Multi-Factor Authentication

Deakin’s Journey to uplift authentication using Single Sign-On and Multi-Factor

DEAKIN UNIVERSITY

Deakin University CRICOS Provider Code: 00113B

Dushyant Sattiraju

Cyber Security Operations Lead

Content

- Single Sign-On Implementation
- Multi-Factor Authentication
- Demo

Deakin University CRICOS Provider Code: 00113B

Why Multi-Factor Authentication

284	5,044,555,541	70,358	77,127,825
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
152,445,165	Adobe accounts
112,005,531	Badoo accounts
105,059,554	B2B USA Businesses accounts

Recently added breaches

777,649	ViewFines accounts
24,853,850	VNG accounts
7,485,802	17173 accounts
10,371,766	TGBUS accounts
188,847	ILikeCheats accounts
6,844,490	CashCrate accounts
27,971,100	Taringa accounts
386,489	Smogon accounts
13,873,674	HiAPK accounts
3,204	Bestialitysextaboo accounts

Source: haveibeenpwned.com

DEAKIN UNIVERSITY

Your digital identity is more than ‘Password123’

DEAKIN UNIVERSITY

Deakin University CRICOS Provider Code: 00113B

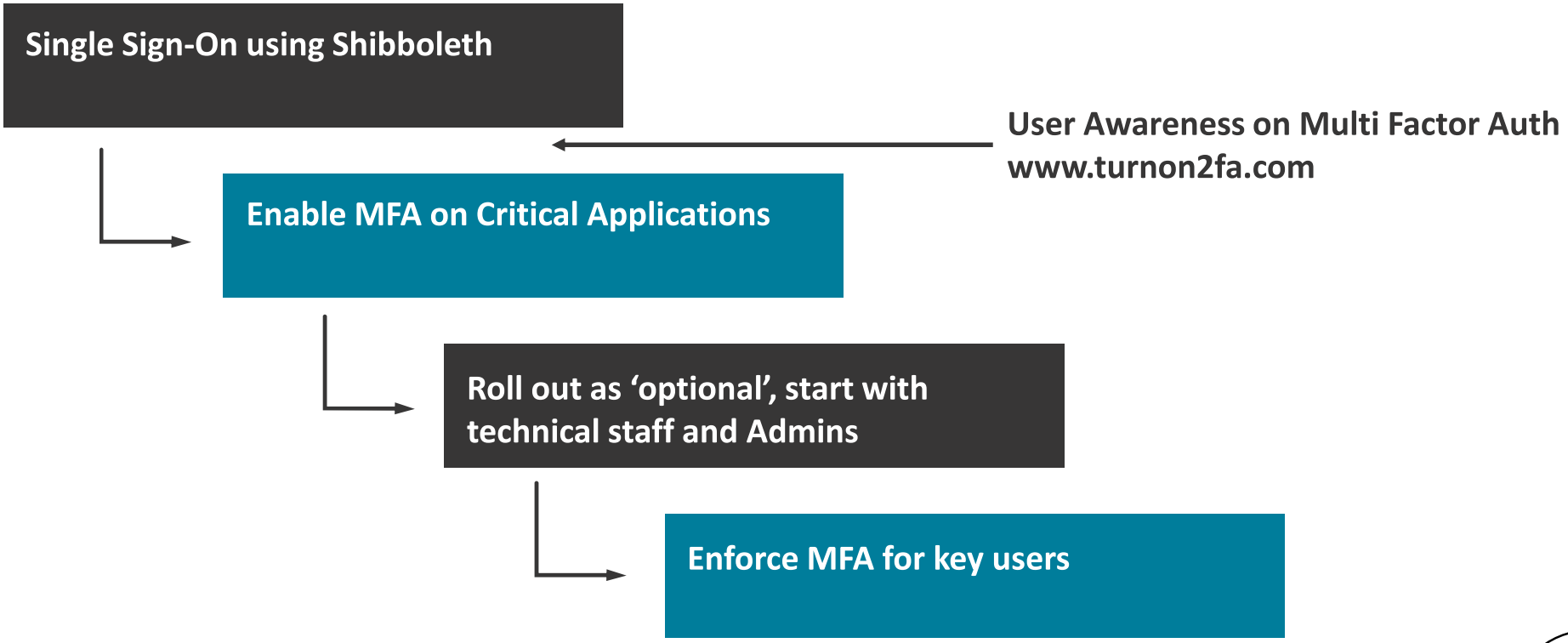
Multi-Factor

- Something you **have**
- Something you **are**
- Something **you know**

Source: Splunk Inc.

DEAKIN UNIVERSITY

Our Journey


Single Sign-On using Shibboleth
User Awareness on Multi Factor Auth
www.turnon2fa.com
Enable MFA on Critical Applications
Roll out as 'optional', start with technical staff and Admins
Enforce MFA for key users

Technology Stack

Shibboleth

BIG-IP Access Policy Manager

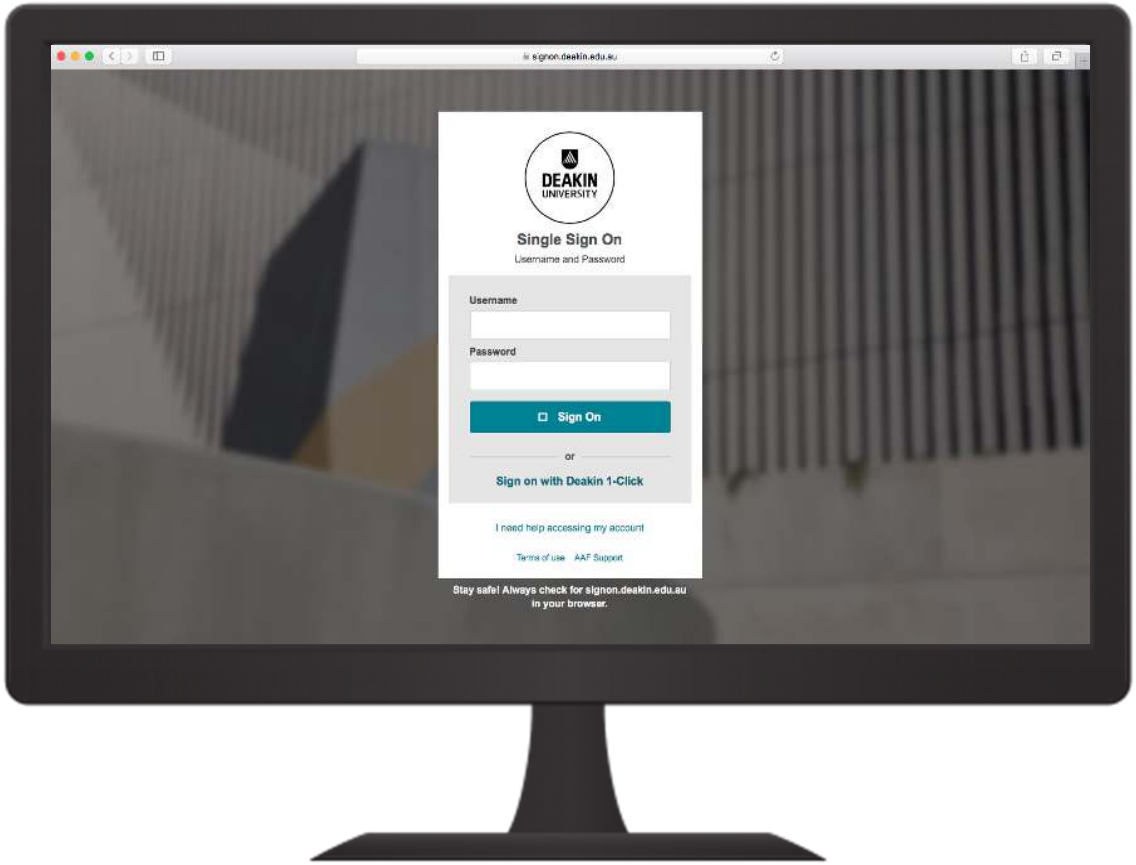
Duo MFA

Source:
shibboleth.net
f5.com
duo.com

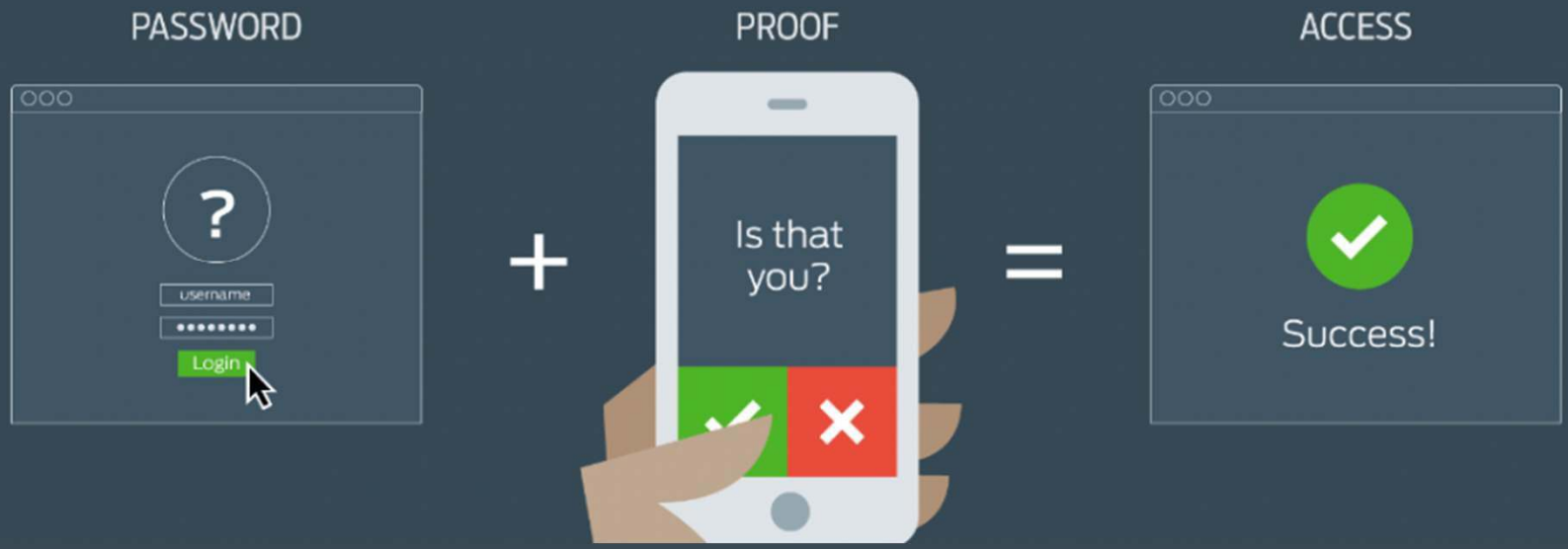
DEAKIN UNIVERSITY

Balance between security and usability

Single Sign-On

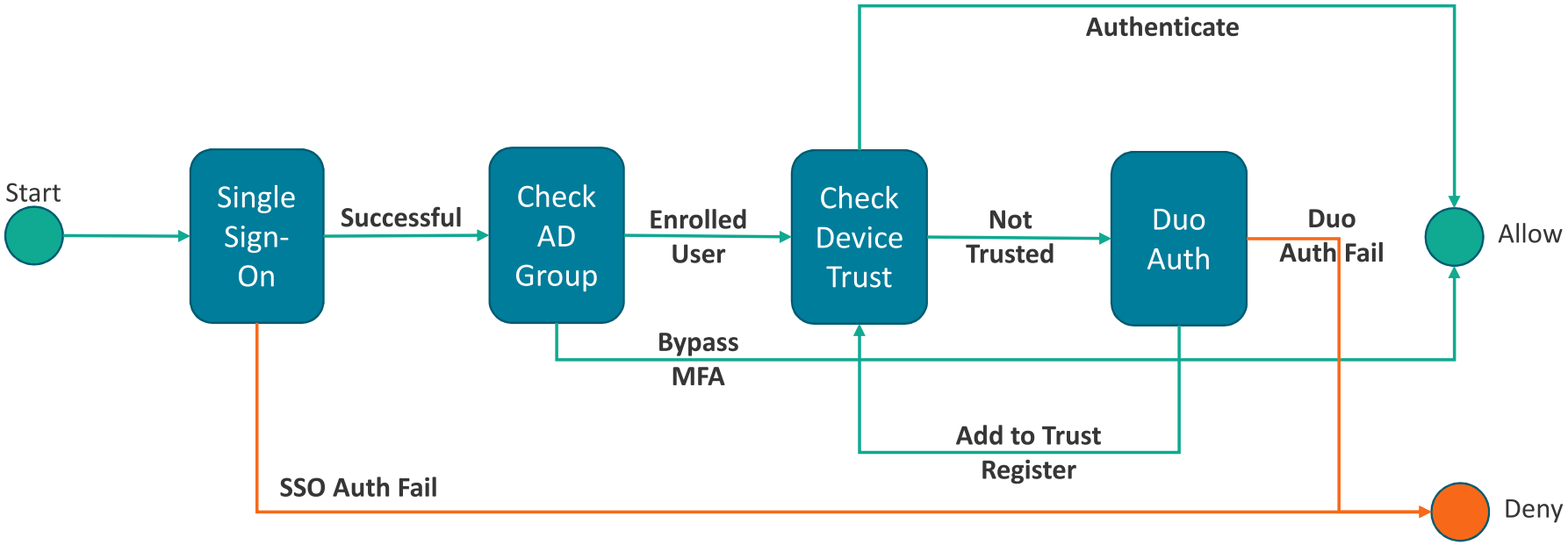


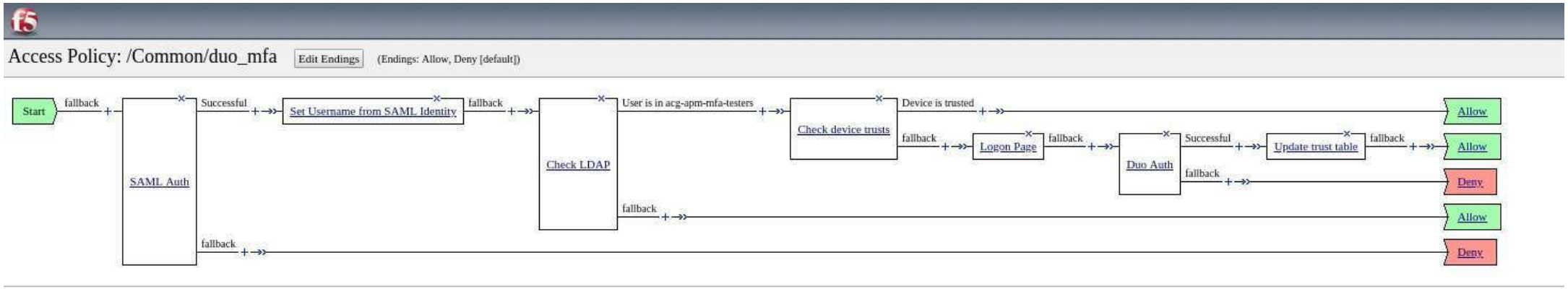
MFA using Duo



Source: Duo Security

MFA Logic Flow




Access Policy: /Common/duo_mfa
Edit Endings
(Endings: Allow, Deny [default])
Start
fallback
SAML Auth
Successful
Set Username from SAML Identity
fallback
Check LDAP
User is in acg-apm-mfa-testers
Check device trusts
Device is trusted
Allow
fallback
Logon Page
fallback
Duo Auth
Successful
Update trust table
fallback
Allow
fallback
Deny
fallback
Allow
fallback
Deny

LiveSlides web content

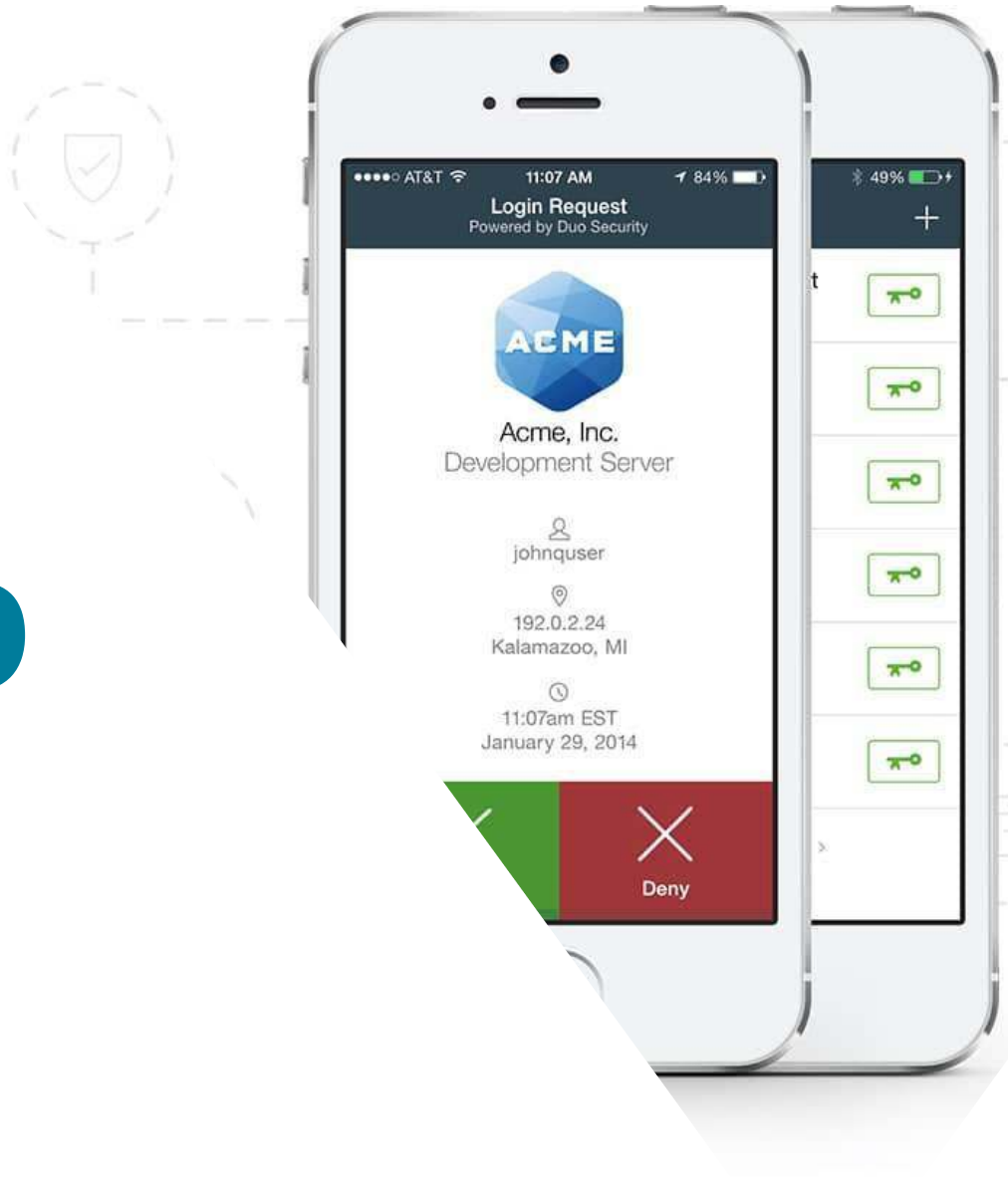
To view

Download the add-in.

liveslides.com/download

Start the presentation.

Demo

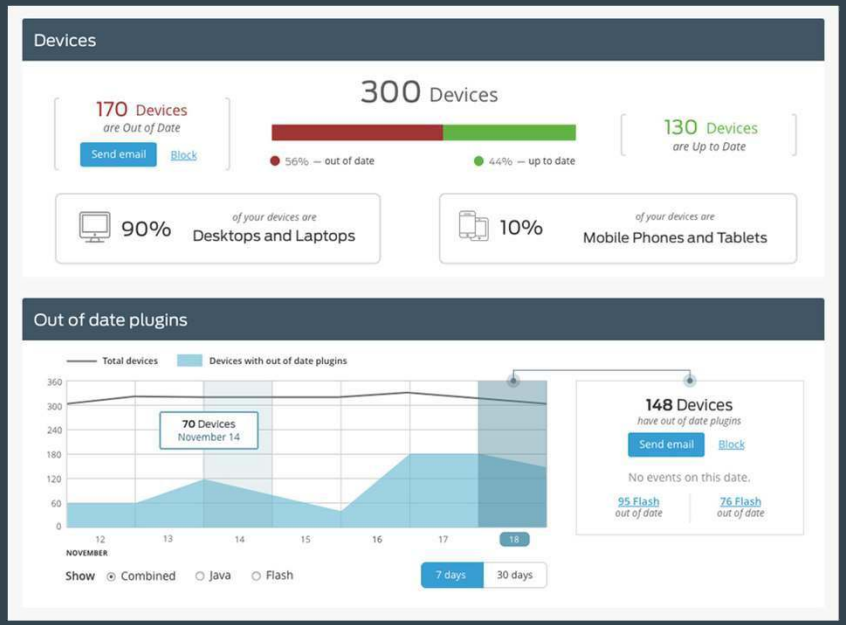

AT&T
11:07 AM
84%
Login Request
Powered by Duo Security
ACME
Acme, Inc.
Development Server
johnquser
192.0.2.24
Kalamazoo, MI
11:07am EST
January 29, 2014
Deny
49%

Demos have failed before...

Source: mirror.co.uk

DEAKIN UNIVERSITY

Advantages



Device Health

Different options

Deakin University CRICOS Provider Code: 00113B

Issues and challenges

- User Awareness
- Reluctance to use personal device
- Session limit for f5 APM
- Duo Look and Feel is not customizable – at this stage

Ben Savage
Ryan Parker-Hill

DEAKIN UNIVERSITY

Deakin University CRICOS Provider Code: 00113B

Deakin University CRICOS Provider Code: 00113B