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**

<table>
<thead>
<tr>
<th>Endpoints in BigFix</th>
<th>Users</th>
<th>Supported Business Units</th>
<th>Team Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>14000+</td>
<td>8000+</td>
<td>175+</td>
<td>10</td>
</tr>
<tr>
<td>11K Windows</td>
<td></td>
<td></td>
<td>8 Technical</td>
</tr>
<tr>
<td>3K Macs</td>
<td></td>
<td></td>
<td>1 PM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 Manager</td>
</tr>
</tbody>
</table>
SECURITY AS A SERVICE

- AUTO PATCHING
- CONFIGURATION MANAGEMENT
- MANAGED ANTIVIRUS
- AUDIT COMPLIANCE

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
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

NORMAL OS
  NTLM
  KERBEROS

SECURE CONTAINER
  NTLM SECRET
  KERBEROS SECRET

HYPER-V HYPERVISOR
MULTIPLE PATCHING SOURCES
Keep the Core Transparent
WALL OF CONFUSION
<table>
<thead>
<tr>
<th>ACTION</th>
<th>IMPACT</th>
<th>REASON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Announce all patch and configuration updates</td>
<td>Release Notes</td>
<td>Phone Call</td>
</tr>
<tr>
<td></td>
<td>CIRCUIT BREAKER</td>
<td>FEEDBACK LOOP</td>
</tr>
</tbody>
</table>
### Baseline Actions by Computer

#### Computer:

- **Baseline:** [EEI Master Baseline December 2015]: Windows OS + Applications

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

<table>
<thead>
<tr>
<th>Baseline Action ID</th>
<th>State</th>
<th>Issuer</th>
<th>Time Issued</th>
<th>Status</th>
<th>Additional Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>168599</td>
<td>Expired</td>
<td></td>
<td>2015-12-30 16:03:32 -0800</td>
<td>Fixed</td>
<td>The action executed successfully.</td>
</tr>
</tbody>
</table>

#### Statuses of Member Actions

<table>
<thead>
<tr>
<th>Member Action ID</th>
<th>Fixlet</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>168777</td>
<td>&lt;EEI Software Updates&gt;: Adobe Creative Cloud Remote Update Manager (Windows)</td>
<td>Fixed</td>
</tr>
<tr>
<td>168790</td>
<td>Flash Player 20.0.0.267 Available - Plugin-based</td>
<td>Not Relevant</td>
</tr>
<tr>
<td>168791</td>
<td>Flash Player 20.0.0.267 Available - Internet Explorer</td>
<td>Not Relevant</td>
</tr>
<tr>
<td>168792</td>
<td>Mozilla Firefox 43.0.3 Available</td>
<td>Fixed</td>
</tr>
<tr>
<td>168793</td>
<td>Adobe AIR 20.0.0.233 Available</td>
<td>Fixed</td>
</tr>
</tbody>
</table>
3 Offer Control At the Edges
<table>
<thead>
<tr>
<th>Self-Service for End Users</th>
<th>Self-Service for IT Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Productivity Software: Microsoft Office 2016</td>
<td>Beta Software Testing: Dell Command Update</td>
</tr>
<tr>
<td>Service Opt-in: Endpoint Backup</td>
<td>Reset Configuration: Enable Windows Store</td>
</tr>
<tr>
<td>Delegated Access: 30 minute Administrator Access</td>
<td>Configuration Opt-Out: 30 minute from AV</td>
</tr>
</tbody>
</table>
36,000
Self-Service Actions
MORE SECURE OPT-IN

SECURE IDENTITY

SOFTWARE RESTRICTION POLICIES

BROWSER HARDENING

OPERATING SYSTEM HARDENING
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

- Auto populate environment variables
- Target Action to a machine
- REST API Call
- Baseline with custom relevance
- Action specific custom relevance
- Embedded Session Relevance for filtering
Measure All The Things
// 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\}"

// 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: WHAT?
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

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Number of Clicks</th>
</tr>
</thead>
<tbody>
<tr>
<td>7Zip</td>
<td>1267</td>
</tr>
<tr>
<td>AdobeCC2015AcrobatProDC</td>
<td>398</td>
</tr>
<tr>
<td>AdobeCC2015AfterEffects</td>
<td>63</td>
</tr>
<tr>
<td>AdobeCC2015Audition</td>
<td>64</td>
</tr>
<tr>
<td>AdobeCC2015Bridge</td>
<td>79</td>
</tr>
<tr>
<td>AdobeCC2015Dreamweaver</td>
<td>131</td>
</tr>
<tr>
<td>AdobeCC2015EdgeAnimate</td>
<td>42</td>
</tr>
<tr>
<td>AdobeCC2015EdgeCode</td>
<td>38</td>
</tr>
<tr>
<td>AdobeCC2015EdgeReflow</td>
<td>38</td>
</tr>
<tr>
<td>AdobeCC2015ExtendScriptToolkit</td>
<td>37</td>
</tr>
<tr>
<td>AdobeCC2015ExtensionManager</td>
<td>43</td>
</tr>
<tr>
<td>AdobeCC2015FlashBuilderPremium</td>
<td>53</td>
</tr>
<tr>
<td>AdobeCC2015FlashProfessional</td>
<td>94</td>
</tr>
<tr>
<td>AdobeCC2015Illustrator</td>
<td>297</td>
</tr>
<tr>
<td>AdobeCC2015InCopy</td>
<td>54</td>
</tr>
<tr>
<td>AdobeCC2015InDesign</td>
<td>256</td>
</tr>
<tr>
<td>AdobeCC2015Lightroom</td>
<td>99</td>
</tr>
<tr>
<td>AdobeCC2015MediaEncoder</td>
<td>53</td>
</tr>
<tr>
<td>AdobeCC2015Muse</td>
<td>47</td>
</tr>
<tr>
<td>AdobeCC2015Photoshop</td>
<td>375</td>
</tr>
</tbody>
</table>
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.
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 available 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
Mozilla 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