

# NAC: Is It Dead Yet?

March 6, 2009

Reginald P. Best, AEP Networks



# What We'll Cover At This Session

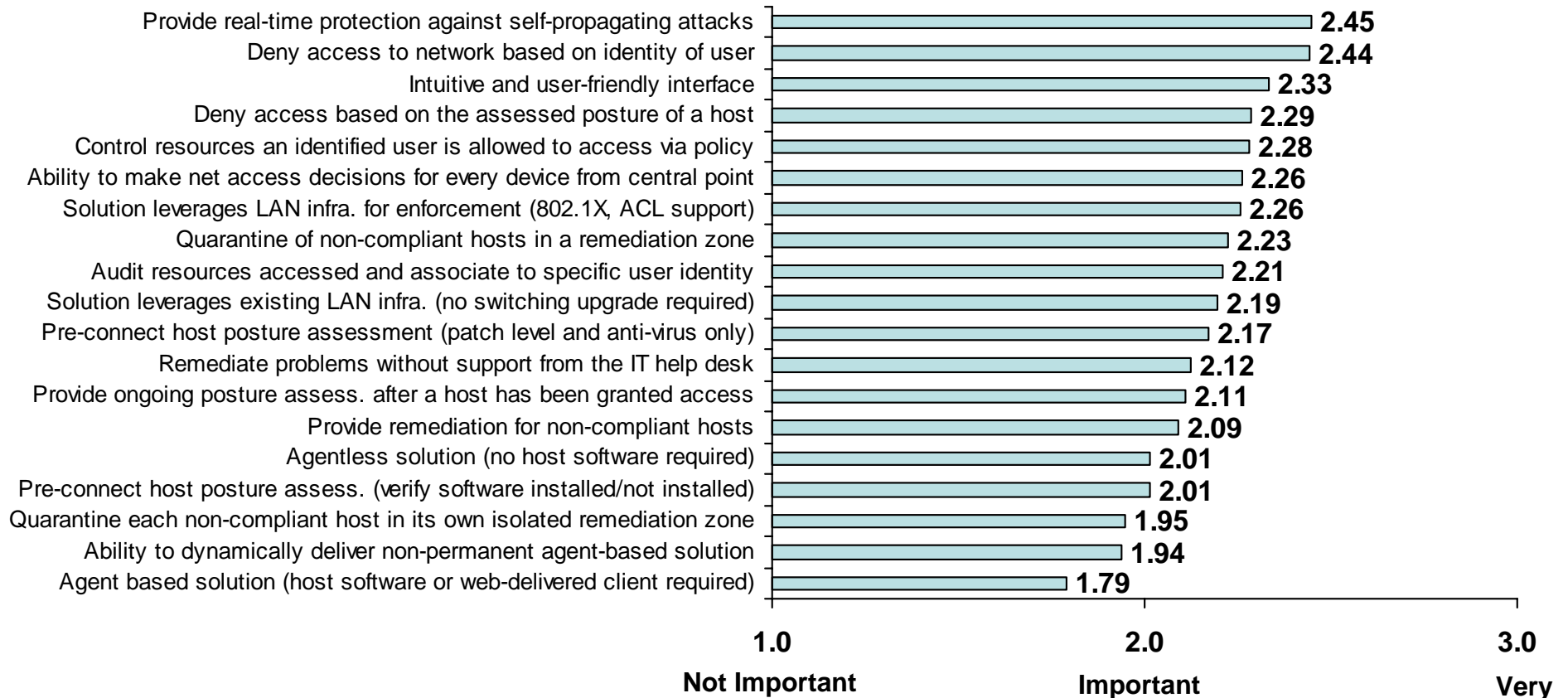


- What's going on with Network Access Control (NAC)?
- What is Identity-based Access Control (IBAC)?
- Compare and contrast NAC vs. IBAC
  - Why hasn't NAC taken off as expected
  - The advantages of IBAC for your network

# NAC Solution Requirements (Current Analysis, 2006)


n=303

## Importance of NAC Solution Features



**Buyers clearly expect NAC to cut down on the threat of self-propagating attacks. Important**  
**Here we see that identity-based access control is a key solution requirement.**  
**The variety of features also contributes to vague expectations among customers.**

# Fundamental Network Access Control (NAC) Objectives



- Pre-connect host posture assessment
- Violating host quarantine
- Violating host remediation
- Post-connect posture monitoring
- Post-connect policy enforcement

# The Result

- NAC provides efficient endpoint compliance checks
  - Anti-virus, firewall, device health, patch level, etc.
- However ... NAC is not enough
  - Once “green-lighted”, a user is free to roam the network
  - NAC protects the network, but not the data center resources within that network
  - Highly complex to install/manage/support

# NAC Vendor Examples/Strategies



- Software-Based
  - Symantec, Microsoft, Sophos
- Hardware Gateway-Based
  - Mirage, Bradford, Juniper
- Switch-Based
  - Cisco, Consentry, Nevis

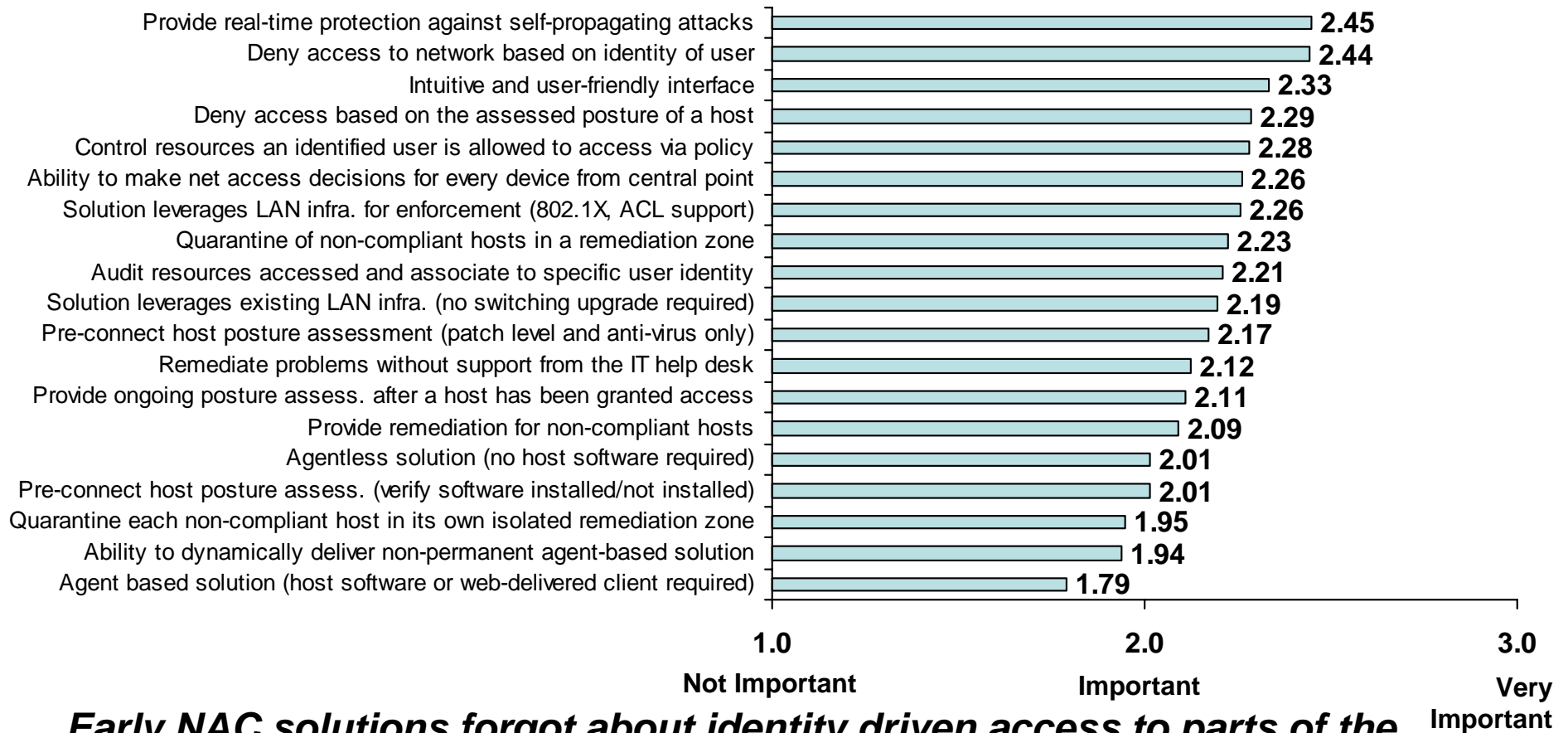
# Why Hasn't NAC taken off as expected?

- Making the network “intelligent” adds cost, complexity
- Many organizations feel they have control over their company issued machines already
- Competing architectures lead to confused customers
  - Confused customers don't buy
- Initial approaches didn't solve many of the key concerns

# NAC Solution Requirements (Current Analysis, 2006)

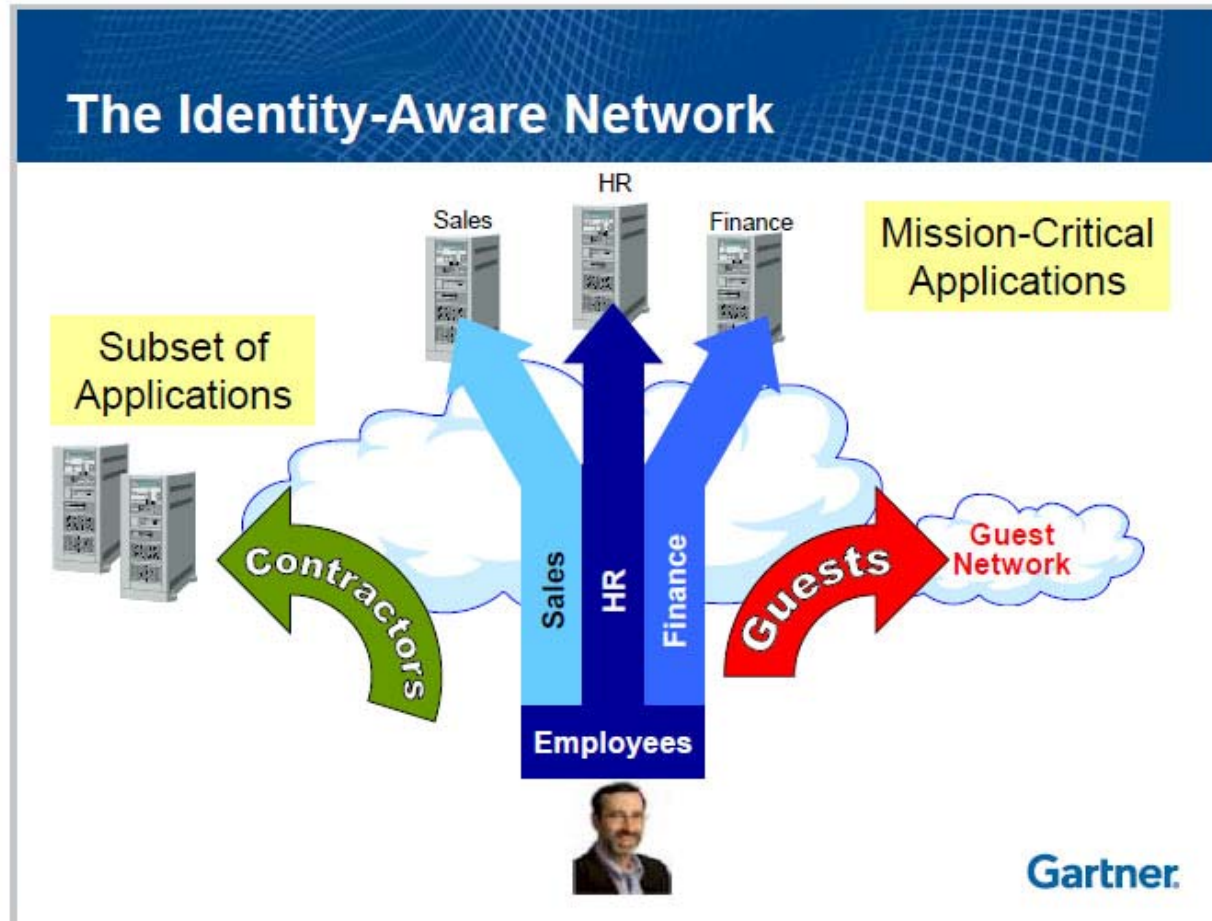
n=303

## Importance of NAC Solution Features



**Early NAC solutions forgot about identity driven access to parts of the network and resources. The focus was on the state of the client PC trying to attach.**

# Enter Identity-Aware Networks (Gartner, 2008)

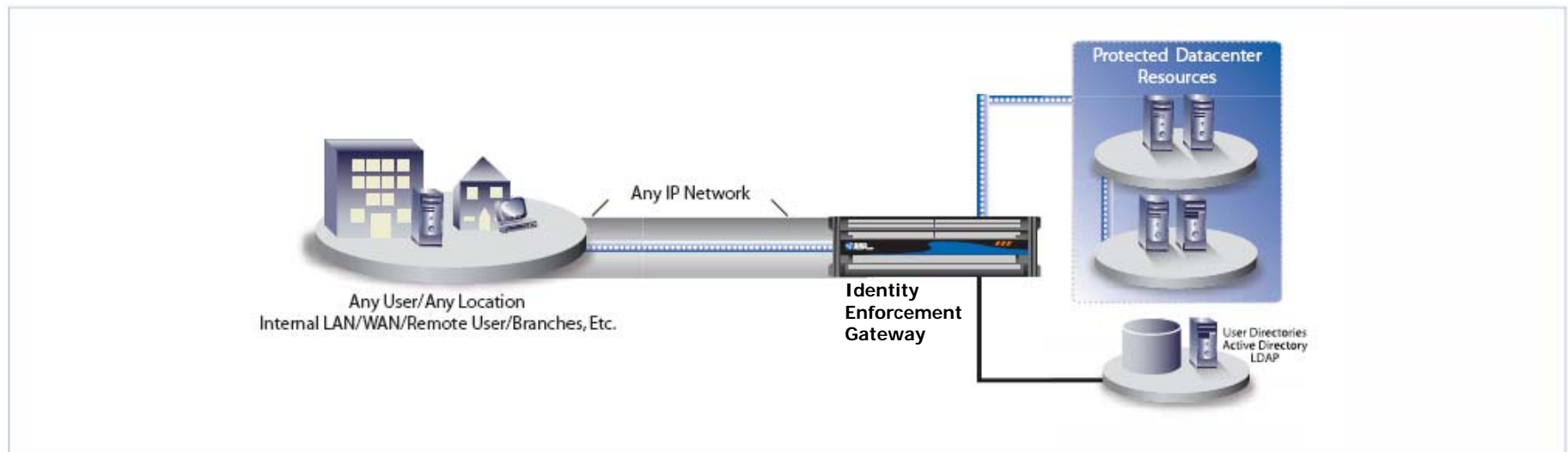


# Identity-Based Access Control (IBAC)

- Define policies for who gets access to which corporate resources
- Store the identity and access policies of every user in a directory, like LDAP or AD
- Authenticate a user identity before allowing them access to the network
- Add NAC functionality for user's machine where necessary (remote access, branch office, guests)

# Architecture Diagram

- IBAC is directly protecting resources

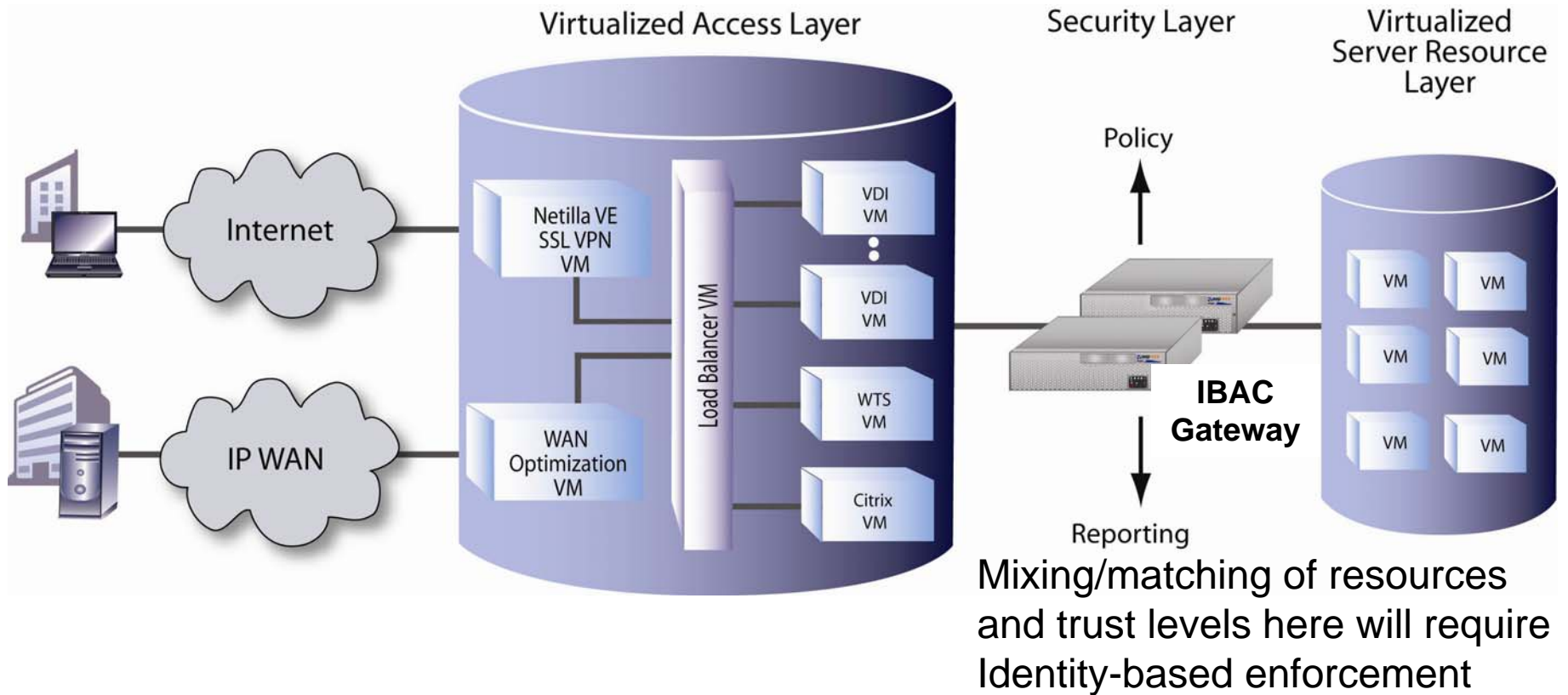


# Compare & Contrast NAC vs. IBAC



- NAC:
  - Get integrated within the network intelligence
  - Complex with lots of switch integration
- IBAC:
  - Brings security as close as possible to protected resources
  - Enhances existing perimeter security
  - Simplified network design and management
  - Incorporates NAC by linking user/machine identity, health scans, and AD group policy

# Virtualized Data Center Architectures Will Drive IBAC



# IBAC Features and Benefits

- **Run access infrastructure on a virtualized cluster**
  - SSL VPNs and access gateways
  - Terminal Servers (WTS, Citrix)
- **Separate back-end application resources on a different virtualized cluster**
  - Minimizes potential for intra-host attacks against most sensitive infrastructure
- **Use IBAC to provide granular identity-driven access control, reporting and visibility**
- **Ring-fencing**
  - Resource access on a “need-to-know” basis
- **Visibility**
  - Traffic passing through IBAC to secured resources is tagged, logged, auditable
  - Create “one-click” audit reports - by user identity - without lengthy cross-platform correlation efforts
- **Simplify Access Control**
  - Focus moves & changes via the directory instead of constant network re-engineering

# Additional Deployment Benefits

- Eliminate the possibility of legitimate users of one application “jumping-off” to disallowed resources
- Provide granular access control and reporting to applications with shared accounts/logins
- Deliver unified resource access control even if multiple directories in use - a common M&A integration concern
- Focus moves & changes in the directory instead of constant network re-engineering
- “one-click” audit reports - by user identity - without lengthy cross-platform correlation efforts

# Summary

---

- NAC – Is it dead yet?
  - Perhaps not, but it's certainly not enough to fully protect a (virtualized) network infrastructure
- What is your priority?
  - Client/host status integrity?
  - Control over who get to what resources on the network?

# Q&A



- Questions?