MAKE ENDPOINTS GREAT AGAIN

"I will build a firewall to protect the perimeter and I will make Cisco pay for it."

CIO Trump

Hello!

I AM BEN GROSS

Manager

bengross@berkeley.edu

@bengross

...and Hello!

I AM RIFF KHAN

Systems Administrator

riff@berkeley.edu

@riffkhan

#1 Public University

#3 Global University

7 Nobel Prizes

77 Faculty Fulbright Scholars

14,500 Employees

55,000+ Students


Winter is Always Coming

“My job is not to protect the campus from the internet. It is to protect the internet from the campus.”

Security Analyst, UC Berkeley

TEAM EEI BY THE NUMBERS

14000+ Endpoints in BigFix

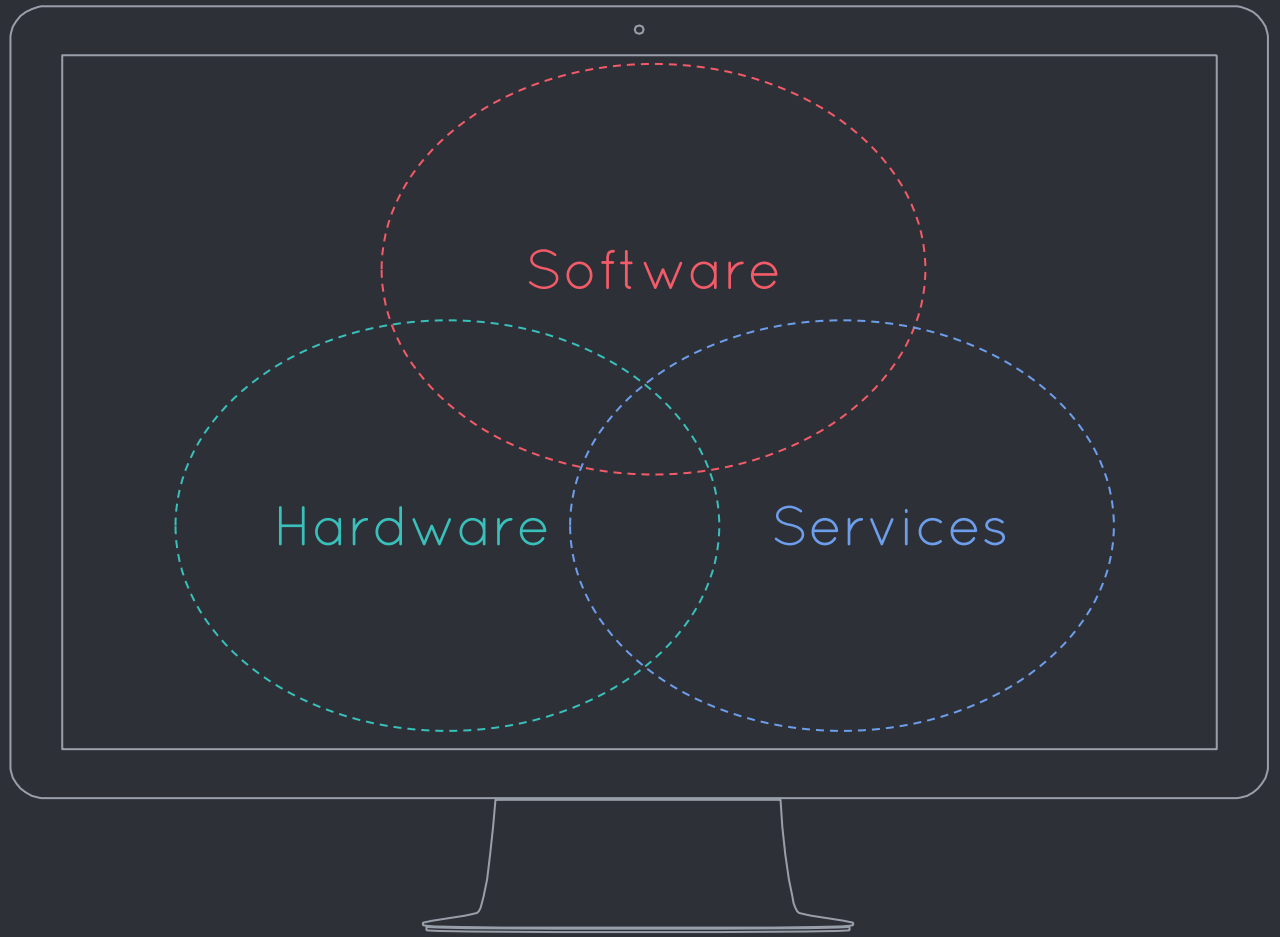
11K Windows
3K Macs

8000+ Users

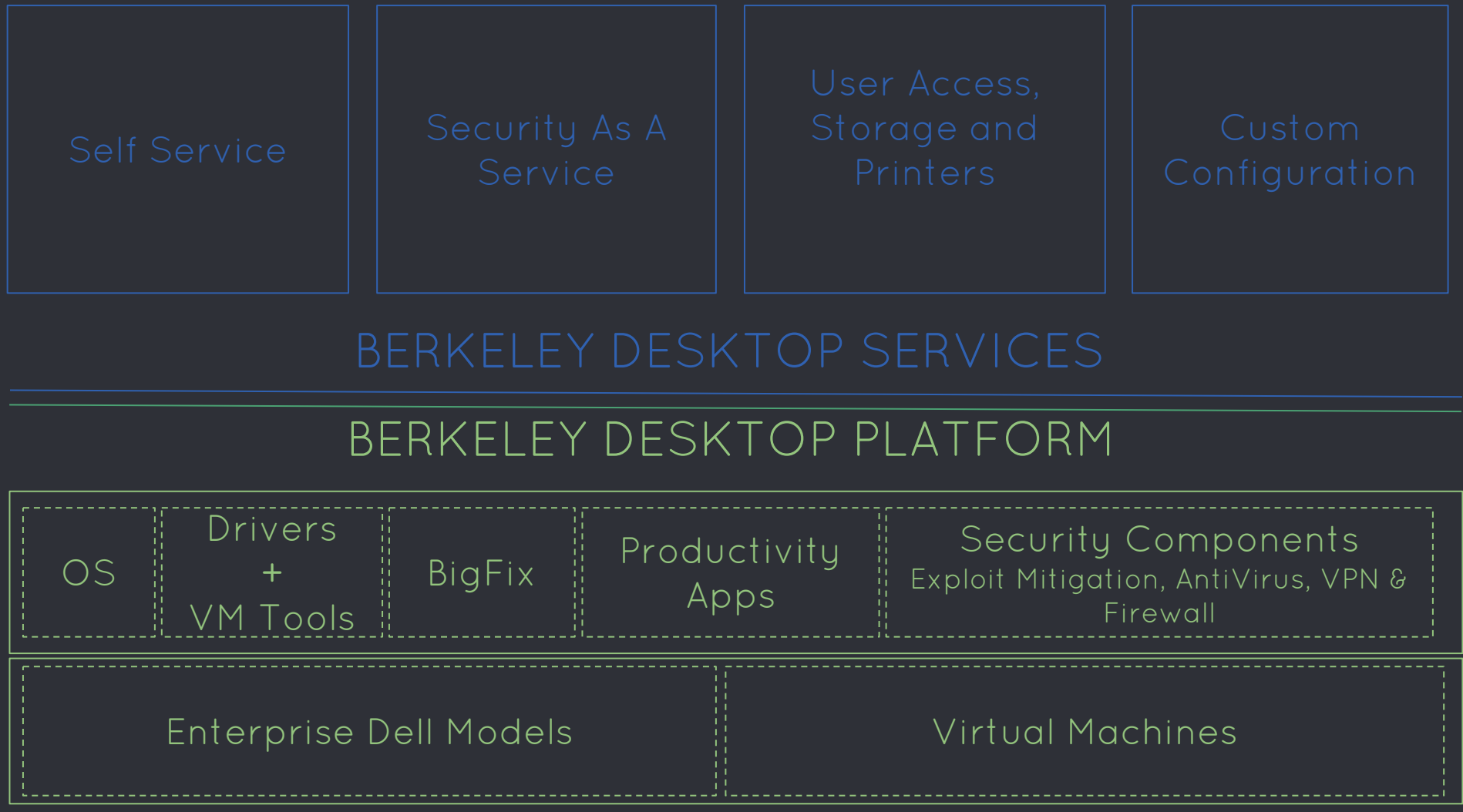
175+ Supported Business Units

10 Team Members

8 Technical
1 PM
1 Manager



BERKELEY DESKTOP ECOSYSTEM


Self Service
Security As A Service
User Access, Storage and Printers
Custom Configuration
BERKELEY DESKTOP SERVICES
BERKELEY DESKTOP PLATFORM
OS
Drivers + VM Tools
BigFix
Productivity Apps
Security Components
Exploit Mitigation, AntiVirus, VPN & Firewall
Enterprise Dell Models
Virtual Machines

AUTO PATCHING

CONFIGURATION MANAGEMENT

MANAGED ANTIVIRUS

AUDIT COMPLIANCE

SECURITY AS A SERVICE

BIGFIX

Patching as a Service

7 Operating Systems

15+ Custom Applications

25+ Total Applications

175+ Departments

10000+ Endpoints

1 FTE worth of time

A Modern SysAdmin has vSphere to run
Puppet to manage Casper to manage MacOS”

"SAY DOCKER ONE MORE TIME!"


WHAT DO YOU MEAN REBOOT? I JUST REBOOTED LAST MONTH!!

"Security at the expense of usability comes at the expense of security."

Avi Douglen, Security Architect and Developer

Design Principles

to MAKE ENDPOINTS GREAT AGAIN

SET SECURE DEFAULTS

KEEP THE CORE TRANSPARENT

OFFER CONTROL AT THE EDGES

AUTOMATE ALL THE THINGS

MEASURE ALL THE THINGS

ITERATE ALL THE THINGS

1 Set Secure Defaults

MINIMIZE THE BLOAT

"I will make sure Java is removed from all endpoints. Java is horrible. We need to retake our endpoints."

CIO Trump

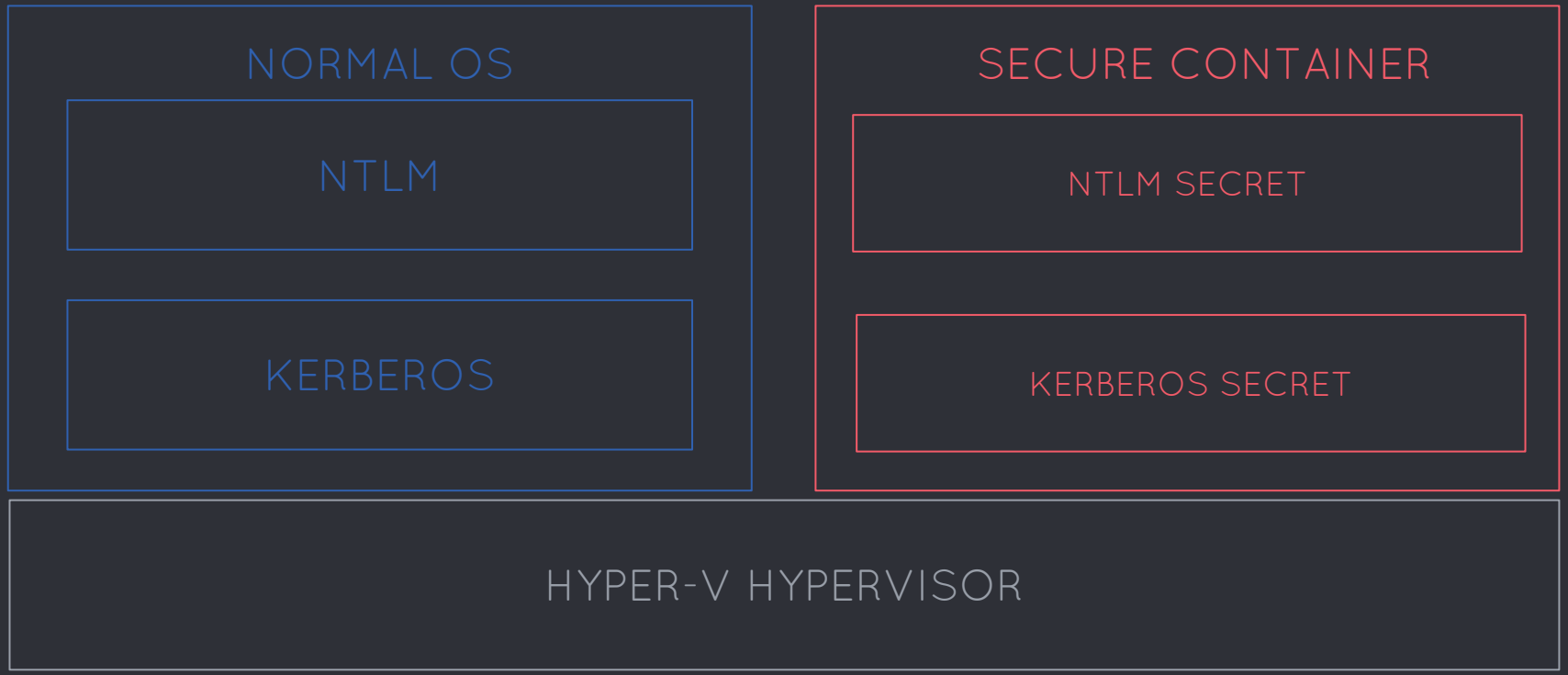
PREVENT LATERAL ACCOUNT MOVEMENT

RENAME LOCAL ADMINISTRATOR + DISABLE LOCAL ADMINISTRATOR + CHANGE PASSWORD TO RANDOM STRING

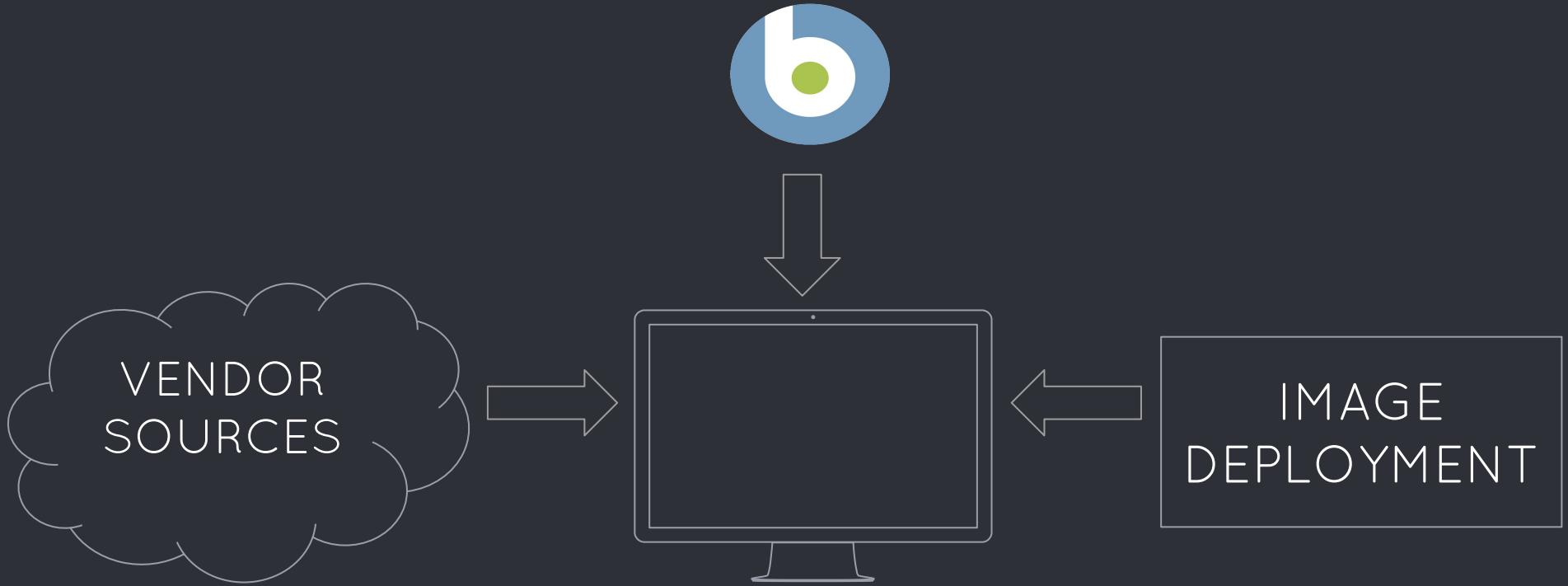
"Make sure you spell check your passwords. Make passwords random again."

CIO Trump

WINDOWS 10: CREDENTIAL GUARD

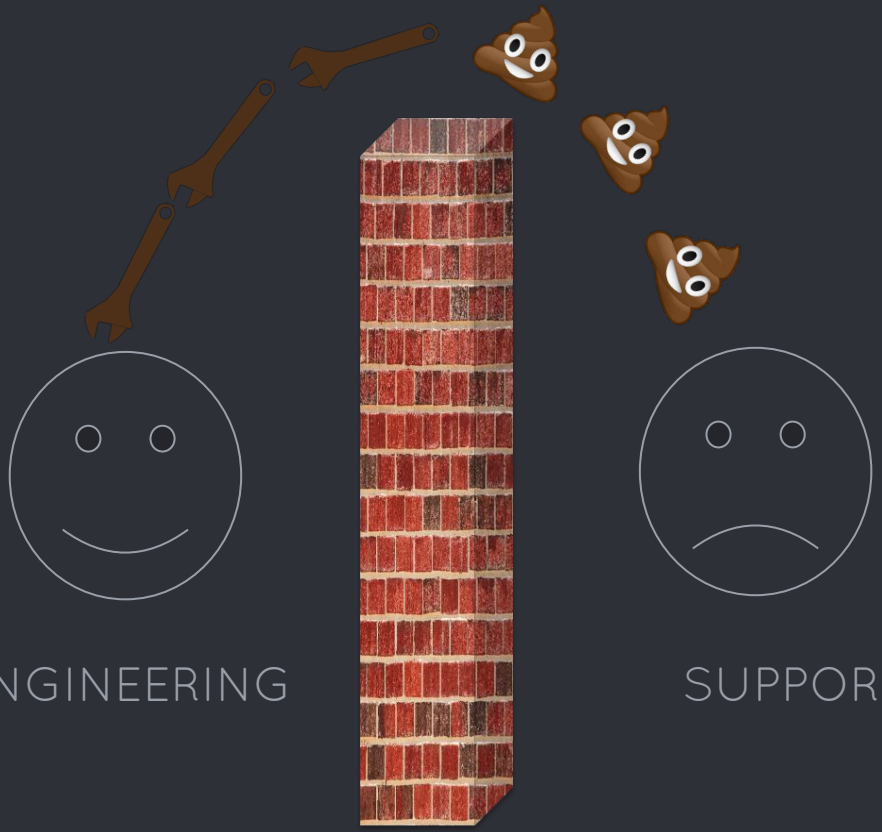


MULTIPLE PATCHING SOURCES



2 Keep the Core Transparent

WALL OF CONFUSION



COMMUNICATIONS

Announce all patch and configuration updates

ACTION
IMPACT
REASON

Release Notes Phone Call

CIRCUIT BREAKER
FEEDBACK LOOP

TOOLS: BASELINE ACTIONS BY COMPUTER

Computer: [redacted]

Baseline: <EEI Master Baseline December 2015>: Windows OS + Applications

Generate Report

Actions taken on computer 3J3KB42. Click on row to see details

Baseline Action ID	State	Issuer	Time Issued	Status	Additional Info
166607	Expired	[redacted]	2015-12-11 11:37:38 -0800	Pending Restart	Waiting for restart to complete action.
168599	Expired	[redacted]	2015-12-30 16:03:32 -0800	Fixed	The action executed successfully.

Statuses of Member Actions

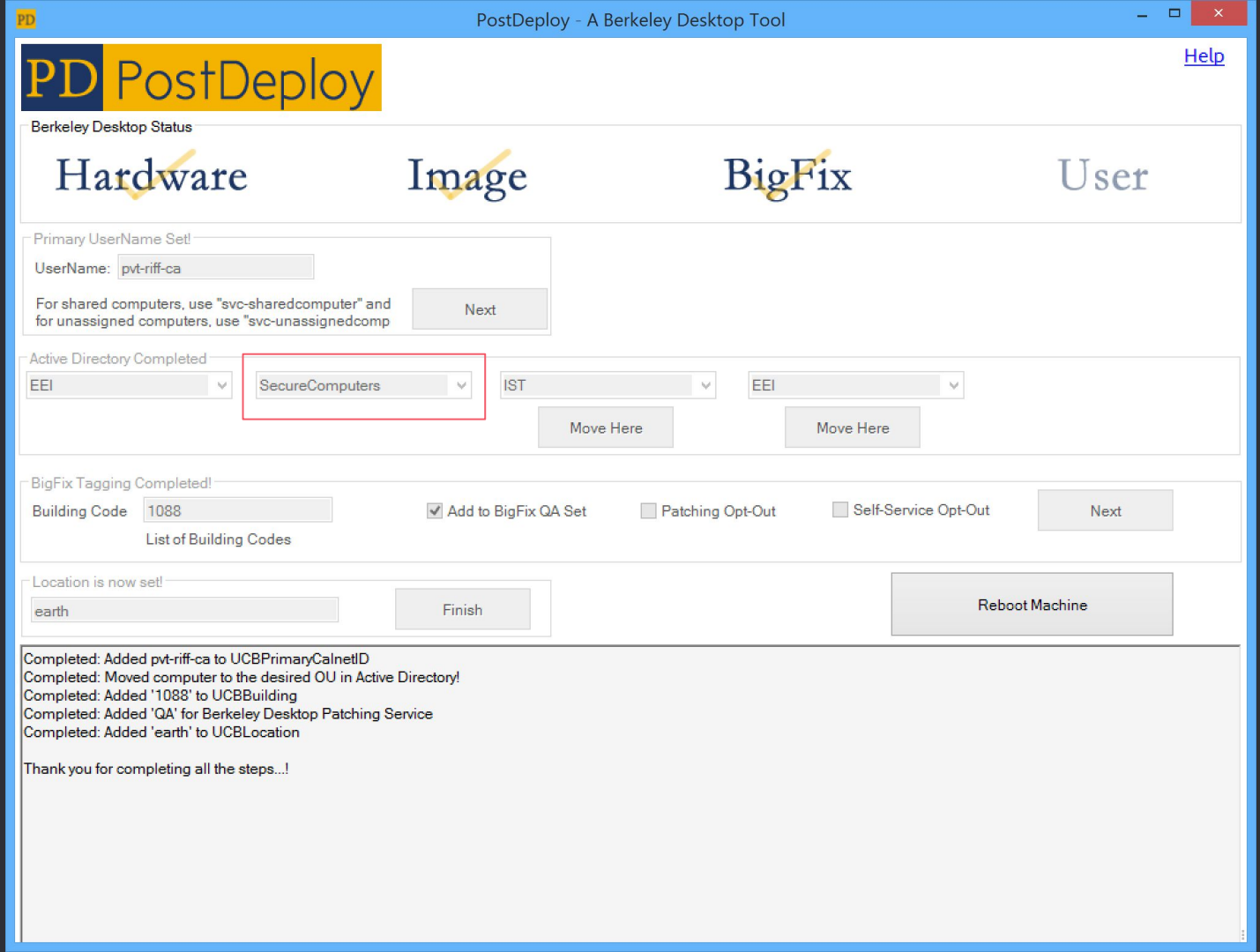
Member Action ID	Fixlet	Status
168777	<EEI Software Updates>: Adobe Creative Cloud Remote Update Manager (Windows)	Fixed
168790	Flash Player 20.0.0.267 Available - Plugin-based	Not Relevant
168791	Flash Player 20.0.0.267 Available - Internet Explorer	Not Relevant
168792	Mozilla Firefox 43.0.3 Available	Fixed
168793	Adobe AIR 20.0.0.233 Available	Fixed

3 Offer Control At the Edges

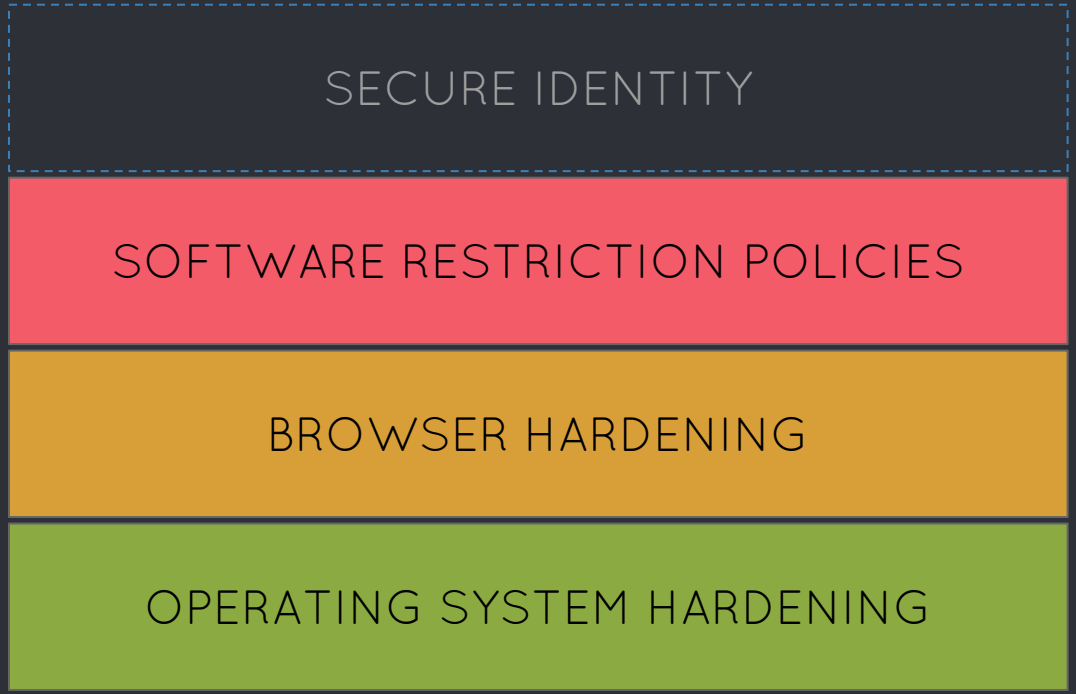
BERKELEY DESKTOP SELF-SERVICE

Self-Service for End Users	Self-Service for IT Staff
Productivity Software: Microsoft Office 2016	Beta Software Testing: Dell Command Update
Developer Tools: Notepad++	Standard Software Opt-Out: Citrix Receiver
Service Opt-in: Endpoint Backup	Reset Configuration: Enable Windows Store
Delegated Access: 30 minute Administrator Access	Configuration Opt-Out: 30 minute from AV

36,000
Self-Service Actions


PostDeploy - A Berkeley Desktop Tool
PD PostDeploy
Help
Berkeley Desktop Status
Hardware
Image
BigFix
User
Primary UserName Set!
UserName: pvt-riff-ca
For shared computers, use "svc-sharedcomputer" and
for unassigned computers, use "svc-unassignedcomp
Next
Active Directory Completed
EEI
SecureComputers
IST
EEI
Move Here
Move Here
BigFix Tagging Completed!
Building Code 1088
List of Building Codes
Add to BigFix QA Set
Patching Opt-Out
Self-Service Opt-Out
Next
Location is now set!
earth
Finish
Reboot Machine
Completed: Added pvt-riff-ca to UCBPrimaryCalnetID
Completed: Moved computer to the desired OU in Active Directory!
Completed: Added '1088' to UCBBuilding
Completed: Added 'QA' for Berkeley Desktop Patching Service
Completed: Added 'earth' to UCBLocation
Thank you for completing all the steps...!

MORE SECURE OPT-IN




WHAT
DIFFERENCE
DOES IT MAKE?!?

"This single project has saved UHS more computer admin time than any other project I've seen at the University in 20 years. You know it must be good if it makes a SysAdmin happy!"

Scott McCoy, University Health Services

4

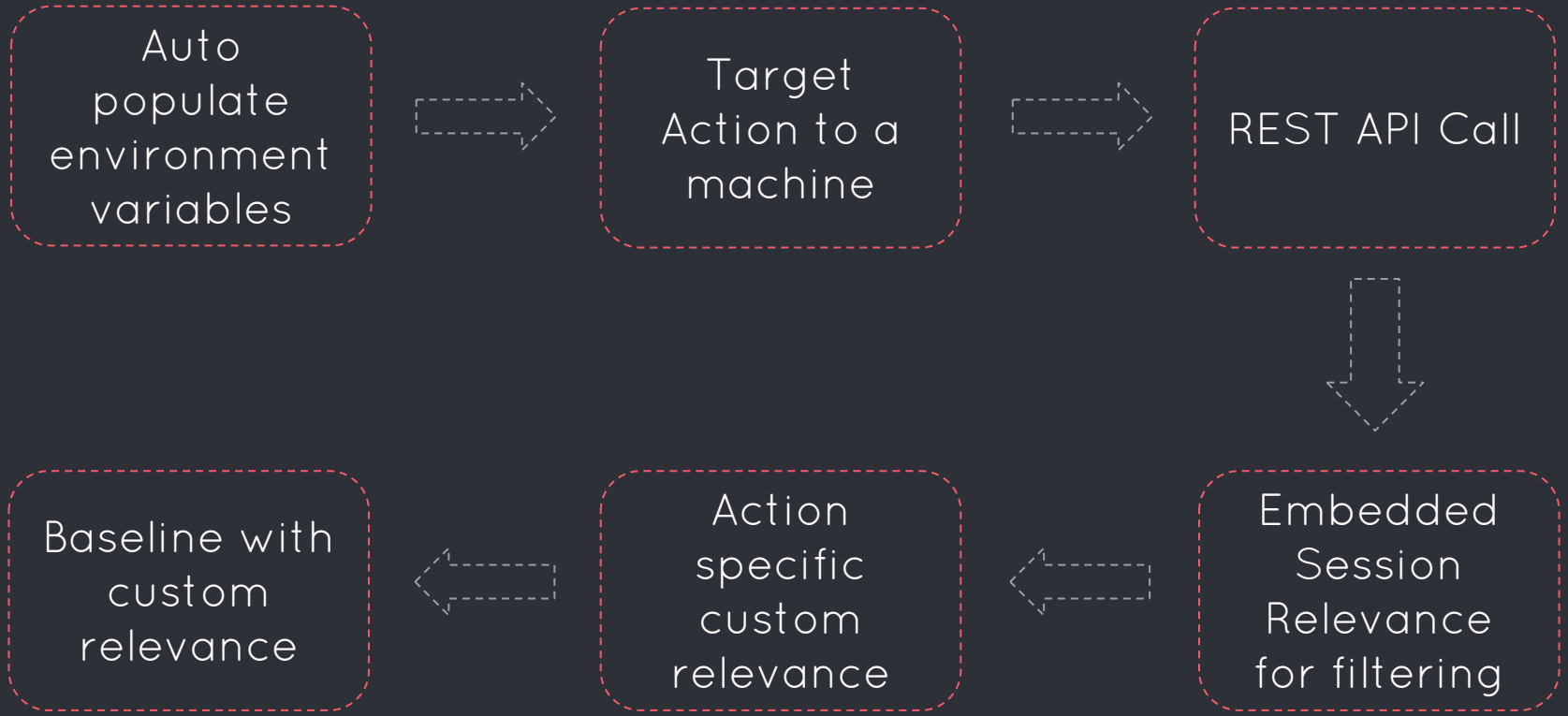
Automate All The Things

"Arbuckle's law... The actual compliance of an organization is in direct proportion to the degree to which its policies are expressed as code"

@dromologue

Justin Arbuckle

RESTFUL AUTOMATION:
Auto-generate Component Baselines



5

Measure All The Things

MEASURE: WHAT?

```
//Action Type
parameter "Type" = "Offer"

// Application Name
parameter "AppName" = "Office2016"

// Action Start Time for Reporting
regset "[registrylocation\{(parameter "AppName" & parameter "Type")}]"
"{parameter "Type" as string & "StartTime"}"="{now}"
```

APPLICATION SPECIFIC SCRIPT

```
// Action Pushed
regset "[registrylocation\{(parameter "AppName" & parameter "Type")}]" "value="
Yes"

// Action End Time for Reporting
regset "[registrylocation\{(parameter "AppName" & parameter "Type")}]"
"{parameter "Type" as string & "EndTime"}"="{now}"
```

MEASURE: WHO?

```
// Logins that Clicked on Self-Service

regset "[registrylocation\{(parameter "AppName" & parameter "Type")}]"
"OfferAcceptedBy"="{names of logged on users}"
endif
```

Accounts Clicking on Self-Service

Total Clicks: 19800
Clicks with Logged Account Name: 13150
Non-Administrator Logon Clicks: 8357
Administrator Logon Clicks: 4681
Unique PVT Accounts: 156

Current Self-Service Applications

Application Name	Number of Clicks
7Zip	1267
AdobeCC2015AcrobatProDC	398
AdobeCC2015AfterEffects	63
AdobeCC2015Audition	64
AdobeCC2015Bridge	79
AdobeCC2015Dreamweaver	131
AdobeCC2015EdgeAnimate	42
AdobeCC2015EdgeCode	38
AdobeCC2015EdgeReflow	38
AdobeCC2015ExtendScriptToolkit	37
AdobeCC2015ExtensionManager	43
AdobeCC2015FlashBuilderPremium	53
AdobeCC2015FlashProfessional	94
AdobeCC2015Illustrator	297
AdobeCC2015InCopy	54
AdobeCC2015InDesign	256
AdobeCC2015Lightroom	99
AdobeCC2015MediaEncoder	53
AdobeCC2015Muse	47
AdobeCC2015Photoshop	375

TAG START TIME

```
regset "[registry Location\{current month as string}]" "{"StartTime"} "="{now}"
```

BASELINE COMPONENTS

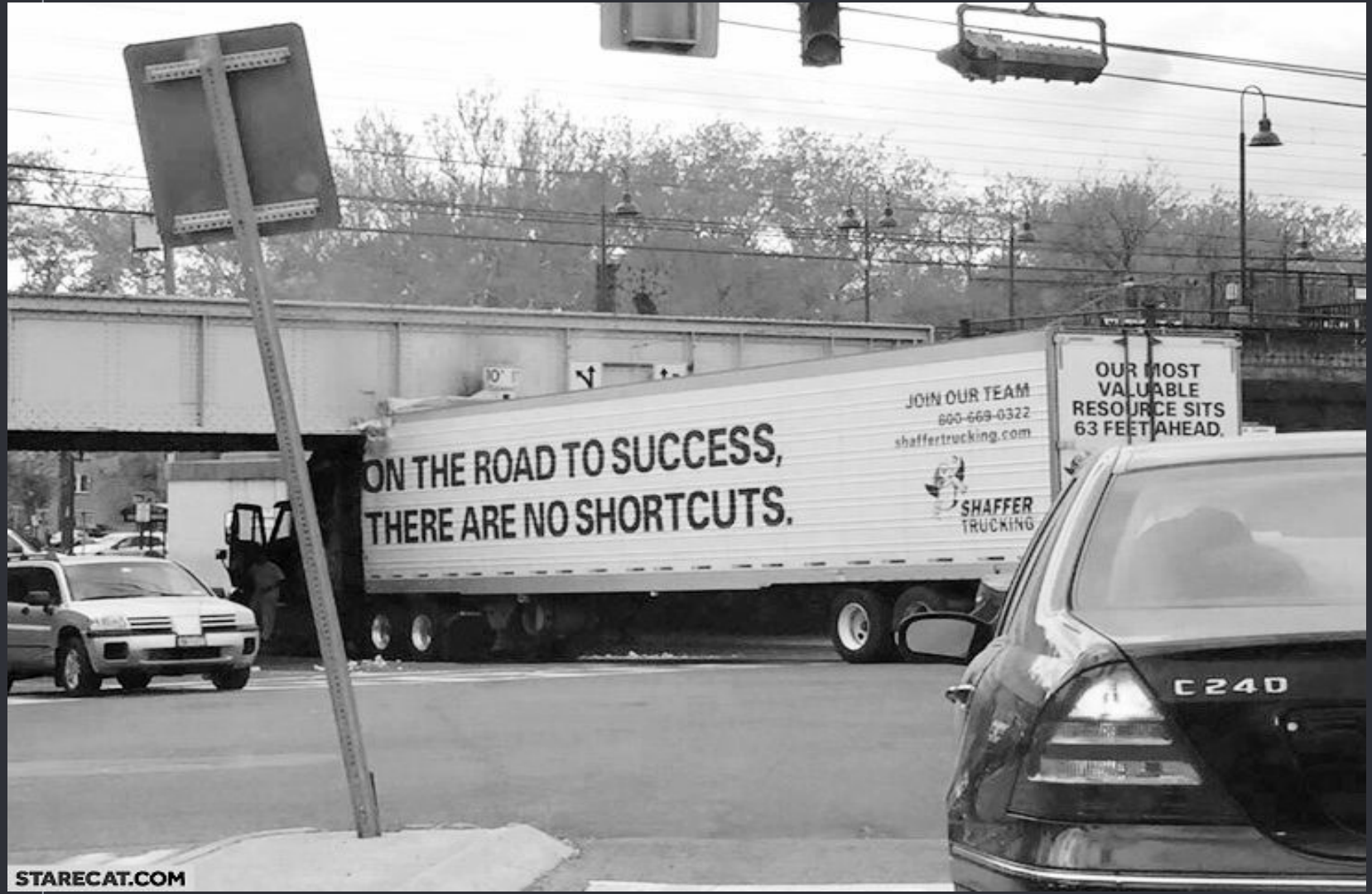
TAG END TIME

```
regset "[registry Location\{current month as string}]" {"EndTime"} "="{now}"
```

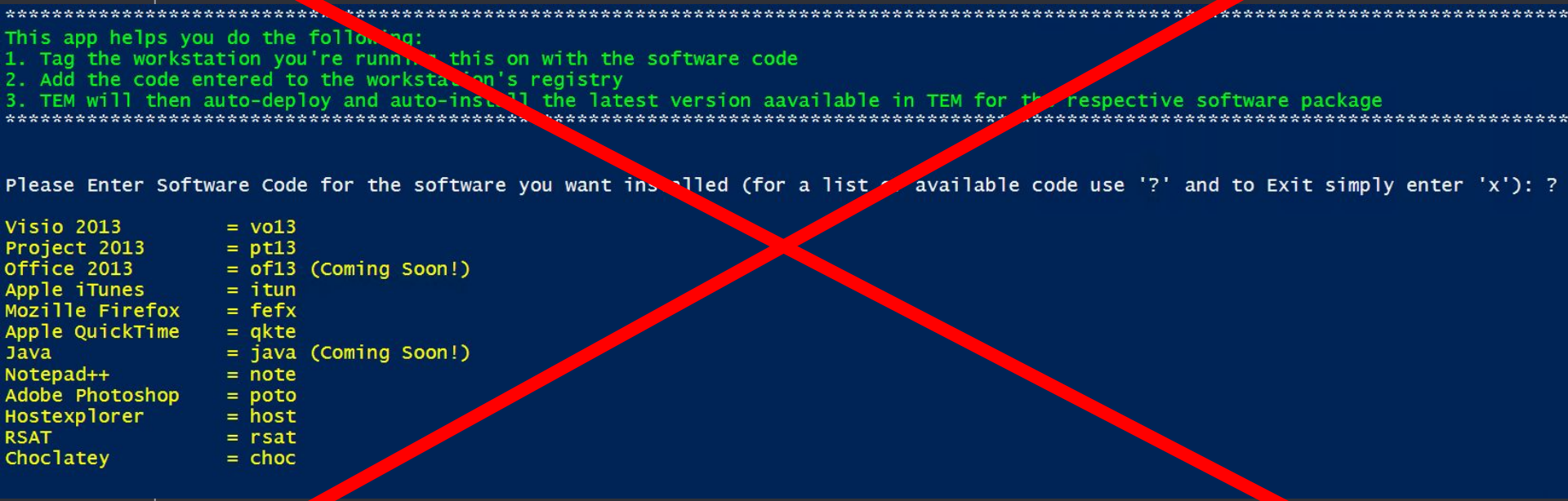
6 Iterate All The Things

"Continuous Deployment is an aspiration not an architecture."

David Woods, Professor Ohio State University


ON THE ROAD TO SUCCESS,
THERE ARE NO SHORTCUTS.
JOIN OUR TEAM
800-669-0322
shaffertrucking.com
SHAFFER
TRUCKING
OUR MOST
VALUABLE
RESOURCE SITS
63 FEET AHEAD.
C240
STARECAT.COM

FAIL FAST


This app helps you do the following:
1. Tag the workstation you're running this on with the software code
2. Add the code entered to the workstation's registry
3. TEM will then auto-deploy and auto-install the latest version aavailable in TEM for the respective software package
Please Enter Software Code for the software you want installed (for a list of available code use '?' and to Exit simply enter 'x'): ?
Visio 2013 = vo13
Project 2013 = pt13
Office 2013 = of13 (Coming Soon!)
Apple iTunes = itun
Mozille Firefox = fefx
Apple QuickTime = qkte
Java = java (Coming Soon!)
Notepad++ = note
Adobe Photoshop = poto
Hostexplorer = host
RSAT = rsat
Choclatey = choc

RECAP

- Set Secure Defaults
- Keep the Core Transparent
- Offer Control at the Edges
- Automate All The Things
- Measure All The Things
- Iterate All The Things

Thanks!

desktop.berkeley.edu

Questions...?

This slide

Intentionally left blank