Consider: Whitelisting to mimic that portion of VDI environment

One advantage (and limitation) of CIT's Virtual Desktop service is that they limit what applications you can run, limiting you to the only the applications they host. (You can package apps for them to host.)

See also

- Consider: Migrate select staff to CIT's Desktop Everywhere
- Evaluate CIT's Desktop Everywhere on Dell Wyse all-in-one system

AWL: Application White Listing

Topic	VDI service	Today's staff desktops	Desktops with white-listing
Application white listing.	100% white listing. If CIT hasn't allowed it, it won't run. • Even run-alone apps won't work unless permitted (such as putty.exe). • CIT makes tools available so IT professionals can use to package (and maintain) any application, which CIT then hosts.	If Admin access required for an install, most end-users can't install new software. However, if software can just be used without installation, user can run it. For example, Putty.exe will work.	Can run in audit-only mode to first learn of potential impact. See below idea for more.
Ensuring work files are backed up.	Integrated into the service. VDI has robust end-user file storage.	Varies. Users might have work data only on their desktop. And that data might not be backed up. Users could be disciplined about only having work data on file shares, cloud storage, and the like. Users who must have unique locally stored data could work to ensure those files get automatically backed up. IT could start using Folder Redirect for Windows systems.	Same as with "Today's staff desktops".
Ensuring work files are accessible by others if person is out.	Same as with "Today's staff desktops".	See answer in "Ensuring work files are backed up." for this column. If files should be able to their supervisor and others, user must be deliberate about making them accessible when using a files share, cloud storage, and the like.	Same as with "Today's staff desktops".
Staff desktop environment is accessible anywhere, even if their office computer hardware is no longer working or accessible (fire, flood, theft, snow emergency, etc.)	No problem. No matter what happens to a user's workspace, their desktop is hosted by CIT and available via any browser or thin-client capable networked computer anywhere, anytime.	Problem! But how likely is this scenario worth protecting against? Answer might depend if files are on a file share, sync'd to a cloud service, or otherwise not isolated to the desktop computer. If files backed up, less convenient.	Same as with "Today's staff desktops".

Idea: Run whitelisting on existing systems, perhaps focusing first on those we believe could be moved to VDI

Why do this at all?

- To reality-check some of the issues involved in moving to VDI, and 100% white listing environment.
- Represents the potential to capture some of its benefits of moving to VDI, but without having to move at all.
    - No other changes for users would be necessary. Users keep their systems as they are, with their current applications and set-ups, and using their current Windows OS version.
- It's something that will also work for Mac OS, unlike VDI which is Windows only. Assumes appropriate tools can be found for Mac.
- Even if just monitoring, and not actually blocking, we'd have clarity and visibility on all the applications being run on monitored computers, whether applications were installed by IT or not.
    - Are there apps we should be installing because they are needed by we don't know about them?

Considerations for not making this investment

This will not reduce support calls for the computers we would be able to add white listing to because such calls are basically down to zero now.

- One reason this is so is that all those systemsl require Admin access to add new programs, and end-users don't generally have this authority.
- However, laptop users tend to have an Admin account. Adding whitelisting (even if just a warning or monitoring) could afford some protection.

This will not provide some of the other advantages of moving to VDI.

- See topics in the above table, other than, "Application white listing."

Phases

Phases can help us think about advantages of this approach:

Phase 1: Learn tools available and what apps are being used today

- Can run in audit-only mode to first learn of potential impact.

Phase 2: Have users approve or reject any non-listed apps

- Chemistry IT then reviews all approved ones for consideration of adding to the white list.

Phase 3: Perhaps not do, but possible: Only allow whitelisted applications to work (same as CIT's VDI service does)

- Users have to wait until Chemistry IT approves any new application requested.

Oliver's idea tool

For IT Admins:

Great Admin interface letting one see unauthorized apps, by user/ machine.

Run through a "clean", newly imaged system with representative applications to build whitelist.

Easy to add new application to whitelist. Easy to approve updates to already whitelisted apps.

Have approved application apply to applilcation's files, etc.

Approval based not just on name. Maybe a hash, publisher, etc.

User experience

For phase 1

Record all non-whitelisted apps.

For phase 2

User launches app:

- If app whitelisted, launches per normal.
- If app not whitelisted, user advised app is not whitelisted and given options:

    - Launch the app. In which case that gets recorded and sent to Admin console for IT follow-up. Including considering adding it to the central whitelist.
    - Cancel the app launch because not app user wanted.
    - Optional option Cancel the app, but permit meta-data of app sent to Admin console for IT follow-up. Including conversation with user on what their needs are. Consult: Options, alternatives, licensing, etc.)

For phase 3 (if done at all)

User launches app:

- If app whitelisted, launches per normal.
- If app not whitelisted, user advised app is not whitelisted and launch stopped.

Technical implementation ideas

In many ways, CIT's VDI service allows less control than having Faronics's DeepFreeze on a computer. And DeepFreeze can prevent necessary updates. But what about Faronics's Anti-Executable Enterprise, if Microsoft's solutions (AppLocker, Device Guard) don't meet our needs?

- http://www.faronics.com/products/anti-executable/enterprise/

Resources

Wyman at ITSO wrote, 2/18/16:

- What we're trying to license for Cornell instead of an antivirus product is an application whitelisting product -- Bit9 (now Carbon Black), to be exact. These things are the inverse of antivirus. They work by enumerating exactly what's allowed to run and denying everything else. Known malware, unknown malware, new application software (unfortunately), exploits, you name it, if it's not on the allowed list, it doesn't go. The support issues, predictably, can be intimidating on unregulated end-user desktops. But on well managed desktops, or servers, it's extremely effective. Far more than antivirus could possibly be.

Faronics's Anti-Executable Enterprise:

- http://www.faronics.com/products/anti-executable/enterprise/

Lock down Windows 10 to specific apps:

- https://technet.microsoft.com/en-us/library/mt592642%28v=vs.85%29.aspx

  Microsoft AppLocker overview:

    - https://technet.microsoft.com/en-us/library/hh831440.aspx

  Microsoft Device Guard overview:

    - https://technet.microsoft.com/en-us/library/dn986865(v=vs.85).aspx

Top 10 Common Misconceptions About Application Whitelisting (FEBRUARY 19, 2014)

- http://resources.infosecinstitute.com/top-10-common-misconceptions-application-whitelisting/