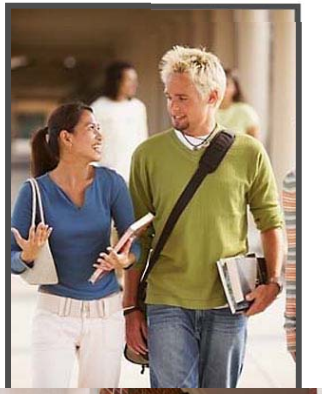
impulse

safe connect

network access control



Introduction

- Impulse Point
- Headquartered in Lakeland, FL
- Founded in 2004
- Exclusive focus on Network Access Control Solution for Education
- Over 300 College, University and K-12 customers
- 3.5 million devices under management
- SAS 70 Type 11/ SSAE 16 datacenter

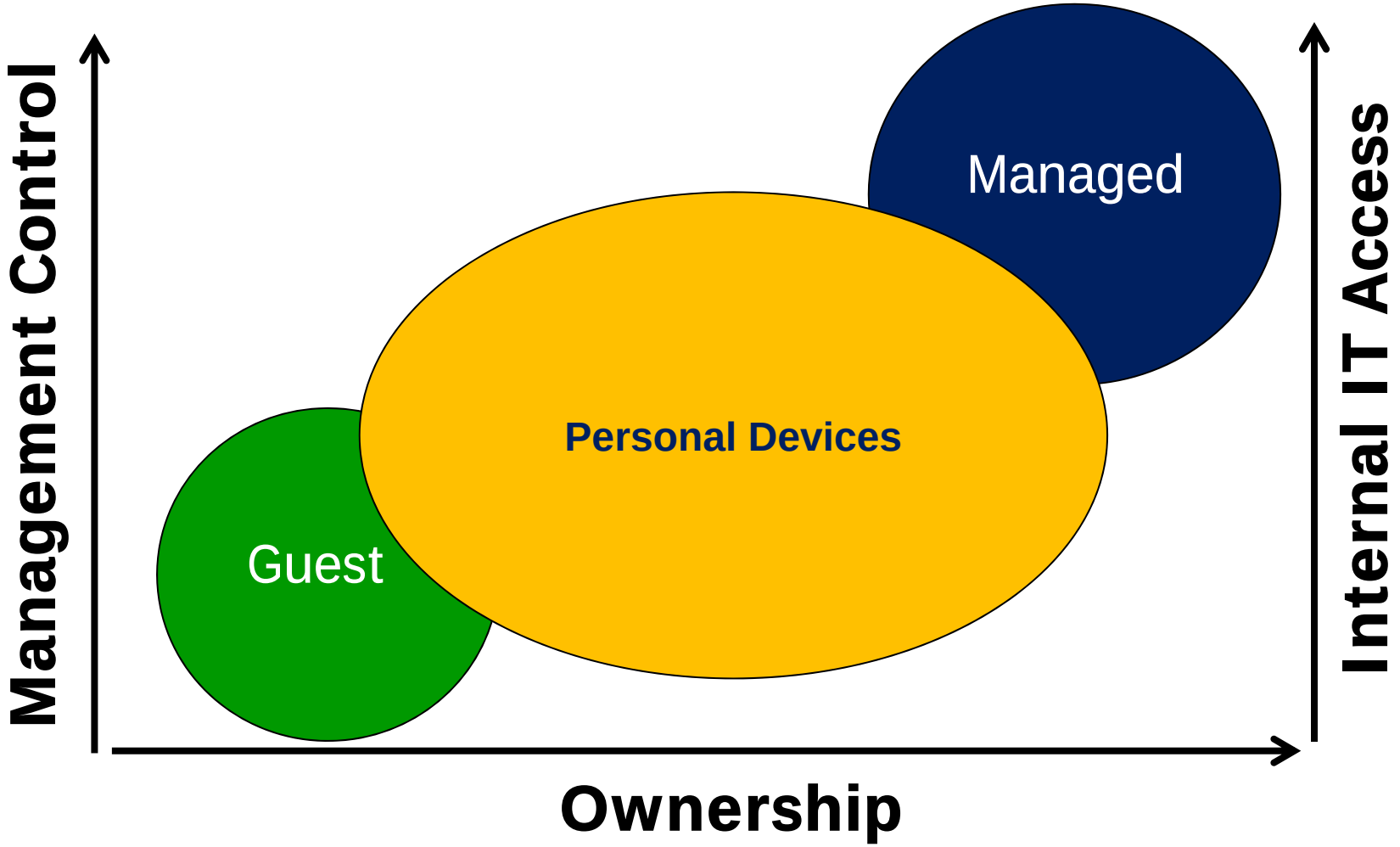
Sample Customers
Colleges and Universities

“We have met the enemy and they are us”

BYOD in Education Defined

The authorized access of non-managed (personal) devices to a network that serves as a conduit for computing resources and applications.

Bring Your Own Device (BYOD)



New World for HiEd

- Competitive environment
- Technology outpacing traditional controls
- Digital literacy is a universal requirement
- Institutional barriers to technologies
- Information collection

Source: Horizon Report 2012

Changes for HiEd IT

- Living ➡ Learning
- The new classroom
- More and bigger content
- Multitude of devices
- Lots of Sessions

Source: Horizon Report 2012

Key Trends

- Access whenever and where ever
- Cloud based technologies
- Decentralized IT Support
- Increase in Collaboration Tools
- Remote and Distance learning
- Internet influence on roles

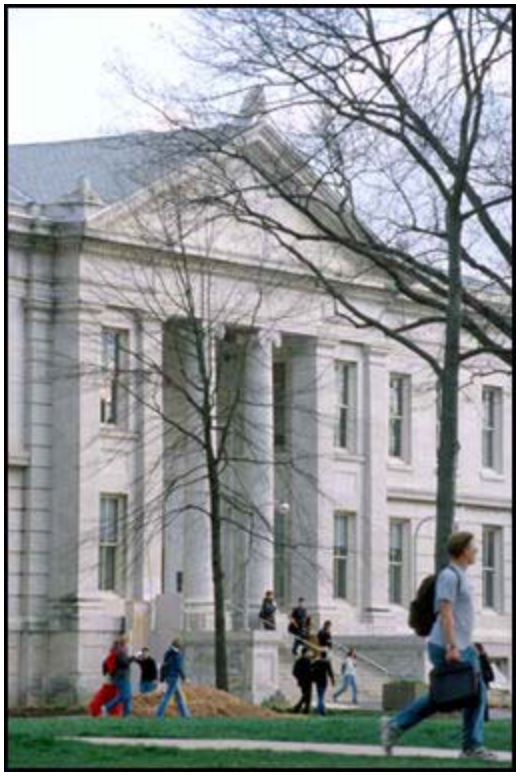
Source: Horizon Report 2012

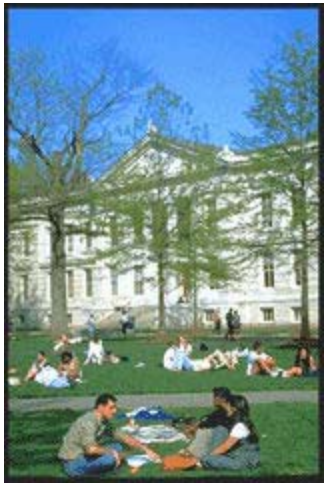
Considerations

- Data Loss
- Unwanted Users
- Unwanted Devices
- Un-desirable Activity
- Credential Sharing
- Getting to a Norm

Striking the Balance

- User buy in
- Academic freedom
- Faculty and Staff participation
- Overcoming institutional barriers to technologies
- Reaching a level of proportional security





NAC Access Control

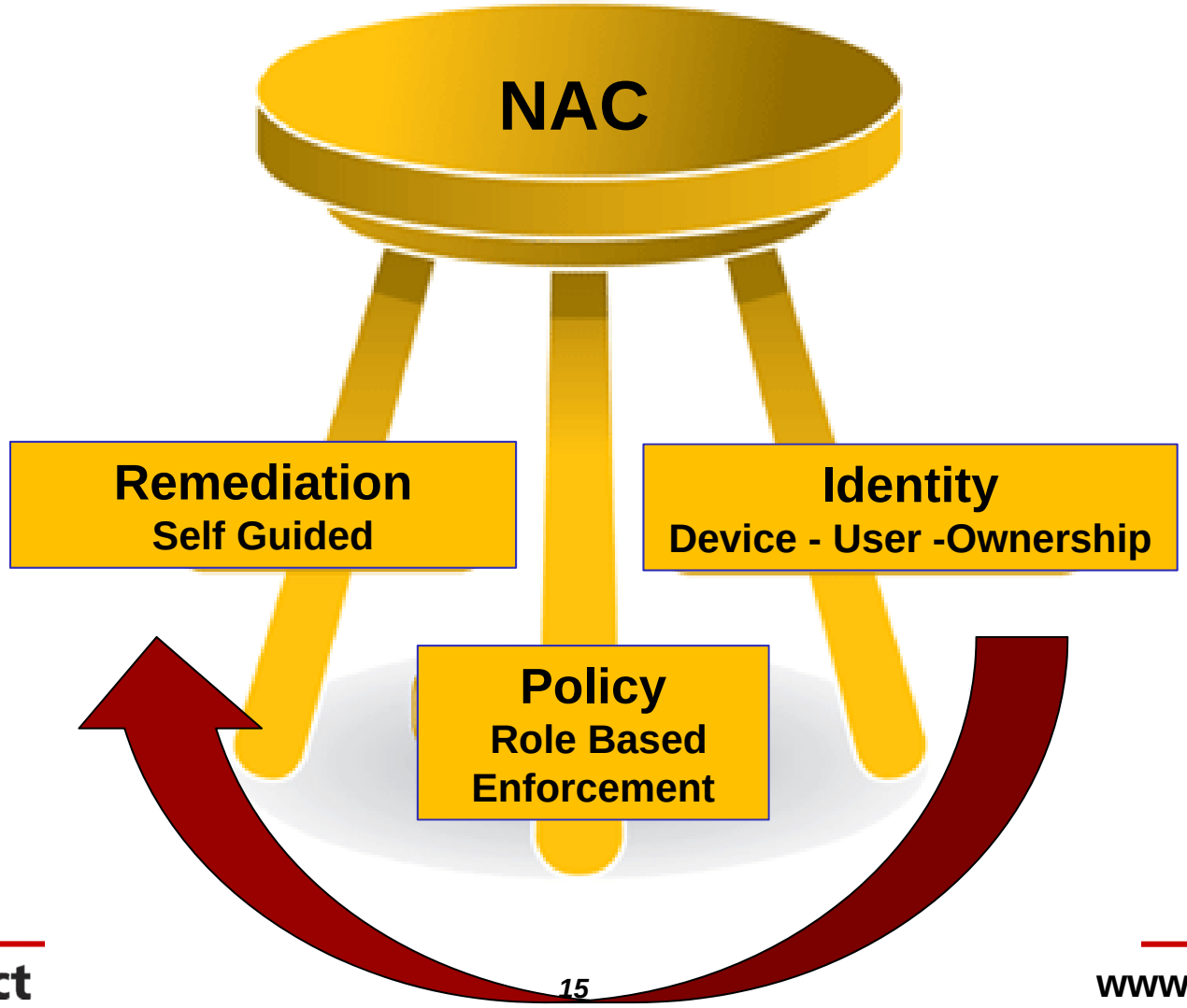
Access Control Trends

- Academic freedom argument being tempered
- Faculty and Staff is no longer off limits
- Device centric world – the network is just transport
- Access to the Cloud
- Shift from Living to Learning

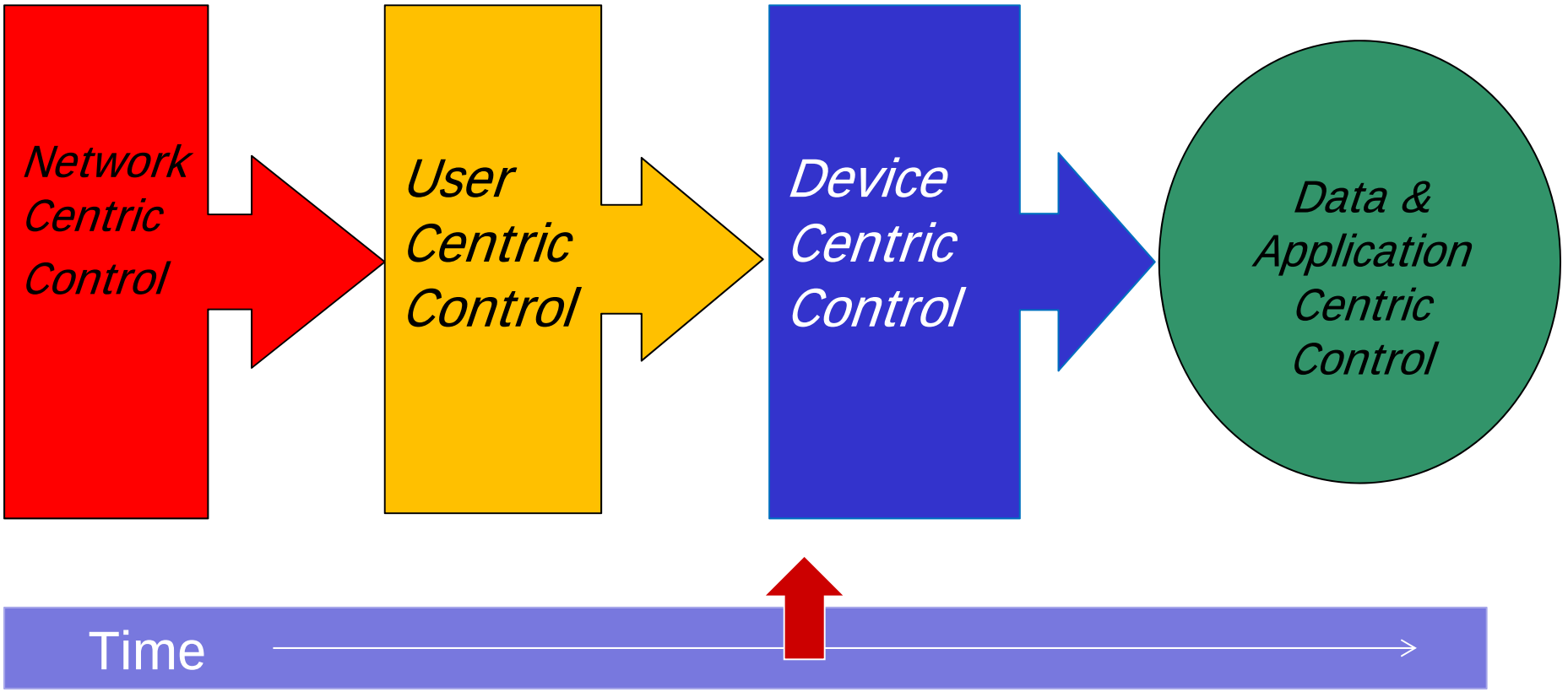
Promise of NAC

- Security solution
- Intended to three things:
  1. Identity Who and What is on your network
  2. Mechanism for creating a security policy
  3. Initiate corrective action
- Automatic – user guided
- Change behavior

Visibility and Control



Evolution of NAC



User Centric Security

- Role/Identity Based
- Devices
- Location
- Application
- Bandwidth
- Address computing behavior/habits

Changing Role of NAC

- Top of the mountain – “watch the watchers”
- Central repository of user identity, device type and role
- Enforcement mechanism
- New control points and levers
- New NAC – “feeder mechanism”
- Move to User & Device Centric Security

Why NAC ?

- Dramatic Increase in unmanaged devices
- Need to know who is on the network (Authentication)
- Need to know what is on the network (Device Identity)
- Need for management and control (Policy Enforcement)
- Different approach to Users and Device types
- Who gets what and how much (Bandwidth allocation)
- Decision based on Information
- Baseline for Mobile Device Management (MDM)

Network Access Security Threat

- Data Loss
- Unwanted users
- Unwanted devices
- Un-desirable activity
- Credential sharing

Changing Role of NAC

- Traditional NAC Review – “watch the watchers”
- Central repository of user identity, device type and role
- Different methods of enforcement
- Integration with Mobile Device Management (MDM)
- New NAC – “feeder mechanism”
- Move to User Centric Security – Less Network Centric
- Different methods of enforcement
- Application control
- Bandwidth allocation

NAC Options

- Do nothing
- Audit
- Warn users
- Device identity and authentication
- Policy enforcement (quarantine)
- User group control and assignments
- Location based control and assignments
- Device based control and assignments
- Application based control and assignments
- Combine to other security elements

Decision Point

- Limit Risk
- Time
- Freedom
- The Network
- User Experience
- Access vs. Control
- Visibility
- Support

Scenarios

BYOD Scenarios

1. Limited Open
2. Secured Wireless
3. Authorized Access

Approach #1

Limited Open

- *Approach*
  - An open wireless SSID created for student and guests
  - User authentication or system checking not required
  - Separate from primary network
  - Internet only

- *Considerations*
  - Unwanted users have access
  - Users are unknown - Anonymous copyright infringement
  - Forum for the spread of Viruses
  - Obligation/burden of support

- *NAC Security*
  - *Identify what devices are connected*
  - *Force users to authentication*
  - *Match user identity to device*

Approach #2

Secured Wireless

- *Approach*
  - Secured Wireless with user authentication required
  - Student and Guest access
  - Separate from wired network segment
  - Internet only

- *Considerations*
  - Does not account for wired or VPN access
  - Access to internal resources
  - No Security policy checks

- *NAC Security*
  - *Match user identity to device (ownership)*
  - Limit or set restrictions by device type
  - *Ability to trace DMCA violators*
  - *Allocate bandwidth by identity and device*
  - *Time based credentials for Guests*

Approach #3

Authorized Network Access

- *Approach*
  - User authentication required
  - Wired and wireless network access
  - Role based access - Student , Staff, Faculty and Guests
  - Access to internal and external resources (data and applications)

- *Considerations*
  - Device landscape – Knowing what devices are on your network
  - Device Control – providing limits or restricts by device type
  - Security policy enforcement - common security settings access those gaining access
  - Focus on learning – Prohibiting certain applications

- *NAC Security*
  - *Identify what devices are connected*
  - *Force users to authenticate*
  - *Match user identity to device*
  - *Security policy checks*
  - *Enforcement Action – Audit, Warn or Quarantine*
  - *Remediation*

Recommend BYOD Best Practices

- *Users authentication (all users)*
- *Identification of all devices*
- *Correlate the devices and their owners*
- *User role assignment based a directory group(s) setting*
- *Standardized security settings (all users)*
- *Limits/restrictions on non-learning applications*
- *Real time/automated notification*
- *Administrative Controls and Reporting*

Questions