Secure Use of VDI in a PCI Compliant Environment

08/23/2018

Dan Flynn

Senior Desktop Services Engineer

BOSTON UNIVERSITY

Overview

- Client: Development and Alumni Relations
- Replace aging Telefund calling system
  - Outbound calling system tied to Alumni systems
- 1 Billion Dollar Fundraising Campaign
- 117,000 Donors
- Giving Day: 11,000 gifts in 24 hours
- First meeting June 2014

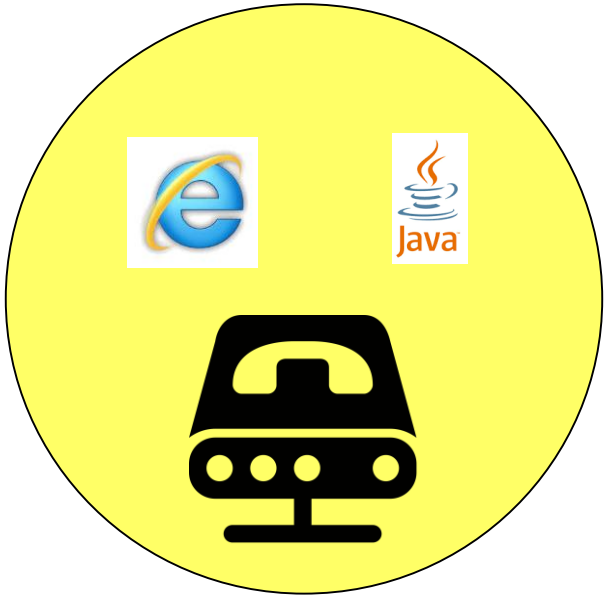
The Campaign for Boston University | CHOOSE TO BE GREAT

BOSTON UNIVERSITY

Overview of old environment

- Windows XP desktops
- USB Modems
- On-prem Servers
- Restricted network
  - Highly restrictive ACLs
  - Non-internet routable
- Manually configured stations
  - Lots of tweaking

Business requirements



- In browser VoIP
- Java based
- IE 11
- Enter credit card numbers on stations
- 20 calling stations
- Browse internet to lookup info while talking with donors
- Access Google drive/apps for call scripts and documentations
- Go Live August 2014 (~ 2 months)

What to do????

2 Computers

- Loss of screen space
- KVM or two Mice/Keyboards
- More network Jacks
- Maintenance
- Switching back and forth

Secure VDI VM

- Voice delay
- VM then in PCI scope
- High risk of outage

Say No

- Not an option
- Revenue impacting
- Current environment EOL
- Time crunch

BOSTON UNIVERSITY

What did we do?

- Extremely locked down Lenovo Tiny Desktops
- Cisco ASA 5506 NAT Firewall
- VMware Horizon Non-persistent VDI Desktop


NEWS BOARD
QUOTE BOARD


current rank on U.S.News
3 ASKS.
EVERY SINGLE TIME.
NO EXCEPTIONS.
Payroll
Questions?
PCI:
PAYMENT CARD INDUSTRY
FISCAL YEAR
2019

Windows Image Build

- Microsoft Deployment Toolkit (MDT)
  - Capture/Deploy
- Plain Windows 7 Enterprise
  - VMware Horizon Client/Java/McAfee/Kace Agent
  - No additional software
- Security Compliance Manager
- Tons of Group Policies
  - Software Restriction Policies
  - Disable As much of the UI as possible
- Internet Explorer Administration Kit (IEAK)
  - Content Ratings
  - Only approved sites

VDI Setup

- Leveraged existing VMware Horizon environment
- Standard Non-Persistent VDI Pool
- Public Internet Access
- Documentation Shortcuts
- Group Policy to force configure client

vmware Horizon

How has it been going?

- Java issues
  - Updates
  - Auto configuration
  - Certificates
- Vendor outages
- Desktop failure
  - Spare units swapped in
  - Excess stations
- Upgrade VDI environment x2
- Update browser restrictions
- Expansion
  - More stations
  - Agganis Arena
    - Same basic setup different software
  - Gifts & Records/Alumni Relations
    - Same desktop setup
    - No VDI used KVMs (used less)

Future Steps

- Windows 10
  - Security Compliance Toolkit
  - App Locker
- P2PE Keypads
- Computer Replacements
- Java?????

Lessons Learned

- Get involved during product selection phase
- Flexibility in setup for future use cases
- Build change into the system
- Secured from the beginning


Q
A