BeyondCorp and Trusted Access

ISSA Hampton Roads
January 9, 2018

Doug Copley, Advisory CISO
doug.copley@duo.com
@DouglasCopley

What came first:

Zero Trust or BeyondCorp?

Forrester: ($500)
https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682

Google: https://cloud.google.com/beyondcorp/

What is zero trust and why should I care?

BeyondCorp Mission & Principles

Mission: To have every Google employee work successfully from untrusted networks WITHOUT use of a VPN.

Principle 1:

Connecting from a particular network must NOT determine which services you can access.

Principle 2:

Access to services is granted based on what we know about YOU and your DEVICE.

Principle 3:

All access to services must be authenticated, authorized and encrypted.

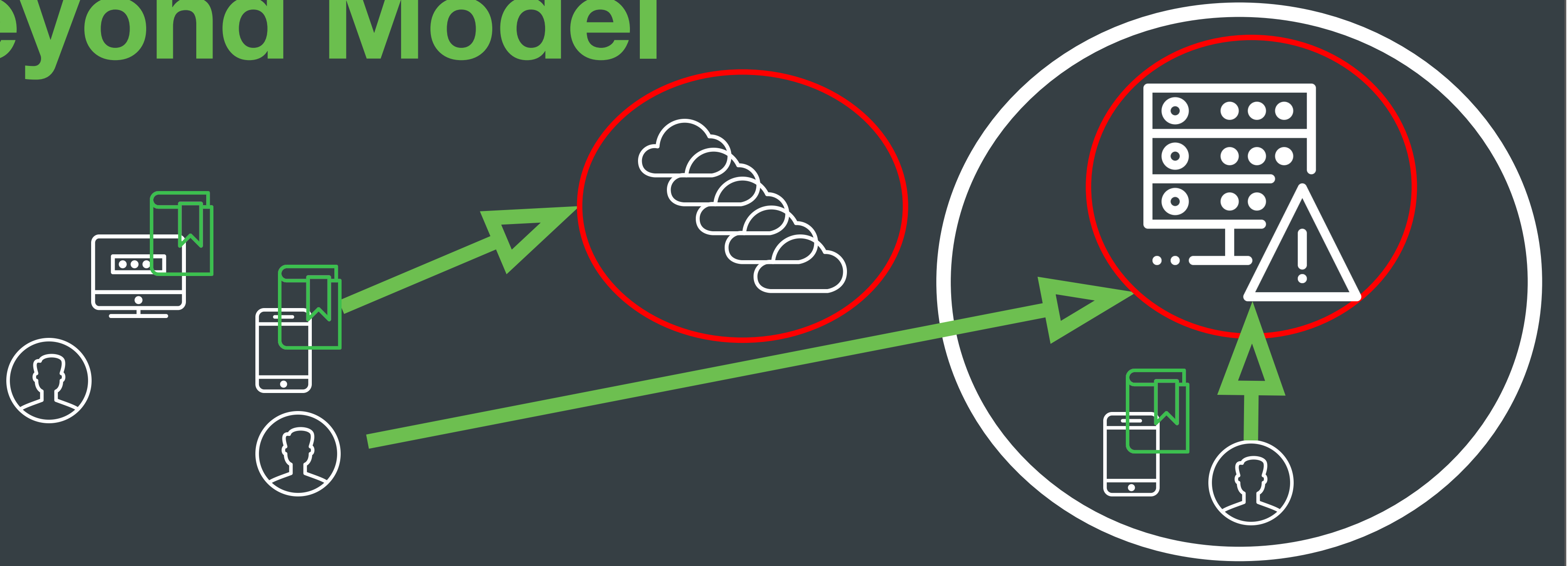
Why is Zero Trust Transformational?

- Puts controls closer to the asset
- Applies concept of protecting from the inside-out
  Protections aren’t defined by where the asset is located
- Protections aren’t (typically) defined by where the user is accessing it from
- Properties of user devices is incorporated into the access control rules

How Does it Help My Business?

- Forces organization to identify critical assets
- Risk-based controls: higher-risk = more layered controls
- Enables organizations to host assets anywhere
- Enables users to access assets from anywhere*
- Controls can be adaptive to the situation
- Enables rapid, secure adoption of new platforms & apps

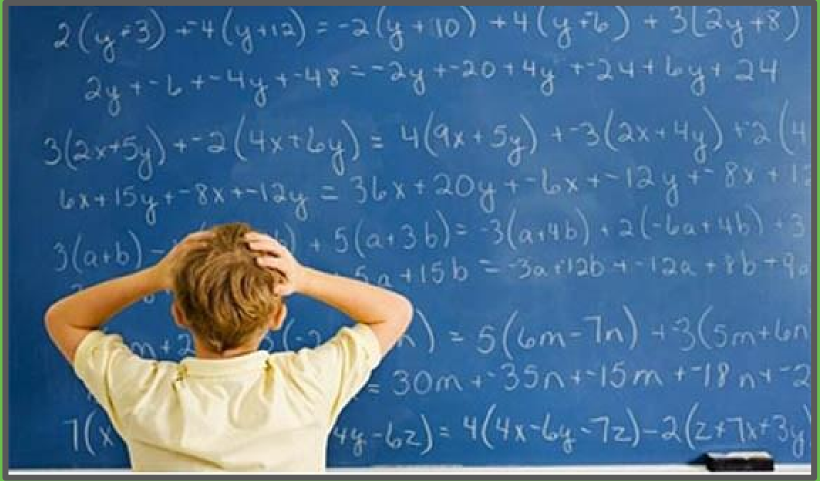
Beyond Model



Lets you protect your assets the same way using the same policies, whether they are accessed internally or externally

So How Does a “Normal” Organization Deploy Such a Model?

Task: Translating what seems like


2(y+3) + 4(y+12) = -2(y+10) + 4(y+6) + 3(2y+8)
2y + -6 + -4y + -48 = -2y + -20 + 4y + -24 + 6y + 24
3(2x+5y) + -2(4x+6y) = 4(9x+5y) + -3(2x+4y) + 2(4
6x + 15y + -8x + -12y = 36x + 20y + -6x + -12y + -8x + 1
3(a+b) + 5(a+3b) = -3(a+4b) + 2(-6a+4b) + 3
5a + 15b = -3a + 12b + -12a + 8b + 9a
= 5(6m-7n) + 3(5m+6n
= 30m + -35n + -15m + -18n + -2
7(x 4y-6z) = 4(4x-6y-7z) - 2(z+7x+3y

Into

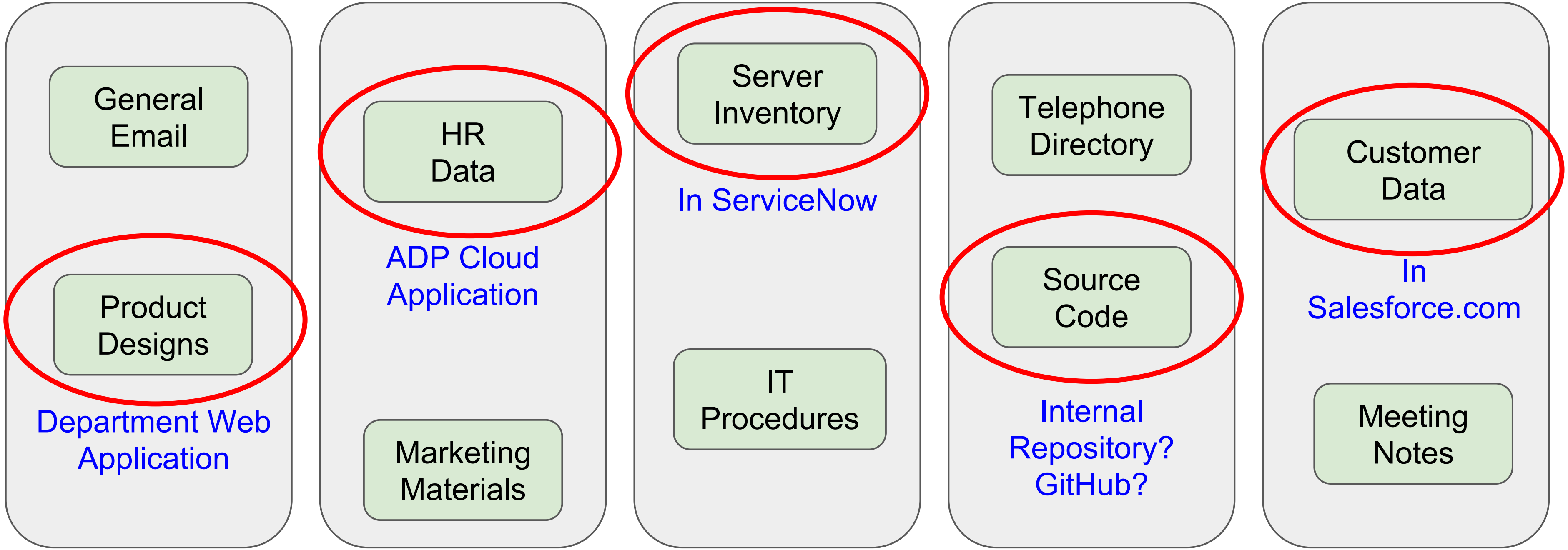
$$2 + 2 = 4$$

Application-centric Security

What are my critical assets?

Where are they?

How much protection is needed?



General Email

Product Designs

Department Web Application

HR Data

ADP Cloud Application

Marketing Materials

Server Inventory

In ServiceNow

IT Procedures

Telephone Directory

Source Code

Internal Repository? GitHub?

Customer Data

In Salesforce.com

Meeting Notes

Establishing User Trust

User Trust

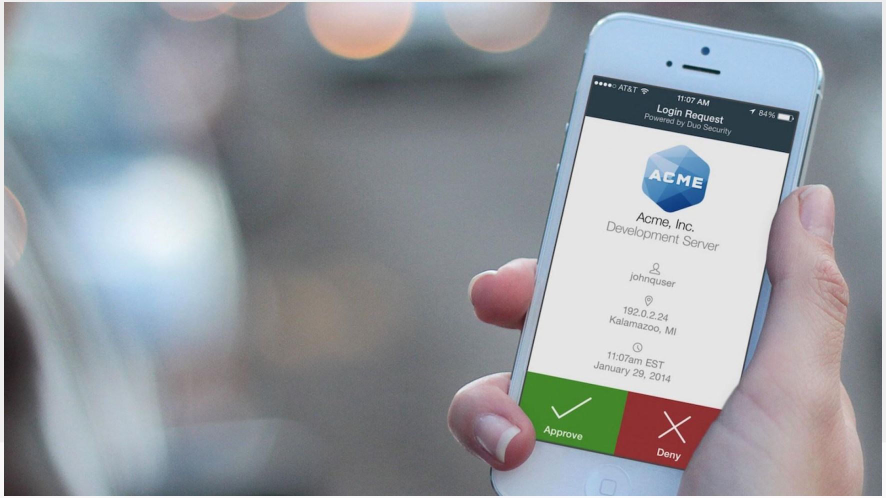
1. Primary auth (AD, LDAP, Azure AD, Google, Okta, etc.)

2. Secondary auth - Duo

3. (other checks - more later)

4. User accesses application

    - Any directory
    - Painless MFA

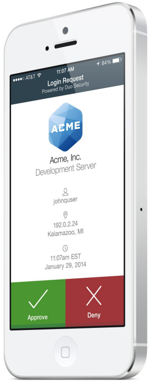


What if an outdated PC is being used?

Are you aware of the devices accessing your applications?

Establishing Device(s) Trust

Authentication Flow - BYOD Allowed


AT&T 11:07 AM 84%

Login Request
Powered by Duo Security

Acme, Inc.
Development Server

johnquser

192.0.2.24
Kalamazoo, MI

11:07am EST
January 29, 2014

Primary device hygiene

1. Operating system current?
2. Browser current?
3. Plugins current?

Secondary device hygiene

1. OS current?
2. Encrypted?
3. Screen lock enabled?
4. Jailbroken?
5. Fingerprint enabled?

EVERY device
Company AND Personal
Agentless

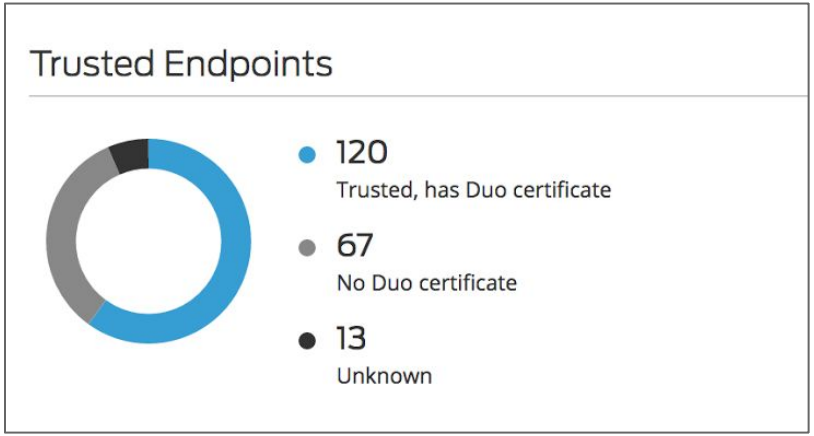
EVERY device
Company AND Personal
App does checks

NO BYOD - DUO Beyond

Detect if a device is managed or unmanaged without installing any agents.

Block access when users use unmanaged devices to access privileged accounts or critical apps.

Provide secure remote access to web-apps without the need for a VPN. (Duo Network Gateway)

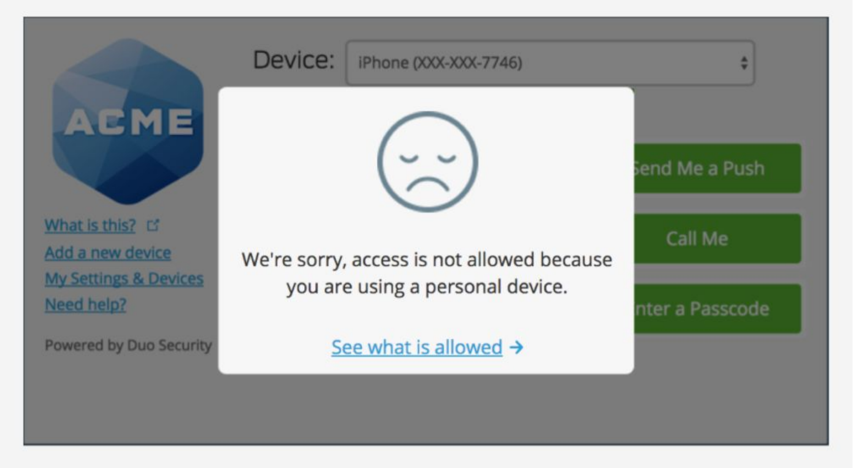


Trusted Endpoints

● 120 Trusted, has Duo certificate

● 67 No Duo certificate

● 13 Unknown



Device: iPhone (XXX-XXX-7746)

We're sorry, access is not allowed because you are using a personal device.

See what is allowed →

Device Hygiene Demo

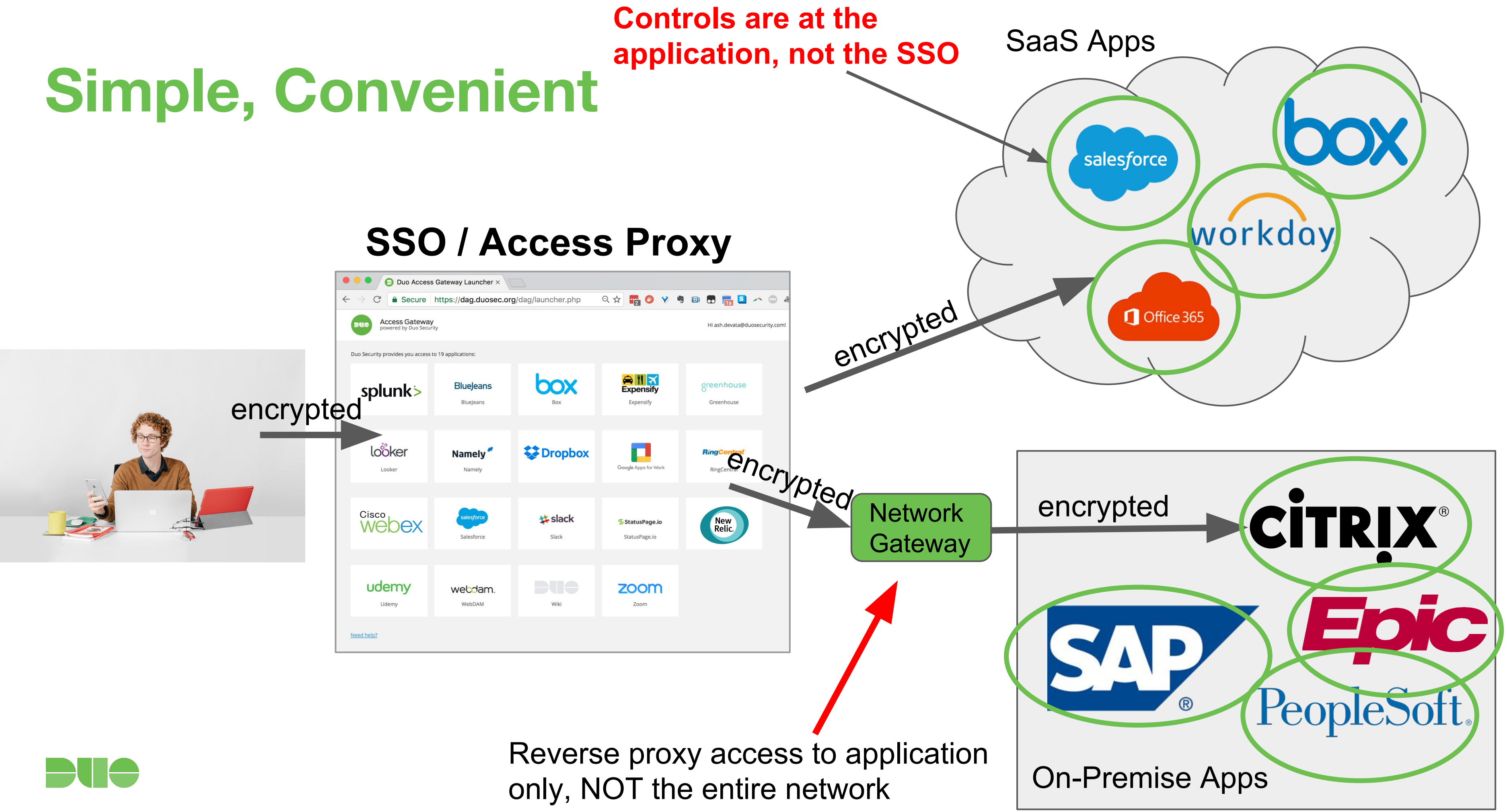
User Acceptance

Self-enrollment

Self-remediate devices

Simple SSO

Simple, Convenient



Controls are at the application, not the SSO

SSO / Access Proxy

Duo Access Gateway Launcher ×

Secure https://dag.duosec.org/dag/launcher.php

Access Gateway
powered by Duo Security

Hi ash.devata@duosecurity.com!

Duo Security provides you access to 19 applications:

splunk>
BlueJeans
Box
Expensify
Greenhouse
Looker
Namely
Dropbox
Google Apps for Work
RingCentral
Cisco webex
Salesforce
Slack
StatusPage.io
New Relic.
Udemy
WebDAM
Wiki
Zoom

Need help?

Reverse proxy access to application only, NOT the entire network

Policy Engine

All assets should NOT be protected equally

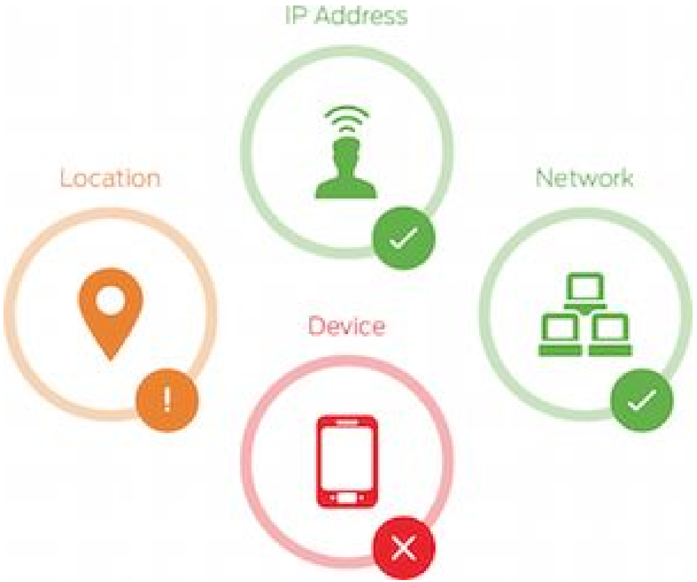
It’s a waste of precious resources

Application Control	Payroll	Email	Conference Room App
No remote access?	✓		
Corp. managed device?	✓		
Location valid?	✓	✓	✓
Browser restriction?	✓	✓	
Fingerprint ID?	✓	✓	

Enforce Policy Based Controls

Get Granular

- Block anonymous networks, out-of-date browsers and plugins, and rooted or jailbroken devices
- Require users to enable screen-lock and use U2F or push authentication
- Ensure all systems are up-to-date



> **“Duo lets our organization be able to enforce our corporate security policies on endpoints.”**

Matt Evans, Solution Architect
Kraft & Kennedy

Efficiency & Enablement

Operational Efficiency with Duo & Beyond Model

- No infrastructure - most operational in 1 day
- Minimal disruption to users
- Easy identification of high risk conditions
- Self-enrollment & self-remediation means fewer help desk calls
- SaaS model provides predictable cost
- Reduce need for MDM and VPN

Admin Console Demo

Wrap it up...

Do uncomfortable things…

Turn your corporate network inside out

Business Enablement with (Duo) Beyond

- Quickly secure applications anywhere
- Fast, secure adoption of business SaaS apps
- Adaptable authentication policies and methods
- Cloud platform scales with business needs

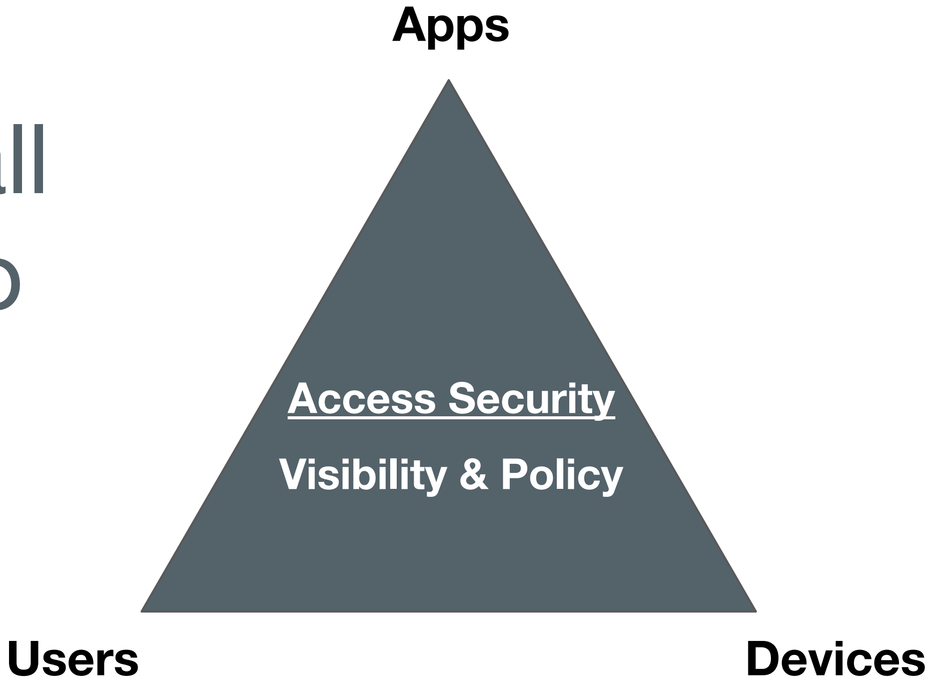
- Using Duo Beyond for M&A activities

BeyondCorp Critical Security Requirements Checklist

1. Must protect ALL apps, users and devices without an agent
2. Must comply with industry security standards (NIST, FIPS, EPCS, etc.)
3. Consistent experience across all applications-O365-VPN-Citrix1
4. Flexible authentication methods
5. Visibility across ALL devices
6. Simple MFA, Easy app access
7. Robust user & device policies
8. Fast to deploy & simple to manage
9. Quickly adopt & secure SaaS business applications

Duo Beyond for Everyone

Secure access for all **users** connecting to any work **app** using any **device.**



Apps

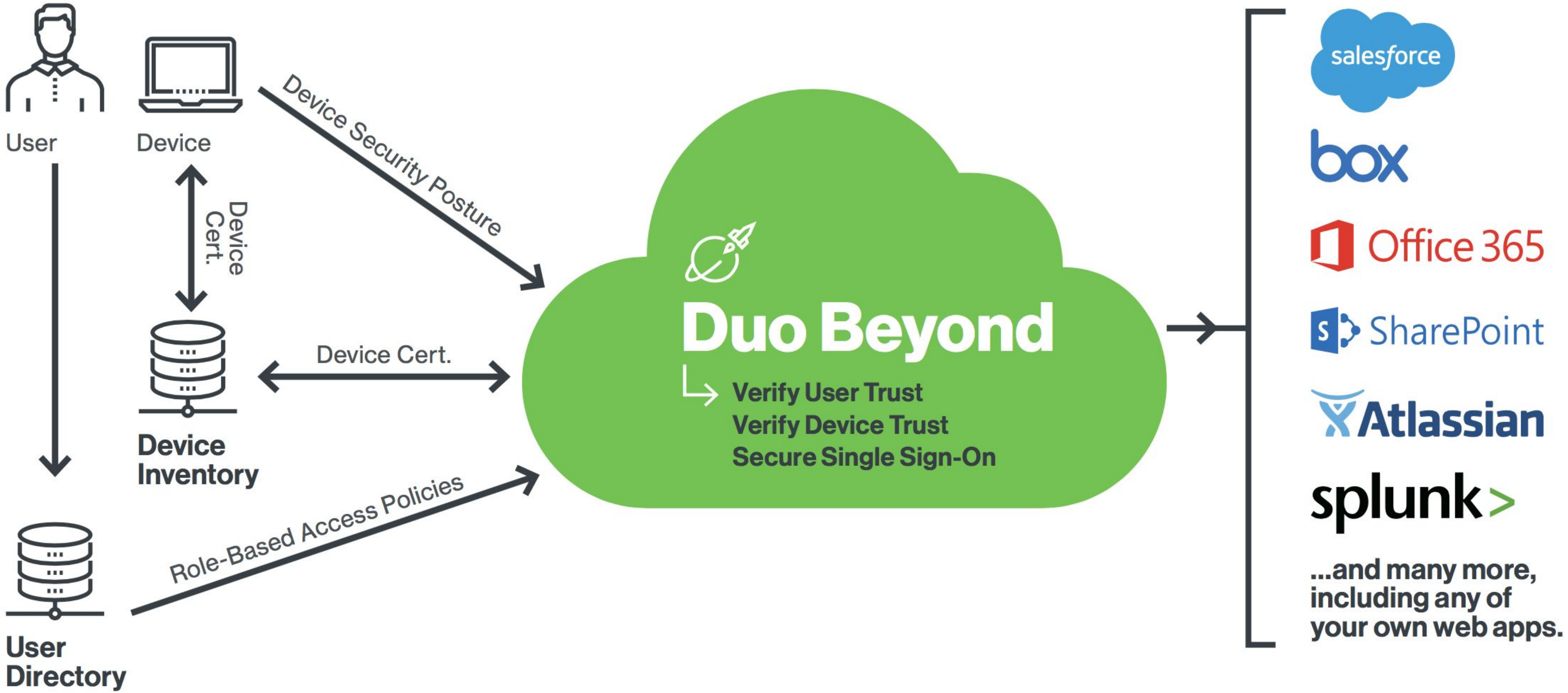
Access Security

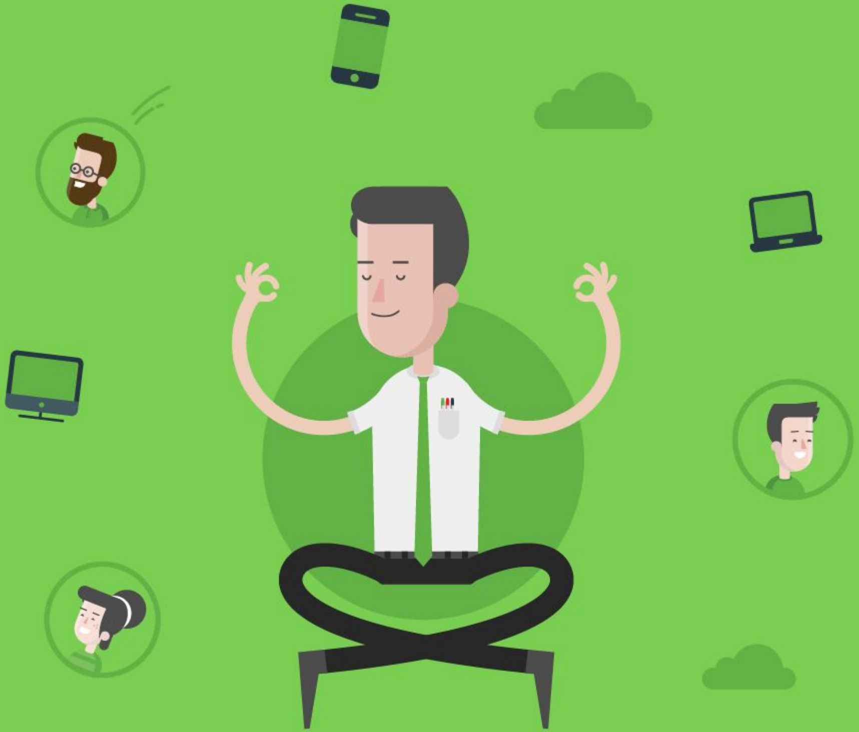
Visibility & Policy

Users

Devices

Duo Beyond


User
Device
Device Security Posture
Device Cert.
Device Cert.
Device Inventory
User Directory
Role-Based Access Policies
Duo Beyond
Verify User Trust
Verify Device Trust
Secure Single Sign-On
salesforce
box
Office 365
SharePoint
Atlassian
splunk>
...and many more, including any of your own web apps.



Security made easy and effective

Thank You!

DUO