



CounterACT for HIPAA

Health Insurance Portability and Accountability Act Compliance

Designed to protect the confidentiality, integrity, and availability of health information, HIPAA has become integral to today's health care system. However, the integration of HIPAA regulations has presented an overwhelming challenge to the health care industry. Compliance is more than just a one time achievement; it's an ongoing process of implementing, updating, and monitoring systems and networks. With the prevalence of managed and unmanaged mobile computing devices (laptops, network enabled PDA's, etc.) connecting to the network, network access control becomes paramount to ensuring HIPAA compliance. ForeScout delivers a comprehensive solution for enforcing network access control and ensuring the safety of critical information from malicious threat exposure.

CounterACT Security Platform

Clientless, Transparent Network Access Control (NAC)

Active Assessment and Protection of Identified Vulnerabilities

Accurate, Automated Protection Against "Zero-day" Threats

Inspect to Connect End Point Policy Enforcement

Regulatory Compliance for Data Security

How ForeScout Can Help

ForeScout's security platform can help covered entities (CEs), such as health care plans, clearinghouses, and providers, to define and deploy organizational policies for securing electronic protected health information (EPHI). This network security enforcement can be accomplished without the need for significant management overhead. ForeScout's CounterACT appliance delivers the ability to achieve HIPAA compliance as it pertains to controlling access to the network, protecting EPHI, assessing and mitigating vulnerabilities, and creating and enforcing information security policies.

Without the requirements of an inline deployment, CounterACT seamlessly integrates with 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.

ForeScout's CounterACT appliance provides HIPAA-required network security, including:

Network Policy Enforcement

Under HIPAA regulations, CEs must implement policies to prevent, detect, contain, and correct any network security violations. The CounterACT system provides the ability to create and enforce granular network security policies, which can be as specific as

controlling a single MAC address, to enforcing organization-wide policies. This allows CEs to permit access to persons or software programs that have appropriate access rights, in order to ensure the confidentiality and security of EPHI.

Once a policy is created, CounterACT provides a full range of automatic enforcement responses, as shown in Figure 1, allowing for an appropriate action to be taken (warn, limit access, quarantine, block, etc.), which corresponds with the policy violation.

Clientless Network Access Control

CounterACT delivers complete network access control over managed and unmanaged devices without the need to deploy an agent or any form of code on the devices. The appliance interrogates all managed and unmanaged 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 several automated enforcement options to ensure network security is not compromised.

Role Based Access

CounterACT, working directly with the directory structure (e.g. Active Directory), can enforce role based access over any network element. This effectively provides access only to

network resources that are assigned to a specific role (e.g. patient billing information only being available to those users with finance domain credentials).

Full Reporting System

CounterACT provides auditable reports covering all detected network security policy violations and their corresponding remediation. 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. This includes a detailed listing of the security policies that are being enforced and the network nodes that were found non-compliant. Also, alerting can be customized to meet organizational requirements. This ranges from real-time security event notification to the user and administrator, and scheduled reports of all security event activity sent via email.

Vulnerability/Assessment

HIPAA requires that organizations must regularly conduct a thorough and accurate risk analysis of the systems and procedures designed to protect EPHI. CounterACT has the ability to scan the network and its hosts, in real time or at scheduled intervals, and detect any potential vulnerabilities in the infrastructure. Once a vulnerability is identified, based upon pre-defined policies the appliance provides a variety of automated responses (i.e., deploying a virtual firewall) effectively blocking the vulnerability from exploit.

CounterACT for HIPAA

Health Insurance Portability and Accountability Act Compliance

HIPAA Security Rule	CounterACT Response
The identity of a person or entity seeking access to EPHI must be verified. All users should have unique identifiers or login IDs to information systems and electronic PHI.	CounterACT works in conjunction with directory structures (such as Active Directory) or identity management solutions and can enforce access based upon pre assigned user IDs.
Limit access to EPHI only to those persons or software programs that have been granted specific access rights.	CounterACT provides the ability to enforce “role-based” access. This ensures that only the parties who have been granted access rights will be allowed connection to restricted-access resources. This is enforced using CounterACT’s connection blocking and virtual firewall technology.
Organization must reduce risks and vulnerabilities.	Endpoint and user compliance policies can be tested using regularly scheduled scans or automatically upon connection to the network. These scans test for OS vulnerabilities, open services, service-patches, unauthorized applications, and anti-virus status. Non-compliant systems can be audited or blocked from network access automatically. Patented deterministic methodology (ActiveResponse) ensures detection of “zero-day” threats from self propagating malicious code as well as sophisticated external or internal hackers. CounterACT also provides a built in Vulnerability Assessment module, which can scan the networks for any known vulnerabilities. Based upon preferences, the appliance can deploy a virtual firewall, effectively blocking the vulnerability on the identified device.
Organizations must maintain audit trails that log all access to system information.	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. It provides both a snapshot overview for quick reporting and detailed information for further forensic exploration. All information is dated and time stamped. All event information can be sent to third-party event managers via a SYSLOG or SNMP stream or to data storage device through OLEDB or JDBC.
Organizations must identify, respond to and mitigate suspected or known security incidents and document security incidents and their outcomes.	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. ActiveResponse ensures detection of “zero-day” threats from self propagating malicious code as well as sophisticated hackers. The compromised system is immediately quarantined from the network, and all events are stored for audit. CounterACT offers the end user the ability to correct minor policy violations using the web-based self-remediation system. The event as well as the success or failure of the remediation is recorded for later audit. Additionally, CounterACT can work with a trouble ticketing system to automatically open a new ticket based upon the security violation.

