Patching a Diverse Set of Campus Computer Labs Using LANDesk

Presenter: Matt Brooks

SUNY Oswego

The “About Us” Slide…

- State University of New York at Oswego
  - 8,000 undergraduate students/FTE + ~2000 Graduate
  - 1,700 full and part time Faculty and Staff
  - 60% PC/Windows Environment
- PC Platform: Dell
  - Latitudes – Laptop
  - OptiPlex – Desktop
  - Precision – High-end/specialized devices
- Approximately 1000 Lab & Instructional computers across the campus.

How Our Labs Traditionally Worked…

- DeepFreeze protection on all endpoints.
- Sophos Endpoint Management (AV) on all lab/instructional computers.
- Upon imaging a lab, both pieces of software installed. AV updated.
  - Machines then frozen and become static.
- In Windows XP & Windows 7 eras, we deployed image in Summer and left through fall semester. Thawed in winter (few updates), then frozen again through spring.
- For a long time, no enterprise management software. LANDesk then acquired in 2010.

First Attempts At Patching

- Once LANDesk became our management tool, we ensured all lab devices had an agent installed.
- We built out software distribution packages for third party applications such as Adobe Reader, Firefox, Flash, and Java.
- The packages would then be pushed to endpoints during break periods such as winter, spring break, and summer.
  - Note: *NO* OS patching was taking place in this process.
  - This process usually coordinated by one or two staff members.
- We continued to re-image every summer with updated configurations.

Flaws In The Process

- Operating System remained un-patched for ~6 months or more.
  - Labs are isolated on a different firewall zone but still presented… ***Security risk***!
- Endpoint protection engine and definitions never updated.
  - Sophos repeatedly tried to update on endpoints during the day. Performance hits!
- Package pushes not 100% reliable.
  - Depended on uniformity of images (not always the case!) & customizations.
- Timing of “patches” sometimes caused problems with the updates (usually just a software installer) not working.

CTS

Patching Using “Patching” Mechanism

- Using LANDesk Core & Agent on clients, set about using the “Patch & Compliance” portion of tool to determine what patches are needed.
- LANDesk Team set up a set of patches to go to Lab clients
  - Included OS and third party.
- Used our overnight “Maintenance Window” for Labs to push patches from the core server.
  - This relied on our clients being on and communicating at the time of pushes.
- Still saw a variety of results (success / failure rates) across various labs & image configurations.
- Multiple hands involved in the process (OS group vs. third-party group).

CTS

Problems We Saw!

- Multiple technicians attempting to coordinate different patches in the same window of time overnight.
- Mixed results on patches going out – some clients would install some but not others?!
- Reporting and accountability – no single point of contact.
- Some clients not communicating – bad Agents.

Revamp Our Workflow!

- Evaluate our patch process through the ITIL/ITSM Lens.
  - How can we ensure everyone knows what the process is this month?
- Accountable Technician (TSP)
  - Each month, cycle through the team and one person is the accountable tech for coordinating the patch cycle, deploying, and ensuring testing and reporting.
  - Involve entire team – Patch selection, testing
- Workflow changes: TSP test machines -> Pilot labs -> Campus
  - If problems are noted at test level, halt patching and evaluate!

Changes to Workflow

- Accountable TSP – prepare list of applicable patches in advance of a group meeting (TSPs, dept. techs, AV group rep, Manager)
- Documentation Using ServiceNow System:
  - Create a REQUEST that generates workflow set of tasks for Accountable TSP.
  - File a Change Management – approval by change group.
    - Enumerates all patches going out to campus lab/instructional computers, timeline, etc.
- Test Group: Each technician has a dedicated test machine for patch testing.
- Quality Assurance!
- Reporting – Accountable TSP sends reports to a patching-list email so all technicians are aware of various parts of the process and status.

Caveats…

- Accountable TSP is acting as a project manager – encouraged to actively push the team to do QA testing on Stage 1 and Stage 2 tests.
- We do have some clients that may be off or have various operational (agent or OS) problems and may not report.
  - Technicians are to review previous month's results and re-check problematic clients in advance of next cycle.
- Months we do not Patch!
  - August (start of semester approaching)
  - December (finals week)
  - April (finals & commencement approaching)
- We are ***not*** doing Feature updates through this process!
- Windows patching only – currently no workflow/process for Mac clients.

Change Request - CHG0030348

Follow | Update and Go Back | Save and Stay | Cop

Assigned to: Michael Schifano

Change Management Form | Notes

Will this change be performed by a vendor? ☐

* Who: Michael Schifano

* Will there be multiple technicians working on this change request? Yes

* Please list the additional technicians involved. David Kahn, Matthew Brooks, Christopher Palian, Ward Andres

* What (Short description): Install patches for Labs and ATCs

* Start Time: 05-19-2018 11:21:31

* Stop Time: 05-27-2018 11:21:37

* Why: As part of the montly patching process to adress updates and sercurity issues

* How: patches will be deployed remotely from the IEM server

* Impact: users may notice changes in the UI of applications that are patched. Patching will take place overnight so users will not be impacted by the actuall installation of the patches.

* Post-Implementation Testing Plan: The patching group will evaluate the patches in bench tests and pilot labs before the patches are deployed campus wide

* Backout Plan: if issues are fpund in testing we will not deploy the patches campus wide

* Does this change request require a campus announcement? ☐

Who is the accountable technician?

Michael Schifano

For which group of computers will the patches be installed?

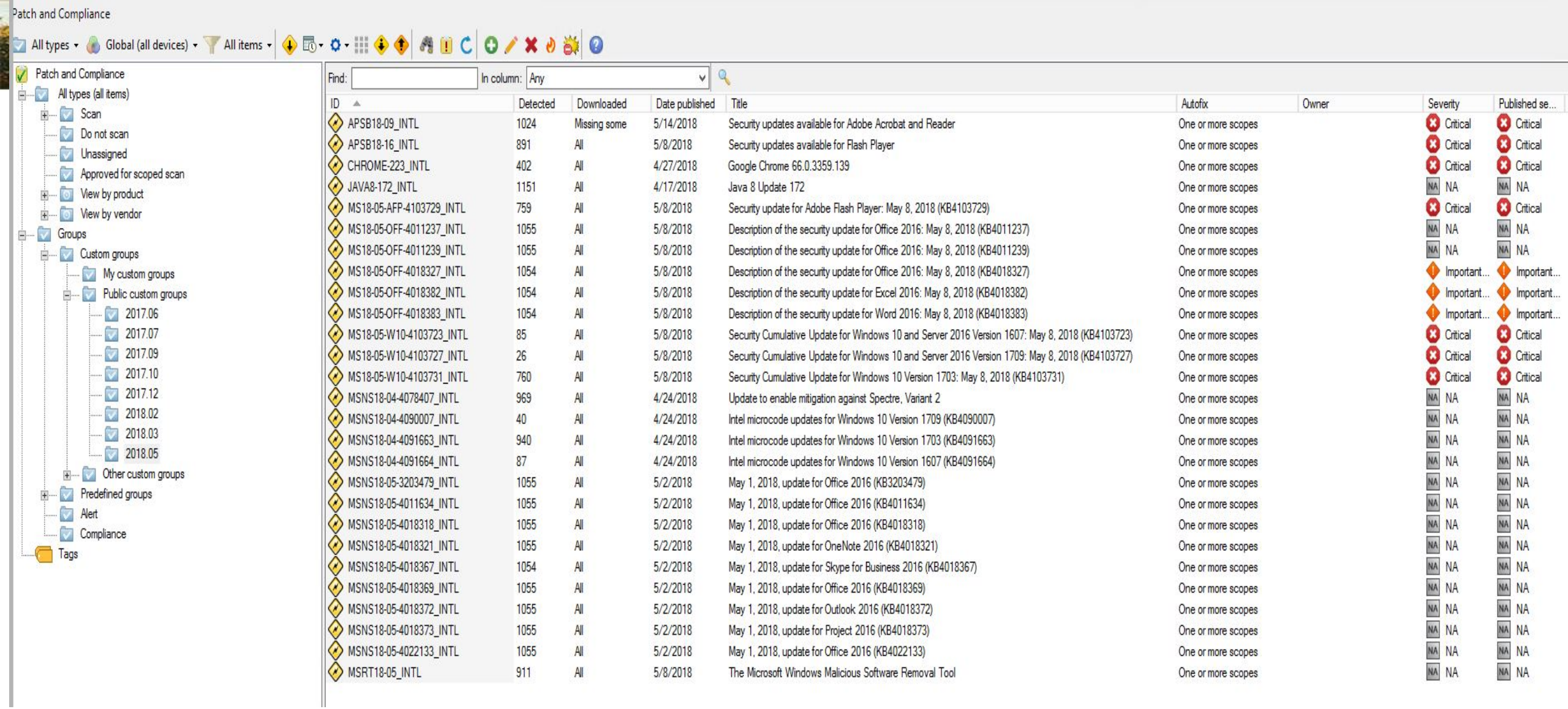
- (●) Lab/ATC Computers
- ( ) Faculty/Staff Computers
- ( ) Both

Please list the approved patches.

Security Cumulative Update for Windows 10 Version 1703: May 8, 2018 (KB4103731)
Security Cumulative Update for Windows 10 and Server 2016 Version 1709: May 8, 2018 (KB4103727)
Security Cumulative Update for Windows 10 and Server 2016 Version 1607: May 8, 2018 (KB4103723)
Description of the security update for Word 2016: May 8, 2018 (KB4018383)
Description of the security update for Excel 2016: May 8, 2018 (KB4018382)
The Microsoft Windows Malicious Software Removal Tool
Description of the security update for Office 2016: May 8, 2018 (KB4011239)
Description of the security update for Office 2016: May 8, 2018 (KB4011237)
Security update for Adobe Flash Player: May 8, 2018 (KB4103729)
Description of the security update for Office 2016: May 8, 2018 (KB4018327)
May 1, 2018, update for Project 2016 (KB4018373)
May 1, 2018, update for Outlook 2016 (KB4018372)
May 1, 2018, update for Office 2016 (KB4018369)
May 1, 2018, update for Skype for Business 2016 (KB4018367)
May 1, 2018, update for OneNote 2016 (KB4018321)
May 1, 2018, update for Office 2016 (KB4018318)
May 1, 2018, update for Office 2016 (KB3203479)
May 1, 2018, update for Office 2016 (KB4022133)
May 1, 2018, update for Office 2016 (KB4011634)
Google Chrome 66.0.3359.139
Intel microcode updates for Windows 10 Version 1607 (KB4091664)
Intel microcode updates for Windows 10 Version 1703 (KB4091663)
Intel microcode updates for Windows 10 Version 1709 (KB4090007)
Update to enable mitigation against Spectre, Variant 2

What is the number of the change request?

CHG0030348


Patch and Compliance
All types
Global (all devices)
All items
Patch and Compliance
All types (all items)
Scan
Do not scan
Unassigned
Approved for scoped scan
View by product
View by vendor
Groups
Custom groups
My custom groups
Public custom groups
2017.06
2017.07
2017.09
2017.10
2017.12
2018.02
2018.03
2018.05
Other custom groups
Predefined groups
Alert
Compliance
Tags
Find:
In column:
Any
ID
Detected
Downloaded
Date published
Title
Autofix
Owner
Severity
Published se...
APSB18-09_INTL 1024 Missing some 5/14/2018 Security updates available for Adobe Acrobat and Reader One or more scopes Critical Critical
APSB18-16_INTL 891 All 5/8/2018 Security updates available for Flash Player One or more scopes Critical Critical
CHROME-223_INTL 402 All 4/27/2018 Google Chrome 66.0.3359.139 One or more scopes Critical Critical
JAVA8-172_INTL 1151 All 4/17/2018 Java 8 Update 172 One or more scopes NA NA
MS18-05-AFP-4103729_INTL 759 All 5/8/2018 Security update for Adobe Flash Player: May 8, 2018 (KB4103729) One or more scopes Critical Critical
MS18-05-OFF-4011237_INTL 1055 All 5/8/2018 Description of the security update for Office 2016: May 8, 2018 (KB4011237) One or more scopes NA NA
MS18-05-OFF-4011239_INTL 1055 All 5/8/2018 Description of the security update for Office 2016: May 8, 2018 (KB4011239) One or more scopes NA NA
MS18-05-OFF-4018327_INTL 1054 All 5/8/2018 Description of the security update for Office 2016: May 8, 2018 (KB4018327) One or more scopes Important... Important...
MS18-05-OFF-4018382_INTL 1054 All 5/8/2018 Description of the security update for Excel 2016: May 8, 2018 (KB4018382) One or more scopes Important... Important...
MS18-05-OFF-4018383_INTL 1054 All 5/8/2018 Description of the security update for Word 2016: May 8, 2018 (KB4018383) One or more scopes Important... Important...
MS18-05-W10-4103723_INTL 85 All 5/8/2018 Security Cumulative Update for Windows 10 and Server 2016 Version 1607: May 8, 2018 (KB4103723) One or more scopes Critical Critical
MS18-05-W10-4103727_INTL 26 All 5/8/2018 Security Cumulative Update for Windows 10 and Server 2016 Version 1709: May 8, 2018 (KB4103727) One or more scopes Critical Critical
MS18-05-W10-4103731_INTL 760 All 5/8/2018 Security Cumulative Update for Windows 10 Version 1703: May 8, 2018 (KB4103731) One or more scopes Critical Critical
MSNS18-04-4078407_INTL 969 All 4/24/2018 Update to enable mitigation against Spectre, Variant 2 One or more scopes NA NA
MSNS18-04-4090007_INTL 40 All 4/24/2018 Intel microcode updates for Windows 10 Version 1709 (KB4090007) One or more scopes NA NA
MSNS18-04-4091663_INTL 940 All 4/24/2018 Intel microcode updates for Windows 10 Version 1703 (KB4091663) One or more scopes NA NA
MSNS18-04-4091664_INTL 87 All 4/24/2018 Intel microcode updates for Windows 10 Version 1607 (KB4091664) One or more scopes NA NA
MSNS18-05-3203479_INTL 1055 All 5/2/2018 May 1, 2018, update for Office 2016 (KB3203479) One or more scopes NA NA
MSNS18-05-4011634_INTL 1055 All 5/2/2018 May 1, 2018, update for Office 2016 (KB4011634) One or more scopes NA NA
MSNS18-05-4018318_INTL 1055 All 5/2/2018 May 1, 2018, update for Office 2016 (KB4018318) One or more scopes NA NA
MSNS18-05-4018321_INTL 1055 All 5/2/2018 May 1, 2018, update for OneNote 2016 (KB4018321) One or more scopes NA NA
MSNS18-05-4018367_INTL 1054 All 5/2/2018 May 1, 2018, update for Skype for Business 2016 (KB4018367) One or more scopes NA NA
MSNS18-05-4018369_INTL 1055 All 5/2/2018 May 1, 2018, update for Office 2016 (KB4018369) One or more scopes NA NA
MSNS18-05-4018372_INTL 1055 All 5/2/2018 May 1, 2018, update for Outlook 2016 (KB4018372) One or more scopes NA NA
MSNS18-05-4018373_INTL 1055 All 5/2/2018 May 1, 2018, update for Project 2016 (KB4018373) One or more scopes NA NA
MSNS18-05-4022133_INTL 1055 All 5/2/2018 May 1, 2018, update for Office 2016 (KB4022133) One or more scopes NA NA
MSRT18-05_INTL 911 All 5/8/2018 The Microsoft Windows Malicious Software Removal Tool One or more scopes NA NA

After Patching

- Accountable TSP leads a patch debriefing review
  - Shares reports/results for campus-wide deployment.
  - Possible issues in patching – reviewed / Discussion
- Any problems with the workflow?
- Our ongoing target is to always reach 90%+ of lab and instructional clients.
- Since we began this new workflow, we've managed to hit 90% of targets in almost every instance.

Improvement?

- Over the span of a few years, we went from virtually no patching or updating to a well-planned & executed ITSM-based process for deploying updates.
- Accountability!
  - One person coordinates the entire process to ensure it's smooth!
- Reporting!
  - We are able to get detailed information about our clients – good and bad!
- Communication!
  - Everyone is aware of what's going on.
- Security!
  - We are patching Windows! Much less risk of exploits in our environment.

CTS

It’s a Wrap!

- Questions / Comments ☺
  - Matt Brooks
Technology Support Professional
SUNY Oswego
matt.brooks@oswego.edu
315-312-2998