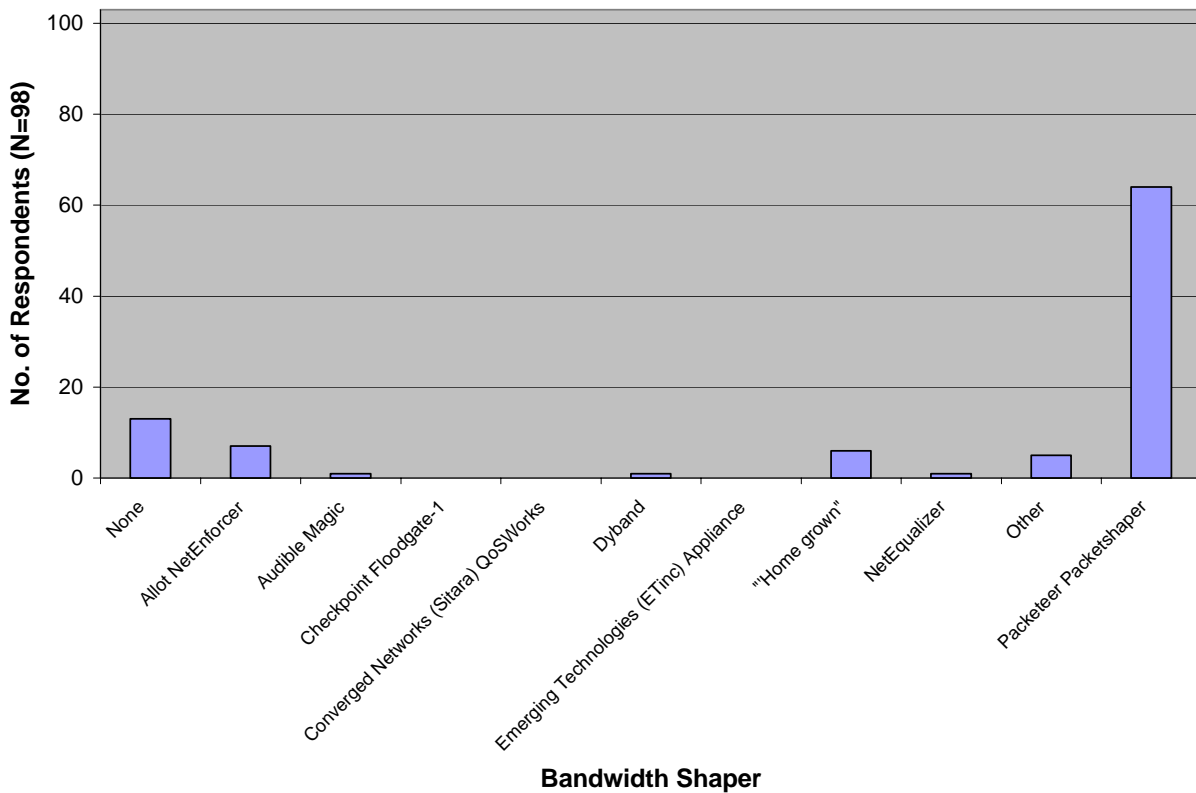


**24. Which bandwidth shaping or Quality of Service (QoS) product or tool does your institution primarily use? (Choose one)**

- We do not use a bandwidth shaping or QoS product or tool
- Allot NetEnforcer
- Checkpoint Floodgate-1
- Converged Networks (Sitara) QoSWorks
- Emerging Technologies (ETinc) Appliance
- Packeteer Packetshaper
- "Home grown" (i.e. developed in-house at your institution)
- Other - Please explain:

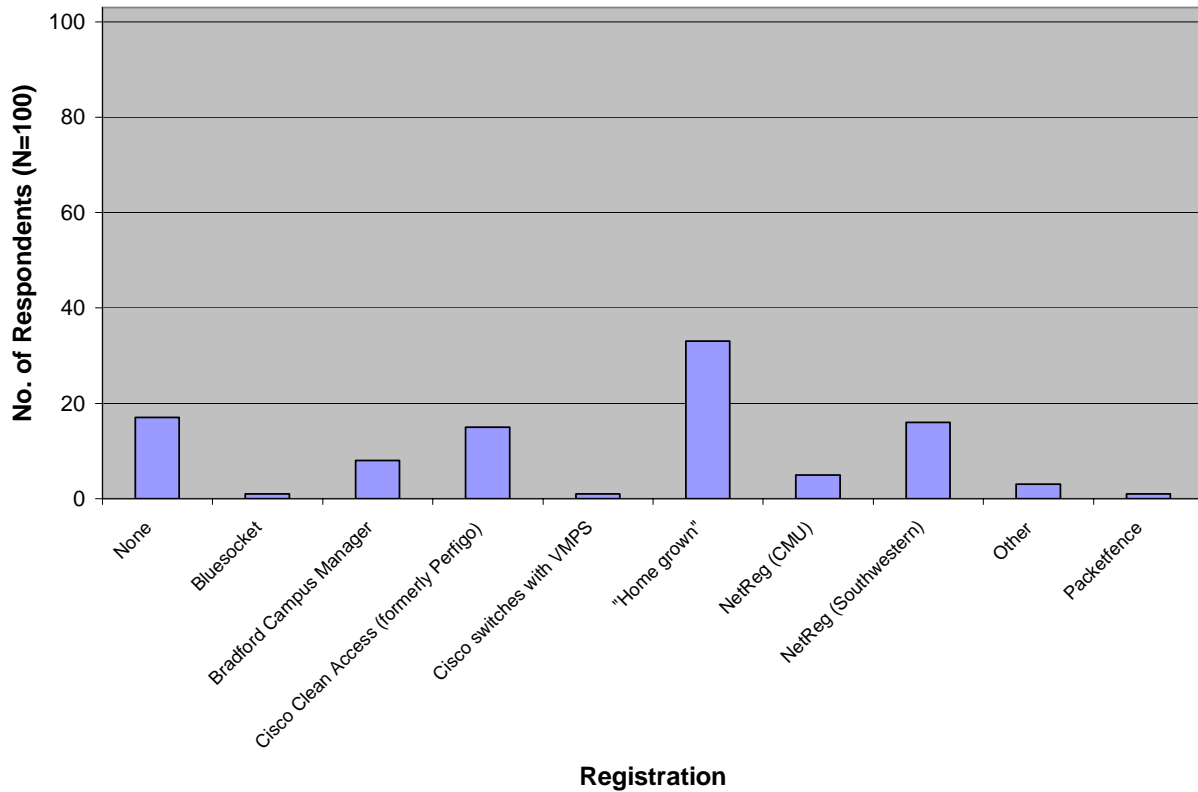


|   | Count | Percentage |
|---|-------|------------|
| None                                    | 13    | 13%        |
| Allot NetEnforcer                       | 7     | 7%         |
| Audible Magic*                          | 1     | 1%         |
| Checkpoint Floodgate-1                  | 0     | 0%         |
| Converged Networks (Sitara) QoSWorks    | 0     | 0%         |
| Dyband*                                 | 1     | 1%         |
| Emerging Technologies (ETinc) Appliance | 0     | 0%         |
| "Home grown"                            | 6     | 6%         |
| NetEqualizer*                           | 1     | 1%         |
| Other*                                  | 5     | 5%         |
| Packeteer Packetshaper                  | 64    | 65%        |

\* - These response options were added post-survey based on responses to the "Other - please explain" response option.

**25. What online network registration product does your institution primarily use? (Choose one)**

- We do not use an online network registration product
- Bradford Campus Manager
- Cisco switches with VMPS
- NetReg (www.netreg.org - Southwestern University)
- NetReg (www.net.cmu.edu/netreg/-Carnegie Mellon)
- Cisco Clean Access (formerly Perfigo)
- "Home grown" (i.e. developed in-house at your institution)
- Other - Please explain:

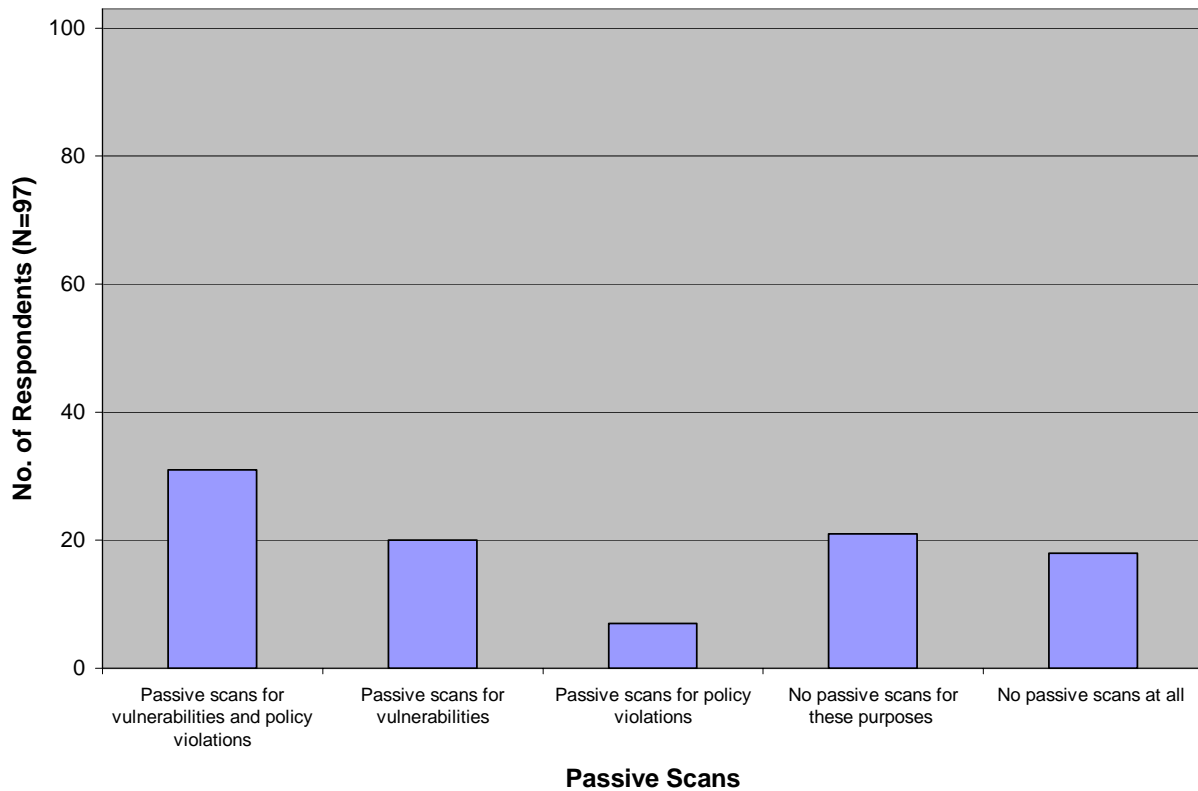


|                                       | Count | Percentage |
|---------------------------------------|-------|------------|
| None                                  | 17    | 17%        |
| Bluesocket*                           | 1     | 1%         |
| Bradford Campus Manager               | 8     | 8%         |
| Cisco Clean Access (formerly Perfigo) | 15    | 15%        |
| Cisco switches with VMPS              | 1     | 1%         |
| "Home grown"                          | 33    | 33%        |
| NetReg (CMU)                          | 5     | 5%         |
| NetReg (Southwestern)                 | 16    | 16%        |
| Other*                                | 3     | 3%         |
| Packetfence*                          | 1     | 1%         |

\* - These response options were added post-survey based on responses to the "Other - please explain" response option.

**26. Does your institution conduct passive scans on the residential computer network by using an intruder detection system or other monitoring tool(s) to assess network vulnerabilities or detect devices that violate your policies and requirements? (Choose one)**

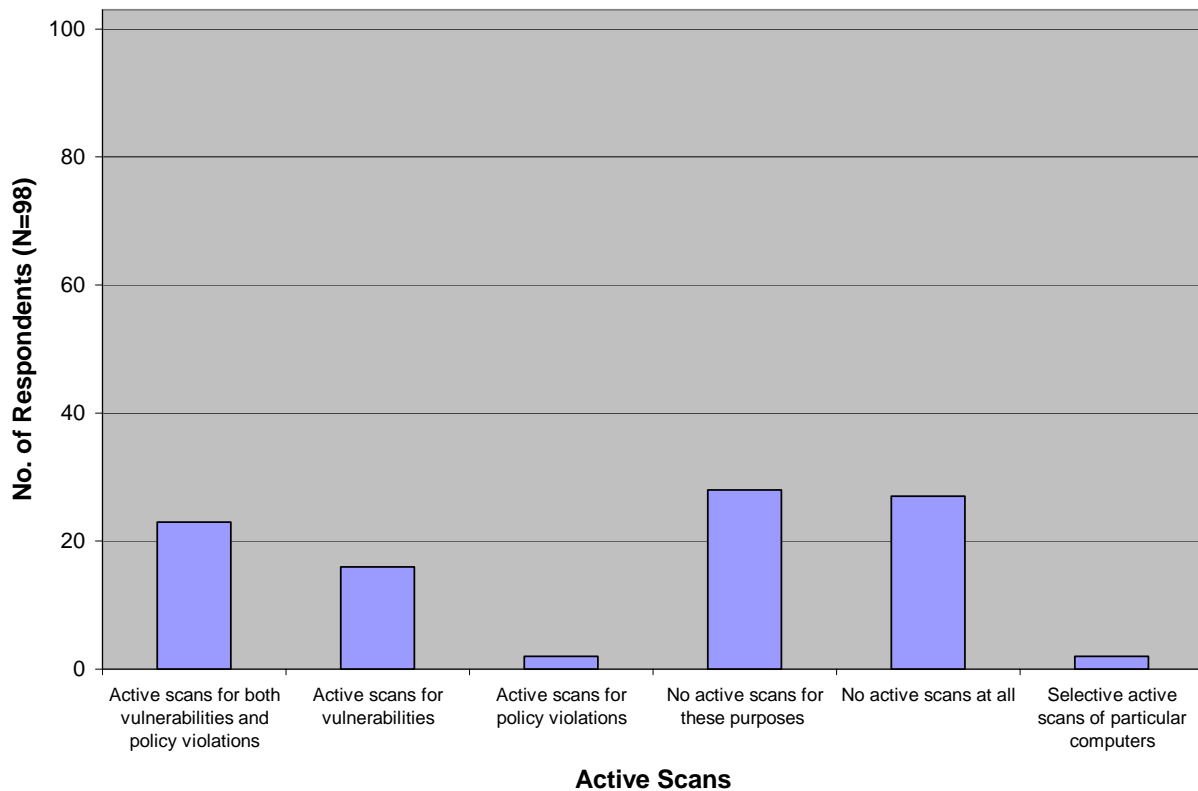
- Yes, we passively scan both to assess network vulnerabilities and detect devices that violate our policies and requirements
- Yes, we passively scan primarily to assess network vulnerabilities
- Yes, we passively scan primarily to detect devices that violate our policies and requirements
- No, we do not conduct passive scans for these purposes
- No, we do not conduct passive scans at all
- Other - Please explain:



|   | Count | Percentage |
|---|-------|------------|
| Passive scans for vulnerabilities and policy violations | 31    | 32%        |
| Passive scans for vulnerabilities                       | 20    | 21%        |
| Passive scans for policy violations                     | 7     | 7%         |
| No passive scans for these purposes                     | 21    | 22%        |
| No passive scans at all                                 | 18    | 19%        |

**27. Does your institution conduct active scans of the residential computer network by directly evaluating hosts on the network to detect vulnerabilities or devices in violation of your policies and requirements? (Choose one)**

- Yes, we actively scan to detect both host vulnerabilities and violations of our policies and requirements
- Yes, we actively scan primarily to detect host vulnerabilities
- Yes, we actively scan primarily to detect devices in violation of our policies and requirements
- No, we do not conduct active scans for these purposes
- No, we do not conduct active scans at all
- Other - Please explain:

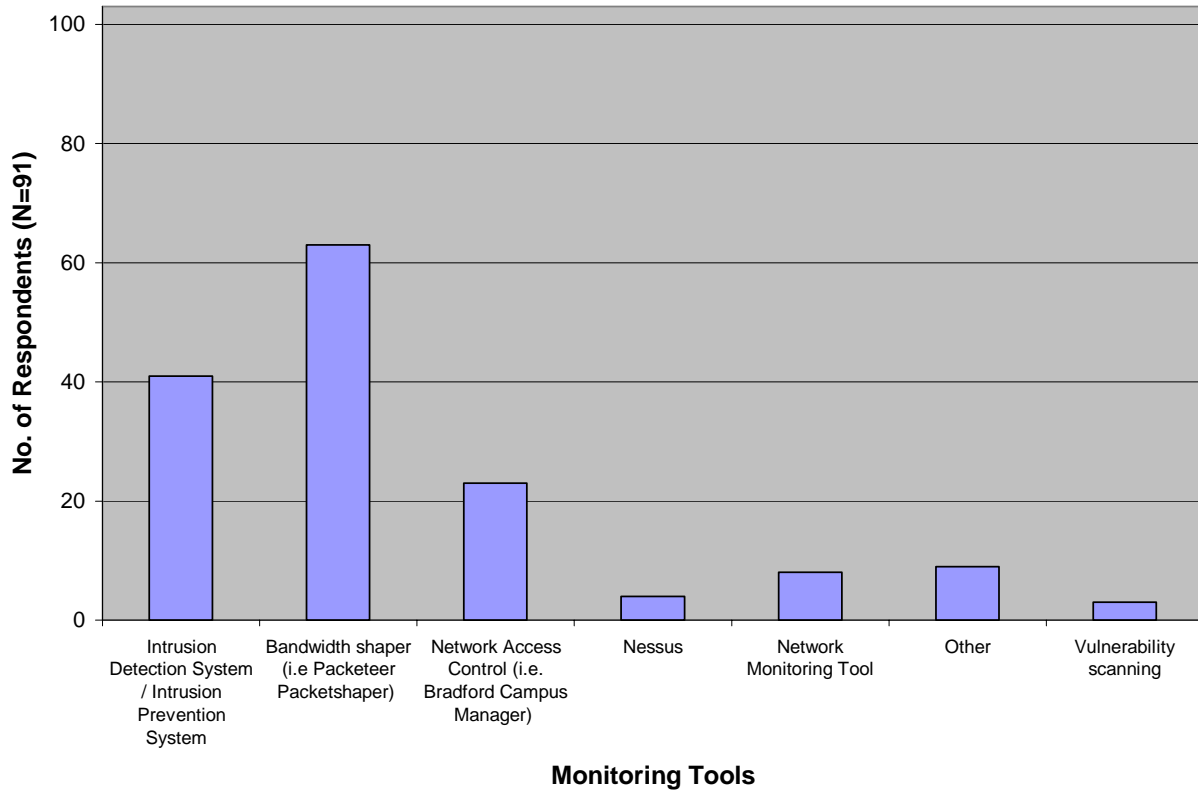


|   | Count | Percentage |
|---|-------|------------|
| Active scans for both vulnerabilities and policy violations | 23    | 24%        |
| Active scans for vulnerabilities                            | 16    | 16%        |
| Active scans for policy violations                          | 2     | 2%         |
| No active scans for these purposes                          | 28    | 29%        |
| No active scans at all                                      | 27    | 28%        |
| Selective active scans of particular computers*             | 2     | 2%         |

\* - This response option was added post-survey based on responses to the "Other - please explain" response option.

**28. What technologies does your institution use to monitor your residential computer network? (Choose all that apply)**

- Intrusion Detection System / Intrusion Prevention System
- Bandwidth shaper (i.e. Packeteer Packetshaper)
- Network Access Control (i.e. Bradford Campus Manager)
- Other - Please explain:

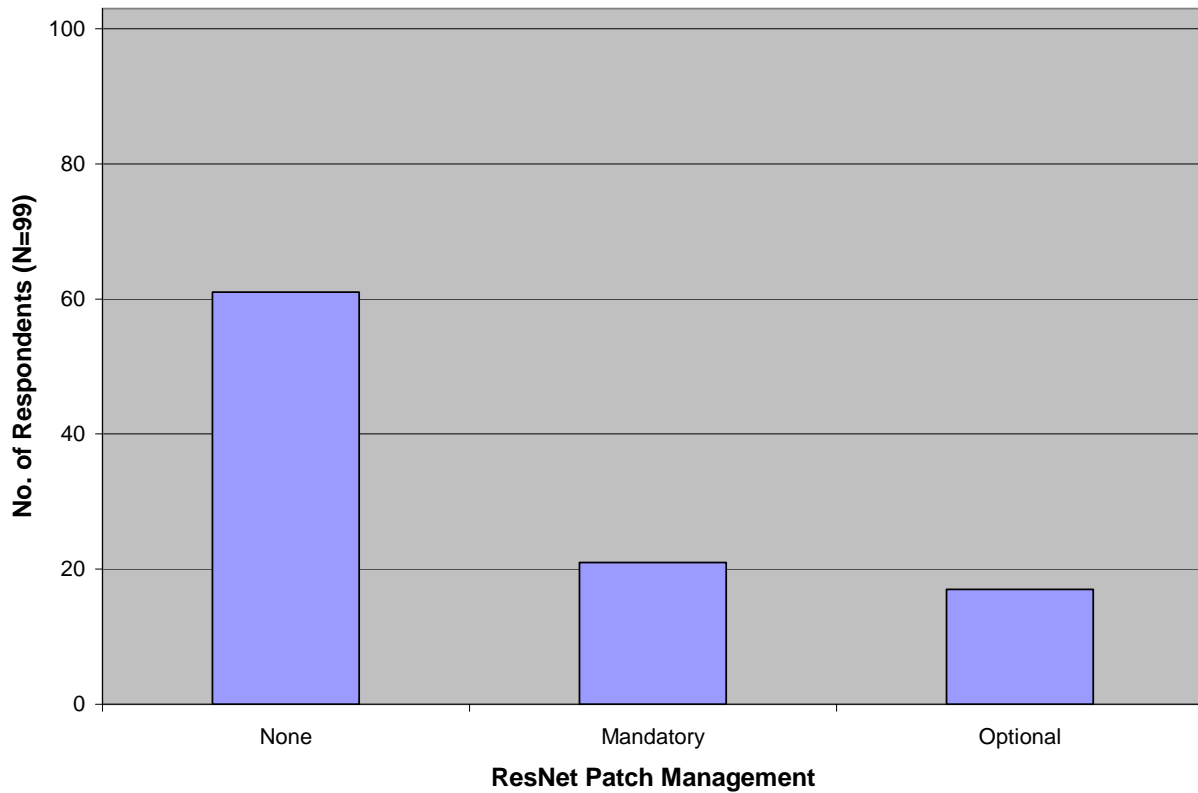


|  | Count | Proportion |
|--|-------|------------|
| Intrusion Detection System / Intrusion Prevention System | 41    | 45%        |
| Bandwidth shaper (i.e. Packeteer Packetshaper)           | 63    | 69%        |
| Network Access Control (i.e. Bradford Campus Manager)    | 23    | 25%        |
| Nessus*  | 4     | 4%         |
| Network Monitoring Tool*                                 | 8     | 9%         |
| Other*   | 9     | 10%        |
| Vulnerability scanning*                                  | 4     | 3%         |

\* - These response options were added post-survey based on responses to the "Other - please explain" response option.

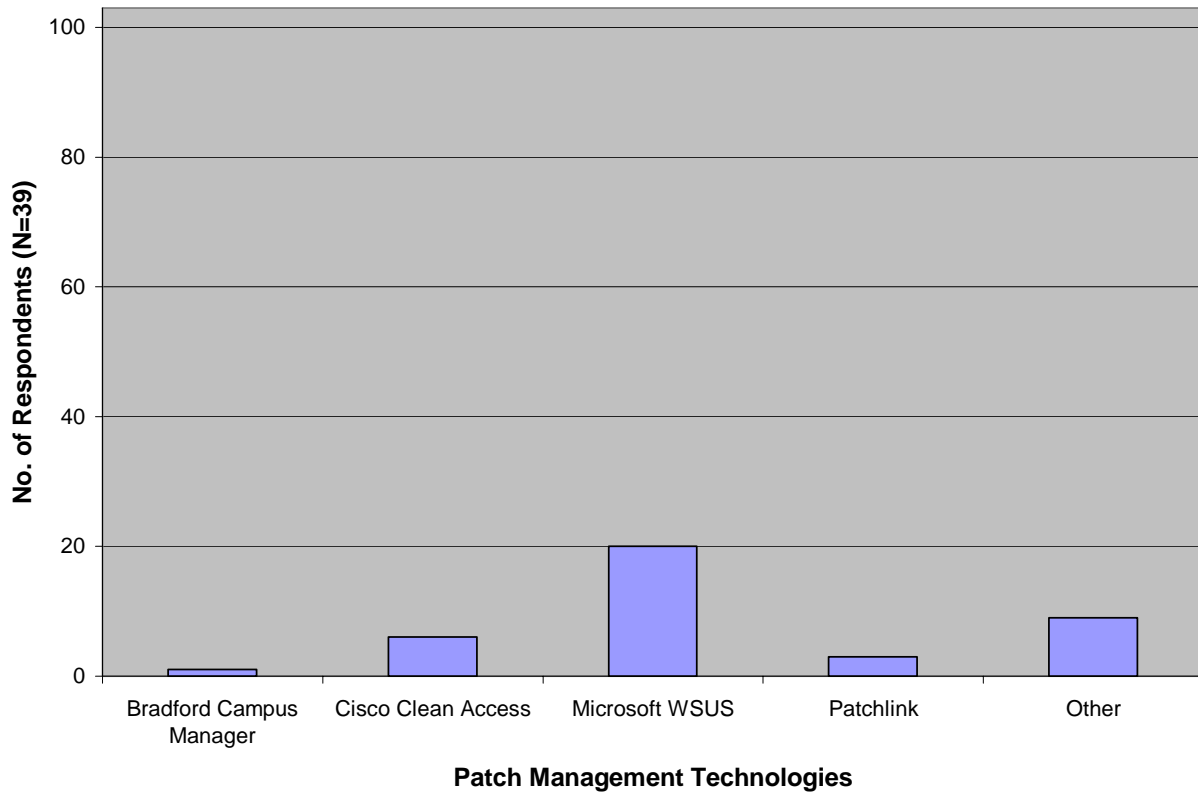
**29. Does your institution use a patch management technology that provides OS or security application updates after a computer is connected to your residential computer network? (Choose one)**

- No, my institution does not have a patch management strategy
- Yes, my institution employs patch management technology mandatory for all computers connected to the residential computer network
- Yes, my institution employs patch management technology but it is optional for computers connected to the residential computer network
- Other - Please explain:



|           | Count | Percentage |
|-----------|-------|------------|
| None      | 61    | 62%        |
| Mandatory | 21    | 21%        |
| Optional  | 17    | 17%        |

**29a. What patch management technology does your institution use?**



|                         | Count | Percentage |
|-------------------------|-------|------------|
| Bradford Campus Manager | 1     | 3%         |
| Cisco Clean Access      | 6     | 15%        |
| Microsoft WSUS          | 21    | 53%        |
| Patchlink               | 3     | 8%         |
| Other                   | 9     | 23%        |

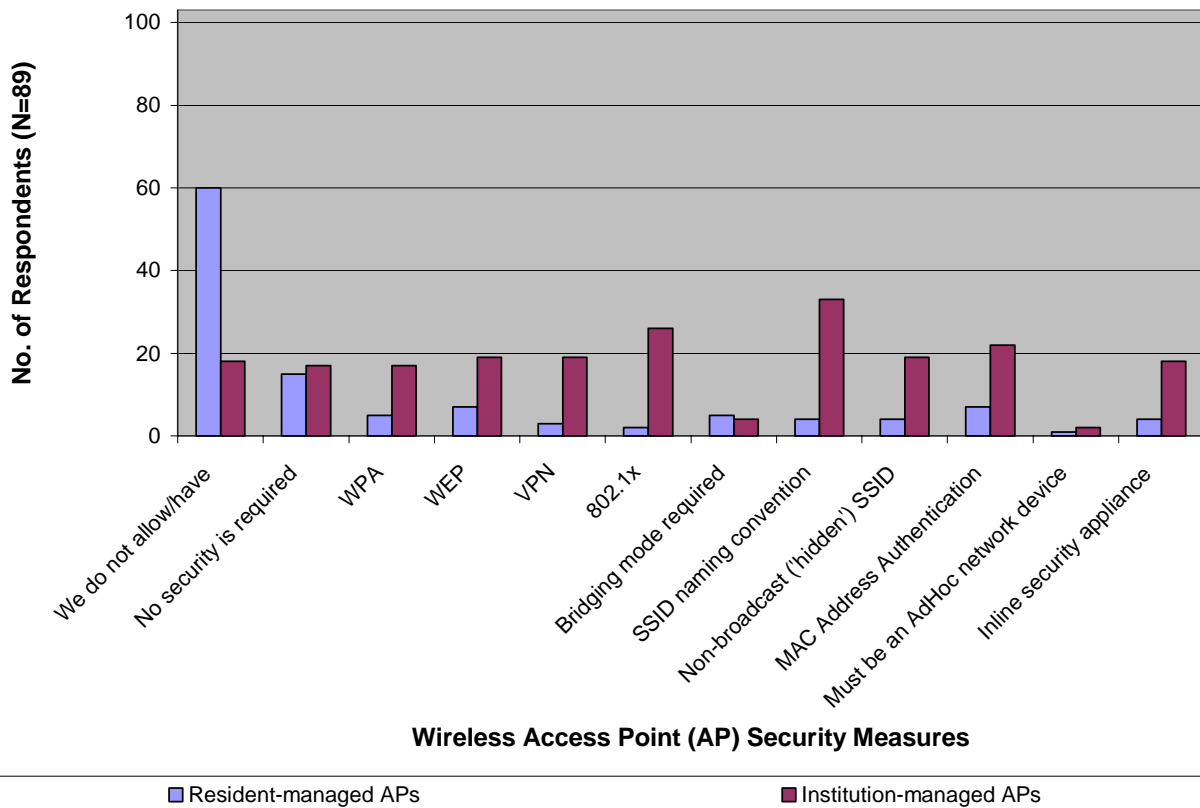
"Other" responses included:

- "Homegrown" (x5)
- Active Directory Group Policy
- ePolicy Orchestrator & NetReg
- Unknown
- "Vendor solutions"

**30. What security methods on the following list are employed or required for wireless Access Points (APs) managed by residents or managed by the institution on the residential computer network? (Choose all that apply)**

Resident Managed APs:    Institution Managed APs:

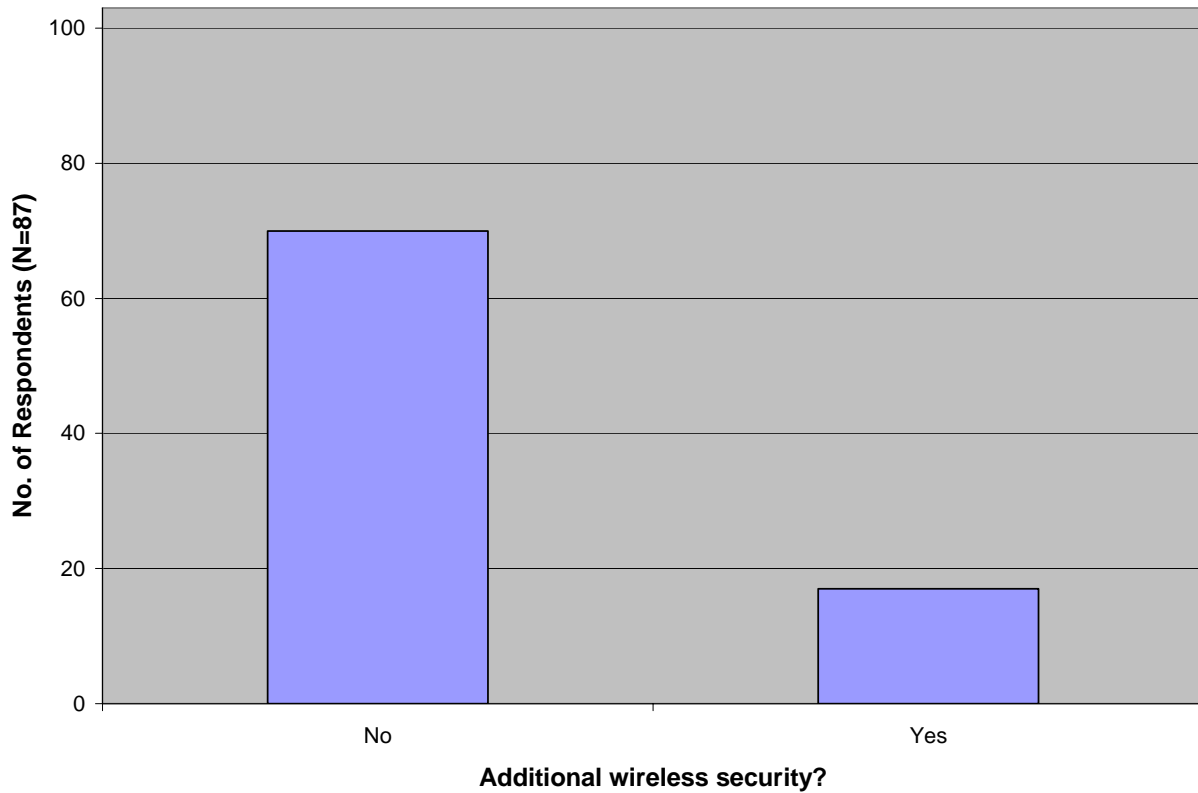
|   |                          |                          |
|---|--------------------------|--------------------------|
| We do not allow / we do not have                            | <input type="checkbox"/> | <input type="checkbox"/> |
| No security is required                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| Wi-Fi Protected Access (WPA)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| Wired Equivalent Privacy (WEP)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| VPN   | <input type="checkbox"/> | <input type="checkbox"/> |
| 802.1x  | <input type="checkbox"/> | <input type="checkbox"/> |
| AP is required to be in bridging mode                       | <input type="checkbox"/> | <input type="checkbox"/> |
| Naming convention for SSID                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| Non-broadcast ("hidden") SSID                               | <input type="checkbox"/> | <input type="checkbox"/> |
| MAC Address Authentication                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| Must be an AdHoc network device                             | <input type="checkbox"/> | <input type="checkbox"/> |
| Generic inline security appliance (i.e. Cisco Clean Access) | <input type="checkbox"/> | <input type="checkbox"/> |



|                                 |                         | Count | Proportion |
|---------------------------------|-------------------------|-------|------------|
| We do not allow/have            | Resident-managed APs    | 60    | 67%        |
|                                 | Institution-managed APs | 18    | 20%        |
| No security is required         | Resident-managed APs    | 15    | 17%        |
|                                 | Institution-managed APs | 17    | 19%        |
| WPA                             | Resident-managed APs    | 5     | 6%         |
|                                 | Institution-managed APs | 17    | 19%        |
| WEP                             | Resident-managed APs    | 7     | 8%         |
|                                 | Institution-managed APs | 19    | 21%        |
| VPN                             | Resident-managed APs    | 3     | 3%         |
|                                 | Institution-managed APs | 19    | 21%        |
| 802.1x                          | Resident-managed APs    | 2     | 2%         |
|                                 | Institution-managed APs | 26    | 29%        |
| Bridging mode required          | Resident-managed APs    | 5     | 6%         |
|                                 | Institution-managed APs | 4     | 4%         |
| SSID naming convention          | Resident-managed APs    | 4     | 4%         |
|                                 | Institution-managed APs | 33    | 37%        |
| Non-broadcast ('hidden') SSID   | Resident-managed APs    | 4     | 4%         |
|                                 | Institution-managed APs | 19    | 21%        |
| MAC Address Authentication      | Resident-managed APs    | 7     | 8%         |
|                                 | Institution-managed APs | 22    | 25%        |
| Must be an AdHoc network device | Resident-managed APs    | 1     | 1%         |
|                                 | Institution-managed APs | 2     | 2%         |
| Inline security appliance       | Resident-managed APs    | 4     | 4%         |
|                                 | Institution-managed APs | 18    | 20%        |

**30a. Are other security methods employed or required for wireless APs managed by residents or managed by the institution on the residential computer network? (Choose one)**

- No
- Yes - Please explain:



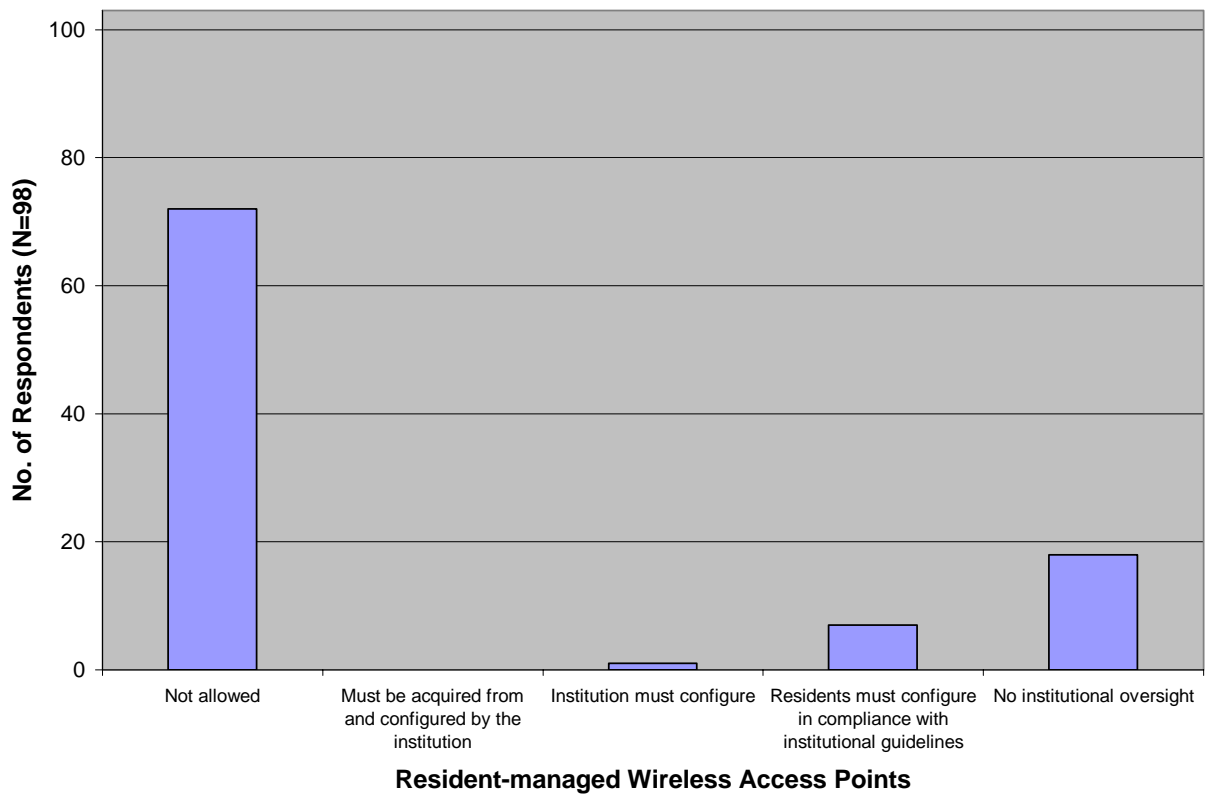
|     | Count | Percentage |
|-----|-------|------------|
| No  | 70    | 81%        |
| Yes | 17    | 20%        |

Open-ended "Yes" responses included:

- Bluesocket (x4)
- NetReg (x2)
- Active scanning on the wireless network
- Captive portal that requires login
- Perfigo
- Radius
- Some ports used by APs blocked at the switch level
- VPN
- Wired network is separate from wireless
- Wireless clients scanned before allowed online
- Wireless users can only access Internet and not campus network

**31. What type of oversight does your institution exert over APs installed by residents? (Choose one)**

- Our institution does not allow residents to install personally-owned APs
- Residents must acquire APs from the institution which are configured by the institution's IT or ResNet staff
- A representative of the institution's IT or ResNet staff configures the resident's personally-owned AP before installation
- Residents must configure APs in compliance with institutional guidelines
- The institution does not exert any type of oversight on the installation of personally-owned APs
- Other - Please explain:



|  | Count | Percentage |
|--|-------|------------|
| Not allowed  | 72    | 74%        |
| Must be acquired from and configured by the institution              | 0     | 0%         |
| Institution must configure   | 1     | 1%         |
| Residents must configure in compliance with institutional guidelines | 7     | 7%         |
| No institutional oversight   | 18    | 18%        |

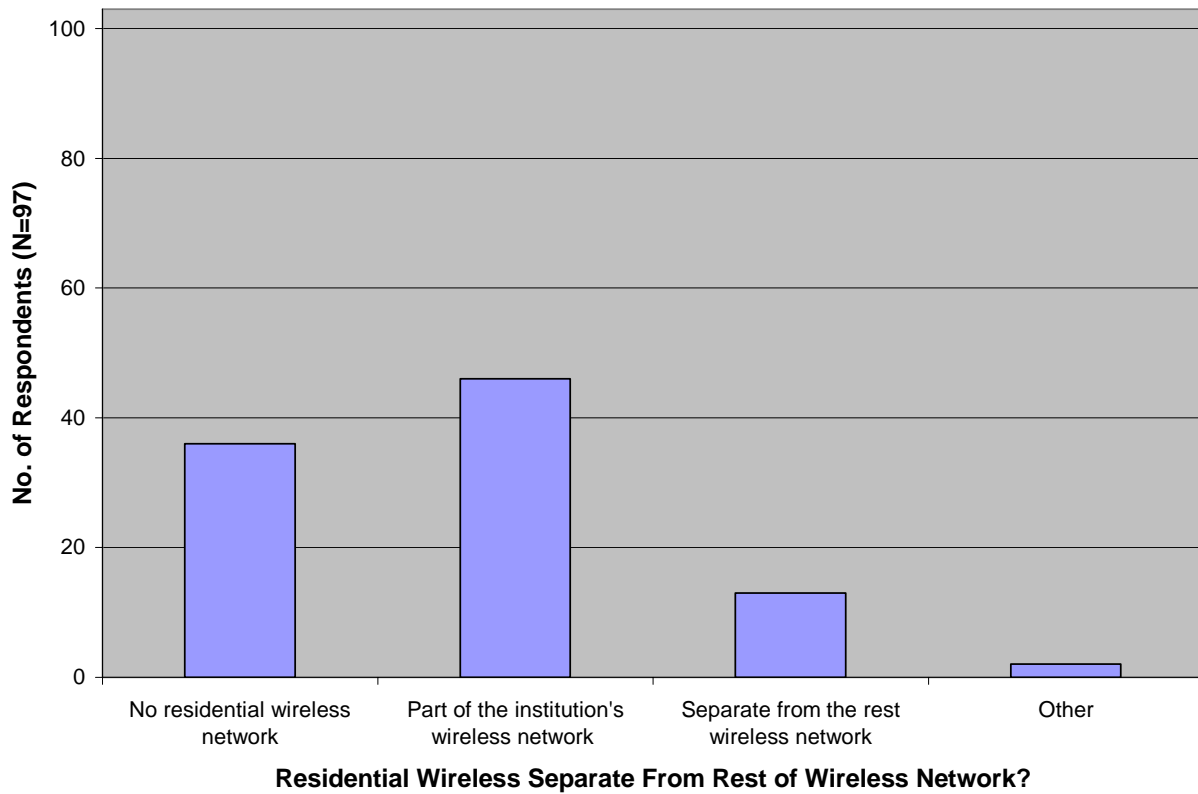
**31a. How do you enforce security requirements after residents install an AP?**

11 respondents responded to this question. Open-ended responses included:

- Disable port if problem discovered (x4)
- Regular audit (x2)
- We do not enforce our requirement (x2)
- Passive detection of NAT
- Spot checks

**32. If your institution employs wireless technology in residential areas, is the residential wireless network a part of the institution's overall wireless network or is it separate from the institutional wireless network? (Choose one)**

- Wireless technology is not provided in residential areas
- Wireless technology provided to residential areas is part of the institution's wireless network
- Wireless technology provided in residential areas is separate from the rest of the institution's wireless network
- Other - Please explain:



|  | Count | Percentage |
|--|-------|------------|
| No residential wireless network            | 36    | 37%        |
| Part of the institution's wireless network | 46    | 47%        |
| Separate from the rest wireless network    | 13    | 13%        |
| Other                                      | 2     | 2%         |

The three respondents who responded "Other" indicated that the wireless networks in their residential areas are heterogeneous.