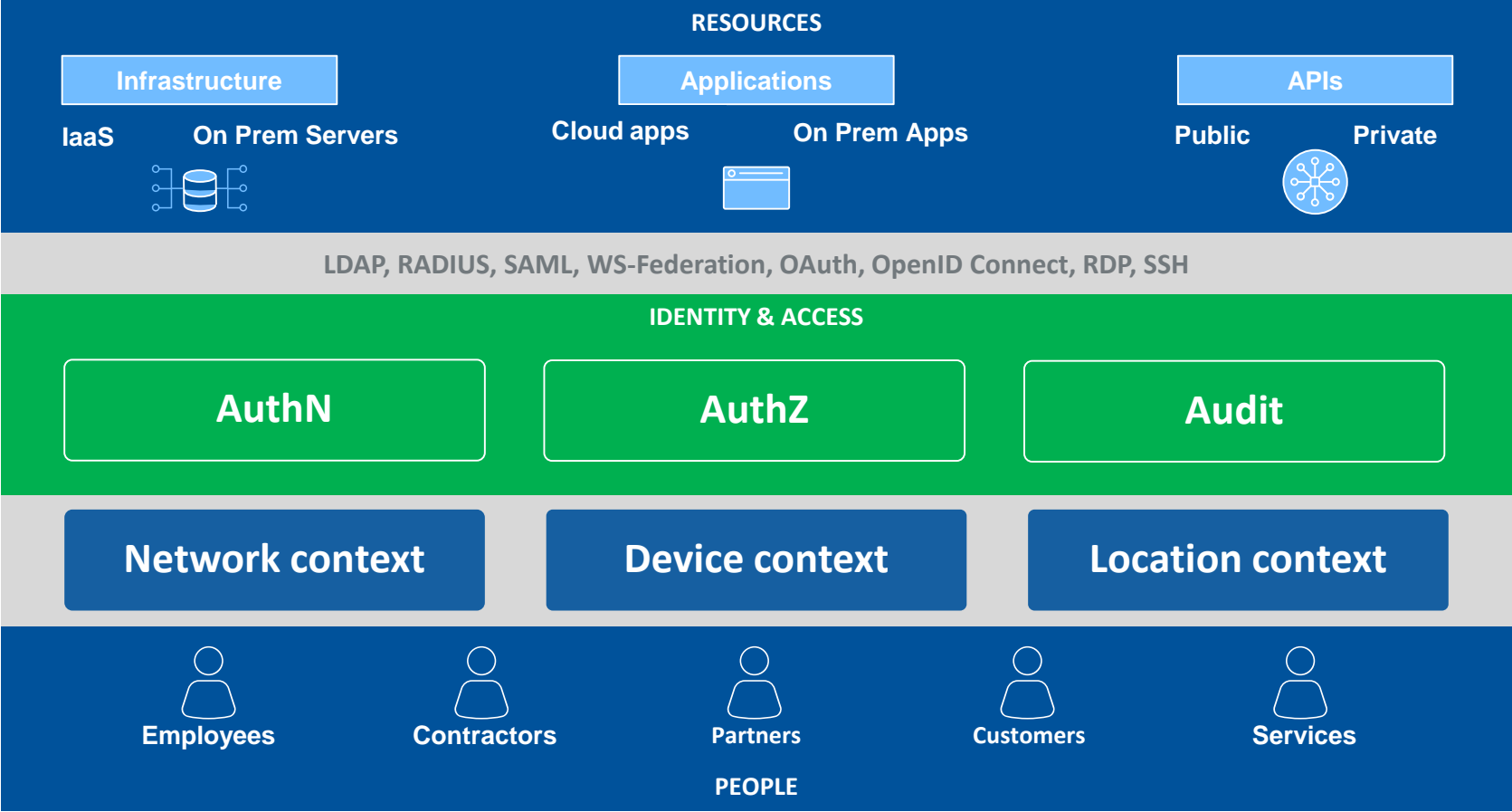
UNTRUSTED



Mobile and Cloud Have Dissolved the Traditional Perimeter



Result: We can no longer assume trust



Time for a Glossary!

RADIUS – Remote Authentication Dial-In User Service

SAML – Security Assertion Markup Language

WS-Federation / WS- Security Framework - Used to generate tokens for applications

OAuth – allows a user to delegate access to an application for another application without passing full credentials

The Building Blocks

Authentication or AuthN

User Management

- Identity Provider
- SSO/MFA
- Lifecycle Management

Device Management

- Fleet Management
- Endpoint Protection
- Security Keys

Authorization or AuthZ

Access Gateway

- Proxy Service
- Certificate Authority
- API & Security Brokers

Authorization Engine

- Data Pipeline
- Edge Processing
- Policy Enforcement

Audit

SIEM

- Audit Logs
- Monitoring
- Alerts

Behavioral Analytics

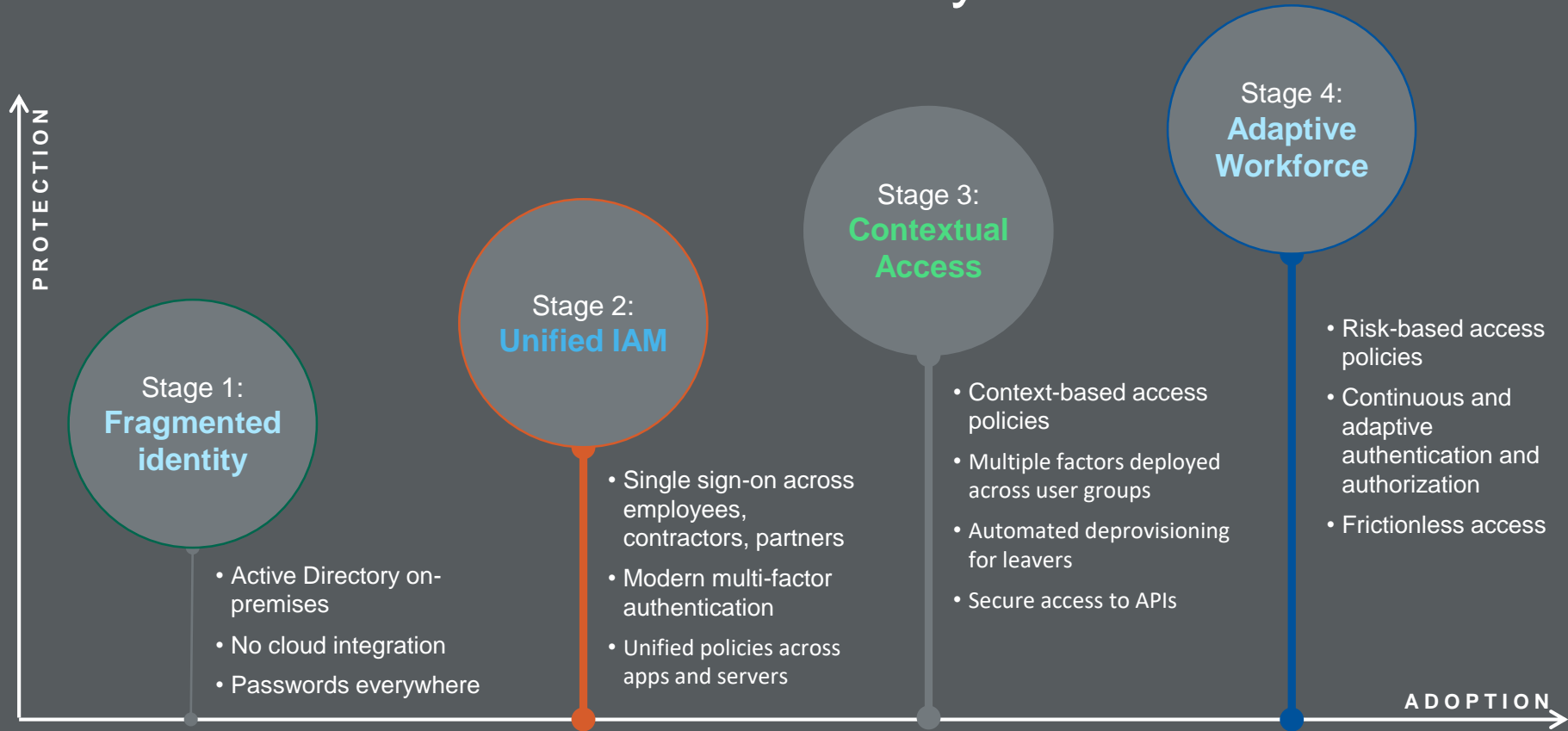
- Intrusion Detection
- Machine Learning
- Threat Assessment

Building Continuity



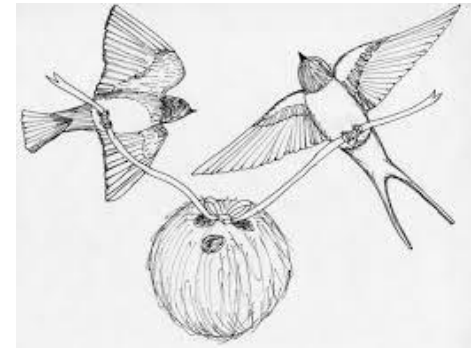
Least Friction Possible!

Zero Trust Maturity Curve



Sounds great but where do I begin?

- “Know thyself”
 - Do I know what applications and devices and people need to be connected?
 - Do I know if their compatibility is available on a single platform?
 - Do I know the migratory path of applications?



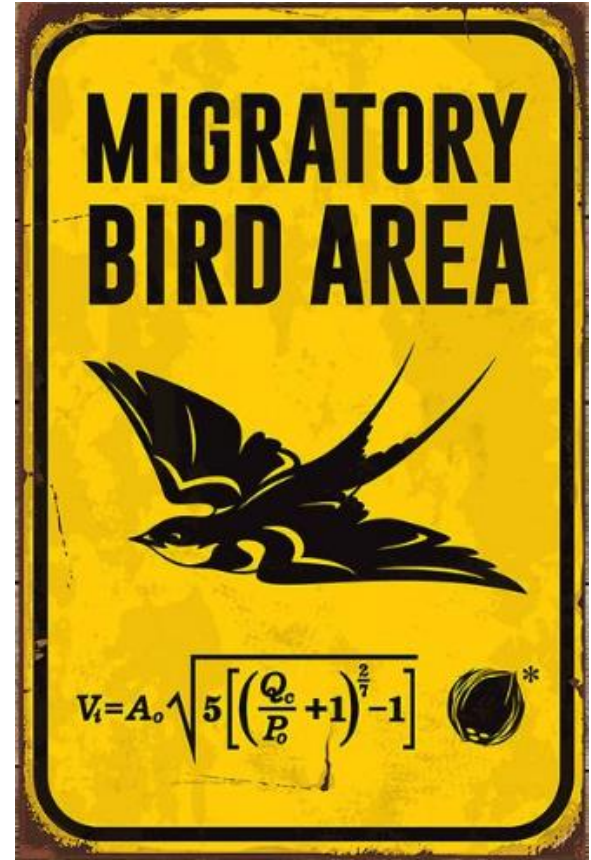
Sounds great but where do I begin?

- Preparations
 - Upgrade any components as necessary
 - Finalize on methodology but understand that 2 methods may be required
 - Pilot on 2 non-critical applications!
 - Review of pilot prior to rollout

ARE YOU SUGGESTING COCONUTS
ARE MIGRATORY?

Recap

- ZTX – Zero Trust Exchange
- Know Thyself!
- Know Thyself! Seriously!
- Upgrade any components – now is the time!
- Pilot and User Acceptance Testing



Identity Access Management

Thank you

LinkedIn

Mike D'Arezzo

Michael.darezzo@eplus.com

