



Enabling Compliance – A Network Approach

Enabling Compliance – A Network Approach

Summary

This paper presents a methodology that uses network security best practices as a foundation for meeting compliance mandates. The fundamental goals of compliance and network security are the same: protect sensitive data from unauthorized access or modification and ensure that the data is available to authorized users when needed. Leveraging well-understood network security concepts and tools allows enterprises to cost effectively satisfy both compliance and security mandates.

Why a Network Approach to Compliance?

Today organizations in all sectors of business and government face an ever-increasing list of compliance mandates. Underlying all of the individual regulations, IT managers are recognizing a recurrent theme. Explicitly or implicitly, a significant part of every mandate is the requirement to build and maintain a network infrastructure with appropriate security controls based on their unique environment.

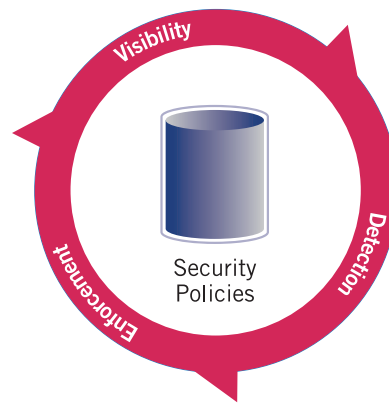
A network approach to enabling compliance focuses first and foremost on the tasks involved with building and maintaining a properly secured network. This focus most efficiently accomplishes the fundamentals of all compliance regulations and delivers substantial incremental benefits for the enterprise. With a network approach to compliance, IT ends up with a well-managed enterprise infrastructure, not just a series of checked boxes for a particular audit. The enterprise understands the means used to protect the confidentiality, integrity and availability of its business critical resources. For IT itself, a network approach to compliance means leveraging tools and resources, increased staff efficiency and cost savings.

Network Security

There are three key elements to address overall network security:

- Visibility
- Enforcement
- Detection and response

Security policies define how the organization will implement these key elements. No network can be shown to be properly secured without a well-defined network security policy.



Visibility

Network visibility is the continuous, fine-grained view of all network traffic. Network visibility is the foundation for network security policy development and policy life-cycle management.

The best approach to developing a security policy involves two steps: 1) determine how the organization's sensitive data is currently being accessed; 2) compare the current access to how the sensitive data should be accessed in a properly secured environment.

Organizations can determine how their sensitive data is currently being accessed by understanding the current traffic patterns in the network. Network visibility enables this detailed view into network traffic. In the security policy design stage, this visibility will show:

- Who is actually accessing sensitive information
- Where they are accessing the information from
- When the access is occurring
- What applications are being used to access the information

-
- A complete list of all applications being used by end users on the networks that contain sensitive information
 - A complete list of applications being used on any servers that store sensitive information.

Once network traffic patterns are well understood, the next step in policy formulation is to compare the observed traffic profile with the proposed security policy. For example, network security and compliance standards such as PCI require limiting network traffic to only the applications and protocols that are essential for business operation. Unneeded applications and protocols not only present unnecessary risks but they consume network capacity and resources. The requirement to limit network traffic to applications and protocols that have a business justification is the network equivalent of the least privilege principal that compliance standards require for end users. The resulting list of applications and protocols can then be prioritized based on business requirements.

Enforcement

Enforcement is the implementation of the security policy. The goal of enforcement is to protect critical resources from unauthorized exposure or modification and to ensure that resources are available when needed. This represents the familiar confidentiality, integrity, availability (CIA) approach to securing sensitive data. In order to ensure confidentiality, integrity and availability, network security and compliance requires the enforcement of the principle of least privilege. This means that users should only have access to the data and resources they need based on their role in the organization. To implement the principle of least privilege, the security policy should define:

- The resources and information a user can access
- Where they can access that information from
- When they can access the information
- What applications they can use to access the information.

Another element of the security policy should be compartmentalization. Compartmentalization means that information and resources should be segregated based on sensitivity and risk tolerance. Networks are traditionally segmented based on trust. The public Internet is often referred to as the red network, the DMZ as the yellow and the private internal network is called the green network. Further segregating the internal network based on the sensitivity of the data stored on or being transmitted over the segment improves security and simplifies design and management.

Compartmentalization is the principal behind the PCI requirement that the Cardholder Data Environment be isolated from the wireless network. For servers, compartmentalization requires that each server only supports applications with a similar level of risk and sensitivity. For example, DHCP and VoIP server applications should not be hosted on the same server. Compartmentalization also requires that the information stored on each server should be as homogeneous as possible. The security policy should prohibit storing HR data, Cardholder data and medical records on the same system. Server virtualization and live migration (automatically moving virtual servers to new physical systems) present unique challenges for data compartmentalization. Some virtual servers may need to be limited to highly secured hardware.

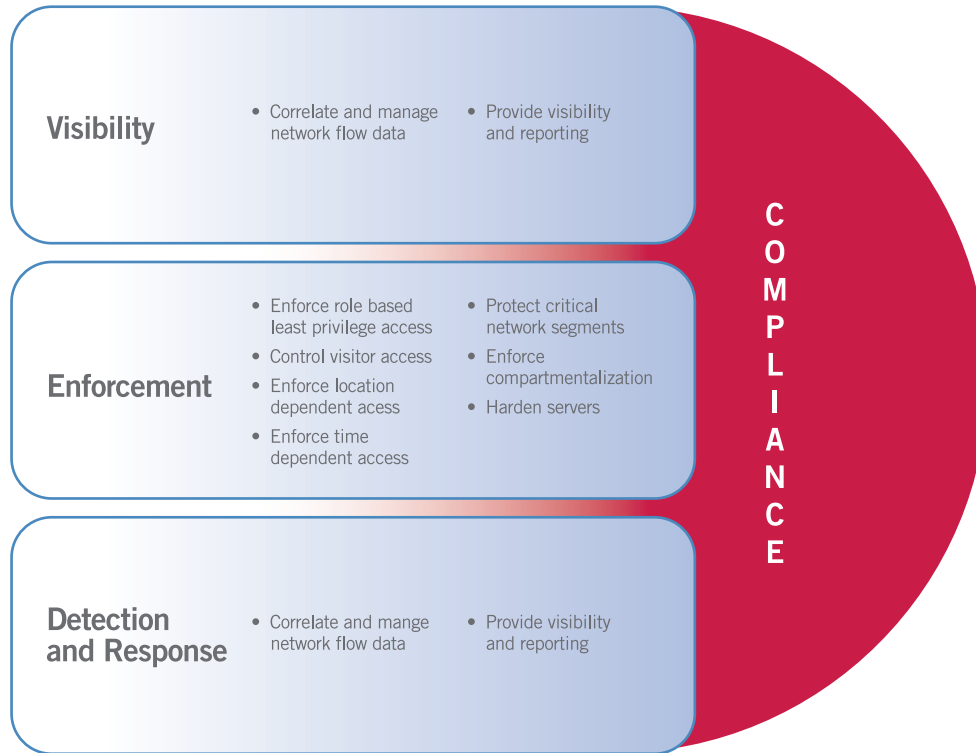
Detection and Response

Detection provides the ability to identify and mitigate threats and non-compliant behavior. Compliance and network security require continuous monitoring of the network to detect threats that could cause data leakage (confidentiality), damage to critical data (Integrity) or denial of access to critical resources (availability). Detection must be able to provide real-time identification of both known and “zero day” threats. Mitigating the threat should include the ability to stop or prevent the attack from succeeding. Threat mitigation should also provide the ability to remove the source of the threat from the network.

Network Security Functions

Network security requires three key elements: visibility, enforcement and detection/response. A network must have a well-defined network security policy that defines how these three elements will be applied to meet business and security requirements. Each of the three key elements is enabled by specific network security functions. For example visibility will result from correlation of network flows, security events and log data. Table 1 shows each key element and the related tasks.

Table 1: Key elements and functions



How does this deliver compliance?

Once these elements and policies are in place, the IT organization has accomplished its responsibility to deliver the infrastructure foundation of compliance regulations.

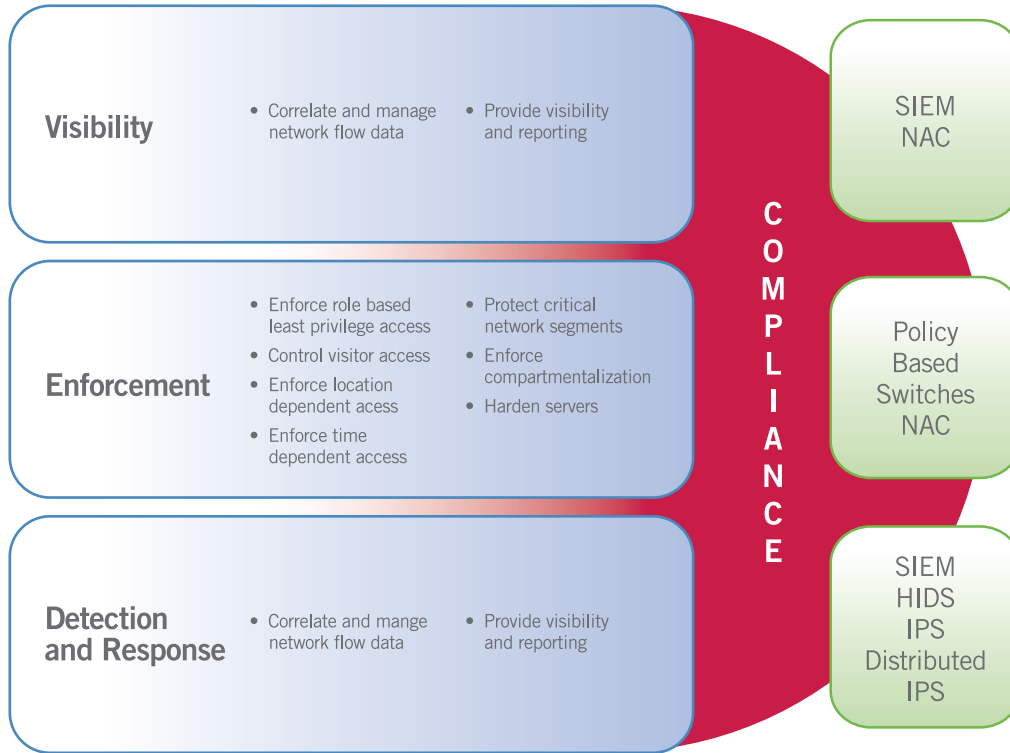
For example the Payment Card Industry Data Security Standard (PCI DSS) is one of the most detailed regulations affecting every retailer or enterprise that accepts consumer credit cards. PCI DSS identifies six guidelines, twelve requirements and numerous explicit steps for securing cardholder data that is stored, process and/or transmitted by merchants or other organizations. Among the six guidelines is the explicit statement, "Build and Maintain a Secure Network." Many of the twelve PCI DSS requirements connect directly to the key elements and functions for network security. The PCI DSS Requirement 7 statement, "Restrict access to cardholder data by business need-to-know" is exactly in the key area of enforcement. The Requirement 10 statement, "Track and monitor all access to network resources and cardholder data" is the requirement for visibility.

Network Security Solutions

Enterasys' complete suite of products delivers the underlying network security that is at the core of compliance. Summarized in Table 2, Enterasys products provide the visibility, enforcement and detection needed to provide network security. Open and standards-based, these solutions are built to work in heterogeneous environments and can provide security services in any network environment.

The following is a description of the Enterasys products and how they can be used to meet compliance requirements. This document is intended as a reference guide. Only a certified compliance auditor can determine if a solution or product satisfies a compliance requirement.

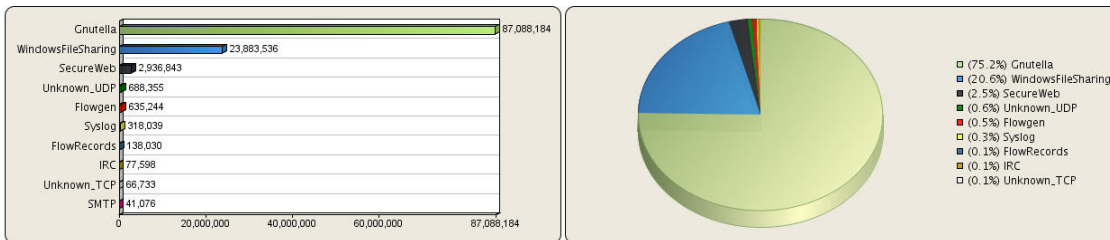
Table 2: Enterasys security solutions



Visibility

1. Enterasys Security Information and Event Manager (SIEM)

The SIEM's Network Behavioral Anomaly Detection (NBAD) sensors can record every flow in the network with application layer detail. NetFlow data from network switches provides additional sources of flow information. Very few switches on the market can send NetFlow records, and most that can only send sampled information. The problem with sampled NetFlow is that it does not give a true picture of what is happening on the network and can cause the SIEM to report false positive results or to miss critical information. Enterasys flow-based switches provide unsampled NetFlow data that maximizes the SIEM's ability to detect "zero day" attacks. This ability reduces the number of dedicated flow sensors that need to be deployed in the network.



The flow data shows the users and applications that are accessing sensitive servers such as those in the Cardholder Data Environment. In the planning stage, this information is essential for developing a security policy that meets compliance requirements. After the security policy is enforced, the SIEM can provide monitoring and reports to validate that the policy is being accurately enforced.

2. Enterasys Network Access Control (NAC)

Web based reports simplify end-system compliance monitoring by providing easy to use dashboards and detailed views of end-systems. Analysts responsible for monitoring end-system compliance can easily tailor the views to present the information they need, in the format they prefer. They can also generate PDF reports of the data.



Enforcement

1. Enterasys policy-enabled switches

These switches provide port level, role based firewalls that can enforce least privilege based on the user's authenticated role. They also provide role and application based quality of service ensuring that essential traffic gets the resources it requires. However, simply providing the enforcement functionality is not enough. Compliance assessments require documenting how the security policy is being enforced. To meet this requirement, the Enterasys Network Management Suite (also known as NetSight) generates reports showing the rules applied to each switch port for each role in the organization. Reports showing how often each rule is being enforced are also generated to provide validation that the rules are functioning as designed. Policies can be applied to both end users and servers.

End Users

Policy-enabled switches provide port level, role based access control and quality of service. For end users this allows the enforcement of least privilege as required by compliance standards such as PCI. Providing controls for visitors and guests that need network access should also be a part of every security policy. A simple way to control visitor and guest users is to set a default policy for anyone who fails authentication. This policy would grant very limited guest access. Guests and visitors might be given only VPN and Internet access with strict rate limits.

Name: Guest

TCI Overwrite Status: Enabled Disabled

Default Actions:

Class of Service: Scavenger [802.1P: 0]

Access Control: Deny Traffic | Contain to VLAN: N/A

Services

Name	Also Used By Roles
Contained Extranet Access [HTTPS]	None
Contained Extranet Access [HTTP]	None
Contained Guest Access	Guest [DHCP], Guest [Printer], Guest [Server], Quarantine
Loop Detect - Gateways	Employee, Guest [DHCP], Guest [Printer], Guest [Server], Prin...
Loop Detection	Employee, Guest [DHCP], Guest [Printer], Guest [Server], Prin...

Add/Remove Services...
Create Service...
View/Edit Service
Show Conflicting Rules...

A simple employee end user policy might state that end systems cannot be servers. For this policy, packets from any server application, Mail Server, DHCP Server, Web Server, etc. would be blocked at the access port. More secure policies, such as those enforcing compartmentalization, restrict access to highly sensitive servers. For example, the PCI compliance standard requires restricting access to the Cardholder Data Environment. Only those users who have a legitimate need should be able to access the servers containing cardholder data. To satisfy this requirement a rule could easily be added to all roles that do not require access that blocks any packet sent to the Cardholder Data Environment.

Servers

For servers, port level access controls and quality of service can be used to harden the server and prioritize essential traffic. For example, to enforce compartmentalization, a server providing email service could have all other applications blocked at the connection port.

Trojans and data leakage are a continuing problem for organizations. Recent data breaches involving Trojan programs installed on credit card systems that send information to unauthorized systems on the Internet have caused major compromises. By hardening these servers at the port level and restricting the IP addresses they can communicate with, these types of breaches can be prevented. A port level policy would be applied that only permits the system to send packets to authorized internal systems all other traffic would be blocked. This policy could be made even more secure by restricting the applications the server can use to send data to the authorized IP addresses. Even if an attacker compromised the system and installed a Trojan, it would be unable to send any information to any Internet address.

2. Enterasys Network Access Control (NAC)

Using the Enterasys NAC solution, IT administrators can also enforce the principal of least privilege, ensuring only the right users have access to the right information from the right place at the right time. When a new device attaches to the network or when a user attempts to authenticate to the network, NAC is involved in enforcing the organization's security policy. If a user authenticates successfully, NAC may modify the user's privileges based on a number of factors including:

- **What type of device is connecting to the network:** End user connections should be treated differently than VoIP devices. IP phones do not authenticate but they should be scanned for vulnerabilities and assigned a role that prioritizes their traffic and, at the same time, applies rate limits. VoIP protocols require priority handling but need very little bandwidth. Rate limits prevent the prioritized traffic from being used for a denial of service attack.
- **The user's authenticated role in the organization:** Compliance requires that users have access to only those resources they require based on their role. For example, someone in a finance role needs access to the finance server but should not be able to send packets to the engineering server.
- **Where the user is trying to access the information from:** Location dependence is important for both security and compliance. PCI compliance requires that the wireless network be kept separate from the cardholder data environment. Anyone connecting from the wireless network must be given a role that blocks access to the cardholder data environment. Users accessing information from physically secure locations are given roles that grant more access than users logging in from public areas such as cafeterias or meeting rooms.
- **When the user is authenticating:** Time dependence enforces security policies that limit the user's access to critical information to specific times such as normal business hours
- **The security state of the connecting system:** If the device connecting to the network does not meet the requirements of the security policy, it should be quarantined or redirected for assisted remediation. The security state of the device is determined by a network based vulnerability scan, an agent based assessment or both.

By combining these factors, Enterasys NAC can enforce complex security policies. For example, to permit a user to access sensitive information only from specific secure locations during normal business hours.

Create Rule

Set the Rule criteria to use in your NAC Configuration. Invert changes the matching logic for criteria to mean NOT the selected value.

Name:

Authentication Method: Invert

User Group: Invert

End-System Group: Invert

Location Selector: Invert

Time Selector: Invert

NAC Profile: Invert

Rule Enabled

Visitors (guests and contractors) who need network access present a unique set of security and compliance challenges:

- **Accountability:** Someone in the organization must be responsible for the behavior of the visitor. This is similar to having an employee sign-in a visitor at the security desk. Enterasys NAC Sponsored Registration lets an authorized employee (sponsor) grant limited network access to a visitor.
- **Tracking:** Enterasys NAC binds the identity of the visitor and sponsor to the visitor's network activity.
- **Control:** The sponsor can assign the visitor to a role that enforces the principal of least privilege. For high security environments, this role would limit the visitor to basic Internet access.

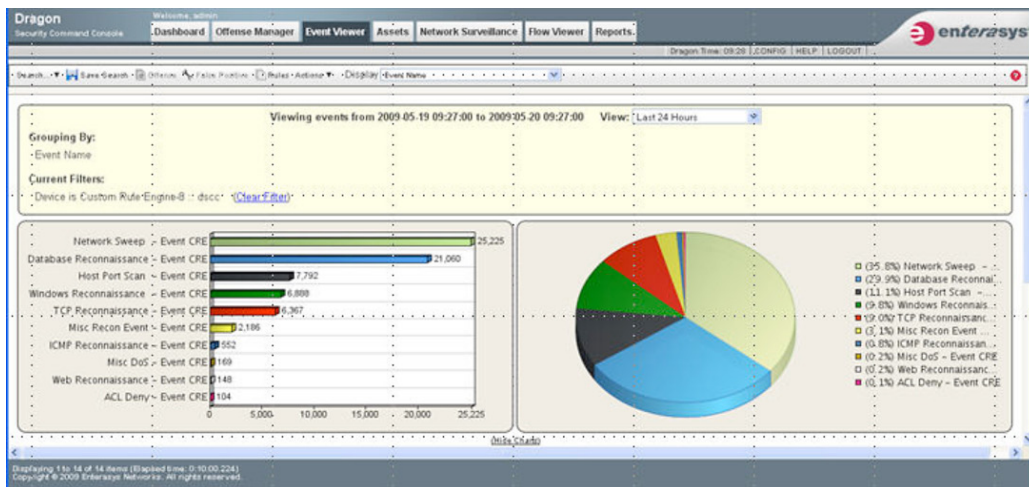
Detection and Response

1. Enterasys Security Information and Event Manager (SIEM)

The problem with networks is not that they produce too little security related information; the problem is that they produce so much information that it overwhelms the people responsible for managing the network. The SIEM collects events and logs from a diverse set of sources including network infrastructure, security devices, servers, operating systems and applications. It normalizes all the events to enable automatic correlation with other events and network flows.

Network flows give a very detailed view of the entire network. The SIEM uses flow sources in the routing and switching infrastructure or distributed flow collectors to gather a detailed history of all network flow activity. It is important that the flow sources provide unsampled data to prevent false positives or missed information. Most vendor's switches and routers can only provide sampled NetFlow which will necessitate turning off some rules in the SIEM to avoid false positives. This will obviously degrade the SIEM's ability to detect some attacks. Enterasys flow-based switches provide unsampled NetFlow data and require no modification of the SIEM's flow analysis rules. The network flows are analyzed to build behavioral models that capture network behavior and generate alerts when anomalous behavior is detected. For example, an anomalous file transfer from a windows server that is not associated with normal in-policy backups occurs. The SIEM detects the event and alerts an administrator of this change in behavior because it could potentially be data theft. Immediately the SIEM begins analysis of the log files and events from the Windows server to determine the user performing the transfer and the exact files that are being accessed. All of this evidence is then accumulated, organized, and made visible within a single Offense (correlated security alert).

By collecting and analyzing security events, logs, network context, vulnerabilities, flow data and identity information, the SIEM is able to detect any type of threat or policy violation including Day Zero attacks. The result is a list of actionable, highly prioritized Offenses that satisfy the basic requirements for both network security and compliance.



Encrypted tunnels protect the security for all configuration commands as well as monitored and analyzed data transmission. Compliance standards require that the integrity of log files must be maintained. To guarantee that log files have not been tampered with the Enterasys SIEM implements extensive log file integrity checks, including NIST Log Management Standard SHA-x (1-256) hashing algorithms. The SIEM also provides an additional layer of encryption options for customers requiring additional levels of file integrity including organizations that need to comply with FIPS 140-2 encryption requirements.

2. Enterasys IPS

The ability to detect and respond to threats is an integral part of both network security and compliance. Enterasys IPS can provide security services for any network and can be deployed in three deployment modes. These deployments can be used to provide additional security behind the Internet facing firewall but their primary focus is securing the wireless and access edges of the network.

Inline IPS – Detection and Mitigation

The Enterasys Inline IPS uses deep packet inspection and protocol analysis to block attacks at the point of detection. It uses an extensive signature library, protocol decoders and protocol anomaly detection to identify and stop attacks. Typically deployed in front of critical resources such as data centers, the cardholder data environment (PCI) or the Electronic Security Perimeter (NERC-CIP), the Enterasys IPS backs up the Internet firewall to provide a second tier of protection from Internet based threats. More importantly, it provides the primary line of defense for threats originating from the access and wireless edges of the network.

Out of Band IPS - Detection

Deployed out of band the IPS can identify threats in large areas of the network. This is the classic IDS deployment where network traffic is mirrored to the sensors for analysis. As with the Inline deployment, packets are tested against a signature library of known vulnerabilities. Protocol decoders and protocol anomaly detection complement the signatures and provide identification of attacks that are not easily detected by the signatures. Out of Band deployments are useful in environments where adding an inline device is not permitted for business or availability reasons. Because Out of Band can cover large areas of the network with a single sensor it provides a cost effective solution for many environments.

Distributed IPS – Detection and Mitigation

Distributed IPS is a patented Enterasys technology that adds an additional enforcement point to either Inline or Out of Band deployments. The biggest weakness in any IPS is its failure to remove the threat or attacker from the access or wireless edge. A traditional inline IPS stops the attack at the point of detection but leaves the source of the attack connected to the network and able to repeat the attack or try another attack. By adding Enterasys Automated Security Manager (ASM) to the deployment, additional enforcement points are added. These additional enforcement points are the ports where an attacker would connect to the network. When either the Inline or Out of Band IPS detects an attack, the source address is sent to ASM where the attacker's network connection is identified. Once the source port is identified, actions can be taken to quarantine the attacker and prevent further attacks.

The highest level of security is achieved by adding Distributed IPS to an Inline deployment. In this configuration, the Inline IPS stops the attack by dropping the attack packets at the point of detection and the Distributed IPS component removes the source the attack from the network at the point of connection. The most cost effective option is to add Distributed IPS to an Out of Band deployment. The Out of Band sensor can monitor large segments of the network eliminating the need for Inline appliances on multiple uplinks. When an attack is detected, the Distributed IPS component will stop the attack by removing the source of the attack from the network. In practice, the best solution is often a combination of Distributed IPS with Inline IPS, for critical sections of the network such as the cardholder data environment, and Distributed IPS with Out of Band IPS for sections of the network with less stringent security requirements.

3. Enterasys Host Sensors (HIDS)

Finally, monitoring the servers containing sensitive information is a requirement for effective network security and compliance. PCI requirements dictate that the integrity of critical system files must be monitored. Enterasys HIDS is a security application used to detect attacks on network servers in real-time. Host intrusion defense is particularly valuable in environments where AES, SSL, IPSec, or other encryption schemes are deployed because the sensor analyzes the data after decryption. Host Sensors deploy advanced techniques to identify rootkits and buffer overflows via a kernel monitoring module. This module traps and analyzes all calls to the kernel to detect the existence of kernel-level rootkits. Host sensors can also detect changes in critical system files as well as changes in file ownership, file modification and truncation of log files.

Key detection features include:

- Monitoring of file attributes such as permission, owner, group, Inode value, size increase, truncated and modification date
- File integrity checking to determine if the content of critical files has been changed
- Analysis of log files using signature policies to detect attacks or compromises
- Monitoring of Windows event logs for misuse or attack
- Analysis of Windows registry for attributes that should not be accessed and/or modified
- TCP/UDP service detection for protection against backdoor services
- Kernel monitoring to detect suspicious privilege escalations and other signs of kernel-level compromises such as rootkits.

Conclusion

Whether or not it is explicitly stated, all enterprise IT projects have an end goal. Unfortunately, the end goal of many compliance projects is just to pass the audit. With this goal the IT project is really being designed only to meet a set of compliance check boxes. There are serious dangers and costs associated with this check box approach. The enterprise may implement multiple point products, succeed in addressing the regulation, and even pass the audit. But, the check box approach may fail to provide adequate network security. Separate point products will not be well integrated and may not provide the comprehensive and integrated security required in today's environment. This approach also creates a much more complex system to manage since the IT staff must become proficient in the management, data analysis and maintenance of each product.

The most effective compliance strategy is to focus on the key elements required for properly securing the enterprise network. By focusing on visibility, enforcement and detection / response, rather than designing around a set of compliance check boxes, the enterprise can maximize its investment in network security with a comprehensive and cohesive security solution that meets its compliance, security and business requirements.

ⁱ PCI Security Standards Council LLC, "Navigating PCI DSS: Understanding the Intent of the Requirements, v1.2", October, 2008, p 4.

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2010 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

