



## Increasing Security by Focusing on the Endpoints

Brandon DeLeeuw, Director of Client Solutions and Support, [bdeleeuw@uncc.edu](mailto:bdeleeuw@uncc.edu)

UNC  
CHARLOTTE



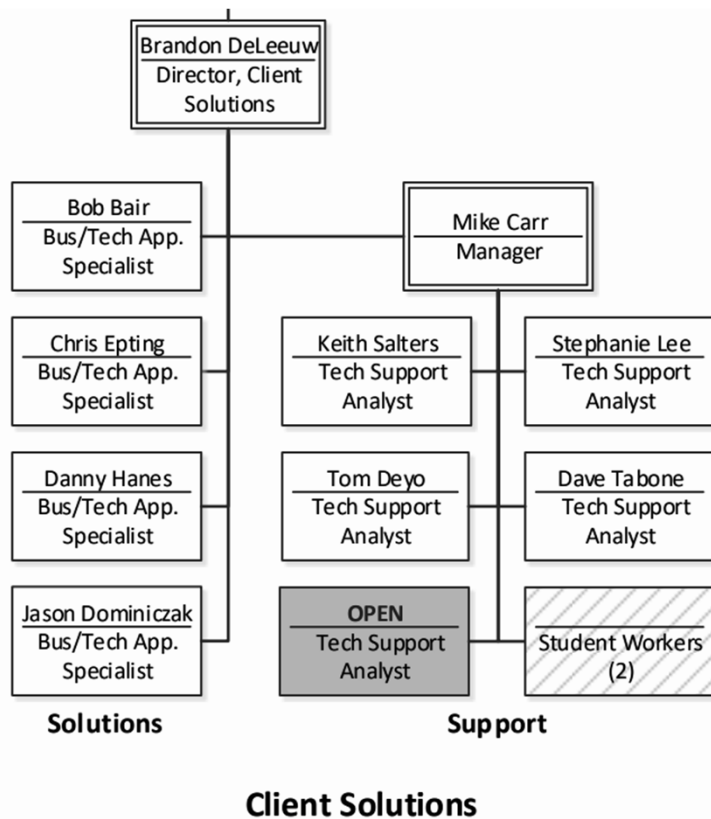
# BACKGROUND



## Why endpoint security?

End user devices are among the most vulnerable parts of an IT infrastructure. To help mitigate the vulnerabilities associated with these devices, the University of North Carolina at Charlotte has focused on leveraging built-in tools that secure these endpoints and reduce costs by leveraging tools that already exist.

# ORGANIZATIONAL CHANGES



# ANTI-VIRUS

## Endpoint Computer Activity Status



- **1093** Active
- **197** Inactive 2+ Weeks
- **99** Inactive 2+ Months
- **12** Not Protected

## Endpoint Protection Client Status

✓ Total active clients in this collection protected with Endpoint Protection: 95.7%

Total devices in this collection: 6625

Endpoint Protection clients in this collection that are active: 6154

✓ Active clients protected with Endpoint Protection: 5890

✗ Active clients at risk: 264

Clients in this collection that are inactive or not installed: 471

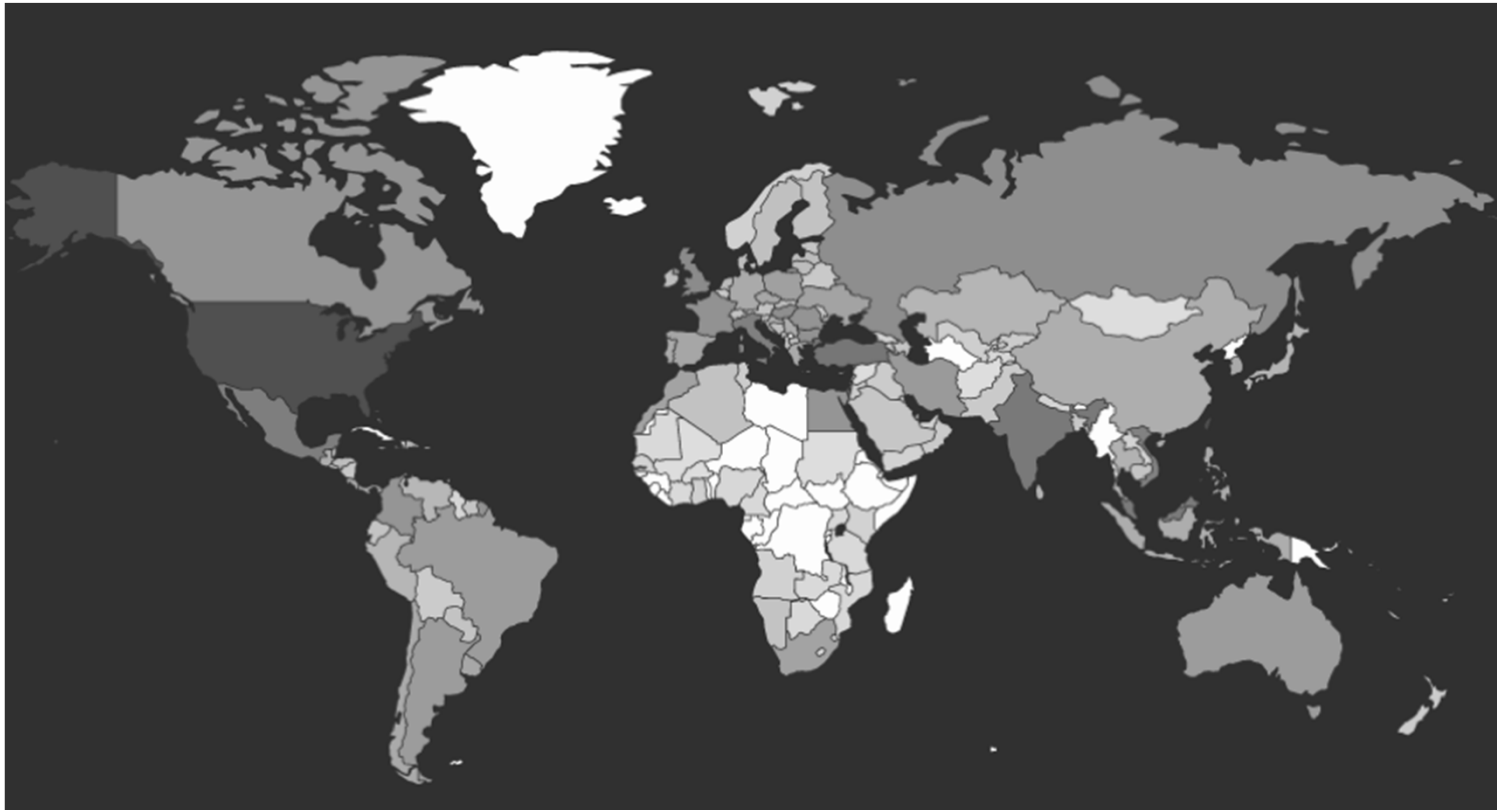
i Endpoint Protection agent not yet installed: 21

i Endpoint Protection agent not supported on platform: 0





























i Configuration Manager client inactive: 408

i Configuration Manager client not installed: 42

# MALWARE AND BOTNETS



# NEW ACTIVE DIRECTORY SCHEME

- └─  university
  - └─  AAFR
    - └─  AAFR
    - └─  ADVANCE
    - └─  ASSESS
    - └─  BCOB
    - └─  CCC
    - └─  CCI
    - └─  CHHS
    - └─  CLAS
    - └─  COAA
    - └─  COE
    - └─  COED
    - └─  EMR
    - └─  GRAD
    - └─  INRS
  - └─  ITS
    - └─  Center for Teaching and Learning
    - └─  Client Engagement
    - └─  Conference-Rooms
    - └─  Enterprise Applications
    - └─  Enterprise Infrastructure
    - └─  Information Security Compliance
    - └─  Labs
    - └─  Leadership
    - └─  Limbo
    - └─  Planning & Administration
    - └─  University Research Computing

# ENCRYPTION

Bitlocker and FileVault

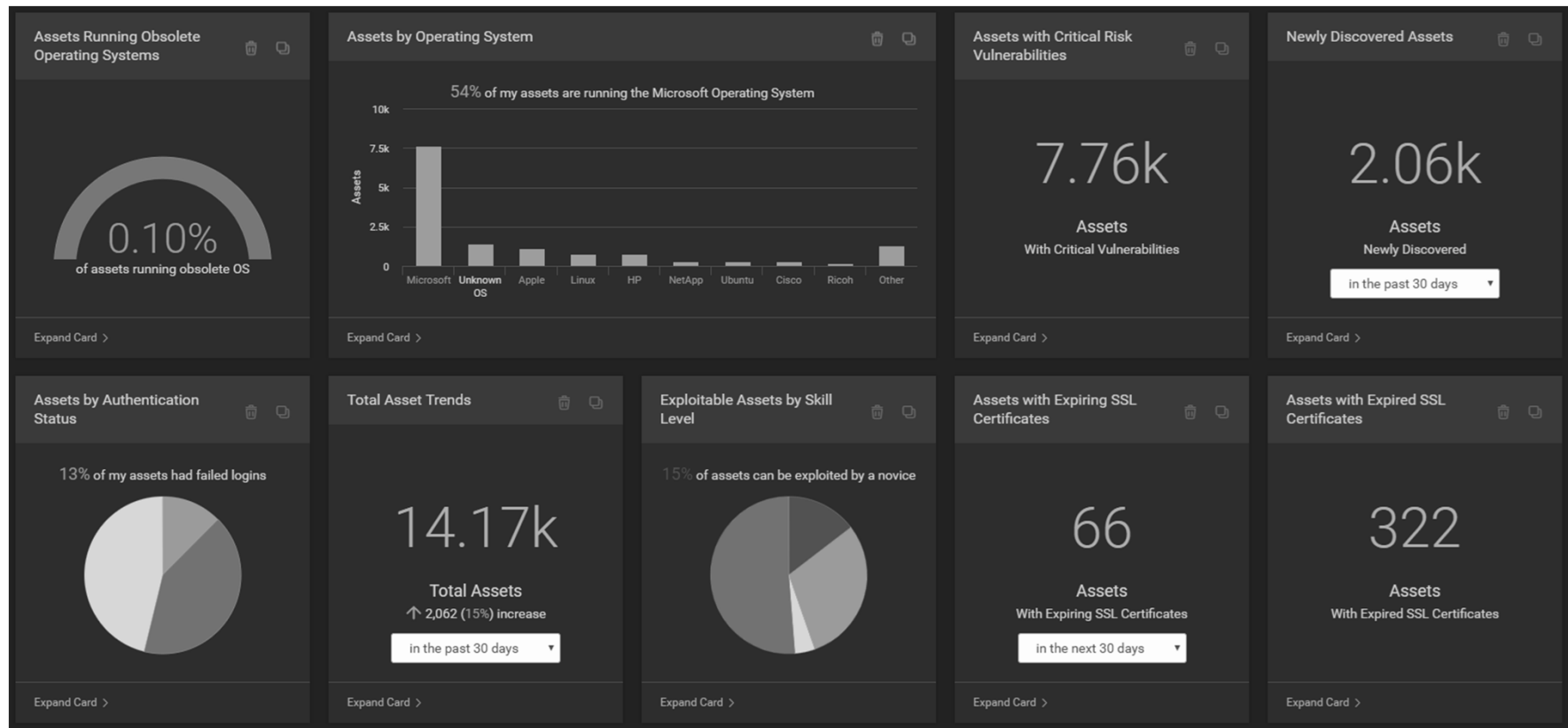
Central Key Store

New Standard

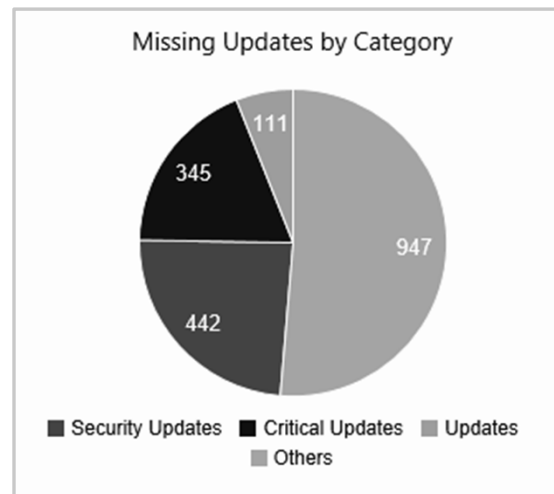




# VULNERABILITY SCANS



# MONTHLY PATCHING



ITS, 20%, 80%

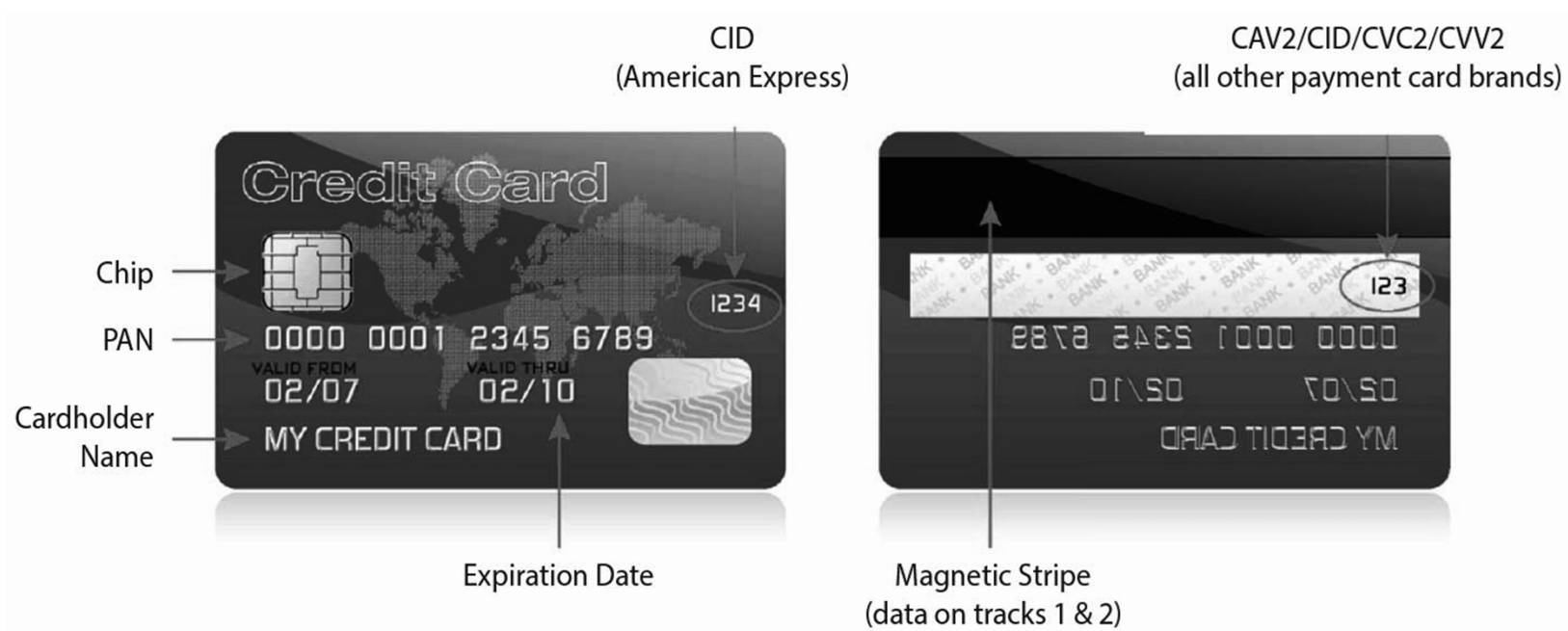
# OPERATING SYSTEM UPGRADES



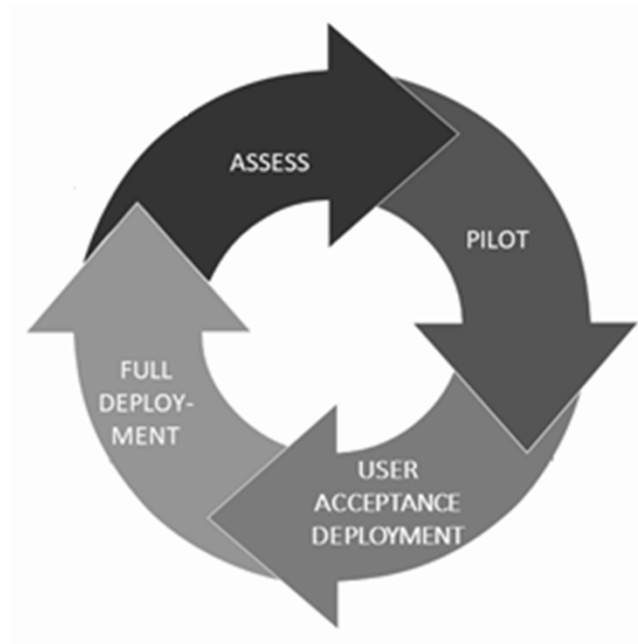
# OPERATING SYSTEM UPGRADES



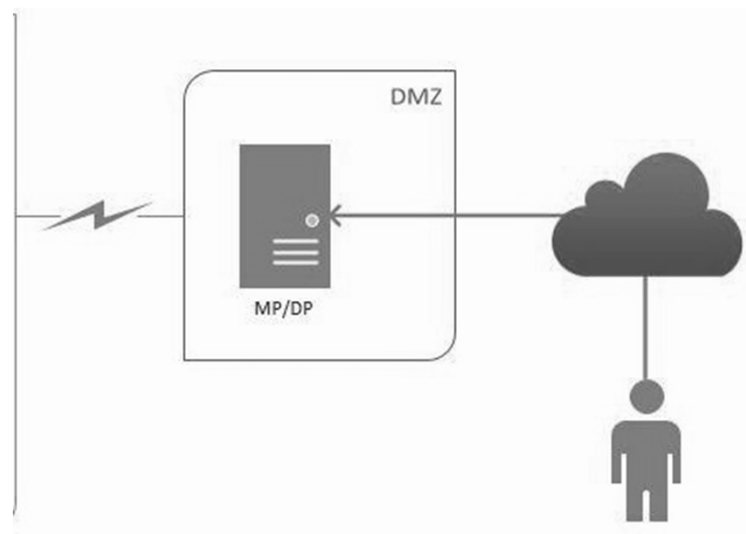
# PCI



# THIRD-PARTY PATCHING



# OFF NETWORK MANAGEMENT





# PRINTERS

Open Relay

Separate VLAN

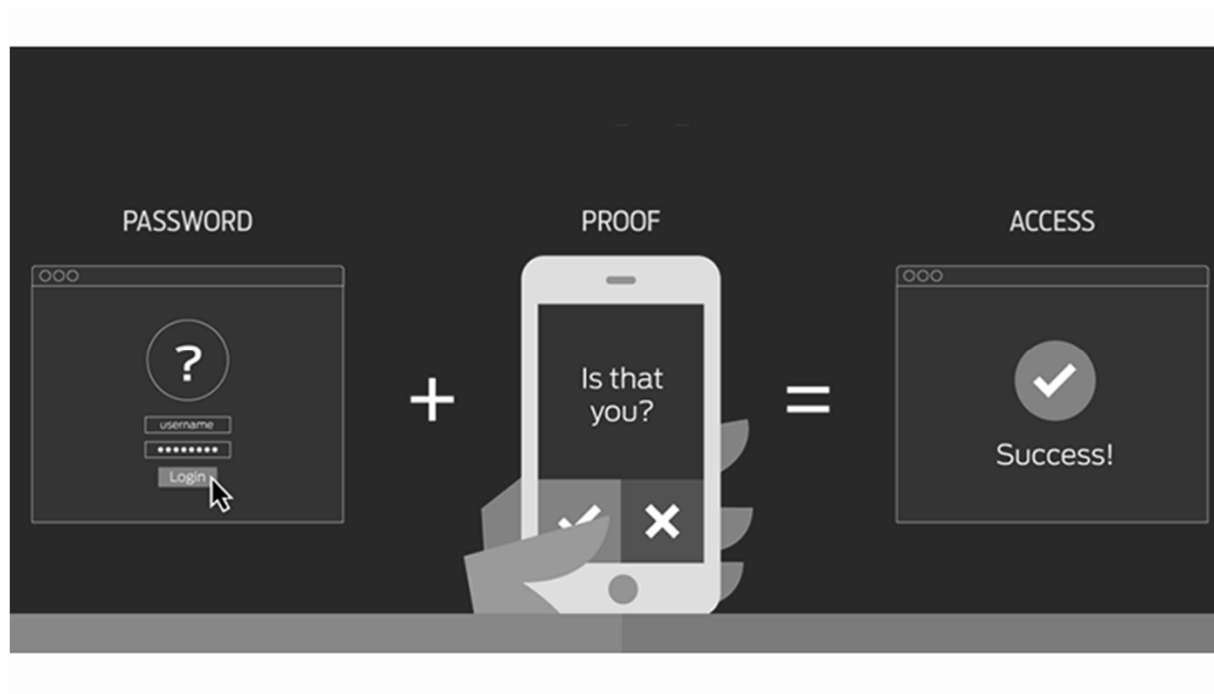
Security Checklist





SPIRION

# DUO



# PHISHING SIMULATIONS

95%

"95% of all attacks on enterprise networks are the result of successful spear phishing"

Source: Allan Paller, Director of Research - SANS Institute



# LESSONS LEARNED

- Have the people who "care the most" "own" the service
- Everything takes time and thoughtful planning
- Use planned/phased rolls outs when able
- Have policy align with practice e.g. encrypting the mobile devices

# Questions