WHITEPAPER

Choosing a Network Access Control (NAC) Solution that is Right for Your Network

BEST PRACTICES IN NETWORK ACCESS CONTROL

ForeScout

NETWORK ACCESS. CONTROLLED.™

Call Toll-Free: 1.866.377.8771 • www.forescout.com

Cutting Through the Network Access Control (NAC) Confusion

Confused about network access control? You are not alone. Over the course of the last two years there has been a significant amount of IT industry attention focused on controlling users and devices accessing the corporate network. It should be no surprise that in this same time the number of mobile computing devices (i.e., laptop computers) surpassed the number of desktops used in corporate networks. With this growing number of devices 'on the move', the challenge IT managers face in securing the network has grown exponentially.

Enter Network Access Control (NAC)

NAC has emerged as a promising new technology to answer the burning question of "how do I secure my IT infrastructure in this ever-increasing fluid environment." The benefit of managing access with NAC is straight-forward: any device connecting to the network is checked for network security compliance, automatically brought into compliance if policy violation(s) are detected, and continually monitored throughout the connection session to ensure the device remains compliant. Integrating identity-based information with the device inspection enables IT managers to ensure only the users with compliant devices are granted access to network resources allowed by job function, providing a virtual, dynamically-segmented network with role-based access control for corporate users and network guests.

Enter Real World Networks

Challenges arise when attempting to apply theoretical concepts into real world networking environments. Complex heterogeneous network environments introduce a significant level of complexity in attempting to implement network access control. A typical corporate network is anything but typical, comprised of endpoints and infrastructure components from numerous vendors with varying configurations. As most companies grow organically, infrastructure and device upgrades are implemented on an "as-needed" basis to handle increasing computing demands and/or to gain additional functionality from newer versions of network equipment (i.e., switches, routers, etc). Additionally, the proliferation of low-cost mobile devices and wireless networks enable end-users to bypass existing security measures by introducing personal devices into the corporate network.

This white paper will look at three key functionality criteria a NAC solution must deliver in order to effectively operate in complex and diverse real-world networks. These criteria are:

1. **Detection and Interrogation of Endpoints**
   Before enforcement of network security policies can be enabled, all connecting devices must be detected. Additionally, several types of inspection mechanisms need to be considered in order to get maximum interrogation with minimum IT management overhead for all detected and identified endpoints.

2. **Policy Creation and Enforcement Actions**
   How easy is it to create policies? What level of policy granularity is necessary for effective device inspection and enforcement actions? Will enforcement of policies disrupt the network or users? These are the questions that must be considered to ensure that the NAC solution will effectively deliver granular levels of access control without disrupting network operations.

3. **Deployment and Integration**
   In order to maximize the benefits of a NAC solution, it has to be seamlessly integrated into the network infrastructure without causing network disruptions. Therefore, multiple approaches to deployment (e.g., out-of-band vs. inline) must be considered to determine the potential impact and level of disruption a deployment method will have on the overall infrastructure. Another determining factor is a NAC system's ability to leverage the existing investment into network infrastructure and equipment without requiring costly upgrades or causing network downtime.

Section 1
Detection and Interrogation of Endpoints

One of the most critical aspects of controlling access is detecting connecting devices and ensuring those devices are in compliance with network security policies. The question remains: How to accomplish access control in a complex network where all access points are not easily defined or even known? A number of methodologies have been introduced to address this primary challenge of NAC, but no one silver bullet exists. In considering the different approaches to detection, a key decision point emerges in the discussion on whether prior knowledge of an endpoint should be required in order to detect it. Prior knowledge of a device implies some form of installed agent be present on the connecting endpoint prior to connection, which identifies the device and provides some level of system diagnostic result to the NAC system.

Agent vs. Clientless NAC

Software agents have become a fairly common element in a typical device configuration as a part of a corporate security policy. It is not unusual to have multiple agents providing a variety of system assessments. This is a positive way to defend an individual system against spyware or viruses, or to enable a configurable VPN connection. Agents have the ability to obtain detailed knowledge of the system in which it resides. Access to the system's registry and file structure provides intimate knowledge of installed applications, active processes, and a host of other system configuration details to provide a system "health" assessment prior to allowing access. At the point of connection, the software client identifies the computer as a managed user device and initiates a further inspection.

Conceptually, this is a good story. The agent obtains in-depth information of the system's level of compliance and provides this compliance information to the NAC system at the time of connection. However, the NAC system is rendered virtually useless when unmanaged or non agent-based devices are introduced into the network. Any device that does not have an agent installed is either summarily denied access to the network or is allowed complete access without any form of endpoint inspection. Neither scenario is an acceptable business practice – while the former disrupts productivity and requires an increased level of manual device processing by the IT staff, the latter introduces an array of security threats and vulnerabilities directly into the network.

Unmanaged systems are only one of the many daunting challenges faced by agent-based NAC systems. Requiring an agent on all managed endpoints introduces a significant management burden associated with the NAC solution deployment. While an agent-based approach may work in a small networking environment with a limited number of endpoints, it quickly becomes impractical as the number of managed or unknown devices increase.

Agent-based NAC systems also pose additional challenges due to OS compatibility issues. Most NAC solutions support the latest versions of Windows and possibly some Macintosh devices, but anything beyond this becomes problematic. This issue becomes even more critical when considering any other type of IP-based devices that are connected to the network for which an agent is simply not an option (e.g., printer, VoIP phone, MES systems, medical devices, etc.). Because a client can never be deployed into these devices, they become potential vulnerabilities that remain undetected and therefore unprotected by the NAC system.

There is, however, one variant in this discussion. Some NAC systems provide a dissolvable or non-persistent agent which can be downloaded and temporarily installed at the point of connection and is then removed once the device is no longer on the network. This approach can alleviate some of the IT management burden in dealing with non managed devices and provide a partial solution for addressing network guest and contractors.

Going Clientless

Clientless NAC systems provide a number of advantages over agent-based solutions, especially when considering network protection scope and scalability, decreased levels of manual IT management and reduction of disruptions to network services.

Scalability

Since a software agent is not required to be installed or downloaded onto the endpoint, the scalability of a clientless NAC system is virtually unlimited. While there may be other factors that determine how well a NAC system will perform (e.g. geographically-dispersed networks), the system itself is not restricted by the type or number of devices it can detect and manage. Clientless systems provide the ability to detect any IP-based device, allowing the complete coverage of a global infrastructure without prior knowledge of any of the connecting devices.

Another clear advantage of a clientless NAC system is that it does not require network managers to educate the users on how to use yet another agent or altering their established logon process in any way. With all detection and inspection being conducted without an agent, end users are not aware that a policy check is taking place… as long as their device is compliant with the corporate security policies. This allows for the least amount of change to end user behavior and experience, which further alleviates the burden on IT resources and staff and significantly contributes to the overall success of a NAC rollout.

Management

Clientless NAC systems significantly reduce the amount of management required to enforce network security policies. Since there are virtually no interoperability issues among the connecting devices, IT management can focus on addressing more critical business issues. By design, a clientless system should cover all IP-based devices, enforcing policies on all devices and thus providing more comprehensive coverage of the network. When a policy violation is discovered (e.g., the NAC system detects a rogue wireless access point) IT management is informed immediately and is able to efficiently respond to the threat or vulnerability. In the meantime, more trivial violations are automatically addressed by the NAC system (e.g., anti-virus definitions are out of date and user is linked to self-remediation).

In addition to the benefit of low management overhead with a clientless NAC solution, IT administrators gain a greater understanding and control over what users and devices are attempting to gain access to the network. This functionality is particularly beneficial when it comes to detecting and managing contractors and other types of network guests who need limited network and/or Internet access but do not have an agent installed on their device. A clientless NAC system need to be able to determine if the device is company owned (managed user/device) and handles devices that are not based on the defined policy and its associated enforcement action.

For example, when a contractor/guest attempts to connect to the network with a clientless NAC system in place, the device would be detected and identified as a guest and forced into either a pre-configured network segment or a virtual local area network (VLAN). The contractor/guest would then immediately gain access to a pre-determined set of appropriate network resources without diminishing the level of security or introducing any threats to the enterprise network. With this process automated, enterprises can be sure that only known and authorized devices are gaining access to the production network,

> **NAC AT WORK**
> **Clientless Device Detection**
> A large hospital under pressure to meet regulatory compliance requirements urgently needed to obtain an accurate count of all devices on their network such as desktops/laptops and peripherals, as well as EKG, CRT and ultra-sound machines.
>
> Within hours of deploying ForeScout's NAC appliance, network managers had a complete inventory of all IP-based devices connected to the hospital network. With all of the devices detected and identified, network managers quickly defined and implemented a set of hospital-wide access policies to gain awareness of all connecting endpoints.

while all others are detected and controlled by the clientless NAC system.

Section 2
NAC Policy Creation and Enforcement

The primary reason to deploy a NAC solution is to ensure that all connecting and connected devices on the enterprise network are in compliance with network security policies. Although policies vary greatly between enterprise networks, there are some basic network security policies that are fairly consistent. The policy of checking whether antivirus software is installed on a device and the anti-virus definitions are up-to-date is an example of a best practice policy common to most security-minded organizations.

Perhaps one of the biggest challenges when deploying a NAC solution is determining which policies need to be enforced and what actions need to be taken to enforce them. One of the most important criteria in selecting a NAC system is the policy creation process. An enterprise-level NAC solution must enable IT management to create customized, granular, and enterprise specific policies to effectively address the security concerns of any organization. Figure 1 features examples of system variables that could be used as the basis for creating a NAC policy.

Figure 1: Table of Enforceable Basic Policy Variables

USER BEHAVIOR	• Network Policy Violations • Audited Responses • Self-Remediation Success	
USER INFORMATION	• Username • Authentication Status • Workgroup	• Email Address • Role/Department • Phone Number
APPLICATIONS	• Illegitimate Applications • Application Versions • Registry Values	• File Information • Modification Date
OS INTEGRITY	• OS Fingerprint • Antivirus Update Status • Missing/Old Service Packs	• Un-patched Vulnerabilities • Open Services • Running Processes
DEVICE INFORMATION	• IP Address • MAC Address • Hostname	• Device Type (Desktop, Laptop, Printer, Wireless, etc)
PHYSICAL LAYER	• Physical Switch • VLAN • Switch Port	• 802.1X • Number of Devices Sharing a Port

NAC Policy Enforcement

The term "policy enforcement" typically causes appre-
hension among IT management. Any time an auto-
mated system is tasked with enforcing policy, there is
a risk of network disruption. Network service and user
experience disruptions typically arise as a result of
binary enforcement by a NAC system (i.e., only allow or
deny), resulting in loss of productivity. The disruptive na-
ture of a NAC system that does not provide an array of
flexible enforcement actions could outweigh the benefit
derived from access control security.

Flexibility is Key

In addition to differentiating between minor, moder-
ate and critical security threats, it is imperative that any
NAC solution provides a full spectrum of enforcement
options. The ability to match the level of enforcement to
the exact level of policy violation is a critical aspect of a
successful NAC implementation.

> **NAC AT WORK**
> **Non-Disruptive Policy Enforcement**
> A financial services company deployed
> ForeScout's CounterACT network
> access control solution in order to
> enforce the company security policy
> banning instant messenger on devices
> connecting to the network. By using
> CounterACT's wide range of flexible
> enforcement options, network manag-
> ers were able to enforce this security
> policy without disrupting employee
> productivity by remotely terminating
> messenger applications and notifying
> the appropriate staff to ensure the il-
> legal applications are uninstalled from
> the device completely.

For example, some organizations consider instant messaging to be a critical business communication
tool, while other enterprises may view it as a security threat. In the latter, even though the presence of
IM is considered a threat, management does not want to keep the user from being productive, and only
wants to notify the user of the policy violation or perhaps disable the application. A NAC system with a
binary enforcement approach will cause disruptions to user productivity by revoking the device's access
to the network while IT management addresses the issue. On the other hand, a NAC system with a range
of enforcement options could prompt the user to remove the application, notify the appropriate staff of
the problem, or simply disable the application remotely without causing any downtime or disruptions.
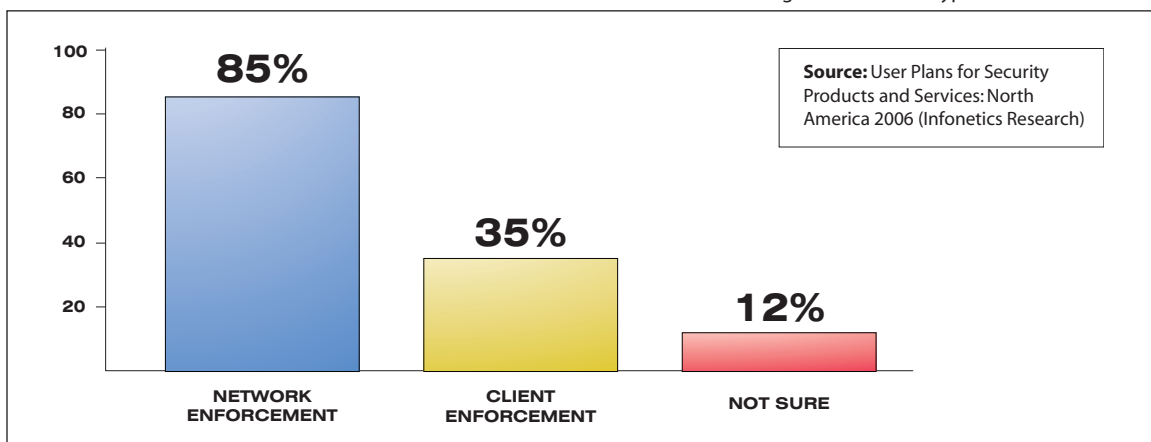
Network-based Enforcement

As the industry matures and enterprises determine suitable methods of NAC deployment for their
specific environments, there has been a notable trend towards network-based enforcement. While some
enforcement can be done on the endpoint by a client-based solution, the deployment and manage-
ment challenges associated with an agent-based NAC system has led the industry towards a network-
based approach. In a recent white paper published by Infonetics Research, it is noted that 80 percent
of survey respondents planned apply enforcement actions over the network rather than relying on any
form of installed client.

Figure 2: Preferred Type of NAC Enforcement

Source: User Plans for Security
Products and Services: North
America 2006 (Infonetics Research)

Post-connect Monitoring and Enforcement

If a device connects and is found compliant, is it allowed access to the network indefinitely? What happens if it's connected for a period of time and then violates a security policy? Will the NAC solution be able to detect this violation and offer the same level of flexibility in enforcement as was offered at the point of connection? Regardless of the benefits of device detection and inspection at the point of connection, post-connection policy enforcement is a critical feature of any effective NAC system.

A NAC solution must continue to monitor all connected devices throughout their network session to ensure that they remain in compliance with corporate security policies and are not acting in a malicious manner. For example, if a user decides to install an unauthorized application after passing the initial inspection, a NAC system that only inspects devices at the point of connection is rendered powerless against the policy violation.

Enforcement Against Malware and Self-Propagating Threats

Many NAC solutions available today are missing a key element of ensuring secure network access control: self-propagating threat detection and mitigation. While the system configuration check is a critical step in determining whether a device should be allowed to connect, it is a pre-emptive method of ensuring policy compliance. However, the presence of malware or any other type of self-propagating code poses an immediate security threat to the enterprise network.

Most enterprise networks already have some sort of anti-malware solution in place, but a NAC system is truly a front-line defense mechanism against such threats. Malicious code is designed to propagate itself as quickly as possible, and can be unleashed onto the network in a matter of seconds. Malware detection and mitigation is a must-have feature for any NAC system, to ensure infected devices are detected and blocked/quarantined before they have a chance to unleash an outbreak across the entire enterprise network.

> **NAC AT WORK**
> **Defending Against Malware**
> A Fortune 100 software company was in the process of deploying ForeScout's CounterACT solution when the corporate network was hit by a previously unknown worm, infecting devices throughout the enterprise network.
>
> When the smoke cleared, the only segment of the network that did not experience massive outages caused by the worm was the building protected by ForeScout's CounterACT. With its full-blocking mode enabled, the device identified the few infected sources on the protected segment of the network, completely blocked all worm traffic, and removed or quarantined any remaining infected devices.

Section 3
Deploying Network Access Control

In evaluating a NAC solution, it is essential to fully understand the complete scope of the deployment process. Similar to the client vs. clientless considerations, there are a variety of ways to deploy NAC into the network infrastructure. For the purposes of this examination, three NAC deployment approaches will be discussed: Switch based NAC, inline and out-of-band appliances.

NAC as part of the Switching Infrastructure

The concept of NAC originated from the switch industry, with the idea of integrating some form of admission control directly into the switch to add an additional layer of security. Like many other theories this one had great merit conceptually, but faced a number of implementation challenges. For instance, the integrated switch approach was designed to only focus on the point-of-connection; as opposed to

pre- and post- connect access control. Admission mechanisms rely on the endpoint communicating through an open standard communication protocol (802.1x) in order to gain access to the network. The switch would look for the 802.1x supplicant upon connection and grant or deny admission based on the identification result.

Other shortcomings of this approach include lack of integrated ability to mitigate self-propagating malware, detection/management of unmanaged system and handling IP based non-user devices. More importantly, this method creates a highly restrictive enforcement environment that is extremely disruptive to network operations. Most legacy hardware is not 802.1x compatible, so deploying this technology requires a "forklift" upgrade of the switching infrastructure, which is disruptive and costly. While 802.1x can be a useful addition to an overall NAC strategy, it is far too limited and restrictive as a stand-alone solution in a broad-based deployment.

Inline NAC

An inline NAC deployment is based on the premise that all data traffic passes through the device to successfully detect, inspect and enforce policy. Once a device connects, the inline NAC appliance begins the process of inspecting each packet. Based upon the traffic emanating from the endpoint, the connecting device can be granted full access or some form of limited access to network resources. Typically, this approach utilizes a 'quarantine by default' method to ensure the system has enough information to determine the health of the endpoint and the access rights associated with the device user. Inline systems typically depend on an agent to achieve a thorough endpoint compliance status inspection.

A bigger challenge of deploying an inline product is the physical effects of introducing another hardware component into the flow of traffic. Inline deployments introduce an additional point of failure and create significant latency risks, both of which are disruptive to users and restrict network performance. If an inline appliance fails, it subsequently blocks any device trying to pass network traffic through it. Both of these downsides negatively impact the end user's experience and are likely to cause network disruptions.

Another point for consideration is the number and location of inline appliances required to achieve a comprehensive NAC deployment. Inline products work best when they are close to the connecting device. Invariably, an inline appliance has to be paired with, and in some cases replace the access layer switch. For a small to medium business, this may be limited to just several appliances, but a global enterprise-wide deployment would require a significant investment in cost, time and resources to implement a complete NAC deployment.

Out-of-Band NAC

Out-of-band NAC deployments leverage the existing network infrastructure to detect, inspect, and enforce policy on connecting and connected devices. This approach requires the device be attached to the network either through a span port on a managed switch/router or through a network tap. From this point of connection, the NAC appliance is able to monitor all network traffic without data actually passing through the device. By deploying in this manner enterprises can avoid the deployment challenges caused by inline deployments, even if a specific network configuration limits some of the available enforcement actions that are otherwise available in an switch span port type of deployment (i.e., physical switch port block).

Leveraging an existing switch infrastructure enables NAC system to be deployed with minimal, if any, modification to the existing network configuration. This prevents immediate and costly switch upgrades allowing a lifecycle extension to existing infrastructure. Additionally, this approach further reduces deployment costs by placing the NAC appliance at a higher level on the network (typically from a distribution layer switch), which provides a greater level of coverage while requiring a smaller number of appliances.

Infrastructure Integration

Seamless integration into the switch infrastructure is a very important requirement for any NAC solution. However, a comprehensive NAC system must extend beyond just hardware in order to fully leverage its policy enforcement capabilities. For example, if a connecting device does not have the required security patches installed, a comprehensive NAC system can streamline the remediation process by leveraging an existing ticketing or remediation systems, or even prompt the end user with self-remediation options to quickly bring the device into compliance and back onto the network. A well integrated NAC system maximizes the value of its policy enforcement offering as well as the value of the existing investment into network infrastructure components.

> **NAC AT WORK**
> **Seamless Integration**
> An agency of the United States Government deployed CounterACT on their inter-bureau backbone as well as VPN gateways and remote locations without making any changes to the intricate infrastructure. In addition to seamlessly integrating with all hardware components, CounterACT integrated with a number of third-party systems including vulnerability assessment, helpdesk and remediation.

Non-disruptive Deployment and Policy Enforcement

The out-of-band approach is by far is the least disruptive method for a NAC deployment. However, the level of network disruptions caused by the implementation of policy enforcement actions is one of the most visible factors in determining the rate of success of a NAC deployment. Adding to the above-mentioned requirement for a flexible range of enforcement actions, it is critical that a NAC system provides administrators with the ability to monitor network security events per their defined policies without taking any actual enforcement actions. By determining the state of the network devices in relation to the requirements defined in the security policies, IT managers can make educated decisions on what type of enforcement actions to take against specific violations to eliminate security vulnerabilities without disrupting end-user experience or network operations.

Conclusion

Network Access Control is quickly becoming a critical network infrastructure element as enterprises work to defend their networks from non-compliant, unauthorized/unknown and/or infected devices. However, in a market saturated by vendors offering NAC solutions, it is important to have a clear understanding of all decision-determining factors in order to attain a NAC system that meets the enterprise security policy requirements. NAC can be powerful tool, but it needs to be evaluated with business process in mind as security always needs to be balanced against business goals, and user and network productivity.

A comprehensive NAC system must provide flexible and granular policy-based coverage with the least amount of network and user disruption. ForeScout's flagship NAC product, CounterACT (see appendix 1 for a detailed description), is a clientless, out-of-band NAC appliance that provides granular policy creation matched with a full spectrum of enforcement actions. ForeScout's NAC enables IT managers to define the appropriate responses to policy violations, effectively delivering a measured approach of enforcement to keep networks safe while minimizing the end-user disruptions. Striking a balance is key and deploying a flexible NAC product, like ForeScout's CounterACT, is the only way to accomplish this critical task.

Appendix
ForeScout's NAC Solution: CounterACT

ForeScout's CounterACT is the only non-disruptive, clientless NAC solution to deliver End Point X-ray™ and Fast Pass™, eliminating the usual mandatory "quarantine upon connection" phase and moving users immediately into productivity. CounterACT detects and identifies all connecting and connected devices without a client, and all security checks include deep interrogation for bullet-proof security, but are immediate and completely transparent to the user. CounterACT delivers a wide range of policy enforce- ment options to custom-fit response actions to policy violations to ensure there are no disruptions to the network or normal business operations. CounterACT is deployed completely out-of-band, and requires no equipment upgrades or costly infrastructure changes.

The ForeScout Difference

ForeScout's clientless NAC is the only solution in the industry that delivers these essential features:

Detects every device connecting to the network without requiring a client

Upon connection to the network CounterACT immediately determines if device is company owned or whether it belongs to a guest or contractor. If the device is a part of the domain, CounterACT launches a device scan to check for policy compliance status. If the device is not part of the domain, CounterACT features multiple enforcement mechanisms to automatically ensure the guest/contractor has enough access to remain productive without compromising the security of the enterprise network. The in-depth scan of managed and unmanaged devices requires no client or agent to reside on the device.

Interrogates all devices for security compliance and malicious code

CounterACT monitors all devices at the point of connection and throughout the duration of the con- nection, for any form of self-propagating malicious threat. If an infected system attempts to gain access to the network, CounterACT's integrated IPS provides real time detection and protection from the spread of known or zero day threats. This is accomplished without quarantine by default requirement, so that compliant users do not experience any change in login behavior. Once CounterACT established the remote login, a deep inspection of the system is conducted allowing for policies to be created and enforced based upon any combination of system variable (i.e., antivirus, OS patch levels, allowed/not allowed applications, active processes, etc.)

Enforcement tailored to violation

CounterACT provides a full spectrum of enforcement actions to provide a high level of flexibility in ad- dressing minor and moderate policy violations. CounterACT enables configuration of granular policies in which the level of restriction corresponds to the severity of a policy violation. This functionality ensures that interruption of user productivity is limited only to critical network security violations.

ALERT AND INFORM	RESTRICTIVE ACCESS	MOVE AND DISABLE
Open Trouble Ticket	Deploy a Virtual Firewall around an infected or non-compliant device	Reassign device from production VLAN to a quarantine VLAN
Send Email		
SNMP Traps	Reassign the device into a VLAN with restricted access to resources and services	Block access with 802.1X
Syslog		Alter the end user's login credentials to restrict or completely block access
HTTP Browser Hijack	Update access lists on switches, firewalls and routers to restrict access	
Auditable End-User Acknowledgement		Block access with device authentication
Self-Remediation	Automatically move device to a pre-configured guest network	Turn off physical switch port
SMS, PatchLink Integrations		Terminate unauthorized applications

Deploy and enforce without disruptions: Out-of-Band Deployment
CounterACT typically is deployed from a distribution switch. The out-of-band deployment ensures
there is no disruption to the network, IT staff and compliant users. With integrations into most switch-
ing infrastructure, when a policy violation is detected, CounterACT can leverage remediation systems to
automatically guide non-compliant users into compliance. See typical deployment architecture in the
diagram below:
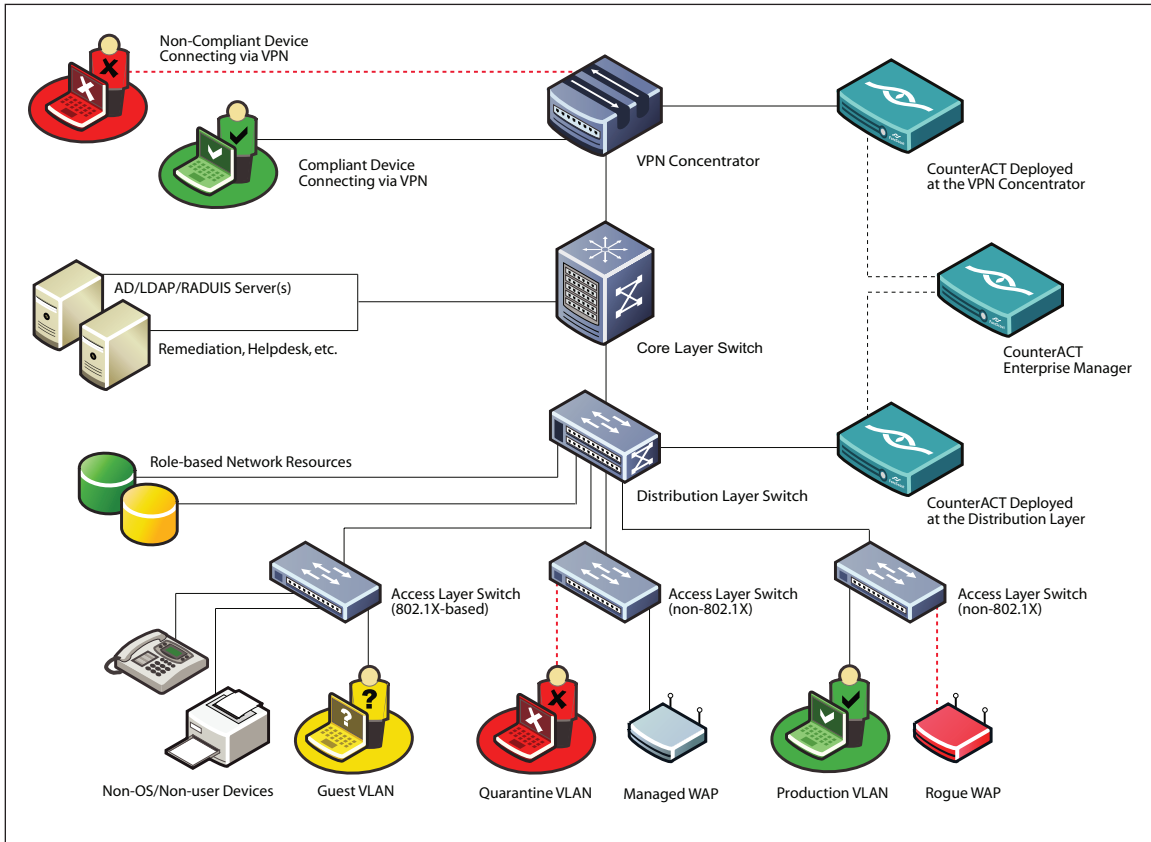
ForeScout Technologies, Inc.
10001 N. De Anza Boulevard, Suite 220
Cupertino, CA 95014, USA

Toll-free: 1.866.377.8771 (US)
Tel: 1.408.213.3191 (Intl.)
Fax: 1.408.213.2283

www.forescout.com