

# Demystifying NAC and Deploying the Right Solution



**Mike Rothman**

President and Principal Analyst  
mike.rothman@securityincite.com

[www.securityincite.com](http://www.securityincite.com)



**Sandy Hawke**

Senior Product Marketing Manager  
sandy.hawke@nevisnetworks.com

[www.nevisnetworks.com](http://www.nevisnetworks.com)

# Historical View of Security



# The Rise of the Insider

---

- Moat doesn't work anymore
- Trust is fleeting
- Guest access
- Mobility
- Post-admission control
- Who goes where MATTERS
- Egress also MATTERS



# “Disappearing Perimeter”

---

- Hard exterior, soft interior is no longer an option
- Devices connecting to the network must be:
  - Authenticated
  - Authorized
  - Safe (patches, AV)
- Enforce segmentation
  - “Hide” critical systems from external parties



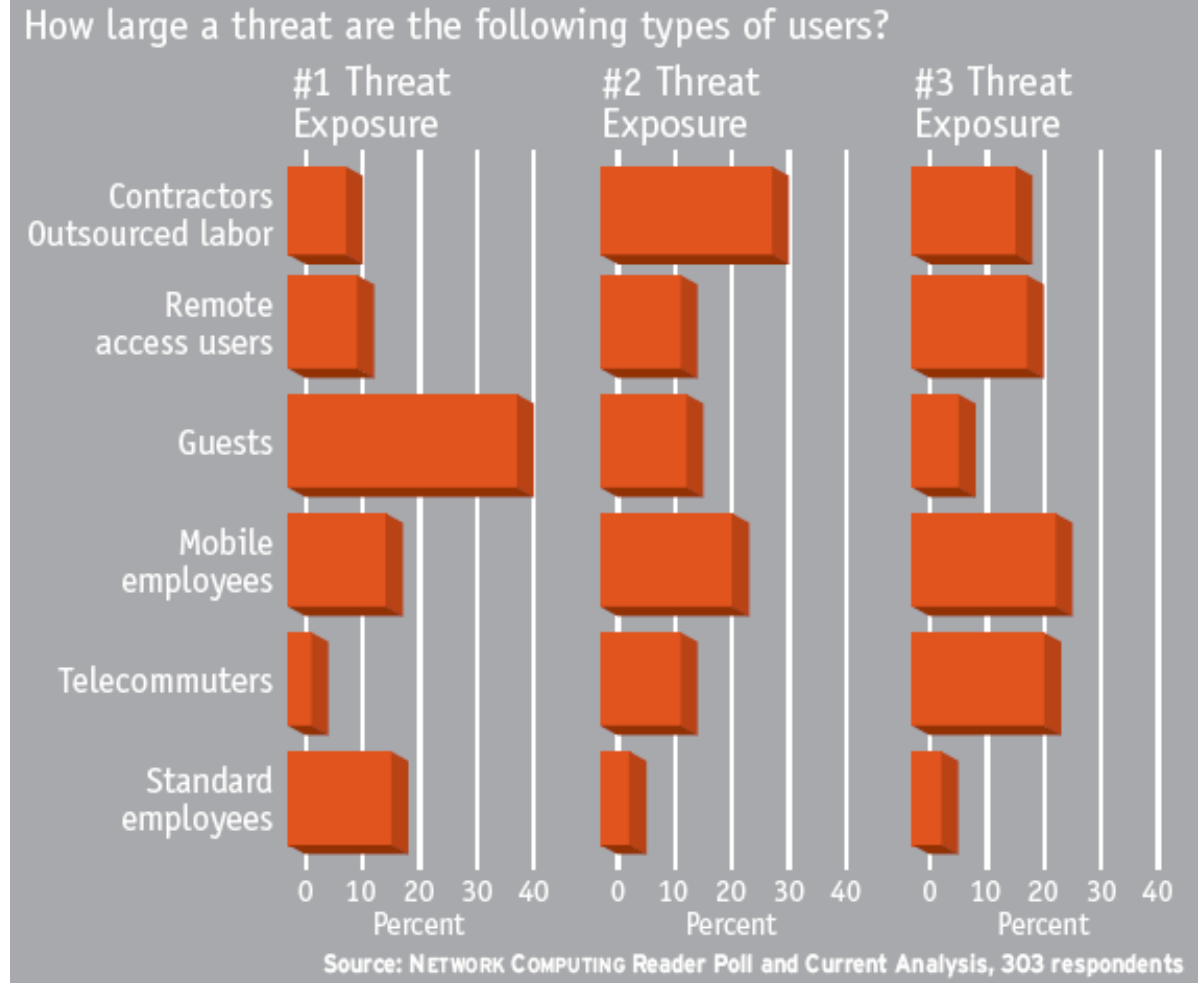
# Who exposes the LAN to Threats?

## Biggest Threats:

#1 Guests

#2 Contractors

#3 Mobile employees



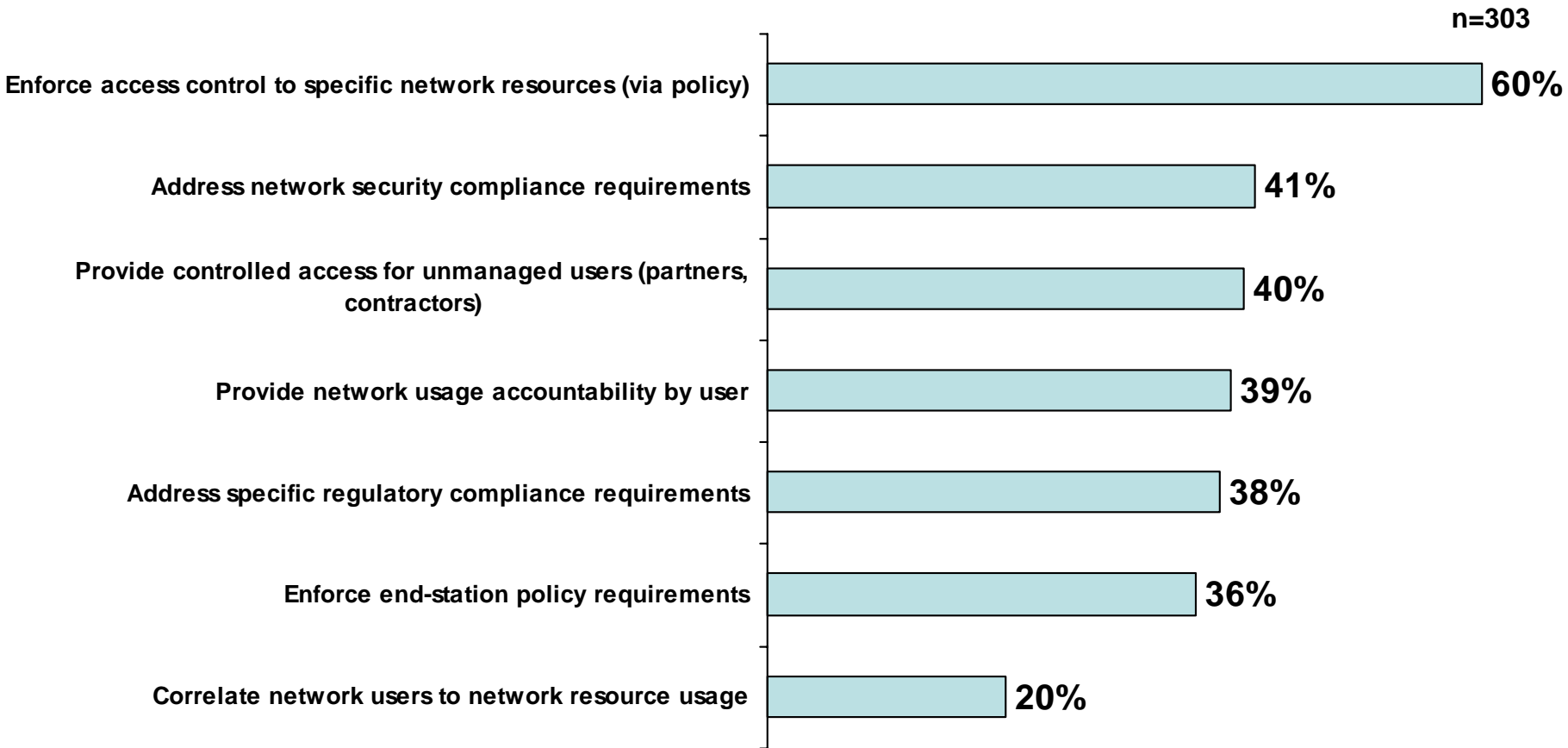
# What does NAC do?

---

- Pre-admission Host Posture Assessment
  - Authentication
  - Patch and AV policy enforcement
  - Quarantine and/or remediation
- Access control
  - Limit access to networks and resources based on attributes
    - Identity, Location, Device, Time
  - Enforce Zones of Trust
- Post-admission monitoring
  - Host posture changes
  - Anomalous behavior (control outbreaks)
  - User access control policy violations



# Top NAC Drivers



Source: *Current Analysis*, 2006



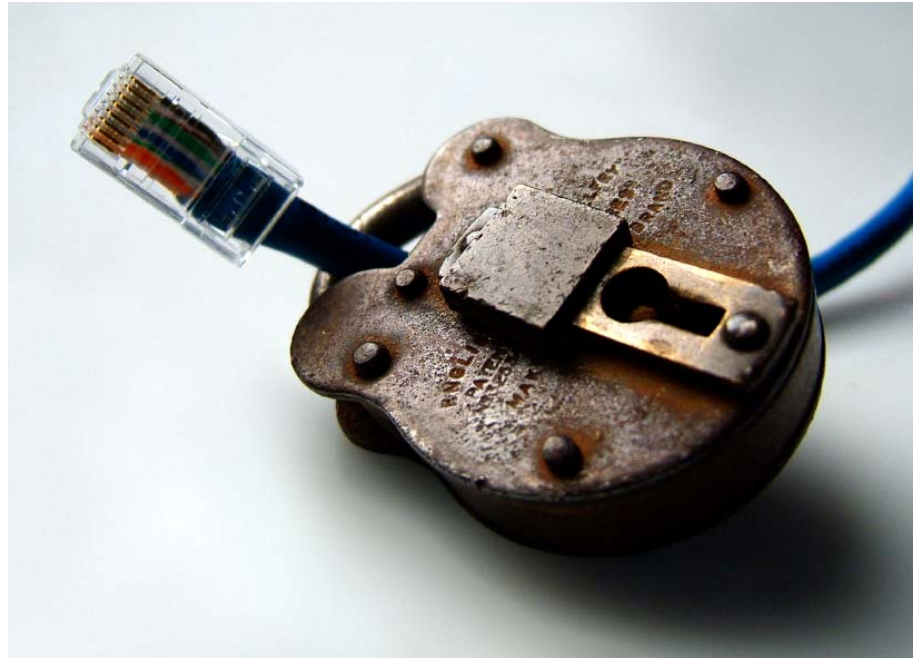
# Deploying Network Access Control

- Should accommodate these types of users:
  - Unmanaged (guests, contractors, etc)
  - Managed – on LAN
  - Managed – connecting remotely (telecommuters, mobile workers)
- Policies
  - Granularity
    - User/Group identity, time, location, device, etc.
  - Quarantine
  - Immediate remediation
- Integrating with existing network
  - Authentication
  - Endpoint Security
  - Perimeter security devices
  - Vulnerability Management
  - SSL VPN
- **Evolution, not revolution**
  - Inline vs. out-of-band



# Long Term: Security's in there!

- Secure Network Fabric
  - LAN re-architecture
    - Process starts over next 12-18 months
  - Access-layer switches hit the big time
- Phased protection
  1. Key resources in data center (core/distribution)
  2. Gradually migrate to access networks (VPN, wireless)
  3. Upgrade switches where appropriate (wiring closets)



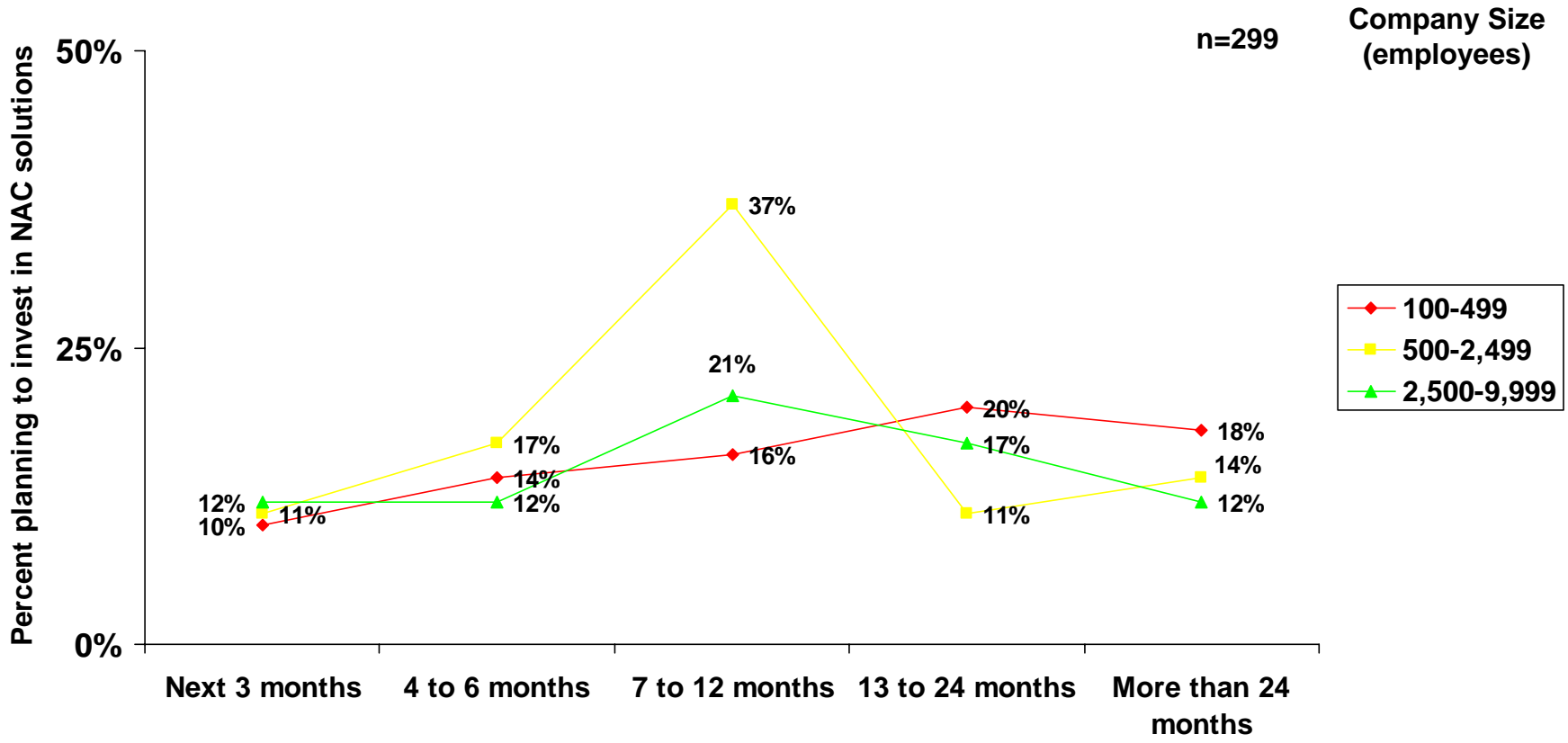
# NAC Selection Criteria

---

- Support for existing infrastructure
  - Evolution, not Revolution
  - Agent religion?
- Policy configuration
  - What kind of policies are supported?
  - How hard is it to configure?
- Ability to get you to secure network fabric
- Integration with alerting/help desk system/patch management
  - Remediation
- Compliance support
  - What kind of reports are available?
  - How does that feed the "compliance process?"



# When to start planning?



Source: *Current Analysis*, 2006

# NAC Action Plan

---

1. Know what you are protecting and why
2. Start with the end in mind
3. Break up the project into phases
4. Make tactical decisions with a strategic view
5. Be realistic about the budget
6. Have implementation contingency plans
7. Make sure you can report on whatever you choose
8. Do your homework
9. Ensure your comfortable with the strategic provider
10. Get a second opinion