



# CounterACT for FISMA

Federal Information Systems Management Act Compliance

Full FISMA compliance takes a combination of trained staff, strong policies, and industry leading technology. There is no “silver bullet” which will cover all criteria, but there are solutions that can significantly contribute to achieving this challenging goal. ForeScout offers a security platform that can help translate organizational policies that apply to securing the information infrastructure and allow for their enforcement without the need for significant management overhead.

## CounterACT Security Platform

Clientless, Transparent Network Access Control (NAC)

Inspect-to-Connect End Point Policy Enforcement

Active Assessment and Protection of Identified Vulnerabilities

Accurate, Automated Protection Against “Zero-day” Threats

Regulatory Compliance for Data Security

ForeScout’s CounterACT appliance delivers the ability for federal agencies and other entities affected by FISMA to achieve compliance as it pertains to monitoring, recording, controlling, and reporting/auditing network access by any device.

Without the requirement for an in-line deployment, the CounterACT appliance seamlessly deploys within an existing network infrastructure. This provides for a scalable, cost effective solution without the need to re-architect the network or upgrade the switching fabric. Additionally, by spanning from the switch, CounterACT can enforce network access control policies from any level of switch/network hierarchy, including access layer, distribution layer, or from the core switch.

### How ForeScout Can Help

Although FISMA requirements are broad, the National Institute for Standards and Technology (NIST) has provided additional clarification as it pertains to information security. NIST Special Publication 800-53 outlines specific requirements for information security. These requirements include:

#### Access Control (AC)

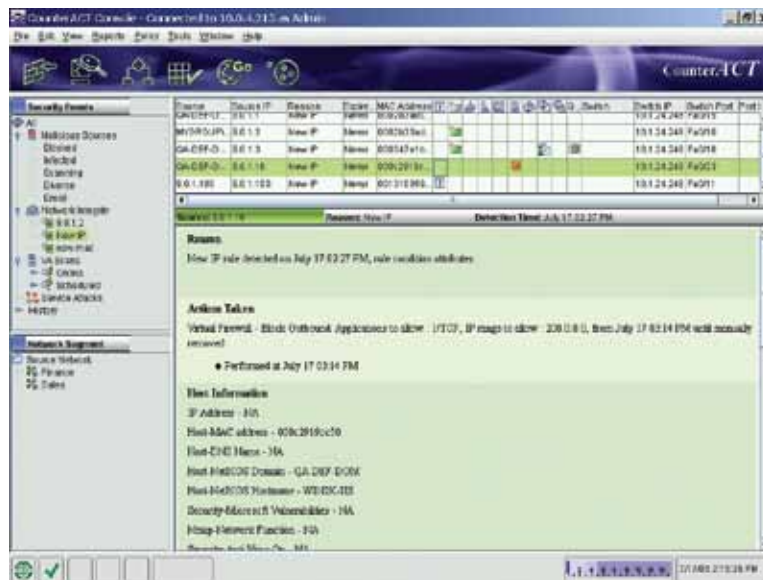
Organizations must limit the access to information systems to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

#### Awareness and Training (AT)

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

#### Audit and Accountability (AU)

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.



ForeScout’s security platform provides complete monitoring, recording, controlling, and reporting/auditing of network access by any device.

# ForeScout Provides FISMA Required Network Security

## Network Policy Enforcement

Create and enforce granular network security policies. Translate access control policies into real-time enforcement. CounterACT allows for the creation of sophisticated policies that can be as specific as a single MAC address to enforcing organization-wide policies (e.g. antivirus is on and up to date). Once policy is created, CounterACT provides a full range of enforcement responses allowing for an appropriate action (warn, limit access, quarantine, block, etc) which corresponds with the severity of the policy violation.

## Clientless Network Access Control

Complete network access control over managed and unmanaged devices without the need to deploy an agent or any form of code on the devices. CounterACT delivers the ability to interrogate devices attempting to connect to the network and determines if they are in line with the pre-defined access policies. This is done transparently without the knowledge of

the end user. If the device is in full compliance with the access policy, it will be granted access to the appropriate network resources. If the device is unknown or not in compliance with policy, CounterACT provides network administrators the measured enforcement capability to ensure network security.

## Transparent Authentication

Allow for the authentication of devices to the network without adding additional steps to users, or the requirement of retraining personnel. CounterACT works with the existing infrastructure and can leverage established directory roles to provide role-based access. This functionality can be extended to work with guest devices, moving them from the public VLANs to "guest" or "quarantined" VLANs upon connection attempt.

## Full Alerting/Reporting System

Alerting can be customized to meet organizational requirements. This ranges from real-time

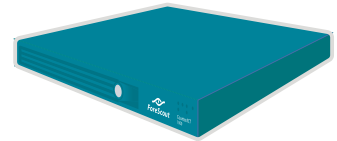
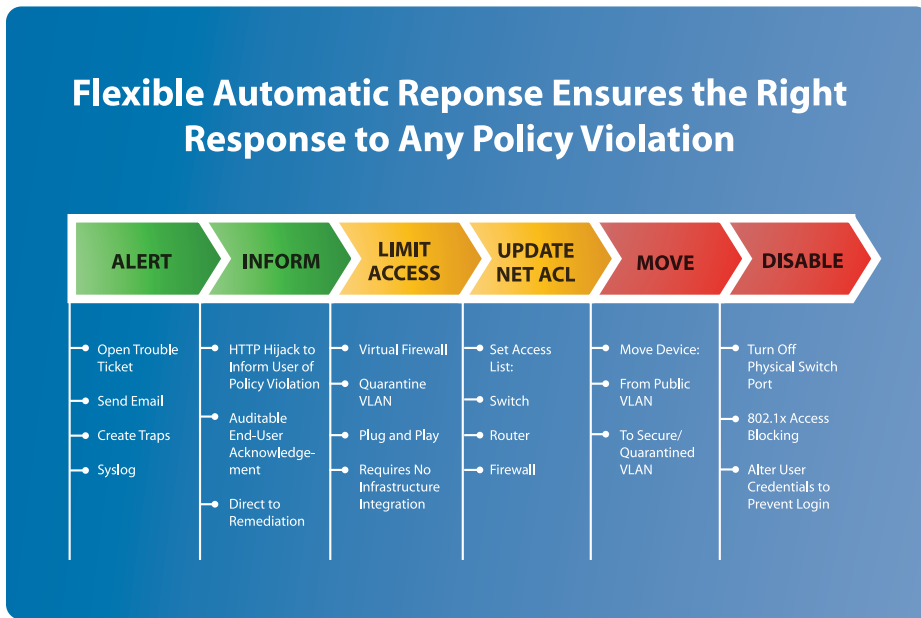
security event notification to scheduled reports of all security event activity sent via email. All information collected and stored by the CounterACT appliance is available for review and both executive and operational customizable reports can be generated in a variety of formats (e.g. HTTP, PDF, etc).

## Vulnerability Assessment/Mitigation

CounterACT provides the ability to scan the network, in real-time or at scheduled intervals, and detect any potential vulnerabilities in the infrastructure. Once vulnerability is identified, the appliance provides the additional ability to deploy a virtual firewall, effectively blocking the vulnerability from exploit.

## Measured Response/Policy Enforcement

Policies are only as good as the ability to enforce them. CounterACT provides a full scope of enforcement options. This can be seen in the following chart:



CounterACT delivers an enterprise class integrated security platform that provides clientless Network Access Control (NAC), policy enforcement, next generation Intelligent Intrusion Prevention™ and Vulnerability Assessment.



10001 N. De Anza Boulevard, Suite 220 . Cupertino, CA 95014  
Tel: 1.866.377.8771 . Fax: 1.408.213.2283 . www.forescout.com



© 2008 ForeScout Technologies, Inc. Products protected by US Patent #6,363,489, March 2002. All rights reserved. ForeScout Technologies, the ForeScout logo, CounterACT, CounterACT Edge and Active Response are trademarks of ForeScout Technologies, Inc. All other trademarks are the property of their respective owners. CAVSym-1108



AC-3 ACCESS ENFORCEMENT	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	CounterACT provides complete network access control based on pre-defined policy of acceptable security state.
AC-8 SYSTEM USE NOTIFICATION	The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.	This can be configured as a rule and via a hijacked HTTP session (and/or utilizing NetSend) can display this notification to devices as they connect to the network or attempt to access network resources. From the dialogue box the end user could be forced to acknowledge the notification before being allowed to proceed.
AC-10 CONCURRENT SESSION CONTROL	The information system limits the number of concurrent sessions for any user.	Depending on the type of session, CounterACT is able to regulate and limit the number of concurrent sessions.
AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.	Real-time notification can be configured to notify any and all appropriate personnel of access policy violation. Additionally, this information is stored for detailed review or administrative reporting.
AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	The organization identifies specific user actions that can be performed on the information system without identification or authentication.	CounterACT provides the ability to move users into quarantined VLANs, which can be configured to allow user access to specified resources without the need for authentication
AC-17 REMOTE ACCESS	The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.	CounterACT provides a variety of methods to monitor and control remote access. Granular rule sets can be created to limit access by user, location, network segment, etc. All information regarding remote connections is recorded and available for review.
AC-18 WIRELESS ACCESS RESTRICTIONS	Establishes usage restrictions and implementation guidance for wireless technologies; and documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.	CounterACT provides the ability to detect, manage, control wireless connections and the users who connect through wireless access points. Granular policies can be created and enforced.
AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES	Establishes usage restrictions and implementation guidance for portable and mobile devices; and documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.	Any device that has an IP connection to the network can be controlled via the CounterACT appliance. Policies can be created and enforced on any network enabled device.
AC-20 PERSONALLY OWNED INFORMATION SYSTEMS	The organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.	CounterACT detects upon connection attempt if the device is a managed or "known" and/or manageable device. Policies can be created to limit or block any unmanaged devices from connecting to the network.



AU-2 AUDITABLE EVENTS	The information system generates audit records for the following events.	CounterACT records end-to-end security events and provides the ability to audit and alert based upon pre-defined criteria of the severity of the event.
AU-7 AUDIT REDUCTION AND REPORT GENERATION	The information system provides an audit reduction and report generation capability.	CounterACT provides both a snapshot overview for quick reporting and detailed information for further forensic exploration.
AU-8 TIME STAMPS	The information system provides time stamps for use in audit record generation.	All captured information is dated and time stamped.
CA-7 CONTINUOUS MONITORING	The organization monitors the security controls in the information system on an ongoing basis.	CounterACT monitors all connected devices for security compliance both at the point of connection and through continuous monitoring. The CounterACT appliance is secured and hardened so that its information is always secure.
CM-2 BASELINE CONFIGURATION	The organization develops, documents, and maintains a current, baseline configuration of the information system and an inventory of the system's constituent components.	CounterACT is a self learning appliance, which discovers and logs all network elements. This information is stored in a database, which allows the administrator the ability to search and correlate data on any and all devices in the network.
IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION	The information system identifies and authenticates specific devices before establishing a connection.	All devices connecting to the network are detected and identified prior to connection. Once identified, appropriate enforcement of policy is applied to the specific device (role based access, guest access, access restricted due to policy violation, etc)
RA-5 VULNERABILITY SCANNING	Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system or when significant new vulnerabilities affecting the system are identified and reported.	CounterACT provides a built in Vulnerability Assessment scanner to scan and identify known vulnerabilities. Additionally, once vulnerabilities are identified, CounterACT provided the ability to apply a virtual firewall rule to protect vulnerable systems from exploits, until the vulnerability is addressed.
SC-19 VOICE OVER INTERNET PROTOCOL	The organization: (i) establishes usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.	CounterACT provides the ability to detect and enforce policy for VOIP connections. This would be based upon the policy for this type of data connection and where it is located within the infrastructure. This is particularly relevant to soft phones which share the same IP connection as a laptop device. All connections are monitored, documented and controlled through the CounterACT system.
SI-4 INTRUSION DETECTION TOOLS AND TECHNIQUES	The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.	Patented deterministic methodology (ActiveResponse) ensures detection of "zero-day" threats from self propagating malicious code as well as internal espionage and/or sophisticated hackers.