



Whitepaper

Securing Visitor Access through Network Access Control Technology

Introduction

The network infrastructure in today's enterprises faces an incredible challenge as both business processes and workforce requirements evolve. According to the Bureau of Labor Statistics, more than seven percent of the employed workforce is made up of independent contractors¹. In addition, large public enterprises are hosting an exponentially higher number of financial auditors due to federal regulations, especially Sarbanes-Oxley. Companies face on average 4,888 labor hours² of multiple external auditors reviewing and discerning their internal controls, with a majority of this time spent "on site" utilizing the corporate LAN. These growing numbers of visitors have caused a heightened sense of awareness for ensuring that the network remains safe, while still permitting these individuals and their unknown devices to remain productive.

Ultimately, the most secure thing that could be done is to not allow access by any foreign device, but this is not practical in today's business climate where organizations are forced to balance security with the needs of the business. For the last several years, the best solution available to IT and security professionals was to create a separate visitor network for conference areas, or a wireless VLAN for guest use only, which resided outside perimeter firewalls. Although this solution partially answered the need, it added one more network to be maintained by an already strained IT staff. In cases where the necessary resources were not available, some enterprises failed to restrict access, and therefore left their network open to the risk of malicious activities. For example, a contractor could connect into a wired LAN in the conference room and run a network discovery tool (e.g. NMAP) to discover what resources are present. Armed with this information, this person could steal information or attack the network without the organization ever being alerted to such behavior. So the question then becomes what is the most effective method for ensuring that outside devices gain appropriate access to remain productive, while not exposing the network to security risks.

The most effective way to ensure the safety of the network from the multitude of onsite visitors is through the deployment of network access control (NAC) technology. In a recent Gartner report, vice president and Research Fellow, John Pescatore said, "Without NAC enforcement, connecting unmanaged devices to sensitive business applications will result in unacceptable levels of business disruption because of network downtime and information compromise."³

Advanced NAC technology can allow administrators to regulate the extent of access granted to visitors and their unknown devices by applying the same compliance rules on these machines as they do to corporate owned resources (i.e., managed devices). With some NAC solutions, controlling visitor access is impractical in nature since it requires the visitor to load a client/agent onto their device to gain access. Typically, this is a show stopper and can severely impair the productivity of these outside resources. ForeScout Technologies' NAC appliance, CounterACT™, solves this challenge by providing a clientless solution, which allows administrators to automatically detect unmanaged systems connecting to the network and grant appropriate access based upon the security requirement of the enterprise.

¹ "Contingent and Alternative Employment Arrangements" February 2005, Bureau of Labor Statistics

² "Survey on Sarbanes-Oxley Section 404 Implementation" April 2006, Financial Executives International

³ "Findings for Secure Use of Employee Owned-PCs" January 20, 2006, Gartner

The ForeScout Solution for Securing Visitor Access

In order to provide a network infrastructure that remains secure during the connection of both known and unknown devices, organizations must employ an enterprise wide NAC system. The more advanced NAC solutions offer organizations a method of seamlessly integrating control into the network with minimal disruption to both employees and onsite visitors.

ForeScout's CounterACT network access control solution provides administrators with easy and flexible technology which meets the demands for complete network security policy enforcement, while still maintaining the highest level of protection from self propagating malware.

CounterACT provides an unparalleled level of access control and policy enforcement over all devices in the enterprise network, regardless of whether they are a company managed device, an unknown device brought in by an onsite visitor, or a non-user based device (i.e., printers, fax, VoIP phones, etc). These access controls are applied to this array of devices regardless of how the device gained connection to the network, whether it is through a wired LAN, VPN, or through a wireless access point (WAP). ForeScout's clientless, transparent system allows for easy deployment and enforcement of network policy ensuring all attached elements meet pre-defined security policies including complete protection from zero day self propagating threats.

To meet the delicate balance between productivity and security, it is imperative that a NAC solution provides for flexibility over the types of security policies that can be deployed, along with how to properly respond when violations occur. CounterACT provides a variety of enforcement responses with the ability to apply measured and appropriate enforcement to specific pre-defined policy violations.

CounterACT Highlights

Point of Connection (End Point Control)

- Network-based, clientless solution- NO desktop client or host agent required.
- Policy control over all devices- managed/unmanaged/non user.
- No change required to user's experience, current configuration, or login process.
- Turnkey appliance with a plug-and-play "Virtual Firewall" feature.

Infrastructure

- Seamless integration with existing network infrastructure- no network change required.
- Not an inline device (typically deployed at distribution layer switch).
- Scalable and easy to deploy with no network redesign.
- Handling of all peripheral devices (printers, VoIP, WAP) in addition to host nodes.

After Connection

- Continuous protection and enforcement- all devices monitored after connection at regularly scheduled intervals or on demand.
- Real-time self propagating malware quarantine- does not rely on signatures or anomaly detection. Includes real-time protection from zero-day threats and malicious attackers.

Implementing Security Policies for Visitor Access

CounterACT provides administrators with the capability to allow visitors to gain access to the network without creating added risk to the network, its critical data, and its users. By utilizing CounterACT for the automatic handling of visitor access, valuable IT resources are not consumed by the manual configuration changes required to gain access, or dealing with the possible headaches of downloading an agent or client to the endpoint device. The security policies are pre-defined by network administrators, and can range in flexibility in order to meet the specific access requirements of the organization.

The most critical decision that needs to be made before the implementation of the NAC solution is the actual security policies the organization would like to enforce on visitors entering the network. Since CounterACT provides the ability to create and enforce granular security policies, any range of policies can be set, including:

- Move all unknown devices to a separate VLAN with Internet access only. The connecting device would be detected as a network visitor and automatically removed from the production network prior to connection. This device would no longer be subject to any further scrutiny, since it is isolated from any network resources.
- Require compliance with all corporate security policies for access to the Internet or other resources. Upon end user granting permission (through device login) to have their system examined for security compliance, CounterACT will interrogate the device to ensure it meets the adequate policy requirements before permitting access to the Internet or any other resources.
- Provide unified access control across entire network. In the case where a policy is established for specific network locations (i.e., conference rooms having only Internet access), the CounterACT system ensures this policy is enforced even when visitors manage to plug in outside of these designated area. For example, if a visitor were to get into an executive office and plug in, the CounterACT appliance would detect the device as a visitor and move it back into a quarantined VLAN.
- Fully block all guest devices, and allow for zero access to the Internet or other resources. CounterACT will recognize all devices that are not recognized as part of the enterprise directory structure (e.g., Active Directory, RADIUS, etc.), and will immediately block access of the device to the network.

Security policies can be created in CounterACT through standard policy templates, or customized using a simple wizard style GUI which guides the process of creating access policies. This set of policies then enables the appliance to detect device activities and endpoint violations. These conditions include a variety of values including device type, authentication, registry values, services, applications, service packs, etc.

Once the appropriate policies have been determined, CounterACT provides a variety of flexible options for real time enforcement of the violation. This measured response continuum ranges

from a simple notification delivered through a hijacked HTTP session that provides a dialogue box notifying the user of the policy to limiting the users' access, to deploying a virtual firewall which walls the device off from specific resources, to complete and immediate disconnection from the network. The administrator has the ability to pre-determine which response should be taken based upon which policy violation that occurred.

Providing Secure Visitor Access- How it works.

CounterACT's unique approach to NAC allows enterprises to achieve maximum security by protecting the network from self-propagating malware and providing the complete ability to authenticate connecting devices before they gain access to critical network resources. When dealing with network visitors, the most critical threat requiring attention is self-propagating malware damaging the productivity of network operations. CounterACT provides a high level of protection as a default "out of the box" policy. Once enabled, the appliance will examine every connecting device (managed or unmanaged) for self propagating threats, including fast spreading network worms, and block/quarantine any malicious traffic.

CounterACT utilizes the patented ActiveResponse™ technique for preventing infection attempts by identifying and suppressing malware before it propagates within the network. The appliance monitors traffic directed towards the protected network for signs of reconnaissance, and then identifies the techniques used, for example port or NetBIOS scans. In response to this activity, CounterACT generates virtual resources sought by malware programs and forwards the information back to them. When the malicious attacker attempts to access the protected network, CounterACT immediately recognizes it, and will prevent it from establishing communication with the targeted location.

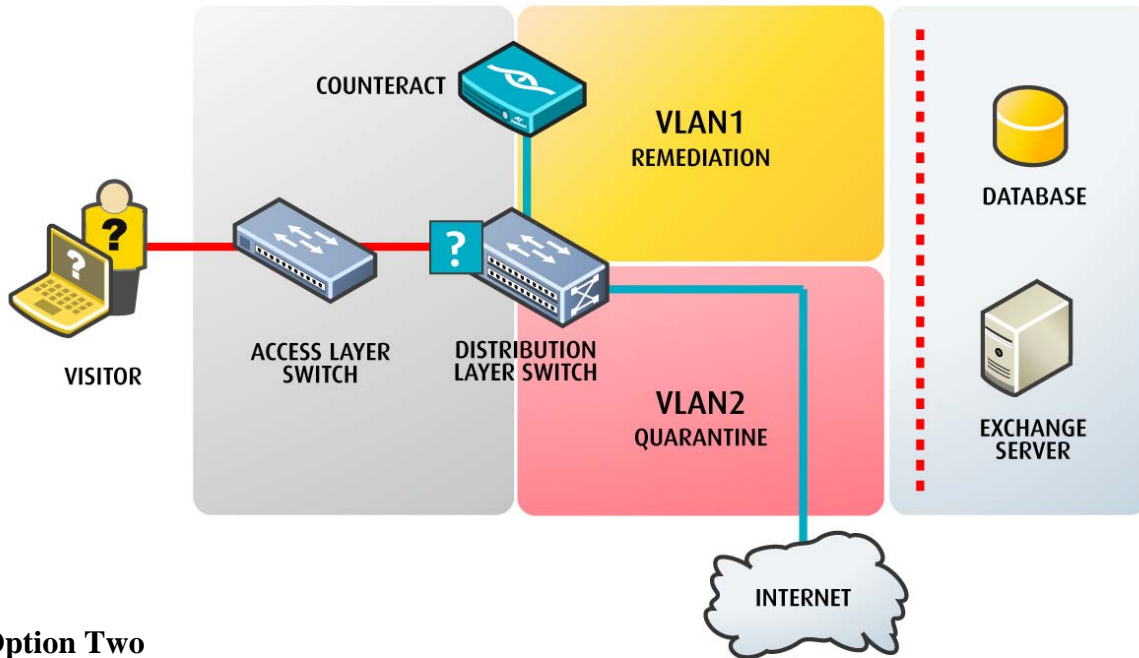
With the threat of self-propagating code in check, CounterACT can focus on determining if the device attempting to connect is a known/managed or unknown/unmanaged resource. This is done through comparison with the information stored in the directory structure (i.e., MAC address in Active Directory) or can be done through watching for successful domain or service authentication attempts. If the device is determined to be a visitor to the network, CounterACT will apply the appropriate pre-determined action for the device.

In using a NAC system to handle visitor access there are two basic options which provide for an appropriate level of network access while still achieving full protection and control over the devices on the network. The first option is to isolate the device, allowing it to remain as unknown and unmanaged. The device can be granted Internet access from this isolated VLAN, but would remain completely separate from the production network.

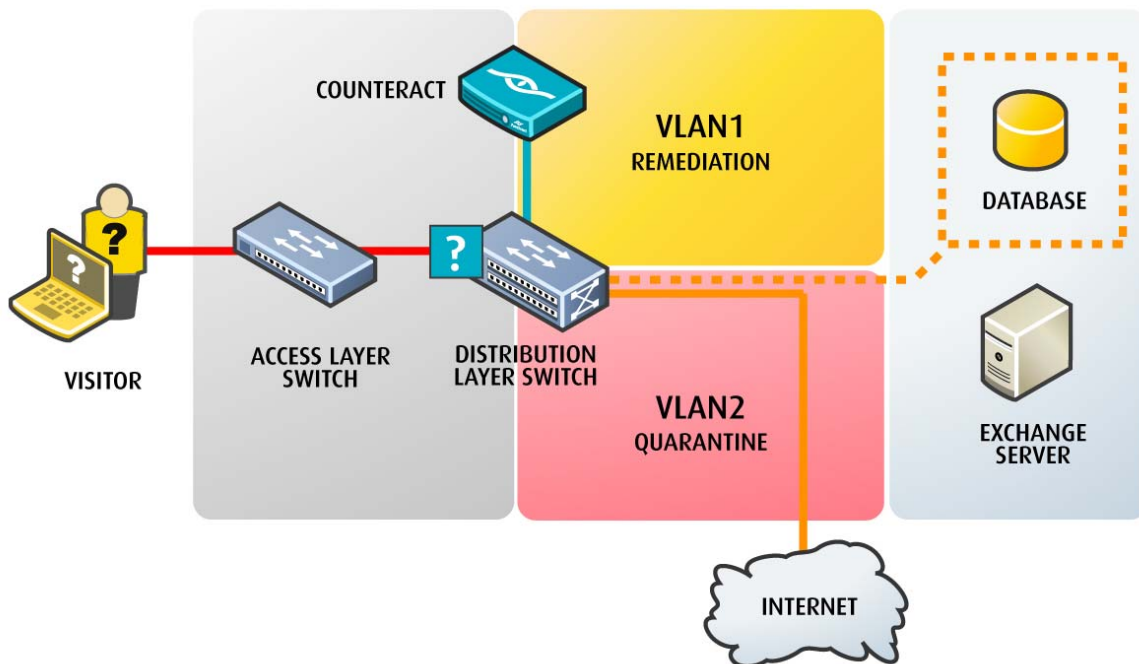
The second option will attempt to authenticate the device, thereby permitting the device to be treated like a known, managed device, with the appropriate access granted. In this option, the end user will be asked to grant the NAC system permission to interrogate the device for security compliance. The user would do this by simply re-logging into their device, thereby providing

CounterACT with the appropriate access credentials to begin its interrogation. If the visitor does not grant permission for the interrogation, or does not have administrator rights to their machine, access will be limited or potentially blocked depending on the pre-defined policy. Typically in this case, the device would simply be moved into a quarantined VLAN as in option one.

Option One



Option Two



Option One: Unmanaged Device Remains Unknown, Limited Access Granted

During the initial deployment of NAC across the enterprise network, the typical security policy first implemented for visitors is to allow devices to remain unknown/unmanaged, and limit their access and protect the network from their potential behavior. This policy does not require the device to achieve security policy compliance, nor requires CounterACT to regulate its compliance status during the session.

- 1. Recognize unknown device automatically.** CounterACT will automatically recognize that an unknown device is attempting to connect to the network, regardless of the connection method (WAP or wired LAN).
- 2. Move unknown device to separate VLAN.** With the multitude of switch integrations offered by ForeScout, CounterACT is able to isolate the specific device and assign it to a designated VLAN. This VLAN can be quarantined from the rest of the enterprise network, and will provide the appropriate access, as pre-determined by the administrator. In most cases, this will be Internet access only.
- 3. Protect network from self-propagating malware.** Regardless of the device remaining unmanaged, CounterACT will continue to protect the network from any self propagating malware, including “zero-day” attacks that may result from this device. This allows administrators to be assured that not only will their critical data be protected, but network uptime and business continuity will not be at risk due to unknown devices.

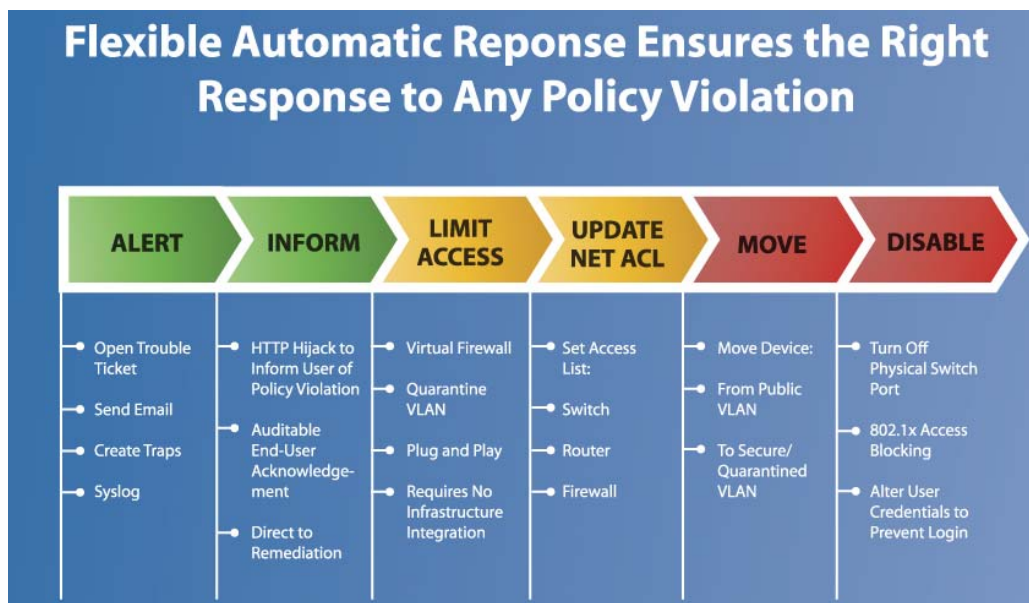
Option Two: Unmanaged Device Obtains Authentication, Appropriate Access Granted

Depending on the policy of the organization, administrators have the option to require unmanaged devices to obtain authentication in order to gain access to the Internet or other critical resources. Once the appropriate policies and enforcements are in place, CounterACT will automatically handle all visitors with minimal disruptions, based upon the pre-defined rules, and quickly move the device through several process steps in order to secure the network during the entire connection of the unknown device.

- 1. Request permission for registry scan.** Upon connection attempt, CounterACT will open an automated dialogue window asking the visitor to grant permission to perform a deep interrogation, or host property scan, of their endpoint. Unlike other NAC solutions, there is no form of agent or client, including Active X, being downloaded to the endpoint. The end user grants this access by simply re-logging into their device.
- 2. Conduct deep interrogation of unknown endpoint.** Upon acknowledgement, CounterACT can conduct a deep interrogation, or host property scan, of the endpoint to determine its status and compliance with corporate security policies. During this time, CounterACT will gather a significant amount of data from the connected device. This information is stored in the built in Network Information Portal™, which provides a search-based database for providing audit trails and forensic reporting in case of malicious activity. If a malicious threat is detected on the visitor device post connection,

CounterACT will block the infection and provide a complete security snapshot of what devices were affected and the remediation that was accomplished by the CounterACT response.

3. Enforce and remediate policy violations. Upon completion of the interrogation, CounterACT will either grant access to the compliant device, or it will follow the appropriate pathway to enforcement, in order to ensure the highest level of network security. CounterACT is one of the few NAC solutions that offers a range of enforcement options that provide for maximum productivity and minimal disruptions. If a network access policy is limited to on or off responses, only very critical violations can be enforced without severely impacting user productivity. The chart below highlights the breadth of enforcement responses available through CounterACT. This extends beyond the functionality of handling network visitors to provide a comprehensive access control solution.



- **Alerts:** CounterACT will alert appropriate network administrators to specific policy violations of unknown devices. This is accomplished through SNMP traps, Syslog export, API level integration with trouble ticketing systems to automatically open a trouble ticket, email, and pager notification.
- **Engage/Inform:** CounterACT will engage the visitor who is in violation of security policy. The appliance will hijack the HTTP session and present the user with a dialogue box explaining which corporate policy has been violated. The visitor can choose to self remediate, or may be instructed to contact a network administrator before being allowed on the network.

- **Limit Network Access:** A key feature of CounterACT is the ability to provide a plug and play virtual firewall which protects critical network resources from unauthorized access, and provides protection of vulnerable systems from threats, including unknown devices.
- **Update Network ACL:** ForeScout has developed a full catalogue of network API level device plug-ins which allows the appliance to communicate with network elements like switches, routers, and firewalls. This response is then used to deny access to a visitor device that is not compliant with network policy, effectively blocking the device from connecting at the infrastructure level.
- **Move:** Similar to the functions described in limiting network access, CounterACT provides a level of flexibility in enforcing network policy. The range of response allows network administrators to control which devices have access to specific areas within the network. Part of this functionality is having the ability to move connecting and connected devices between public, restricted and quarantined VLANs.
- **Disable:** The most definitive enforcement is to deny network access to a device which does not comply with the network security policies. CounterACT can do this through its own blocking mechanisms or work with network elements to close connection. In the case of switch integration, this could be accomplished through turning off the port that the device is attempting to connect to. The “virtual firewall” feature is built in to every CounterACT appliance.

4. Continuous Monitoring of Visitor Device. Upon successful connection to the network, CounterACT will automatically recheck the endpoint after the initial interrogation phase. The default setting for rechecking attached devices is every 10 minutes, but can be customized based upon the administrator/network requirements. During every interrogation, CounterACT ensures that the device maintains compliance with security policies. In addition, CounterACT will also continue to employ its real-time threat prevention technology to ensure that the network remains safe from any self propagating malware, including “zero-day” attacks, that may propagate from this or any other devices on the network.

Conclusion

As enterprise networks continue to evolve with the rapidly increasing number of onsite visitors, the demand for easy to deploy, cost effective, and flexible access control security systems will only grow. ForeScout delivers a network access control solution that provides for maximum security of vital resources through its policy enforcement and built-in threat prevention engine, while ensuring maximum productivity for valuable onsite contractors, auditors, and other visitors. By implementing CounterACT and the appropriate level of security polices, enterprises can automatically secure their networks with little concern over the access of visitors and their unknown devices.