MODULE 6A: AUDITING END-USER COMPUTING DEVICES

OBJECTIVES

- Bring Your Own Device (BYOD) Policies
- Challenges of BYOD
- Network Access Control (NAC)
- Mobile Device Management (MDM)
- Data Loss Prevention (DLP) Systems
- Auditing End-User Computing Devices

BACKGROUND

- The computing power available to the everyday user has grown exponentially over a generation to the point where today’s small desktops and laptops are far more powerful than the room-filling supercomputers of 20 years ago, while mobile phones and tablets are now packing as much power as some modern laptops. The power of these devices means that end users can do more today with a laptop or phone than at any time in history. This also means that these devices need to be managed closely in a business environment, as a powerful, unmanaged system can present a significant risk to business operations.

BYOD

- Bring Your Own Device (BYOD) Policy – Allows employees to bring their home devices (laptops, mobiles
  - Companies were initially thrilled by users bringing their personal devices. No cost, easy transition from work to home and vice versa. Flexibility!
  - By the 2010s, security, audit, and legal teams began to question the wisdom of this practice, as a personally owned device storing company-owned data can create a difficult legal situation if the employee leaves, and technical controls to address this were only partially effective.
  - **<u>The challenge of device ownership remains a key point to consider when auditing end-user systems.</u>**

BYOD

- Auditors should examine the organization's BYOD policy, and data ownership policies as well.

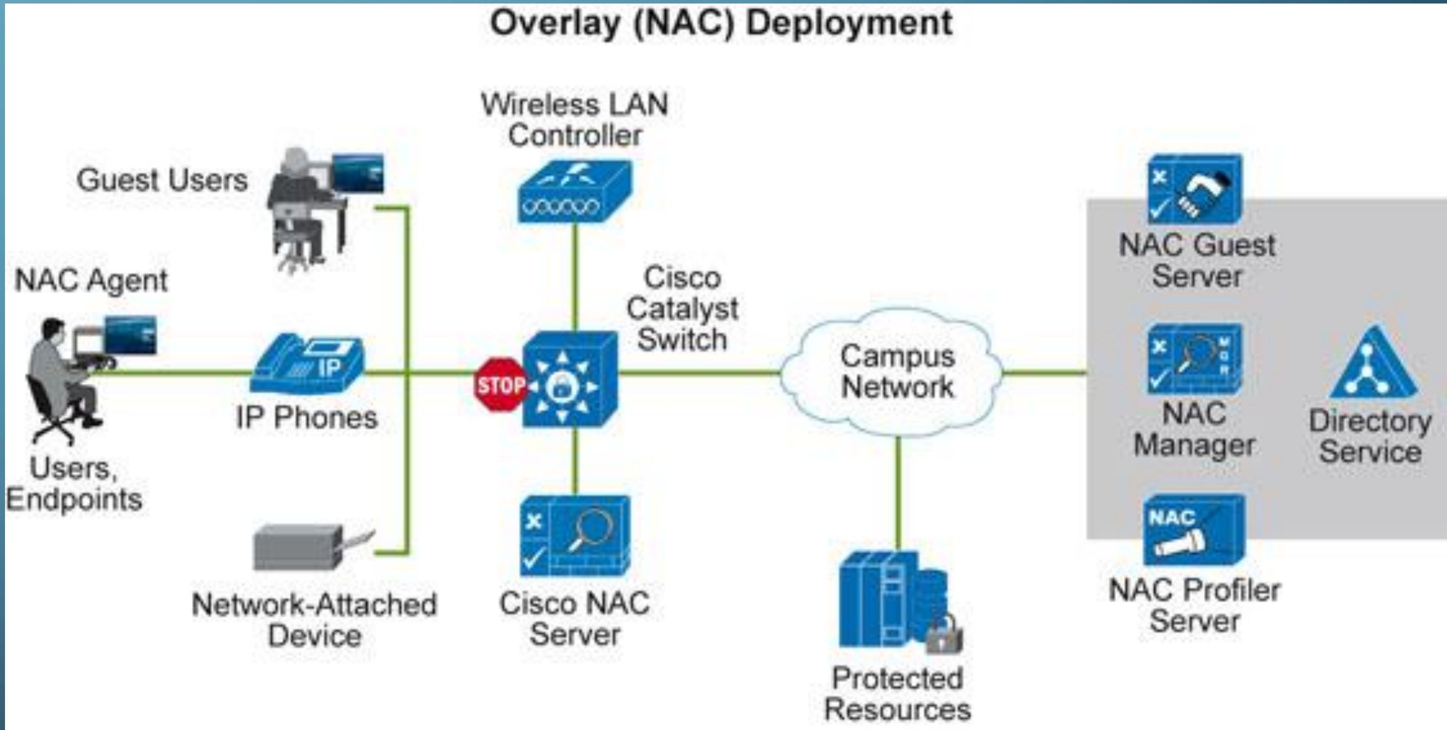
- Take a look at WVU's BYOD Policy: https://it.wvu.edu/policies-and-procedures/acceptable-use/byod

THE CHALLENGE

- The true challenge of a BYOD environment is that users are bringing inherently non-enterprise devices into your enterprise environment.
- How do you enforce group security policies for devices that aren't part of the group (i.e. a domain)?
- How do you maintain data security in your organization if data is stored on devices that are not managed by, nor the property of the organization?

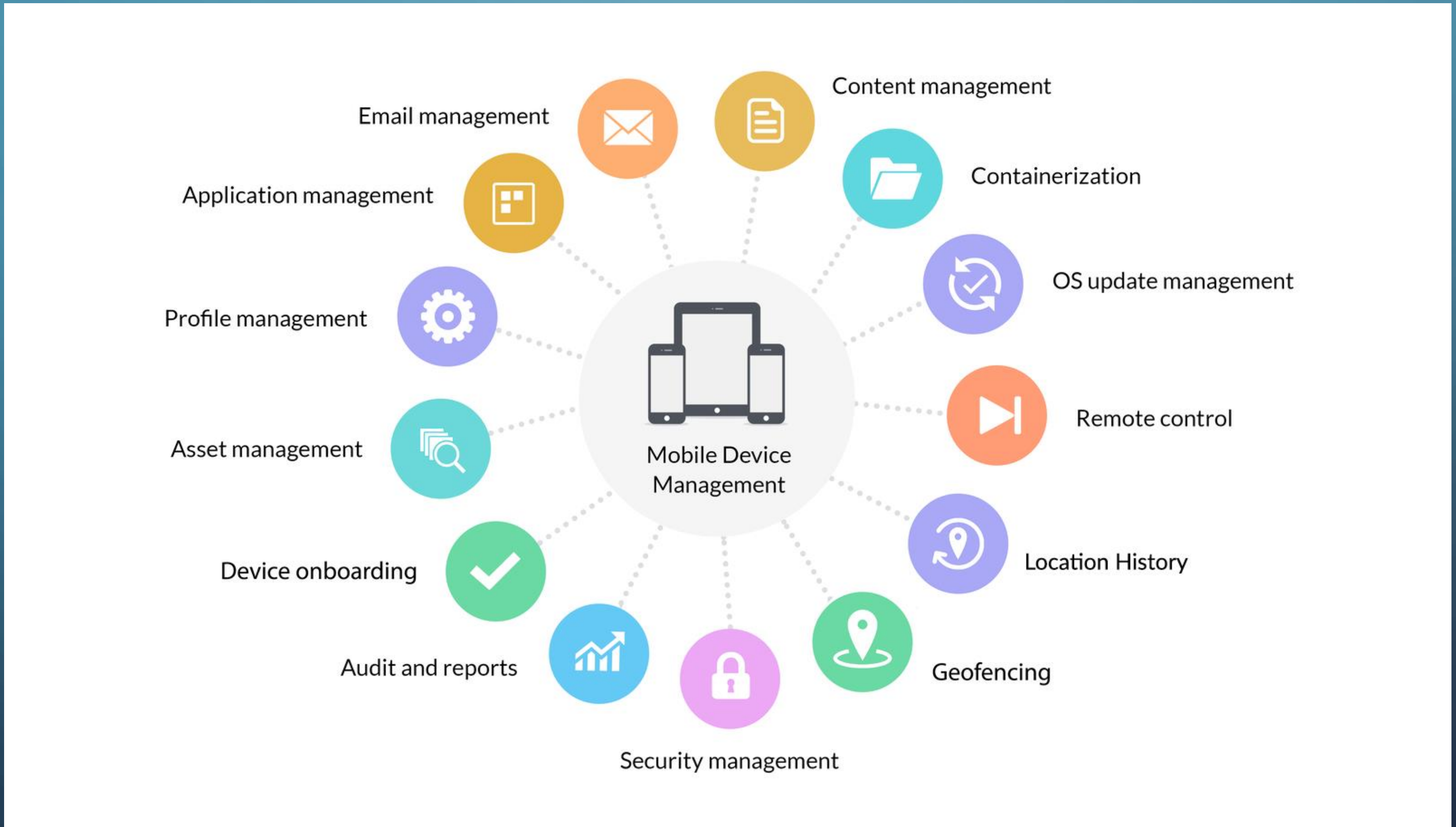
NETWORK ACCESS CONTROL

- Network Access Control (NAC) is a suite of technologies that can restrict access to the enterprise network based on a series of conditions.
- Device “health condition”



http://www.caysec.com/2010/09/cisco-nac-vs-8021x.html

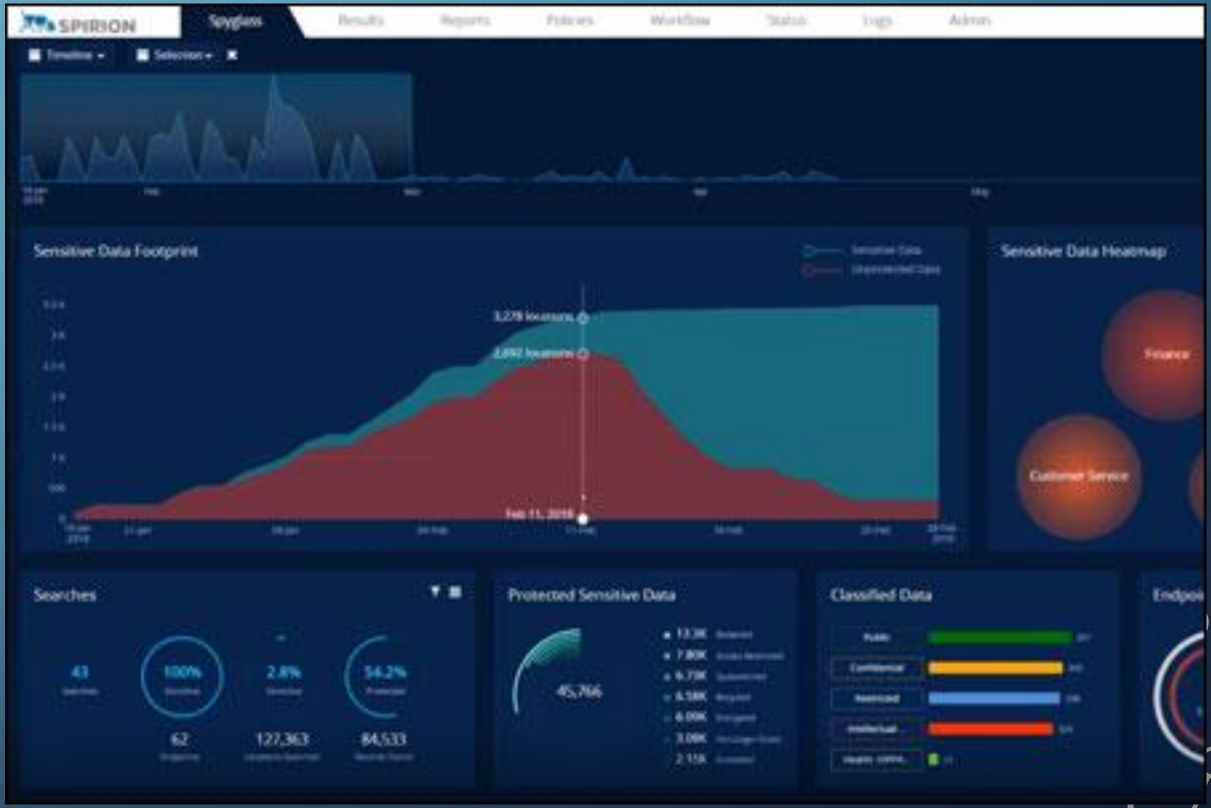
MOBILE DEVICE MANAGEMENT (MDM)



https://www.manageengine.com/products/desktop-central/mobile-device-management-mdm.html

DATA LOSS PREVENTION (DLP) SYSTEMS

- Can be run on a network or locally installed on systems. Scans for “sensitive” data on endpoints.
- Could be useful for helping to manage data security in a BYOD environment



AUDITING END-USER DEVICES

- If a company has a BYOD policy, it's unlikely that the auditor will be able to examine employee's personal devices.
- Rather auditors will assess if the organization has implemented potential risk mitigating controls such as NAC or MDM to best practices and standards in place
- Auditors should also examine company policies around mobile devices and data ownership