TEST REPORT

Tolly.

#212105

March 2012

Commissioned by
ForeScout Technologies, Inc.

ForeScout CounterACT

Comparative Network Access Control Evaluation vs. Bradford Networks, Cisco Systems and Juniper Networks

EXECUTIVE SUMMARY

The use of Network Access Control (NAC) solutions is growing in organizations of all sizes. This is being driven by the demand for greater access to network resources by different users on a variety of endpoints, including managed and personal mobile devices. This, coupled with the increase in malware and targeted threats, and the various compliance directives for asset integrity, protection, network segregation and data privacy bring NAC to the forefront as an effective defense.

NAC offerings, once focused purely on authenticating users and their devices, have evolved to offer broader capabilities, including endpoint discovery and configuration assessment, policy definition/enforcement, guest management and endpoint remediation.

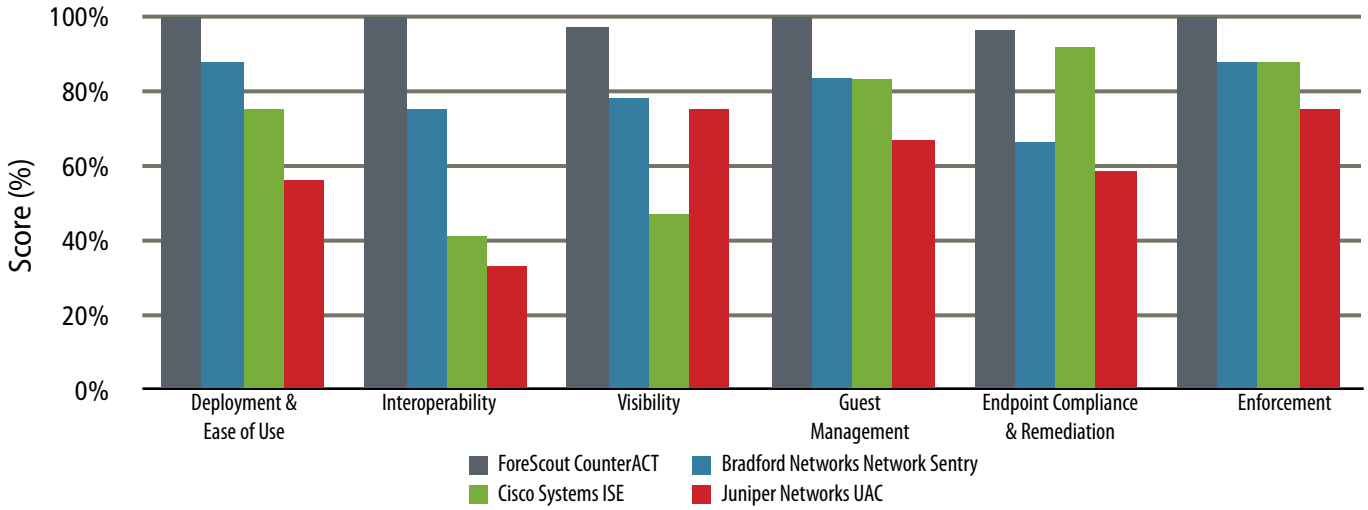
...<continued on next page>

THE BOTTOM LINE

ForeScout CounterACT:

1. Offers greater ease-of-use, integrated functionality, vendor interoperability and scalability
2. Enables faster deployment with less operational impact, utilizing agent-less, real-time device assessment (including mobile) with customizable policy templates
3. Provides extensive built-in policies with automated device classification, enforcement and remediation options
4. Combines a rich feature set, flexible implementation, easier administration and scalability into one solution, contributing to a lower total cost of ownership

Network Access Control Systems
Overall Score Across Key Areas



Notes: Bars above indicate the percentage scored of the total number of available points in a given category. Individual items were scored 0-4, with "0 "meaning no support and "4" meaning the solution delivered full support. Thus, a 100% indicates that a given product was rated a "4 out of 4" for all points in a given area.

Source: Tolly, January 2012

Figure 1

Executive Summary, Continued...

Mid-tier and large organizations, typically faced with managing a heterogeneous infrastructure, diverse access requirements, and dynamic and complex networks, can benefit from a NAC solution that provides policy-based management and is flexible to deploy, easy to use and uncomplicated to manage.

This evaluation found that though most NAC products seem to offer comparable features, there remain considerable implementation, administration and functional differences across vendors.

These deployment and management differences can materially impact the overall effectiveness of a network access control implementation and can result in a higher total cost of ownership.

Additionally, buyers should not assume that large network infrastructure vendors offer extensive and flexible NAC solutions. In the areas examined for this evaluation, NAC "pure-play" vendors ForeScout and Bradford bested "infrastructure" vendors Juniper and Cisco in almost every category.

Four NAC products were evaluated in 34 criteria areas across 6 categories. ForeScout CounterACT scored the highest in each category, Bradford Networks Network Sentry, on average, placed second with Cisco Systems ISE and Juniper Networks UAC alternating at 3rd and 4th place. See Figure 1.

Background

Many organizations conduct a comprehensive appraisal of network security products prior to purchase. To expedite this assessment process, ForeScout Technologies, Inc. commissioned Tolly to evaluate four of the top-selling network access control products: their own, ForeScout CounterACT for Network Access Control solution versus Bradford Networks Network Sentry, Cisco Systems ISE and Juniper Networks UAC. Areas covered in this evaluation include: deployment, interoperability, guest management, remediation, endpoint compliance, enforcement and scalability.

The evaluation found that ForeScout CounterACT delivers substantial user/device intelligence, and more comprehensive NAC functionality with or without an agent (software on the endpoint). Tolly found that CounterACT is highly interoperable, leveraging the user's existing infrastructure, while providing a mature and flexible policy engine with extensive remediation and enforcement capabilities.

CounterACT's integrated approach, which has a minimal impact on existing endpoints and the operating environment, can be centrally administered with an intuitive management console.

Tolly found that Cisco and Juniper employ a multi-component approach to NAC. Their approach would seem to be optimized to operate within a significantly more homogenous, static and recently upgraded network and security infrastructure. They also require fully managed endpoints with respective Cisco or Juniper agents to support full NAC functionality.

Relative to ForeScout and Bradford's NAC offerings, Tolly found that Cisco and Juniper offer more complex, inflexible and potentially costly (in terms of necessary switch and network upgrades, software agent management and administrator attention) approaches to NAC. They seem to have a higher risk of implementation failure, if the operating environment is more expansive, diverse and dynamic, which is usually the case with medium-to-large enterprises.

ForeScout CounterACT Comparative NAC Functionality and Ease-of-Use

Tolly. Certified

January 2012

Bradford Networks Network Sentry, while providing similar basic functionality to ForeScout CounterACT, does not provide many of the "extras" across the various categories under evaluation. As a result, their approach does not operate as seamlessly, has greater agent reliance for NAC functionality, and does not provide as easy a means to centrally manage policies across numerous deployed appliances.

To quantitatively represent the findings, Tolly engineers assigned a numerical grading system (0-4) in addition to logging their experiences to asses each of the criteria. "0" represents a solution not meeting the success criteria, while "4" represents a solution meeting all success criteria, as set forth by engineers at the beginning of each evaluation. A full definition of the scale can be found in the legend of Figure 2.

Readers should note, however, that even though some solutions received the same score in a given category, readers should reference the associated table to

determine differences/strengths of a given solution, as the same numerical score does not denote the products are identical in their strengths/weaknesses.

Test Results

Usability and Deployment

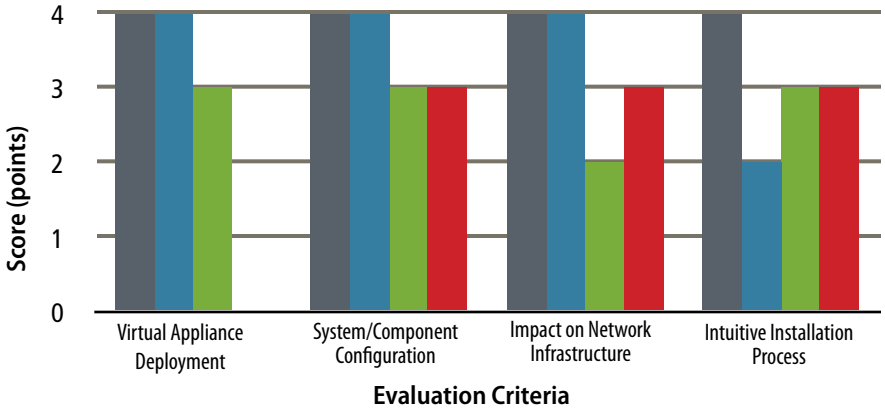
Tolly engineers evaluated the usability and deployment process for each solution using a qualitative approach. Engineers noted the time to deploy and configure a system, how intuitive the installation/configuration process was, how many steps were involved, how many components to configure, the impact on network, as well as virtual appliance availability and functionality.

Tolly engineers rated ForeScout a 4/4 for all evaluation criteria as engineers found ForeScout to have the most complete and integrated NAC solution; with identical functionality in either a virtual or physical appliance. In addition, ForeScout has the fewest components to install and configure, with an intuitive Graphical User Interface (GUI) to aid in installation/deployment. See Figure 2 and Table 1.

The ForeScout appliance does not have to be inline to achieve full NAC capabilities and needs only a SPAN port configured on a single switch to be able to listen in (monitor) and profile the network.

Cisco and Juniper require considerably more components to configure and manage. Bradford Networks also proved to be more difficult to deploy, even with a recent GUI upgrade.

Engineer Rating of Ease-of-Use and Deployment Capabilities for NAC Devices



Scoring Legend	
4	Meets all Success Criteria of Evaluation
3	Meets all Success Criteria of Evaluation, but with caveats
2	Meets most Success Criteria of Evaluation
1	Meets some Success Criteria of Evaluation
0	Does not meet Success Criteria of Evaluation

Notes: Bars above indicate the number of points scored out of the total. Individual items were scored 0-4, with "0 "meaning no support, and "4" meaning the solution delivered full support. Solutions may offer more capabilities, see Table 1. Juniper UAC supports virtual appliance deployment, but is only for demo and testing purposes. 'Time to deploy' was measured in this evaluation but was unable to be assigned a score. See Table 1 for corresponding information.

Source: Tolly, January 2012 Figure 2

Ease-of-Configuration & Impact on System and Network Infrastructure

Any new component, to be added to an existing network must be configured properly in order to fully integrate and provide full functionality. Unfortunately for some NAC approaches, this can require infrastructure upgrades and provisions that can impact overall deployment cost, effort and deployment timeline.

Tolly engineers evaluated the ease-of-configuration: whether the user was required to deploy multiple components and if so, how complex was the deployment and interoperability of those components.

To determine the impact on the network, engineers observed what network configurations were required in order to deploy the NAC solution (i.e. servers/switches). Readers should note that this does not assess the impact of managing and configuring agent software on endpoint devices. See Figure 2 and Table 1.

Both ForeScout CounterACT and Bradford Networks Network Sentry scored a 4/4 in both of these categories. For ease-of-configuration, Cisco ISE and Juniper UAC each received 3/4. For Impact on Network, Cisco received a 2/4 score, while Juniper received a 3/4 score. See Figure 2 and Table 1.

ForeScout installation requires simple configuration of physical NICs and virtual switches (for their virtual appliance – a physical appliance is also available). The device operates out-of-band, although can be configured for inline operation. Once the network configuration is complete, a user need only set up the console and install the license to begin using the solution.

ForeScout CounterACT requires less configuration than the other solutions under evaluation. Only a SPAN port on the switch where the appliance is connected (ideally to the switch with the most visibility), as well as read/write SNMP credentials and/or CLI credentials to retrieve deeper information must be configured. The credentials to directory servers must also be provided.

For Bradford Networks Network Sentry's configuration/installation, the virtual appliance (VA) is the only component required for full virtual installation. Some NAC functionality requires additional modules, which are licensed separately.

Bradford Networks, though receiving a 4/4 for both ease-of-configuration and impact on system, requires slightly more network configuration and thus has a higher impact on the system than ForeScout CounterACT. Bradford Networks requires network switches to be configured for Command Line Interface (CLI) access, SNMP access, trap configuration for notification and credentials for Active Directory/LDAP for authentication.

Although Cisco ISE also received a 3 out of 4 grade for ease-of-configuration, Cisco ISE requires more effort to set up the ISE system, as well as a great deal more configuration both on the device and to the network than Juniper UAC.

Cisco ISE can operate in a standalone or distributed environment but is not a "plug-and-play" system. Additional configuration of various Cisco network infrastructure devices and endpoints must be completed (and maintained) in order for ISE to

Engineer Observation Summary: Usability and Deployment

Corresponds to Scored Data in Figure 2

	Evaluation Criteria	Engineer Observations			
		ForeScout CounterACT	Bradford Networks Network Sentry	Cisco ISE	Juniper UAC
System/ Component Configuration	Is the user required to deploy multiple components?How many? How complex is the deployment and interoperability of those components?	User is not required to deploy multiple components: up to 4,000 endpoints are covered with a single virtual appliance. Requires configuration of physical NICs and virtual switches on ESX server.	User is not required to deploy multiple components for a virtual deployment. Other components are licensable features which require a license key.	User is not required to deploy multiple components, however, extensive network configuration must occur in order to for the appliance to perform any of its roles.	User required to install a minimum of one standalone Juniper UAC appliance. The configuration, however, must be done manually.
Impact on Network Infrastructure	What network configurations were required to deploy NAC solution (E.g. switches, configuration servers...)	Requires no actual configuration changes, but users must provide credentials (switch/SNMP/ domain/ Active Directory, etc.)to the appliance.	Requires no actual configuration changes, but users must provide credentials (switch/SNMP/ domain/ Active Directory, etc.)to the appliance.	Requires 802.1X and RADIUS to be set up/ configured on network devices.	Requires extensive configuration. Depending on environment, customer will need to configure: RADIUS, 802.1x, Infranet Enforcer policies and Active Directory. Existing Juniper switches can be configured to communicate with UAC.
Time to Deploy*	How much time did it take to set up and deploy a system in the network?	~16 man-hours	~ 16 man-hours	~40+ man-hours	~24 man-hours
Intuitive Installation Process	Is the GUI self-explanatory, or is there a long learning curve? How easy was the solution to install and configure?	Provides good documentation, which allows for quick and easy ramp-up. Walks users through how to set up and configure their environment	Relatively simple installation with a complete, if outdated, interface. Utilizes discrete components, which are allowed to be configured disjointly of supporting policies.	The GUI is well-documented, however, setup and deployment required extensive vendor support.	Relatively easy appliance to deploy with a "Guidance" tab, which walks through users how to set up and configure their environment
Virtual Appliance	Can the deployment be based on virtual appliance?	Provides full functionality in virtual environments.	Provides support for virtual environments, but moderate configuration is required.	Provides support for virtual environments, but cannot perform inline posture assessment/ enforcement.	Does not provide support for virtual environments. Virtual appliance is only for demo and testing purposes.

Notes: *'Time to Deploy' could not be assigned a numerical score, and thus was not included in Figure 2, but should be taken into consideration when determining a solutions' over all ease-of-use and deployment.

Source: Tolly, January 2012 Table 1

perform any of its roles: Information, Administration, Policy Service, Network Access Device and Monitoring.

In addition to the configurations required for installation, Cisco ISE requires significant configuration changes to existing network hardware, thus their 2 out of 4 rating. 802.1X as well as RADIUS must be configured on network devices including wireless access controllers, switches and VPN concentrators in the network, as well as 802.1X supplicant/Cisco agent on any managed device to access the network, in order for Cisco ISE to provide complete network access control functionality

With Cisco ISE, any devices that are not to be authenticated (i.e. printers) must have Mac Authentication Bypass (MAB). To take full advantage of available capabilities Cisco ISE uses NTP, RADIUS, AAA, VLANs, 802.1X, MAB, WebAuth, Device tracking, DHCP snooping, ACLs, Cisco Security Group Access, Logging, syslog and SNMP, all of which need to be configured either on the ISE appliance, the network device, server or all of the above.

For Juniper's initial configuration/ installation, the user is required to install a minimum of one standalone Juniper UAC appliance. The client will perform an initial configuration via the console, but any further configuration must be done via the GUI. Hence, the 3 out of possible 4, grade for ease-of-configuration.

Juniper's impact on existing network infrastructure, depending on the environment, is moderate with a 3 out of 4 grade. Users will be responsible for configuring RADIUS, 802.1X, and Intranet Enforcer policies, as well as needing to configure an administrator account for Active Directory. If Juniper switches are already present in the network, they can be reconfigured to communicate with the Juniper UAC which will provide policing for the authenticated users.

Time and Steps to Deploy and Configure

Engineers attempted to determine ease-of-use by noting how much time was required to deploy and configure a solution on the network. Also noted was component complexity and intuitiveness of the setup/ configuration process. Please note that solutions are not graded in a (0-4) scale in this area as the time to deploy served as the measurement metric for this criteria.

Tolly engineers found that ForeScout CounterACT was the most intuitive and easy-to-use/easy-to-deploy solution among those evaluated. CounterACT's installation guide allows less-experienced users to conduct advanced functions. The GUI is well-developed and presents rich details. The policy engine supports simple to complex logic. Easy-to-understand presentation of data aids users in policy development and troubleshooting. To help users develop and troubleshoot policies, CounterACT ships with numerous built-in templates that can be adjusted to support different policies (such as anti-virus or patch management). CounterACT also supports an expandable architecture for network and security infrastructure interoperability; Once a dictionary file is downloaded and installed, all of that component's attributes are integrated into the system automatically. See Figure 2 and Table 1.

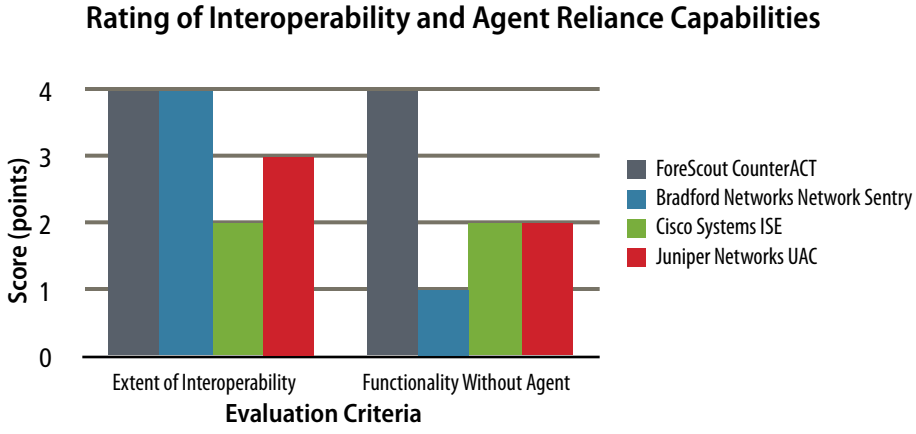
Engineers were able to have the ForeScout solution up and running within the span of two 8-hour work days. Due to its flexible policies and wealth of options, engineers spent an additional 8-hour work day tweaking policies to reflect their specific requirements.

Bradford Networks Network Sentry took around the same time as ForeScout to configure/deploy, however, engineers noted that the length of time spent was not due to many options to configure, but rather due to a complicated user interface and installation process. Bradford Networks utilizes a Web portal, which engineers found to be non-intuitive with a complex layout, even though Bradford boasts a recent GUI upgrade. The total time to deploy and configure the solution was ~16 work hours. However, this did not include some of the more extensive policy creation and system tuning (such as guest networking and unknown device classification) as was achieved during the same two-day time period as ForeScout CounterACT.

On the other side of the spectrum, Cisco ISE took engineers a work week to get up and running. This is due to the large amount of configuration that is needed on the appliance, as well as the complexity of the components that must be configured: network infrastructure, basic guest management, compliance and profiling.

Engineers found Cisco's installation to be challenging and resource-intensive for first-time users. Installation required several different forms of documentation, lab testing, and WebEx conferences with Cisco in order for engineers to configure the system to work in the test environment.

The Juniper UAC proved to be relatively easy to deploy, with a "Guidance" tab which guides users through configuration steps like initial system setup, guest users, user realms/roles, sign-in policies, etc. Despite the intuitive interface, it still took engineers 3 full work days (~24 work hours) to implement the solution. During this time, only basic functionality was configured. Other NAC functionality, such as guest



Scoring Legend	
4	Meets all Success Criteria of Evaluation
3	Meets all Success Criteria of Evaluation, but with caveats
2	Meets most Success Criteria of Evaluation
1	Meets some Success Criteria of Evaluation
0	Does not meet Success Criteria of Evaluation

Notes: Bars above indicate the number of points scored out of the total. Individual items were scored 0-4, with "0 "meaning no support, and "4" meaning the solution delivered full support. "0" score is represented by the absence of the vendor in a given category. See Table 2 for definitions of "success criteria" and additional details.

Source: Tolly, January 2012 Figure 3

management and extensive policy creation, were not able to be addressed in the allotted time.

Virtual Appliance Availability and Functionality

For each solution, engineers determined whether it could be deployed on a virtual appliance, how many components were required for successful installation, the extent of the visibility and classification functionalities, and their variation between the physical and virtual appliances. Engineers also noted the impact on network infrastructure and what changes, if any, needed to be made in order to accommodate a virtual appliance. See Figure 2 and Table 1.

ForeScout CounterACT scored a 4/4 in this area as the CounterACT virtual appliance can be quickly and easily installed and managed in VMware consolidated data centers, and provides identical functionality to the CounterACT physical appliance. The CounterACT Enterprise Manager (which centrally manages policy and configuration across multiple CounterACTs) is also available as a virtual appliance. The device coverage for either physical or virtual models is the same. Once physical NICs and virtual switches are configured, users need only to set up the system through a wizard GUI and install the license to begin using CounterACT.

Bradford Networks also received a 4/4 score as it is also able to be deployed as a single virtual appliance, but requires an Open Virtualization Format (OVF) deployment file. Once installed, it requires configuration via a Web-based wizard then reboots to allow users to configure NAC properties.

Cisco ISE received a 3/4 score, as Cisco can be deployed as a virtual appliance, but it cannot perform inline posture assessment/ enforcement, a key NAC function. As far as system complexity, Cisco ISE can operate in a standalone or distributed network, but is not a "plug-and-play" system. Additional configuration of network infrastructure must be completed in order for ISE to perform any of its roles ("personas"). Such "personas" are Information, Administration, Policy Services, Network Access Device and Monitoring.

Juniper's virtual appliance, on the other hand, is for demo and testing purposes only, but in order to deploy the virtual appliance, the customer is required to install a minimum of one standalone UAC appliance. The client will perform the initial configuration via the console. The virtual appliance was used for this evaluation, since it has the same functionality as would the physical appliance, the UAC virtual appliance is not commercially available.

Interoperability and Agent Reliance

Extent of Interoperability

Tolly engineers attempted to determine to what extent a given solution integrated with the existing network. The "network" used for the evaluation replicated a typical medium-to-large enterprise environment and addressed how many different switch, VPN, Wi-Fi vendors are supported, as well as what types of authentication servers and user directories are supported.

The evaluation found that ForeScout CounterACT supports multivendor and heterogenous networks and integrates easily with their plug-in architecture. This allows for faster and easier integration and provides greater security coverage and policy enforcement. Cisco and Juniper offer the least interoperability and are heavily

reliant on their own products and special configurations. See Figure 3 and Table 2.

Based on publicly-available vendor documentation, the evaluation found that CounterACT supports the widest range of devices of all solutions tested, supporting most major switch, VPN and Wi-Fi vendors and most popular user directories from Microsoft, Novell and Oracle/Sun, including, but not limited to, Active Directory and Lotus Domino. In addition to hardware infrastructure, CounterACT supports integration with a wide range of endpoint protection suites, host-based security systems (HBSS) and Security Information Event Management (SIEM).

CounterACT successfully detected both test switch vendor types, Cisco and Juniper, Juniper firewall (the only VPN device), and the Microsoft Active Directory server, thus earning them a 4 out of 4 score for interoperability.

Bradford Networks also received a score of 4 out of 4 for interoperability, with similar, if not quite as extensive built-in support for popular switch, VPN and Wi-Fi vendors.

Based on publicly-available vendor documentation, engineers found that Cisco ISE only supported/detected other Cisco devices out-of-the-box, with little information on devices from other vendors. However, like Bradford and ForeScout, Cisco ISE can support any AD or any LDAP-capable system, thus earning them a 2 out of 4 score.

Juniper UAC provided slightly better vendor/device support, with some major switch, VPN and Wi-Fi vendors, such as Juniper, Cisco and Nortel for VPN, included out of the box. Based on publicly-available

Observation Summary: Interoperability and Agent Reliance

Corresponds to Scored Data in Figure 3

	Evaluation Criteria	Engineer Observations			
		ForeScout CounterACT	Bradford Networks Network Sentry	Cisco ISE	Juniper UAC
Extent of Interoperability*	How many different switch, Wi-FI and VPN vendors are supported? What authentication servers and user directories are supported?	Supports most major switch, VPN and Wi-Fi vendors. Supports most popular user directories including, but not limited to, Active Directory and Lotus Notes out-of-box. Supports any AD or LDAP-capable system.	Supports most major switch, VPN and Wi-Fi vendors. Supports most popular user directories including, but not limited to, Active Directory and Lotus Notes out-of-box. Supports any AD, Sun, or LDAP-capable system.	Fully supports Cisco switches only out-of-box. Supports any AD or LDAP- capable system.	Supports some switch, VPN and Wi-Fi vendors out-of-box, including Juniper, Cisco and Nortel. Interoperability can be expanded by using dictionary files. Supports any AD or LDAP-capable system.
Functionality without Agent	What functions are available for a machine with no agent: Visibility for new devices?	Will discover and fully classify a newly added device in <2 minutes with no agent required.	Supports visibility for newly connected devices.	Supports visibility for newly connected devices.	Supports visibility for newly connected devices.
	What functions are available for a machine with no agent: Classification of device type?	Classifies devices by: IP Address, MAC address, NetBIOS Hostname, Domain Member, OS Class, Network Function, OS Fingerprint, and NIC Vendor	Supports classification of device by DHCP lease analysis only. (OS, IP, ports, vendor OUI) Static IP, limited classification.	Through the profiling policy, Cisco ISE can detect information about the machine such as OUI, IP address, uptime, description, MAC address, hostname and DHCP identifier.	Does not support classification of device type without pre-existing 802.1X client.
	What functions are available for a machine with no agent: Inspection of machine and user information?	Performs inspection and obtains: User, Manageable (Domain), Windows Manageable (Secure Connector), Secure Connector Type, HTTP User Agent, Switch IP, Switch Port, Switch Port Action, Switch Port Connection Status, Switch VLAN ID and Name, Number of Hosts on Port, Switch Vendor, Signed In Status, Open Ports, Authentication Login and Admission	Does not support inspection of endpoint without dissolvable/ persistent agent or directory-based scan.	Does not support inspection of endpoint without client agent.	Does not support inspection of endpoint without client agent.
	What functions are available for a machine with no agent: Notification, remediation and quarantine capabilities?	Supports notification, remediation and quarantine capabilities: Notification: HTTP Notification, HTTP Redirect to URL, Send Balloon Notification, Send Email, Send email to user. Remediation: Disable External Device, Kill Instant Messaging, Kill P2P, Kill process (Linux/Mac/Windows), Run Script (Linux/Mac/Windows), Set Registry Key, Start AV, Start Updates (Windows/Mac), Update AV, Windows Self Remediation. Quarantine: ACL, Assign to VLAN, Switch Block, Virtual Firewall, Wireless Host Block.	Notification: HTTP redirect to captive portal. Remediation: None without client agent. Quarantine: Assign to VLAN, switch port blocking and ACL.	Notification: HTTP redirect to captive portal. Remediation: None without client agent. Quarantine: Assign to VLAN, switch port blocking and ACL.	Notification: HTTP redirect to captive portal. Remediation: None without client agent. Quarantine: Assign to VLAN, switch port blocking and ACL.

Note: Extent of interoperability was determined from publicly available vendor documentation - not tested by Tolly.

Source: Tolly, January 2012

Table 2

vendor information, engineers determined the interoperability can be expanded by using dictionary files.

Juniper can also support any AD or LDAP-capable system, thus earning Juniper UAC a 3 out of 4 score.

Agent Reliance

Many organizations prefer to avoid introducing additional endpoint client software (agents) into a network, if possible. In addition to added operational, deployment and maintenance costs, additional agents also open the door to potential problems associated with: conflicts due to the use of multiple agents on a single endpoint, endpoints that can not support an agent, or those endpoints that are not corporate-managed. NAC vendors offer different agent and agent-less options from which endpoint identification, assessment and policy enforcement capabilities will vary.

Tolly engineers attempted to determine the extent to which each solution relies on on an agent/client to perform basic tasks: visibility for a new device, classification of device type, inspection of a device to assess configuration and security details, as well as notification, remediation and quarantine capabilities.

Tolly found that Cisco, Juniper and Bradford are heavily reliant on agents in order to classify the device type, inspect endpoints for user information and to perform any remediation or quarantine tasks. See Figure 3 and Table 2.

ForeScout, as a "pure-play" NAC vendor, offers considerably more interoperability with a customer's existing infrastructure, while offering a multi-factor device interrogation method, which does not rely on the use of agents to perform key NAC tasks.

ForeScout CounterACT was able to fulfill all success criteria, demonstrating extensive functionality without an agent, and thus received a 4 out of 4 score for this area. Without an agent, CounterACT was able to discover and fully classify a new device, along with device type, in under 2 minutes. CounterACT is also able to perform an inspection of the endpoint to obtain comprehensive information on the user, from which policies can be applied (such as disabling the use of a USB drive). CounterACT also supports comprehensive notification, remediation and quarantine capabilities without an agent. See Table 2.

Bradford Networks Network Sentry, while also a "pure-play" vendor, lacks the majority of its functionality without an agent, thus scoring a 1 out of 4. While it will provide visibility for a new device, that new device type cannot be classified or inspected beyond DCHP and static IP. Bradford shares the same limited notification, remediation and quarantine capabilities as Cisco and Juniper: the solutions will only support HTTP redirect to a captive portal for notification and supports assignment to VLAN, switch port blocking and ACL for quarantine. See Table 2.

Cisco ISE received a 2 out of 4 score as it supports slightly more classification of device type than Bradford Networks. Cisco ISE can obtain certain information about an endpoint such as OUI, IP address, uptime, description, MAC address, hostname and DHCP identifier.

Juniper UAC also received a 2 out of 4 score. Without an agent, Juniper's visibility is limited to network information, such as IP and MAC address; it is unable to provide OS type or any further details without authenticating with the UAC. See Figure 3 and Table 2.

Visibility

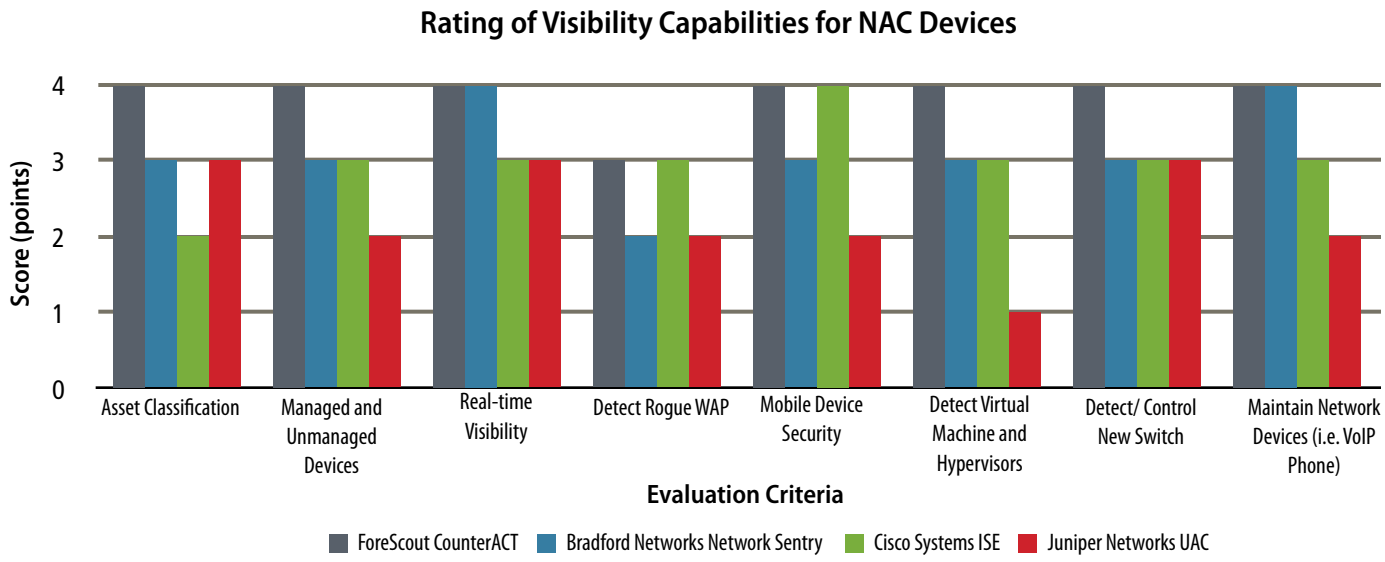
Tolly engineers attempted to determine to what level solutions under test were able to provide visibility into the network. Engineers evaluated if a product was able to provide built-in classification and support- and to what extent-for managed and unmanaged devices, the time to detection, ability to detect a rogue wireless access point (WAP), ability to detect a VM, ability to detect and control a new switch and ability to identify/exclude new devices.

ForeScout CounterACT scored the highest of all vendors across the board for all evaluation criteria. Tolly found that ForeScout offers the most comprehensive and intuitive asset classification by being able to identify, classify and sub-classify devices, such as location or user type, in real-time. In addition to device fingerprinting, CounterACT offers a rules engine to allow for flexible identification and classification of new and unusual network-based devices (i.e. online medical equipment). See Figure 4 and Table 3.

Asset Classification

For these criteria, engineers evaluated if a product included built-in classification of devices, and if so, how flexible is it to support additional devices.

ForeScout CounterACT scored a 4 out of 4 in the asset classification category as it supports a very flexible built-in classification policy, which classified network devices such as Windows, Linux, Mac, iPhone, iPad, printer and VoIP phone accurately in under 2 minutes. See Figure 4 and Table 3.



Scoring Legend	
4	Meets all Success Criteria of Evaluation
3	Meets all Success Criteria of Evaluation, but with caveats
2	Meets most Success Criteria of Evaluation
1	Meets some Success Criteria of Evaluation
0	Does not meet Success Criteria of Evaluation

Notes: Bars above indicate the number of points scored out of the total. Individual items were scored 0-4, with "0 "meaning no support, and "4" meaning the solution delivered full support. "0" score is represented by the absence of the vendor in a given category. See Table 3 for definitions of "success criteria" and additional details.

Source: Tolly, January 2012

Figure 4

Bradford Networks Network Sentry scored a 3 out of 4 as classification is limited without the agent installed for non-DCHP devices. Tolly engineers experienced difficulties with Bradford while attempting to detect and classify network devices, specifically, a great deal of troubleshooting was required to classify an HP printer. See Figure 4 and Table 3.

Cisco ISE received a 2 out of 4 grade in asset classification, as they include built-in classification for many different devices for 20+ vendors. However, the classification accuracy is very low before the environment is tuned. Cisco can be configured to support an extensive list of devices, however, this would require a great deal of attention/configuration from the administrator. See Figure 4 and Table 3.

Juniper received a 3 out 4 score as UAC does support built-in classification by OS type, agent type, role, domain and IP. However, Tolly engineers encountered limitations with the switch vendors that Juniper supported out-of-the-box. This can be remedied if the administrator manually configures and maintains custom dictionaries to support additional vendors.

Extent of Support for Managed and Unmanaged Devices

Tolly engineers attempted to determine to what degree a solution can classify a known device. Specifically, is the system able to classify new and unmanaged devices? And if so, how specific is the classification of managed devices vs. unmanaged?

ForeScout CounterACT received a 4 out of 4 score in this area. While Bradford and Cisco both received 3 out of 4 and Juniper received a 2 out of 4. See Figure 4 and Table 3.

ForeScout CounterACT supports full, built-in classification of devices without an agent. However, in order to obtain the same level of device, configuration and security posture details of non-domain machines, the ForeScout SecureConnector agent must be installed as either "persistent" or "dissolvable".

Bradford Networks Network Sentry supports manual classification, however, any device connected will only report basic information until the agent is installed for domain and non-domain devices.

Cisco ISE also supports only partial classification. Engineers could gather most identifying information about the endpoint, but the system requires the agent to gather the status of the OS or software.

Juniper UAC supports even less built-in classification and essentially needs a third-party solution to supplement MAC address identification and authorization.

Real-Time Visibility

Engineers attempted to determine how long each solution requires to "see", classify and present information about new devices, measured from the time that the new device is connected to the network.

ForeScout CounterACT received a 4 out of 4 score as the endpoint was fully and accurately identified and classified in under 2 minutes. The endpoint is also represented in the GUI in under 2 minutes with full configuration and policy details. See Figure 4 and Table 3.

Bradford Networks Network Sentry also received a 4 out of 4, as they also identified and classified the endpoint in under 2 minutes, but required considerably more time for the endpoint to be present in the GUI, and only present basic endpoint details.

Cisco ISE received a 3 out of 4 score as the endpoint gets fully identified and classified, but takes up to 10 minutes for this to occur. The time varied based on "refresh" and switch polling options.

Juniper UAC also received a 3 out of 4 score, as classification/identification occurs quickly, but the users must first manually log in. See Figure 4 and Table 3.

Detect Rogue WAP

Engineers evaluated whether or not a solution could detect a secure Wireless Access Point (WAP), as well as a rogue WAP, as the ability to do this can protect a network against unauthorized and/or unintentional access.

Engineers found ForeScout CounterACT quickly detected the secured WAP in the network. Although it did not detect the unsecured WAP, ForeScout was able to enforce its policy, forcing the endpoint connected to the unsecured WAP to download the CounterACT agent (ForeScout SecureConnector) in order for CounterACT to assess compliance. Since CounterACT did not detect the unsecured WAP, but did prevent access to the network, CounterACT was scored a 3 out of 4. See Figure 4 and Table 3.

Bradford Networks Network Sentry scored a 2 out of 4 as it can only detect a rogue WAP if it is connected to an endpoint that is connected to the network. This makes it difficult for administrators to have a great amount of control and visibility into possible rogue devices in large deployments.

Cisco ISE received a 3 out of 4 score as it does not provide built-in support for detecting rogue WAPs, but if the device does not have its MAC address whitelisted, Cisco ISE can prevent it from accessing the network.

Juniper UAC received a 2 out of 4 score as it cannot detect rogue WAPs, but it will blacklist any unauthenticated device by default, so the device will be prevented from accessing the network.

Mobile Device Security

The prevalence of employees and guests using their personal computers, tablets and smart phones to access the workplace network necessitates a NAC solution to be able to identify and enforce security policies for mobile devices. Tolly engineers attempted to determine to what extent a given solution could identify a mobile device and assess what level of detail can be collected without an agent.

Ability to detect personal and mobile devices gives an organization a broader means to apply policy based on the type of user (employee or guest), the type of mobile device and the desired level of segregated access to network resources.

ForeScout CounterACT received a 4 out of 4 grade as CounterACT can correctly classify mobile devices by type and user via HTTP hijack, without an agent. See Figure 4 and Table 3.

Bradford Networks Network Sentry received a 3 out of 4 as it can classify a device by type, but is unable to provide any user details beyond "capture/authenticate" without an agent.

Cisco ISE received a 4 out of 4 score as it can classify mobile devices via Web authorization. However, mobile users cannot connect via 802.1X unless they have the Cisco AnyConnect mobile client installed and configured to support moving between authorized networks.

Juniper UAC was scored a 2 out of 4 as it does not support built-in mobile device detection, but it can be configured manually. Juniper does support limited MAC-based classification.

Detect Virtual Machines and VM Hypervisors

Increased data center consolidation and the popular use of virtual machines (VMs) can introduce security risks as new systems which do not follow configuration policies can be rapidly provisioned and/or appear on a network. Tolly engineers attempted to determine to what extent a NAC solution could detect that a VM was in use, as well as its hypervisor.

ForeScout CounterACT, using its default fingerprinting policy, was able to accurately detect if a VM was in use. However, only 1 out of 3 ESX servers running was correctly identified as a hypervisor. The remaining two were categorized as "other." Additional policy adjustment would be required for better classification. Engineers rated CounterACT a 4 out of 4 for its functionality in detection of VMs. See Figure 4 and Table 3.

Bradford Networks Network Sentry was scored a 3 out of 4 as it does not support

Observation Summary: Visibility

Corresponds to Scored Data in Figure 4

	Evaluation Criteria	Engineer Observations			
		ForeScout CounterACT	Bradford Networks Network Sentry	Cisco ISE	Juniper UAC
Asset Classification	Does the product include built-in classification? How flexible is it to support various devices?	Supports built-in classification and provides extensive support for various network devices.	Supports built-in classification, but is limited without agent installation for non-DHCP devices unless using IP range classification rules.	Supports built-in classification for many different device types for 20+ vendors, however accuracy is very low before environment tuning.	Supports classification by OS, agent type, role, domain and IP. However, encountered limitations with many switch vendors.
Managed and Unmanaged Devices	Is the system able to classify unmanaged devices? How specific is the OS classification of unmanaged vs. managed devices?	Supports full classification without agent. However, non-domain machines must have the agent installed to display user or connected devices.	Supports manual classification definition, however any device connected will only report basic information until the agent is installed.	Supports partial classification. User can gather most identifying information from the endpoint, but requires the agent to gather the status of the OS or software.	Supports partial classification, but requires a plug-in to a third-party application for MAC profiling.
Real-Time Visibility	From the time of connection, how long until the endpoint is being managed by the system? How long until it is presented in the GUI.	Endpoint is fully identified and classified in <2 minutes	Endpoint is identified in <2 minutes. Requires a few additional minutes to show up in GUI with basic information. Will admit/ deny from network depending on the policy immediately.	Endpoint is identified and classified within 10 minutes of plug-in. Time varied based on refresh and switch polling options.	Endpoint is identified quickly once user manually logs into Juniper UAC.
Detect Rogue WAP	Can the system identify rogue wireless access points?	Supports detection and identification of most rogue NAT devices by enforcement of compliance policies.	Supports identification of rogue device only if it is connected to an managed endpoint. Difficult to detect and manage in large-scale deployments.	Does not support built-in classification, however, if device does not have its MAC address whitelisted, it is prevented from accessing the network.	Does not support rogue WAP identification. UAC blacklists by default.
Mobile Device Security	Can the system classify a mobile device? What level of detail can be collected without an agent?	Can correctly classify device type, OS and provided user authentication via http without an agent.	Can classify device type, but cannot provide details beyond capture/ authentication without agent.	Can classify mobile devices via WebAuth authentication policy creation. Mobile users cannot connect via 802.1X unless they have the Cisco AnyConnect mobile client installed.	Juniper UAC does not support detection of mobile devices out of the box, but it can be configured manually. Limited MAC-based classification.
Detect Virtual Machines and Hypervisors	Can the system identify new virtual machines? Can it detect and monitor VM hypervisors?	Accurately detects VMs and ESXi 4 hosts by default.	Can be configured to identify VMs, but will display host and VM OS info. No built-in distinction between physical and virtual system.	Supports built-in profiling policies for detecting VMs, but did not classify any hypervisors.	Juniper UAC cannot distinguish between virtual and physical machines.
Detect and Control a New Switch	How long until a system starts to manage a newly connected switch? Will he system automatically sync and begin working with the switch?	Supports built-in detection , classification and management in <2 minutes. To query for information, users need only install the switch plug-in.	Supports detection in ~5-10 minutes, but isolated by default, credentials are required for management.	Will not automatically work with any network device until it is manually configured, and primarily with Cisco infrastructure.	Switch and system must be manually configured in order to communicate with each other.
Maintain Network Devices	How does the system handle network devices that should be excluded from the NAC policy? Will system know to ignore devices such as VoIP phones and printers from relevant policies?	Provides easy configuration for admit/deny for certain classes of devices, allowing those devices to bypass policies when needed.	Supports automatic admit/deny for certain classes of devices, can be configured to bypass policies for device classes.	Requires configuration through MAB policy in order for certain classes of devices to bypass certain policies.	Must be classified through third-party application or MAC address to allow certain devices to bypass certain policies.

Source: Tolly, January 2012

Table 3

built-in VM detection or distinction between virtual/physical machines. However, Network Sentry can be manually configured to do so and display host and VM OS information.

Cisco ISE also received a 3 out of 4 score as it does support built-in policies for detecting VMs and hypervisors, but did not detect either virtual machines or ESX servers during the evaluation.

Juniper UAC, while being able to detect virtual machines, could not distinguish between physical and virtual machines, thus earning them a 1 out of 4 score.

Detect and Control New Switch

Tolly engineers attempted to determine to what extent a given solution could detect and control a new switch in the network. Ability to detect and control a new switch prevents unauthorized access to the network, while being flexible enough to support new upgrades or additions to the infrastructure.

The engineers' evaluation criteria for this aspect of the evaluation included determining how long until the system starts to manage a newly connected switch, and will it automatically begin working with the new switch, once correctly identified.

Engineers rated ForeScout CounterACT a 4 out of 4. The evaluation found that ForeScout CounterACT detected both new switches (both Cisco and Juniper switches were present in the deployment), almost instantaneously, in well under 2 minutes. CounterACT could also control the switches in the deployment once the switch plug-in for CounterACT was installed. See Figure 4 and Table 3.

Bradford Networks Network Sentry was given a 3 out of 4 score by engineers, as the solution will "see" the new switch in 5-10 minutes, but credentials and configuration are required to manage the switch, it is not done by default, as with the CounterACT.

Cisco ISE was also rated a 3 out of 4 by engineers, as it can be configured to operate with certain infrastructure, primarily Cisco, but will not automatically work with any network device. Cisco provides documentation to configure certain Cisco infrastructure to work with Cisco ISE, but this configuration must be completed in order for the network device to be managed by Cisco ISE and provide authentication and authorization. See Figure 4 and Table 3.

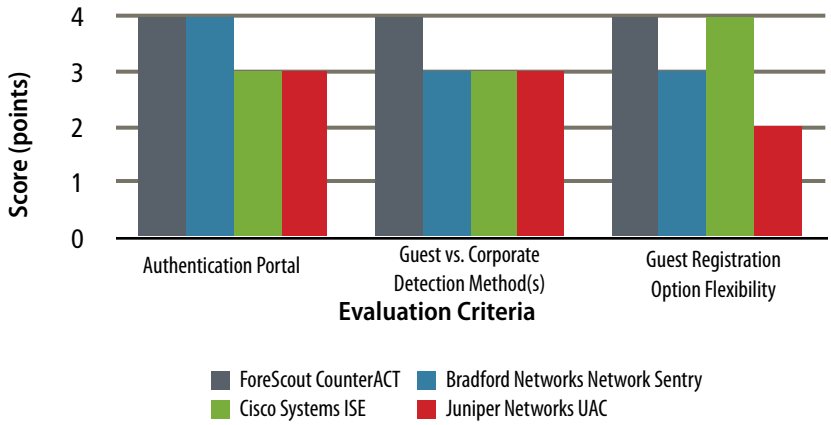
Juniper UAC scored a 1 out of 4, as it does not support new switch detection and control out-of-the-box. In order to support this capability, the switch and system must be manually configured in order to communicate with each other. See Figure 4 and Table 3.

Identify and Exclude New Devices

Tolly engineers attempted to determine to what extent a given solution could handle network devices that should be excluded from the NAC policy. Specifically, if a given solution would automatically "know" to ignore certain network devices from certain policies.

A solution's ability to support this functionality allows network administrators to support new network technologies and expand visibility into the network. It also decreases policy errors and end-user frustrations.

Rating of Guest Management Capabilities for NAC Devices



Scoring Legend	
4	Meets all Success Criteria of Evaluation
3	Meets all Success Criteria of Evaluation, but with caveats
2	Meets most Success Criteria of Evaluation
1	Meets some Success Criteria of Evaluation
0	Does not meet Success Criteria of Evaluation

Notes: Bars above indicate the number of points scored out of the total. Individual items were scored 0-4, with "0 "meaning no support, and "4" meaning the solution delivered full support. "0" score is represented by the absence of the vendor in a given category. See Table 4 for definitions of "success criteria" and additional details.

Source: Tolly, January 2012

Figure 5

ForeScout CounterACT received a 4 out of 4 grade by engineers for its ability to identify/exclude network devices. CounterACT provides easy configuration for admit/deny for certain classes of devices (i.e. VoIP phones), allowing those devices to bypass policies when needed. See Figure 4 and Table 3.

Bradford Networks Network Sentry also received a 4 out of 4 rating as it also offers easy configuration to admit/deny certain classes of devices, allowing those devices to bypass policies as needed.

Cisco ISE received a 3 out of 4 grade as it requires a user to configure via a MAB policy in order for certain classes of devices to bypass certain policies.

Juniper UAC received the lowest score of the group at 2 out of 4, as it requires significant configuration for the solution to allow/deny certain device classes. In addition, this configuration must be done by MAC address or through another third-party application.

Guest Management

Automated provisioning of Internet access for guests remains one of the leading use cases for network access control: to ensure appropriate guest access to corporate networks. Tolly engineers found that all systems evaluated offered fairly strong guest networking capabilities, but that CounterACT offers broader detection methods without requiring agents.

Tolly engineers evaluated all solutions in three key areas: Authentication Portal, Guest vs. Corporate Detection Method(s) and Guest Registration Options. See Figure 5 and Table 4.

Authentication Portal

Tolly engineers attempted to determine to what extent a given solution was able to present an authentication page to a guest through the browser. This provides flexibility to guests and end users, without forcing them through a single VLAN. This provides options for access and creates a positive user experience. Furthermore, this capability reduces deployment costs and prevents a possible single point of failure scenario.

ForeScout CounterACT received a 4 out of 4 rating as it quickly and easily configures to provide guest users with options for authentication and network access.

Observation Summary: Guest Management

Corresponds to Scored Data in Figure 5

	Evaluation Criteria	Engineer Observations			
		ForeScout CounterACT	Bradford Networks Network Sentry	Cisco ISE	Juniper UAC
Authentication Portal	Is the system able to present an authentication page through the browser?	Supports authentication page through the browser with minimal configuration.	Supports authentication page through the browser with minimal configuration.	Requires moderate configuration of the guest management policy to support the authentication page through the browser.	Requires moderate configuration to support the authentication page through the browser.
Guest vs. Corporate Detection Method(s)	What methods are used by the system to identify the guest vs. the corporate machine? Does the guest process affect all users? How flexible is the policy?	Supports built-in identification by domain, but can be configured to identify guests by many other metrics. Provides a flexible, fully-customizable policy. When policy is matched for guests, users can define custom actions.	Supports identification by MAC address and user authentication. Guest is defined based on device type or authentication state. Engineers found the policy to lack extensive flexibility.	Supports identification based on several metrics, specifically domain and network access. Guest process does not impact corporate users.	Differentiation between 'Guest' and 'Corporate' machines must be defined manually by the user when they log in. Roles can be customized to apply to all users.
Guest Registration Options	How flexible are the guest registration options/process? How much control does the operator have over the registration process?	Supports flexible guest registration and management via registration code, "skip registration", enter credentials (customizable), enter username/password, and approval via email, domain contact person, or guest e-mail/ mobile. Can also be set to approve automatically.	Does not support Guest request for authorization at time of testing. Guest is able to approve themselves, or be pre-approved by an administrator.	Supports flexible guest policy creation and management. Administrators can define groups to manage guest accounts, which allow guests to self-authenticate.	Requires 'Juniper Networks Enterprise Guest Access' to support guest approval functionality.

Source: Tolly, January 2012

Table 4

Bradford Networks Network Sentry received a 4 out of 4 as it also provides relatively easy configuration.

Cisco ISE scored a 3 out of 4 as it supports a guest management policy that requires moderate configuration to be used in conjunction with the authentication and authorization policy to present a guest user an authentication page when they connect to the network.

Juniper UAC also received 3 out of 4 since, while they support a guest authentication portal, Juniper UAC can enforce a redirect policy through the Infranet Enforcer. A policy needs to be defined directly on the enforcer in order for the redirect to work properly.

Guest vs. Corporate Detection Method(s)

Tolly engineers attempted to determine what methods are used by the system to identify guest vs. corporate machines. They also attempted to determine how flexible the policy is, and if it is affecting all users or just guests. The primary function of this feature is to provide a positive user experience without compromising the networks' security posture.

ForeScout CounterACT scored a 4 out of 4 as it has both integrated and flexible guest detection capabilities. By default, guests can be identified by domain. Additional detection capabilities include devices, device configuration, 802.1x supplicant, location and time. The administrator can define different rules and respective actions for any identified attribute. See Figure 5 and Table 4.

Bradford Networks Network Sentry received a 3 out of 4 rating. While guest identification is supported, it requires more configuration and offers less intuitive guest management policies. Guests are identified by MAC address and user authorization. The guest is defined based on the device type or authentication state, thus resulting in a much less flexible guest management policy.

Cisco ISE also scored a 3 out of 4 as it supports identification based on several metrics, specifically domain and network access. The guest process does not impact corporate users.

Juniper UAC also scored a 3 out of 4 as the differentiation between "guest" and "corporate" users must be defined manually by the user, thus impacting the corporate user experience. Roles can be identified by the administrator to apply to all users. See Figure 5 and Table 4.

Guest Registration Options

Tolly engineers attempted to determine the flexibility of the guest registration options and to determine how much control the operator has over the registration process. This feature allows for lower management costs and gives corporate hosts easier methods to govern guest access by business unit, not just an "on/off" access policy.

ForeScout CounterACT received a 4 out 4 score from Tolly engineers as they support a built-in, flexible guest registration and management policy. Administrators can configure guest users to authenticate via registration code, "skip registration", "enter credentials" (customizable), "enter username/password" and issue approval via e-mail, domain contact person, or guest e-mail/mobile. The policy can even be set to approve automatically. See Figure 5 and Table 4.

Bradford Networks Network Sentry was scored a 3 out of 4 by engineers as the guest management policies are limited to either self-registration by user (no approval required) or pre-approved/configured host. There are no dynamic approval tools for guest users.

Cisco ISE was rated a 4 out of 4 by engineers for its ability to allow administrators to define groups to manage guest accounts, which allow guests to self-authenticate and check compliance with the environment.

Juniper UAC scored a 2 out of 4 as it does not offer guest registration built-in. Juniper requires an additional appliance: "Juniper Networks Enterprise Guest Access" in order to obtain similar levels of functionality to Cisco and ForeScout CounterACT.

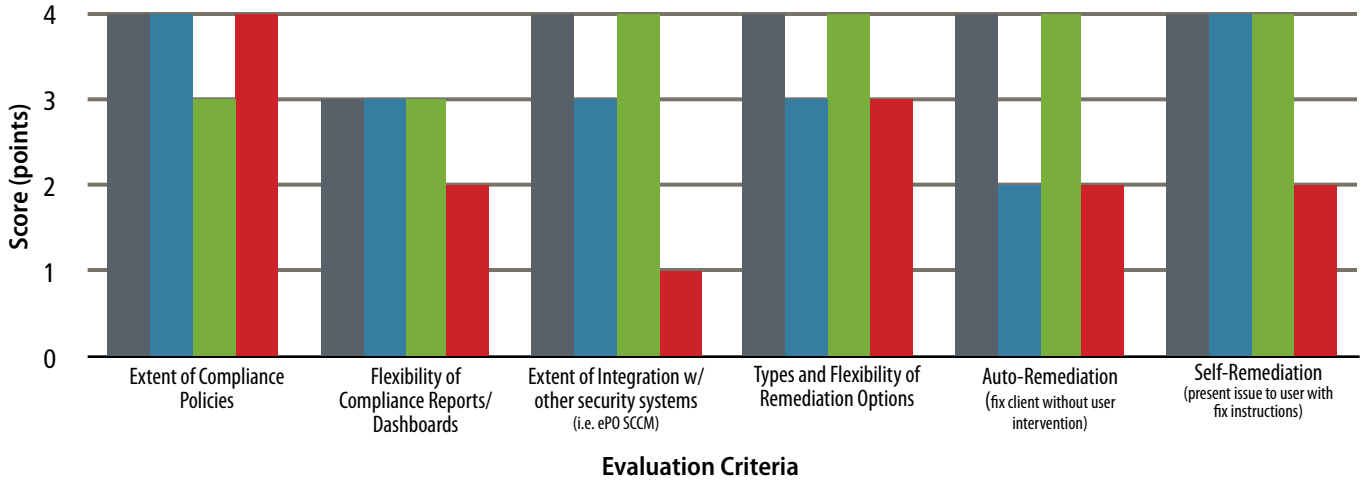
Endpoint Compliance and Remediation

NAC provides the means to identify and attempt to resolve endpoint configuration issues or security policy violations. Though all the systems offer endpoint compliance and remediation capabilities, the levels of usability, flexibility and functionality to enforce policies vary greatly among solutions evaluated. See Figure 6 and Table 5.

Extent of Compliance Policies

Tolly engineers attempted to determine if a given solution comes with built-in compliance policies, and if so, how much flexibility is allowed within those policies.

ForeScout CounterACT scored a 4 out of 4 according to Tolly engineers. CounterACT supports a broad number of built-in policies with a policy engine that offers greater flexibility to support numerous compliance scenarios. Policies support time, location, device, applications, PCI



Scoring Legend	
4	Meets all Success Criteria of Evaluation
3	Meets all Success Criteria of Evaluation, but with caveats
2	Meets most Success Criteria of Evaluation
1	Meets some Success Criteria of Evaluation
0	Does not meet Success Criteria of Evaluation

ForeScout CounterACT
Bradford Networks Network Sentry
Cisco Systems ISE
Juniper Networks UAC

Notes: Bars above indicate the number of points scored out of the total. Individual items were scored 0-4, with "0 "meaning no support, and "4" meaning the solution delivered full support. "0" score is represented by the absence of the vendor in a given category. See Table 5 for definitions of "success criteria" and additional details.

Source: Tolly, January 2012

Figure 6

compliance and more. These policies can be fully customized using an intuitive interface to allow for simple or complex rules and actions. See Figure 6 and Table 5.

Bradford Networks Network Sentry also scored a 4 out of 4 as it supports some built-in compliance policies, though less than CounterACT. Network Sentry can check operating system configuration and anti-virus status and compliance with customizable policies.

Cisco ISE scored a 3 out of 4 as it supports posture service to check for compliance. Cisco ISE requires 802.1X and an agent to check compliance and remediate.

Juniper UAC scored a 4 out of 4 as its supports pre-defined compliance policies for AV and system updates. Juniper UAC can also define custom settings based on Network/OS/patch settings. See Figure 6 and Table 5.

Flexibility of Compliance Reports/ Dashboards

Engineers attempted to determine to if a given solution came with built-in compliance reporting and dashboards, and if so, to determine the flexibility of the reporting function.

ForeScout CounterACT scored a 3 out of 4 according to Tolly engineers. CounterACT supports built-in compliance reports. The administrator can design custom reports and can also share operational details through CounterACT's built-in Web portal. Reports can be configured to be run automatically or "on-demand" depending on administrator preference. See Figure 6 and Table 5.

Bradford Networks Network Sentry also received a 3 out of 4 due to similar functionality as ForeScout CounterACT. Users can view scan results from the dashboard, conduct scans and host summary panels, but this information is not available as a scheduled report.

Cisco ISE supports built-in reporting on environment and posture compliance. Cisco scored a 3 out of 4 as it allows

Observation Summary: Endpoint Compliance and Remediation

Corresponds to Scored Data in Figure 6

	Evaluation Criteria	Engineer Observations			
		ForeScout CounterACT	Bradford Networks Network Sentry	Cisco ISE	Juniper UAC
Extent of Compliance Policies	Does the system come with built-in compliance policies? How much flexibility in compliance policies is offered?	Supports built-in and flexible compliance policies. Checks data AV/system/ application/ PCI compliance. Policies can be custom-defined as needed.	Supports built-in compliance policies. Can check AV/AS/OS functionality and compliance with customizable policies	Supports posture service to check for compliance. Requires 802.1X and NAC agent to check compliance and remediate.	Supports pre-defined compliance policies for AV and system updates. Can define custom settings based on Network/ OS/ patch settings.
Flexibility of Compliance Reports/ Dashboards	Does the system come with built-in compliance reporting and dashboards? How flexible are these reports?	Supports built-in compliance reports. Administrators can design custom reports containing relevant data on a schedule.	Users can view scan results from the dashboard, scans, and host summary panels, but are not available as a scheduled report.	Supports built-in reporting on environment and posture compliance. Allows administrators to generate somewhat custom reports.	Supports built-in reporting through user access log, but not configurable and no dashboard.
Extent of Integration w/ other security systems (i.e. ePO, SCCM)	Is the system capable of pulling endpoint compliance from pre-existing security systems? Is the system capable of triggering a scan?	Integrates with 19+ third-party security systems. Can trigger system scans/ compliance checks on-demand or when a new endpoint joins the network.	Can update Windows or AV. Integrates with any system which can send Syslog or SNMP traps using Bradford Integration Suite with extensive configuration.	Integrates with several AV and patch management applications. Can write own compliance policy conditions.	Can not integrate with any other third-party security system.
Types and Flexibility of Remediation Options	How rich are the built-in remediation methods? Can the user create their own remediation process?	Provides extensive and customizable remediation capabilities.	Provides admin-configurable remediation policies for each user/ device, but is limited to updating AV, windows update, unless managed with another patch program.	Provides customizable remediation, however remediation options limited to Agent, Profile and Compliance module options.	Provides relatively limited remediation options. User will be prompted to perform whatever remediation processes need to take place.
Auto-Remediation (fix client without user intervention)	Can the endpoint be fixed without requiring any intervention from the end-user or system operator?	Supports built-in auto-remediation which can update software patches on the client, prompting the user for anything they may need to do.	Supports limited auto-remediation through integration with PatchLink (Lumension) or BigFix.	Can be configured to support auto-remediation.	Provides limited auto-remediation capabilities. Can only automatically update AV, etc..
Self-Remediation (present issue to user with fix instructions)	Can the user be presented with remediation instructions to fix their endpoint without the intervention of the IT team?	Can be configured to support self-remediation, with customizable options such as e-mail notification or popup notification with instructions for installing the necessary patches.	Can be easily configured to support self-remediation. Policy can be configured to include a message on user screen with details and instructions.	Supports self-remediation through the NAC agent, where users will be provided with information and instructions to resolve issues on their own.	Does not support built-in self-remediation, but can be configured to provide notifications and instructions to an endpoint.

Source: Tolly, January 2012 Table 5

administrators to generate reports, but reports are limited in their customization capabilities.

Juniper UAC scored a 3 out of 4 as it supports built-in reporting through the user access log, but these reports are not customizable/ configurable and there is no dashboard available.

Extent of Integration with Third-Party Systems

NAC can assure that an endpoint meets security standards such as appropriate OS installation and use of endpoint protection. Tolly engineers attempted to determine if a given solution was capable of assessing the existence and use of endpoint security software and initiating actions such as anti-virus updates or scans. This reduces the risk of malware, unwanted applications, endpoint protection gaps and other security risks.

ForeScout CounterACT earned a 4 out of 4 score as it supports integration with a large number of third-party host-based security systems (19+)[1], including anti-virus, patch management and more. The system allows

[1] Number of interoperable systems not verified by Tolly. See http://www.forescout.com/product/interoperability/ for more information.

administrators to assess compliance and trigger actions (such as an anti-virus scan) "on demand" as endpoints join the network, or at scheduled intervals after endpoints are already connected. Administrators can write their own compliance policies and remediation scripts. See Figure 6 and Table 5.

Bradford Networks Network Sentry scored a 3 out of 4 as it can trigger scans of third-party security systems using the Bradford Integration Suite, or by itself to update Windows or AV.

Cisco ISE received a 4 out of 4 score as it integrates with several AV and patch management applications. Cisco ISE also allows administrators to write their own compliance policy conditions.

Juniper UAC, on the other hand, cannot integrate with any other third-party system. Juniper received a 1 out of 4 score as UAC can create custom compliance policies and trigger updates with some pre-defined third-party AV, firewall and malware vendors. It cannot, however, provide reporting or integrate with solutions to the extent of the other NAC solutions under evaluation.

Types and Flexibility of Remediation Options

Tolly engineers attempted to determine the extent to which each solution was able to provide endpoint remediation mechanisms, and if the user could create custom remediation scripts. The broader the remediation options, the better means for an IT administrator to leverage current endpoint protection investments and reduce time spent with manual endpoint problem identification and resolution.

ForeScout CounterACT was scored a 4 out of 4 by Tolly engineers for its flexible built-in remediation options, which allow the policy to be completely and easily customizable by the administrator.

Bradford Networks Network Sentry scored a 3 out of 4 as it is limited in its remediation capabilities. The built-in remediation capability is restricted to updating AV for the supported vendors, launching Windows update or integration with PatchLink and BigFix for remediation.

Cisco ISE scored a 4 out of 4 for providing customizable built-in remediation options, though they are limited to agent, profile and compliance module options.

Juniper UAC scored a 3 out of 4. While it provides relatively limited remediation options, the user can be prompted to perform whatever remediation processes need to take place. Policies for self-remediation are not built-in, but can be configured.

Auto- Remediation

Tolly engineers attempted to determine to what extent the endpoint could be fixed without any intervention from the end-user or the system operator. This allows for less of an impact on the users' workflow, reduces helpdesk queues, overall support costs and promotes a positive user experience.

ForeScout CounterACT scored a 4 out of 4 for comprehensive and flexible auto-remediation policies. These policies can identify conditions from which CounterACT can perform background services such as: update software on a client, re-activate agents, change registry settings, disable peripherals, terminate application processes and initial system patches. CounterACT also supports custom scripting to allow for more advanced and custom endpoint remediation capabilities.

Bradford Networks Network Sentry scored poorly, a 2 out of 4, for its auto-remediation as it is currently only compatible with PatchLink (Lumension) or BigFix. Without one of these two, no remediation can be performed without any user intervention.

Cisco ISE scored a 4 out of 4 because it is able to be configured to support remediation without any user intervention. The remediation is done through the agent, which can be configured to automatically remediate the endpoint.

Juniper UAC does provide some remediation capabilities, though they are limited in scope, earning Juniper a 2 out of 4 score. Juniper is only able to automatically update AV on an endpoint without any user intervention. See Figure 6 and Table 5.

Self-Remediation

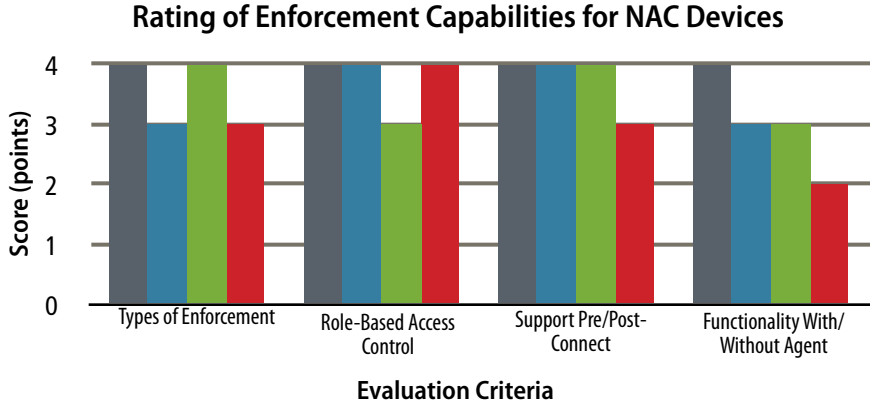
Engineers attempted to determine the extent to which a given solution allowed a user to fix an issue via remediation instructions without needing to involve the IT team.

ForeScout CounterACT was scored a 4 out of 4 for flexible and intuitive self-remediation policies. If the administrator configures self-remediation for devices that are not compliant, the user can be notified in a variety of ways, including HTTP redirection, endpoint alerting with indication of compliance violations and links, or using the ForeScout agent (ForeScout SecureConnector) to indicate which remediation options to enable. Additional notification options include e-mail and pop-up notification, depending on the preference, and presents the user with instructions for installing the necessary patches. In case of the agent-less approach, HTTP redirection will occur.

Bradford Networks Network Sentry also scored a 4 out of 4, though the built-in self-remediation process is not nearly as intuitive as CounterACT. Network Sentry's built-in remediation policies are not very rich, but they can be written/configured to include a message on the user's screen with appropriate troubleshooting/remediation instructions.

Cisco ISE also received a 4 out of 4 score, although ISE requires an agent to provide any information to the user for them to resolve issues independently.

Juniper UAC scored a 2 out of 4 as Juniper does not support self-remediation options, but it can be configured to provide notifications and instructions to an endpoint. See Figure 6 and Table 5.



Scoring Legend	
4	Meets all Success Criteria of Evaluation
3	Meets all Success Criteria of Evaluation, but with caveats
2	Meets most Success Criteria of Evaluation
1	Meets some Success Criteria of Evaluation
0	Does not meet Success Criteria of Evaluation

ForeScout CounterACT
Bradford Networks Network Sentry
Cisco Systems ISE
Juniper Networks UAC

Notes: Bars above indicate the number of points scored out of the total. Individual items were scored 0-4, with "0 "meaning no support, and "4" meaning the solution delivered full support. "0" score is represented by the absence of the vendor in a given category. See Table 4 for definitions of "success criteria" and additional details.

Source: Tolly, January 2012 Figure 7

Enforcement

Types of Enforcement

Tolly engineers attempted to determine the granularity and flexibility of the built-in enforcement policies in a given solution. This allows an administrator to have scalable options based on the existing network architecture. Administrators are able to enforce a policy when and where they choose, not just based upon what a NAC solution can do.

ForeScout CounterACT was rated a 4 out of 4 by engineers for supporting highly flexible and configurable actions to enforce, manage, notify, authenticate, remediate and restrict. Enforcement includes ACL, VLAN, TCP reset, switch port blocking and virtual firewall. See Figure 7 and Table 6.

Bradford Networks Network Sentry scored a 3 out of 4 as it supports fewer options for enforcement. Network Sentry supports configurable enforcement via ACL/ VLAN/ DCHP and switch port blocking.

Cisco ISE also scored a 4 out of 4, though it does not boast as many configuration options as CounterACT. ISE enforces through the agent and supports VLAN and ACL enforcement. ISE can also enforce remediation processes as well as limited control of applications/services.

Juniper UAC scored a 3 out of 4 as it can enforce policies that will permit and/or deny access to certain resources in the environment only if the end-user has OAC or Pulse installed on their machine. Juniper UAC can also use Juniper firewalls (called Infranet Enforcers) to deploy firewall policies.

Role-Based Access Control

Tolly engineers attempted to determine to what extent a given solution could apply role-based access control (RBAC), or access based on a user group. This functionality enables access policies to follow the end-user regardless of how they connect, what network they are accessing, or whether or not the organization requires 802.1X authentication.

ForeScout CounterACT scored a 4 out of 4 for their RBAC's ability to define a policy based on user role. Though engineers note it takes some light initial configuration, CounterACT uses domain administrator credentials in conjunction with its user directory plug-in to dynamically apply a role-based access policy. See Figure 7 and Table 6.

Bradford Networks Network Sentry also was scored a 4 out of 4 by engineers due to its highly-configurable RBAC policy; Network Sentry provides role-based definition of devices and users either exported from Directory services or locally on the appliance. However, engineers note

Observation Summary: Enforcement

Corresponds to Scored Data in Figure 7

	Evaluation Criteria	Engineer Observations			
		ForeScout CounterACT	Bradford Networks Network Sentry	Cisco ISE	Juniper UAC
Types of Enforcement	How rich are the built-in enforcement policies? How granular and flexible are they?	Supports highly flexible and configurable actions to enforce: manage, notify, audit, authenticate, remediate and restrict.	Supports configurable enforcement via ACL/VLAN/DHCP and switch port blocking.	Supports enforcement via agent, VLAN and ACL. Can enforce remediation processes as well and provides limited control of applications/services.	Enforces by plugging into different Juniper infrastructure and agents to disseminate permission resources.
Role-Based Access Control	Can the system apply a RBAC (access based on user group)?	Supports authentication based on user role via configuration on the endpoint.	Requires moderate configuration. Supports authentication based on local or directory-based users and groups.	Supports authentication based on user groups. Can be configured to authenticate users with certain permissions.	Supports authentication based on user groups. Can be configured through the realm-based logon.
Support Pre/Post-Connect	Can the system apply both pre-connect NAC methods and post-connect methods?	Provides extensive and efficient pre and post-connect NAC methods with minimal configuration.	Supports pre-connect through 802.1X and supports post-connect via profiling rules, agent/integration suite monitoring.	Supports pre-connect through 802.1X or MAB. Post-connect enforcement is supported by VLANs and ACL policies.	Supports pre-connect through 802.1X agent program. Post-connect enforcement is supported by agent/HostChecker.
Functionality With/ Without Agent	Does the enforcement rely on the existence of an agent, or is it available without an agent?What functions are lost if the machine does not have an agent?	Enforcement does not rely on agent, can enforce on any domain computer. Any endpoint not on the domain can be forced to download an agent for a deeper inspection.	Without an agent, Bradford can only place client in a VLAN. If agent is installed, can enforce normally.	Enforcement can be performed without an agent when authenticated through the web authorization page.	Requires an agent to enforce. Can only place client in VLAN without agent.

Source: Tolly, January 2012 Table 6

that this was the most complex and cumbersome solution to configure.

Cisco ISE earned a 3 out of 4 rating as it can be configured to authenticate users with certain permissions, but that required more administrative effort.

Juniper UAC scored a 4 out of 4 for their built-in ability to map different AD groups to certain roles within the user realm.

Support Pre/ Post Connect NAC

Engineers determined a given solutions' ability to apply both pre-connect and post-connect NAC methods. This security feature allows an organization to assess the endpoint security state both before and after a device is connected to the network. Pre-connect NAC requires greater enforcement flexibility, as an inflexible, strict policy can trigger access blocking for even minor endpoint compliance infractions. Post-connect NAC allows organizations to identify policy violations and malicious activity even after a device is allowed access.

Engineers rated ForeScout CounterACT a 4 out of 4 as it can restrict access to certain VLANs using ACLs or virtual firewalls after a short initial configuration of only a few minutes. CounterACT supports 802.1X and non 802.1 device authorization mechanisms. Additionally, CounterACT allows for post-connection endpoint assessment in real-time via the ForeScout SecureConnector agent, with or without an agent. See Figure 7 and Table 6.

Bradford Networks Network Sentry also was rated a 4 out of 4 by engineers, as it also supports pre/post connect capabilities, though with a few more steps/ configuration than CounterACT. Using Radius, pre-connect enforcement can be configured, however there needs to be an external Radius configured and integrated in order to work properly.

Juniper UAC was rated a 3 out of 4 by engineers as Juniper supports 802.1X authentication via Juniper OAC, Pulse, or other methods of 802.1X authentication. If Host Checker is being used it will continuously check the system to make sure it is in line with the compliance policies.

Cisco ISE scored a 4 out of 4. Pre-connect Using 802.1X and MABs ISE can control the

Observation Summary: Scalability

	Evaluation Criteria	Engineer Observations			
		ForeScout CounterACT	Bradford Networks Network Sentry	Cisco ISE	Juniper UAC
Max number of endpoints per appliance	How many endpoints can be managed from a single appliance?	Up to 4,000. Licenses are available from 100 up to 4,000 devices per single appliance.	Unlimited*. Scalability is based on licensing, not hardware restrictions.	Single server running admin/policy services/monitoring nodes can manage 2,000 endpoints. Device 3315 running all services can manage 3,000 endpoints. Device 3355 running all services can manage 6,000 endpoints. 3395 and Virtual Machine running all services can mange 10,000 endpoints.	The IC4500 scales to support from 25 to 5,000 simultaneous endpoint devices. The IC6500 network access server scales to support up to 15,000 simultaneous endpoint devices
Max number of endpoints per deployment-managed by a single console	How many endpoints can be managed by a single deployment (Single GUI with single configuration)	Up to 400k using the Enterprise Manager. Requires 100 separate CounterAct devices.	Unlimited* by NS550VM or NS550RX.	Up to 100,000 Max Concurrent Endpoints per ISE instance.	Up to 15,000
Scalability Ease-of-Use (i.e. easy to use with multiple endpoints, appliances, switches, etc...)	Is the GUI designed for large deployments? Does it group appliances, switches, etc. for scalable configuration and management? Can you select multiple devices for configuring at once? How many appliances are transparent to policy management and endpoint?	Intuitively groups devices, ports, VLANs and domains with global policies.	Groups for ports can be created. For grouping and management of multiple appliances, separate Control and Application Server is required.	Possible to scale, but not without significant configuration. As integration is largely tied to Cisco infrastructure, every network device would need to be configured.	Juniper UAC GUI is easy to use and easy to configure multiple Authentication realms/roles, Infranet Enforcers, and RADIUS clients.

Note: "Max Number of Endpoints Per Appliance" and "Max Number of Endpoints Per Deployment" assessments are based on the study of publicly-available vendor documentation. * While theoretically device support is unlimited, in practice, users may encounter hardware constraints.

Source: Tolly, January 2012

Table 7

machine's access to the network resources. Using dACLs and VLAN controls through the connected network devices, ISE can control the endpoints access post-connection and can also force machines to download agents and perform posture assessment before gaining any further access.

Functionality With/Without Agent

If a solution is able to function without endpoint agents, it offers additional flexibility because it can be deployed in environments that are not suitable for 802.1X. Tolly engineers attempted to determine if the solutions' enforcement relied on the existence of an agent (802.1X supplicant), or if it was available without agent. Engineers also evaluated what functions were lost if the machine does not have an agent.

Engineers rated ForeScout CounterACT's enforcement functionality without an agent a 4 out of 4. It can enforce network policy on any endpoint regardless of whether or not that endpoint contains an agent. It can also remediate domain endpoints with or without agents. Non-domain endpoints can be remediated by ForeScout's SecureConnector agent. See Figure 7 and Table 6.

Bradford Networks Network Sentry was rated a 3 out of 4 by engineers as it is not capable of enforcement without 802.1X beyond placing the client in a VLAN. With an agent, however, it can fully enforce.

Cisco ISE was also rated a 3 out of 4 as it provides limited enforcement without an agent. Without 802.1X supplicant, Cisco ISE can perform enforcement through WebAuth and MABs and from there use VLANs and ACLs to provide enforcement of policies.

Juniper UAC was scored a 2 out of 4 as it requires an agent for any enforcement capabilities. Without an agent, it can only

place in a VLAN. With an agent, however, Juniper can enforce normally.

Manageability/Scalability

The means to easily scale and manage multiple appliances, thousands of endpoint devices and policies across devices and networks are critical features for NAC to support when managing the vastly distributed environments of medium-to-large enterprises.

Tolly engineers evaluated the scalability of each solution based on publicly-available vendor documentation. As such, no grading scale is used to evaluate vendors in this category. Evaluation criteria included the maximum number of endpoints allowed for a single appliance and the total possible endpoints, and their respective policies, that can be centrally managed. Publicly-available vendor-documentation and licensing models were used as the basis for all scalability claims. See Table 7.

Endpoints Per Appliance

Tolly engineers utilized publicly-available vendor documentation to assess how many endpoints can be managed from a single appliance. Scalability maximums are based upon vendor licensing, rather than hardware restrictions.

ForeScout CounterACT can support up to 4,000 endpoints from a single appliance. Licenses are available in increments of 100, 500, 1,000, 2,500, and 4,000 devices per single appliance.

Bradford Networks Network Sentry can be deployed with license caps from 2,000 to 20,000 network ports per appliance (physical or virtual). Physical appliances, NS500X and NS500RX can manage up to 2,000 ports in the network, while the NS1200X, NS8200X, NS1200RX, and NS8200RX can manage up to 10,000 ports in the network. The NS2200RX and NS9200RX can manage up to 20,000 ports in the network.

Bradford Networks Network Sentry virtual appliances such as the NS500VM can manage up to 2,000 ports in the network while the NS1200VM and NS8200VM can manage up to 10,000 ports in the network. The NS2200VM and NS9200VM can manage up to 20,000 ports in the network.

"Ports" in the network include edge switch ports as well as connection capacity of wireless LAN access points and controllers.

Cisco ISE can potentially support up to 10,000 concurrent endpoints per appliance.

The Juniper IC4500 can scale to support 25 to 5,000 simultaneous endpoint devices. The IC6500 network access server can scale to support up to 15,000 simultaneous endpoint devices. See Table 7.

Endpoints Per Deployment

Tolly engineers also researched how many endpoints can be managed from a single console, specifically, a single GUI with a single configuration. Once again, only publicly-available vendor documentation was used to obtain this information and draw conclusions. More endpoints per deployment allows for greater scalability with lower costs. Licensing for all is based upon concurrent IPs, not users, which allows for larger deployments.

ForeScout CounterACT Enterprise Manager can centrally manage appliance configuration, policies and licensing for up to 100 CounterACT appliances, each of which can manage up to 4,000 endpoints. This enables one central appliance and its respective GUI to have real-time visibility, dynamic policy management and active enforcement of up to 400,000 endpoints per deployment.

Bradford Networks Network Sentry, while potentially supporting an unlimited[2] number of ports per deployment via licensing with the NS500VM, will still be subject to real-world hardware constraints. Bradford centrally manages licenses of multiple appliances, not endpoints. While enabling license and policy management of each appliance, it does not dynamically nor uniformly coordinate policy management across all appliances. Tolly engineers were unable to find substantial documentation on potential large-scale policy management, however, multiple appliances can be deployed and managed via the NS500VM or NS550RX.

According to Tolly engineer findings, Cisco ISE can potentially manage up to 10,000 concurrent endpoints per deployment. This could be achieved through the following deployment scenarios: a single server running admin/policy services/monitoring nodes can manage 2,000 endpoints. Device 3315 running all services can manage 3,000 endpoints and Device 3355 running all services can manage 6,000 endpoints. Together the 3395 and Virtual Machine running all services can mange 10,000 endpoints.

The Juniper IC4500 can scale to support 25 to 5,000 concurrent endpoint devices. The Juniper IC6500 network access server can scale to support up to 15,000 simultaneous endpoints. See Table 7.

[2] Assessment based on publicly-available vendor documentation. While theoretically device support is unlimited due to licensing modules, in practice, users may encounter real-world hardware restrictions

Manageability

The means to easily scale to manage thousands or tens of thousands of endpoints at multiple sites is a crucial feature for any NAC offering. Tolly engineers examined each solutions' ability to scale, including its ease-of-use with multiple endpoints, switches, and appliances, as well as its design for a large deployment. This includes the ability to group devices (appliances, switches, etc.) for a scalable configuration and management, ability to select multiple devices to configure at once and the number of appliances in a given policy and endpoint management instance. This provides an integrated, centralized and more automated approach to assure policy management across multiple networks and their respective infrastructure– essentially lowering the cost of ownership for medium-to-large and globally-distributed enterprises.

These features allow administrators greater user visibility and decreases the time to resolve issues within the network. It also allows for faster and easier deployment of global policies.

Based on publicly-available vendor information, Tolly engineers found that ForeScout CounterACT intuitively groups devices, ports, VLANs and domains with global policies.

Bradford Networks also offers port grouping, but in order to group and manage multiple appliances, a separate Control and Application Server is required. As referenced in the "Endpoints Per Deployment" section, this service enables license management and the ability to facilitate managing policy on a per appliance basis, as opposed to across appliances. This adds more administrative overhead in order to to maintain appliances and their respective policies across domains/networks.

Cisco ISE can potentially scale, but not without significant configuration. With Cisco ISE, every network device would need to be configured, as successful integration is largely dependent on an existing Cisco infrastructure This results in time-consuming management of multiple devices and components in a single deployment.

The GUI on Juniper UAC, according to information gathered by Tolly engineers, is easy-to-use and easy-to-configure. It requires managing multiple realms/roles, as well as multiple components such as the Juniper UAC, agent and switches, firewall and VPN (infranet enforcers) devices. To extend network and security infrastructure requires additional administration effort. Depending on the size of the deployment, the necessity of managing multiple components and extending interoperability could impact the total cost of ownership.

Evaluation Setup & Methodology

To evaluate the features and functionality of each vendors' NAC solution, engineers created a microcosm of a typical enterprise environment. The environment included AD/DNS/DHCP servers, Windows/ Macintosh/Linux endpoints, hypervisors and virtual machines, managed switches, VoIP phones, printers, access points, and mobile devices.

The network configuration utilized a single VLAN for all corporate traffic, and two separate VLANs for remediation and quarantine. At the core was a Juniper EX4200 48-port switch, connected to a Juniper EX4200 24-port POE switch and two Cisco Catalyst 3550 48-port switches.

All endpoints, printers and NAT devices were connected to the Cisco switches. The VoIP phone was connected to the Juniper POE switch, with the rest of the virtual and physical infrastructure connected to the core Juniper switch.

The entire deployment was connected to the internet via a Juniper SSG140 Firewall/ Router.

Deployment & Ease-of-Use

Each product was scored on the effort required to integrate into an existing network topology, its ability to be deployed as a virtual appliance, additional system/ network configuration required and its installation process.

Each solution was deployed using vendor-supplied installation and administration guides, publicly available in each product's support area. Engineers documented the installation process, noting time and steps needed to fully integrate the solution into the network. Engineers also noted any guidance the solution offered during the installation process, in addition to referring to documentation.

The deployment tasks included the appliance installation, network integration, and policy configuration according each vendors' best practices.

Interoperability & Agent Reliance

Engineers evaluated the extent of device interoperability, using vendor documentation as well as the solution's management interface to determine which network (Switch, Wi-Fi, and VPN) vendors could be identified and managed out-of-box.

Next, prior to adding managed endpoints, engineers documented each solutions' capacity for detecting/managing machines with no agent installed. This portion of the evaluation was centered around visibility, classification, inspection, and quarantine/ remediation capabilities.

First, engineers confirmed that each solution was able to detect newly-connected devices, and then scored solutions depending on how much information was available without their respective agent present.

Engineers then determined which inspection, remediation and notification actions were available on each client, without having to install an agent through the management console.

Visibility

Each product was evaluated based on its ability to detect and classify various devices on the network. Devices included rogue APs, mobile devices, VMs and hypervisors, managed switches and other managed devices.

Each solution was evaluated on the time needed for a newly connected device to appear in the administration console and how much information was supplied. Additionally, an overall assessment of asset classification was developed based on the findings.

Engineers evaluated each solutions' prerequisites for detecting and controlling a new switch added to the network and how each solution dealt with IP phones or printers, which should be excluded from any NAC policy.

Guest Management

Engineers analyzed how each solution detects, classifies and/or registers guest devices versus corporate devices. Engineers verified the solutions' Web authentication portal functionality, guest registration methods and how each differentiated between guest and corporate machines.

Endpoint Compliance & Remediation

Engineers evaluated the extent of each solutions' built-in compliance policies and remediation methods. Additionally, engineers examined each solutions' flexibility in defining and implementing additional policies.

A solutions' compliance reports and dashboards were evaluated for ease-of-use and customization. The extent of integration, if any, with third-party security systems, such as McAfee anti-virus and ePolicy Orchestrator, was noted by engineers.

Each solution was configured to provide both auto-remediation and self-remediation. Engineers noted the extent of each implementation.

Enforcement

This evaluation involved enforcing restrictions on client devices, whether through Role-Based Access Control, 802.1X, or through the client agent.

Each solution was evaluated based on the different types of policy enforcement available to administrators. For each enforcement vehicle, engineers verified that a policy could be created and enforced, noting the amount of configuration required for each method.

Scalability

The supported number of endpoints per appliance/deployment was gathered from vendor-published documentation and was not verified by Tolly.

Engineers evaluated each solutions' architecture and management interface, taking note of organizational models, grouping and overall layout, to assess its suitability for large deployments. This included how each solution groups large quantities of devices by default, configures multiple devices and creates/implements policies to multiple deployments.

About Tolly…

The Tolly Group companies have been delivering world-class IT services for more than 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.
You can reach the company by email at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Interaction with Competitors

In accordance with Tolly's Fair Testing Charter, Tolly contacted the competing vendors inviting them to review the test methodology and their results prior to publication. Cisco and Juniper declined to participate in the evaluation. Bradford Networks accepted the invitation to participate in the evaluation. Comments from Bradford Networks are included in the main document as appropriate.

For more information on the Tolly Fair Testing Charter, visit:
http://www.tolly.com/FTC.aspx

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

212105-fw1-mts-wt-29March2012-VerP