Project Management Office
UC Information Technologies (UCIT)
University of Cincinnati
PO Box 210658
Cincinnati, Ohio 45221-0149

Suite 400, University Hall
51 Goodman Drive
(513) 556-9089

MEETING MINUTES
IT MANAGERS COMMITTEE

DATE: NOVEMBER 12, 2013
TIME: 9:30 PM TO 11:00 AM
LOCATION: UNIVERSITY HALL, RM 454
CHAIR: DOM FERRARI AND ERMA FRITSCHE

CALL TO ORDER

Dom Ferrari opened the meeting and introduced Bruce Burton, Associate Director, from Telecommunication and the NOC. Bruce was hosting a MDM product by the Airwatch team.

Present: There were several people in attendance so to save time for the demonstration, Airwatch asked for the names of departments/colleges in the room in lieu of formal roll call or introductions. There were representatives from: AFIT, Law College, Athletics, A&S, Libraries, UC Clermont, UCBA, LCOB, CEAS, CECH, and CAHS.

BUSINESS

Airwatch provided a demonstration of their mobile device management tool (MDM). It is the mobile app security program being piloted by CoN. They gave a brief background on the development of MDM/BYOD policies and applications, from the evolution of the Blackberry to Apple mobile devices, with no central management. As mobile devices began to proliferate, IT staff complained of death by a 1000 cuts from managing them.

With the paradigm shift in security technology, Airwatch now leverages links pushed out to users to allow them to manage MDM control and security. Their app allows users to authenticate, IT staff to set permission levels, control devices from a centralized management point, etc., which enables the IT staff to better manage the security and usability for devices that fall within their organizations' BYOD responsibilities. Jason, the presenter, said Airwatch is the world's largest provider and offers the most scalable solution for MDM. They make providing support for IT and Held Desk staff easier with a combination of architecture and providing a scalable product. They have surpassed supporting more than 40,000 devices.

The demonstration lasted for about an hour and some of the features they highlighted are listed below. At the end of the demonstration, the vendor opened the floor for a 20 minute question and answer session. Following the Q&A session, Dom spent the last 15 minutes for announcements and asked committee members for updates of projects previously discussed in the IT Managers committee (see announcements and updates below) meetings.

Features Airwatch Highlighted in their Demonstration

- Can push down configuration to mobile devices based on access and permissions based on login ID. For example, library loan equipment can have policy assigned with each new login. Devices with permanent owner won't require new policy with each login.

- Every device can be seen on a control panel for IT and Security staff but can also drill down to specific devices details from main management page.

- Supports different use cases, for example, iPad program in Athletics, branch campuses, for different security levels for Law school students. Policies can be global or can get as granular as needed by college/department/unit.

- Can configure dashboard to only see devices that are out of compliance, certificate expiring, etc.

- Can see when device last checked in, from where, enrolled in Airwatch or jail broken or if it is fully compliant device.

- Can see devices' active certificates, mac address, battery life,

- Tool bar notes specific issues about the configuration of the device, shows which apps sit on the device, whether UC owned or personally owned. Offers tracking abilities, can remotely send info to devices, reset password, or can do enterprise wipe if needed, or just wipe some data (take work info off, leave personal info on). GPS tracking can be blocked according to University policy. Can hold data for up to 30 days via Airwatch settings for tracking/privacy purposes, but is configurable by UC, can do full or selective wipe of data. Can prevent even IT admin from doing full wipe on personally owned devices to avoid mistakes.

- Can give UC the 50,000 mile overview or the need to fully manage every device (full god rights). Any feature can be turned on or off for selective IT admins based on role.

- Can require a 4 digit password etc.

- Can be configured so that each unit looks like it is its own entity, multi-tenant architecture.

- Every unit can have custom branding

- Offers auto compliance with drop down lists for configuring compliance rules, blacklist/whitelist apps, can blacklist apps for HIPAA FERPA compliance on med campus. Can have multiple approaches to alert individual device owner of compliance issues. Can send emails, pop up messages, like IOS device out of compliance, then can selectively start removing access to force user back into compliance. This is operational scalability and can be configured to automatic at initial configuration.

- Can setup multiple Wi-Fi profiles, for downtown, branch campus, main campus, setup for VPN, etc.

-
- Raul (Airwatch rep) explained that security certificate can tie into our systems to leverage certificate control, and can lock students into specific apps, can lock down device in the room only if needed.

- Students can remove Airwatch profile, but they lose all granted access. Enrollment and compliance can be configured as requirements for network access.

- App development issues – can select apps you want to send or make available, set in console controls, by group, college, can send push auto with a notice that says UC would like to install this app, or just be available for user selecting in an app catalog.

- Can provision access to be managed by Airwatch. Include terms of use, like no GPS tracking, if a user declines use then they will not be able to install app. Can push apps out by AD, etc.

- Able to run analytics and get feedback from users, leverage proxy to access devices behind firewall. Can introduce authentication auto-wrapped by Airwatch app so that developer does not need to write authentication into the program.

- Splash page can be tailored to user, so they only see their device. Can GPS track device if it is lost, forgotten, wipe sensitive data if needed, reset password remotely, etc.

- Airwatch can push out any app/security content down to devices, securely connect to clouds, LMS, CMS systems, with all security policies in place. Can disallow opening 3rd party emails for example to avoid viruses. Can make an app available for specific time periods, like for a test, and will notify students of time constraints while locking it down to the specific app.

Q&A Session

Question: What about the order of precedence for conflicting policies, global vs. department level?

Answer: Can be configured at granular level.

Question: Does it have the ability to set subscriptions for reports to generate and send automatically?

Answer: Yes.

Questions about profile building for MDM.

Answer: Can configure profiles to be time sensitive, so one policy for on campus hours and no policy for off campus hours. Example, policy 8 am – 5 pm, then drop it for personally owned devices after 5 pm.

Also can be pushed out to specific devices too, just to IPads, etc., like for Athletics, User group = LDAP users. Example, can send out policies to seniors only, etc.

Question: What if device is too old and cannot connect or doesn't have enough memory.

Answer: It just doesn't push down to old devices, latest versions of software will send a message notification that this device cannot be enrolled in this program. Can have different work flows for integrating devices.

Question: What about device bandwidth limits and unauthorized access for some applications?

Answer: Airwatch has very thin profile so does not take up much memory, the application will stop and notify user that device can't accept app that was requested. Is it logged that an app didn't successfully download? Answer: yes. Can also pull back apps on IOS v.7. Licenses can also be reallocated in v.7 too. Can choose to let end user back up or not, configurable by IT admin. Similar features on Android devices as well.

Question: LDAP directories, can child group override setting?

Answer: Is possible but with the caveat that it causes some limitations in authenticating.

Airwatch does not integrates with Bb yet but they are working with Bb to develop it. Devices can be configured for a one-time policy check in if a device is assigned to an individual, or can be configured for every new login for devices in a loaner programs.

Question: Where is the check in check out policy clarification?

Answer: From the control console.

Question: Can it see secure wireless?

Answer: Airwatch recognizes if the device and user has access for wireless and allows device connection or launches a browser to allow enrollment.

Question: What about employees who have multiple roles, such as staff during the day, student at night?

Answer: Only 1 active MDM profile at a time on a device. Use case - Airwatch IOS devices limit to 1 MDM profile but Airwatch created a containerized workspace to enable management of more than 1 profile over the restriction of the IOS device. Can we have multiple containers? Depends on IOS operating system backend, but when possible it is transparent to end user. Can show up as an app icon on desktop to create multiple containerized profiles for managing multiple roles.

Question: Can documents/content be shared between devices?

Answer: Yes, it has a content locker with multi-collaboration tools, read only, edit, etc., and tracks actions that have been done on document.

Question: What's the motivation for the end user:

Answer: Offers lots of apps easily available, acts like helpdesk feature for new employees, stuff just works to end user because all work is done by IT behind the scenes….is highly configurable. Can wipe lost devices, can track devices. Works with apple TV. Has lock down capability balanced with app availability. Airwatch is partnering with Pearson and other text book publishing companies.

Question: Can Airwatch be used for GPS tracking for crime related issues?

Answer: GPS tracking is always available but not always visible to IT admin if configured that way. Can set policy for MDM as opt in or opt out for crime issues. Does it offer admin access to individual devices? No, only to groups. Can set it to notify…MDM was not developed for crime/law enforcement purposes, but can be used with opt in or opt out policies, like for finding lost device, find my iPhone, iPad app, etc.. It can wipe all devices in a specific group at one time or block all apps at one time, is highly configurable. However, these features can be blocked even from IT admins to avoid accidental blocking or wiping.

At the end of the demonstration, Diana Noelcke said Airwatch would not be rolled out as an enterprise tool until the associated security and compliance policies are established. UCIT is working with UC legal and others to develop them now. Airwatch offered to help with that. They have a tool kit available for customers for developing policy and can share it with UC.

Data Center Update

We aren't currently connected to the CARE generator, but we will be after the planned shutdown. The shutdown will occur on 12/29. It will start on evening of 28th at about 8 pm. Electricians will work 8 – 12 hours to install the new UPS and generator, and then UCIT will reverse the shutdown process. When complete, we will have generator protection for the data center. Email announcements will go out soon and UCIT will make specific unit contact as well.

Erma requested that communication be sent sooner rather than later since people leave for vacation well before the shutdown date.

McAfee ePO Update

Bo said the consultant has been on site the past 2 weeks and encryption is enabled now but MAC is not supported yet. Bo will send out communication with update when it is. He will send out more information. Dom said AFIT consolidated with enterprise ePO for the pilot and they see immediate benefits. Contact Matt Williams for assistance and more info will be forthcoming from OIS. Matt also has documentation to share.

Mass Storage Update

Don Rainwater will have a report by the end of the week and will share it with this committee. Another update from Don, concerning the hardware availability relative to the demo today is the Apple Software Volume Purchase Program (ASVPP). This program allows UC departments to purchase iOS apps and iBooks using UC funds. Interested parties should contact Don for details or call him at 556-9020.

UniverSIS Update

Pat Krekeler and Gary Grafe will present status of UniverSIS replacement project at December meeting.

HIPAA, FERPA, etc., Data Security Compliance Update

Bo said the University asked for a penetration test. Office of Information Security (OIS) will be performing scans on public facing machines the week before data center outage. This is just heads up, it is called penetration but is really a vulnerability test. Bo will reach out and contact departments but it should NOT be a disruption. It is a best practices type scan; a good opportunity for us to see where we have vulnerabilities. Dom said we still need to meet external auditor's standards and this penetration scan will help make sure we are in compliance.

Dom told the group that he will post the agenda for December meeting and encouraged all to add items for discussion on the draft agenda. This is the mechanism they should use for bringing issues and ideas to the committee.

ACTION ITEMS

- Diana Noelcke – Follow up with Airwatch to review their policy toolkit to see if it is useful for UCIT.
- Don Rainwater – Share mass storage update report with committee members next week (week of 11/18).
- Don Rainwater – Send out data center shutdown notices in early December before IT staff leave for vacations.

ADJOURNMENT

November 12, 2013 11:00 AM