THE EVOLUTION FROM AUTHENTICATION TO IDENTITY ASSURANCE

James Mandelbaum
Field CTO of Identity
RSA
@Jmandelbaum

#RSACharge
LEARN HOW TWO-FACTOR AND MULTI-FACTOR AUTHENTICATION HAS EVOLVED TO INCLUDE PUSH, BIOMETRIC AND FIDO AUTHENTICATION WHILE MAINTAINING YOUR CURRENT INVESTMENT IN TECHNOLOGY AND INFRASTRUCTURE.

YOU WILL SEE HOW WE LEVERAGE POWERFUL RISK ANALYTICS LIKE USER BEHAVIOR AND DEVICE INFORMATION TO DETERMINE ACCESS POLICIES DYNAMICALLY WHILE MAINTAINING A CONSISTENT USER EXPERIENCE.

IT'S NOT ABOUT RIP AND REPLACE, BUT ENHANCEMENT.
LEARN HOW TWO-FACTOR AND MULTI-FACTOR AUTHENTICATION HAS EVOLVED TO INCLUDE PUSH, BIOMETRIC AND FIDO AUTHENTICATION WHILE MAINTAINING YOUR CURRENT INVESTMENT IN TECHNOLOGY AND INFRASTRUCTURE.

YOU WILL SEE HOW WE LEVERAGE POWERFUL RISK ANALYTICS LIKE USER BEHAVIOR AND DEVICE INFORMATION TO DETERMINE ACCESS POLICIES DYNAMICALLY WHILE MAINTAINING A CONSISTENT USER EXPERIENCE.

IT'S NOT ABOUT RIP AND REPLACE, BUT ENHANCEMENT.
You are Failing!
We are Failing!
A Lack of Confidence

87% of board members and C-level executives lack confidence in their organization's level of cyber-security.
User Malfunction (PIBCAK)

73% are concerned about poor user awareness and behavior around mobile devices.
With GDPR

It only gets worse!

The greater of €10 million or 2% of global annual turnover
Confirmed data breaches involving weak, default or stolen passwords

Web application attacks where credentials are harvested from customer devices

Point-of-sale breaches featuring stolen credentials leveraging legitimate partner access

The Four Pillars of Identity and Access Management

Each Pillar is dependent on each other for a complete picture of a user and the capabilities

No one pillar can operate without taking the other into consideration

Authentication  Authorization  Governance  Lifecycle

NEVER LEAD WITH LIFECYCLE – EVER!
The Four Pillars of Identity

Each Pillar is dependent on each other for a complete picture of a user and the capabilities

No one pillar can operate without taking into consideration the other

Authentication  Authorization  Governance  Lifecycle
The Problem
**Traditional Authentication:** User Name / Password
Traditional Authentication: User Name / Password

Sacrifices Security for Convenience
Traditional Authentication: User Name / Password

Bill Burr

Father of modern-day password regrets original guidance

"I think I could have done a better job of figuring out some of the things that we now know, or at least of guessing them"
Traditional Authentication: Two Factor Authentication

`;--have i been pwned?

Check if you have an account that has been compromised in a data breach

jim@ pwned?

Oh no — pwned!

Pwned on 10 breached sites and found no pastes (subscribe to search sensitive breaches)
Sacrifices Convenience for Security

Traditional Authentication: Two Factor Authentication

Not always a bad thing, you must consider use case
Traditional Authentication: Two Factor Authentication

Sacrifices Security for Some Convenience
How do we even the scales?
How do we even the scales?

Easy To Use
Any Device
Any Location
Any Resource
How do we even the scales?

Easy To Use
Any Device
Any Location
Any Resource

Security
Convenience

Secure
Repeatable
Scalable
Compliant✅
New Authentication: Identity Assurance
New Authentication: Identity Assurance

Context and Risk now become part of the Equation
New Authentication: Identity Assurance

Context and Risk now become part of the Equation

This creates a level of **Assurance** Required for Access
New Authentication: Identity Assurance

User
- Groups
- Roles
- IP Address
- On Net
- Off the Net

Context

Risk

Identity Assurance

Role in App
- User
- Admin
- Privileged

Application

USER EXPERIENCE

Level of Assurance IS Met

Level of Assurance NOT Met

Challenge Token
(you may have already)
New Authentication: Identity Assurance

More Context Means More Assurance Capabilities

Build Static Go/No-Go and Challenge rules
New Authentication: Identity Assurance

User
Groups
Roles
IP Address
On Net
Off the Net

Context

Identity Assurance

Risk

Application

Role in App
User
Admin
Privileged

Geo IP
Trusted Location (un)
Device (Known?)
Authentication Method
Has Session?

More Context Means More Assurance Capabilities

Build Static Go/No-Go and Challenge rules

Add in DYNAMIC RULES for Identity Assurance

RISK ENGINE
Behavioral Analytics • Device Profiling • Login Frequency
INTELLIGENCE DRIVEN IDENTITY ASSURANCE

Static User and Context Rules

Identity Assurance Engine

Behavior-based Confidence

PASS

Deny

Location
Role
Network
Device
Session
App

Static User and Context Rules

Identity Assurance Engine

Behavior-based Confidence

Location
Role
Network
Device
Session
App

Approve
Tokencode
RSA SecurID
Fingerprint
Eyeprint ID
FIDO

#RSACHARGE
We have moved from being able to meet a challenge to…

*Is the person really who they say they are?*

*That’s “Identity Assurance”*
**AUTHENTICATION** → **CONTINUOUS ASSURANCE**

**Typical authentication flow**

1. User tries to access a resource
2. Site / resource challenges the user
3. User enters credentials, accesses resource
4. To remove session: Time out occurs or user logs out

**Continuous assurance flow**

1. User tries to access a resource
2. Site / resource uses continuous assurance
3. User only asked for credentials if necessary
4. Session removed if: Times out, logs out, or if user activity dictates

#RSACHARGE
A NEW APPROACH TO IAM

- **Identity Assurance**: Is it risk- and context-aware?
  - Are you sure?
  - Is it convenient?

- **Identity Governance**: Is it actionable?
  - Who has access to what?
  - Can you prioritize your risk?

- **User Lifecycle**: Is it proactive?
  - Is it efficient and fully automated?
  - Is it business-driven?
Integration with NetWitness
THANK YOU

ANY QUESTIONS?

JAMES.MANDELBAUM@RSA.COM