



Massachusetts Standards for Protection of Resident Personal Information — Massachusetts 201 CMR 17

Meeting and validating key security management requirements with Enterasys Networks solutions

Massachusetts Standards for Protection of Resident Personal Information — Massachusetts 201 CMR 17

Introduction

New security requirements have been enacted for any business, regardless of physical or operational location, that handles the personal information of any resident of the Commonwealth of Massachusetts. Personal information includes social security numbers, driver’s license numbers, and financial records. The regulation, [201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth](#)ⁱ, establishes the minimum standards for safeguarding Massachusetts residents’ personal information. The security requirements mirror the control standards already defined by frameworks like CobiT, NIST and ISO. The standards are also similar to other industry or federal regulations, such as HIPAA and PCI, which safeguard personal information. Organizations under the Massachusetts standard have a regulated duty to implement sufficient security controls to ensure that protected records are confidential and safe from inappropriate use. Non-compliance may result in fines of up to \$5,000 per violationⁱⁱ.

The strongest foundation for meeting compliance is applying network security best practices. The fundamental goal of compliance and network security is to protect sensitive data from unauthorized access or modification and ensure that the data is available to authorized users when needed. Applying well-understood network security concepts and tools enables enterprises to cost effectively satisfy both compliance and security mandates. There are three key elements to address for overall network security: network visibility, policy enforcement, and intrusion or anomaly detection and response – all based on the organization’s security policies.



Enterasys Advanced Security Solutions - Overview

Enterasys, the network infrastructure and security division of Siemens Enterprise Communications GmbH & Co KG, is a leading global provider of Ethernet switching and routing solutions as well as advanced network security solutions. The complete suite of Enterasys products delivers the underlying network security framework that is the key to meeting compliance mandates. (See also [Enabling Compliance – A Network Approach](#).) With more than 25 years of experience providing networking and security products, the company’s innovative technology and solutions reduce complexity through leading wired/wireless integration, protect investments with long technology life cycles and provide built-in security. Table 1 summarizes the key network security elements, the required functions and the solutions delivered by Enterasys.

Network Security Element	Functions	Solutions
Visibility	<ul style="list-style-type: none"> Correlate and manage network flow data Provide visibility and reporting 	Security Information and Event Manager (SIEM) Network Access Control (NAC)
Enforcement	<ul style="list-style-type: none"> Enforce role-based least privilege access Control visitor access Enforce location dependent access Enforce time dependent access Protect critical network segments Enforce information compartmentalization Harden servers 	Policy-based Switching Infrastructure NAC
Detection and Response	<ul style="list-style-type: none"> Detect known attacks Respond to attacks Detect server compromise Correlate flow data, event data and log data Detect Zero Day attacks 	SIEM Host Intrusion Detection (HIDS) Distributed Intrusion Prevention (IPS)

Table 1: Network security, functions and solutions

This white paper focuses on the key element of visibility and the Enterasys SIEM solution as a critical tool to address the Massachusetts regulation.

Enterasys SIEM integrates previously disparate functions – including log management, security information and event management and network activity monitoring – into a total security intelligence solution. Enterasys SIEM provides users with crucial visibility into what is occurring with their networks, data centers, and applications to better protect IT assets and meet regulatory requirements.

Enterasys SIEM Out-Of-The-Box Compliance Management

Enterasys SIEM provides out-of-the-box compliance content to enforce:

- Accountability: Proving who did what and when
- Transparency: Providing visibility into the security controls, the business applications, and the assets that are being protected
- Measurability: Metrics and reporting around risk within a company

A monitoring and management solution that spans the network and security technologies in the enterprise environment is key to supporting and validating compliance initiatives. Enterasys SIEM brings to enterprises, institutions, and government agencies the accountability, transparency, and measurability that are critical to the success of any IT security program responsible for meeting regulatory mandates.

Specific benefits of an Enterasys SIEM compliance management solution include:

- Out-of-the-box compliance reports to assist meeting specific regulations, including PCI, HIPAA, and the Massachusetts standard
- An easy-to-use reporting engine that does not require advanced database and report writing skills, resulting in an improved ability of staff to produce required compliance reports
- Delivery of compliance workflow and security controls, resulting in decreased financial risk to the organization for non-compliance
- Remediation through Enterasys patented Distributed IPS that reduces the time to respond to threats and compliance violations

Conclusion

Organizations required to meet the “Massachusetts Standard for the Protection of Personal Information” will gain efficient compliance enablement with Enterasys SIEM’s ability to deliver complete visibility of the network traffic and security events (who did what, when and where). The audit process is eased by SIEM’s centralized point for tracking and monitoring threats and compliance violations. SIEM’s capabilities address a wide spectrum of essential technical, administrative and physical information security safeguards that are fundamental to meeting the new Massachusetts standard. For details, see the summary provided in Appendix A.

For additional security protection, Enterasys provides a completely integrated suite of advanced security applications:

- Enterasys IPS -- advanced prevention, detection and response capabilities for network, host-based and wireless deployment
- Wireless Intrusion Prevention (WIPS) – continuous scanning, threat detection, classification and prevention for rogue APs, ad-hoc mis-association and next generation threats
- Enterasys Network Access Control (NAC) -- a flexible inline or out-of-band solution for pre-connect and post-connect network access control
- Enterasys Network Management Suite (NMS) -- centralized visibility and control for large multi-vendor networks to streamline administrative tasks.

Enterasys SIEM, in combination with these other security applications, provides comprehensive threat detection and dynamic threat removal for LAN, WAN, wireless networks, host and server systems. Deployment of Enterasys solutions results in the capability to secure any network from any vendor.

Appendix A

Requirements of the Massachusetts “Standards for the Protection of Personal Information of Residents of the Commonwealth” supported by Enterasys SIEM and other advanced security solutionsⁱⁱⁱ.

17.03: Computer System Security Requirements Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, shall have the following elements:	
Specified Rule	Enterasys SIEM Capability
3.1 Designating one or more employees to maintain the comprehensive information security program	Enterasys SIEM provides a centralized security management dashboard to support specific logging, auditing, and reporting functions required by the employees designated to maintain the information security program.
3.2 Identifying and assessing reasonably foreseeable internal risks to the security, confidentiality, and/or integrity of [...] electronic [...] records	Enterasys SIEM delivers automated assessment and prioritization of risks to the underlying networked infrastructure that stores protected resident confidential information. Enterasys IPS can detect and block network based attacks. Enterasys NAC can assess the vulnerability state of end systems connecting to the network
3.5 Preventing terminated employees from accessing records	Enterasys SIEM's advanced correlation engine supports out-of-the-box rules for the detection of terminated employees accessing systems that store protected resident information. Enterasys policy based switches provide identity and role based least privilege control at the access ports of the network. Enterasys NAC provides access control based on user identity, role, time, and access location. Identity and role information can be leveraged from existing identify management databases.
3.8 Identifying [...] computing systems [...] that store personal information	Enterasys SIEM provides automated discovery of networked systems (assets) supporting efforts to classify systems that store protected resident information.
3.10 Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to personal information	Enterasys SIEM continuously monitors networked systems and detects specific threats that might compromise personal information.
3.11 Reviewing the scope of the security measures at least annually	Enterasys SIEM provides long-term retention and analysis of collected network and security information to support periodic or annual reviews of the security process.
3.12 Document responsive actions taken in connection with any incident involving a breach	Enterasys SIEM provides extensive workflow for documenting security incidents and responsive actions taken.

17.03: Computer System Security Requirements Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, shall have the following elements:	
Specified Rule	Enterasys SIEM Capability
(1) Secure user authentication protocols including:	
(a) control of user IDs and other identifiers;	Although Enterasys SIEM does not specifically control user IDs, it does provide extensive monitoring of access to systems by user ID which can help enforce specific user-based access policies.
(b) a secure method of assigning and selecting passwords;	Enterasys policy based switches provide identity and role based least privilege control at the access ports of the network. Enterasys NAC provides access control based on user identity, role, time and access location
(c) control of data security passwords to ensure that such passwords are kept at a location separate from that of the data to which such passwords permit access;	Not directly applicable to Enterasys SIEM, however Enterasys SIEM does collect and process events from systems that manage user access and identity.
(d) restricting access to active users and active user accounts only;	Not directly applicable to Enterasys SIEM, however Enterasys SIEM does collect and process events from systems that manage user access and identity
(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;	Enterasys SIEM provides an important alerting function as a result of log and event correlation. Enterasys SIEM has out of the box rules that can detect attempts to access expired accounts. Enterasys SIEM has out of the box reports for authentication and access control activity. Enterasys policy based switches provide identity and role based least privilege control at the access ports of the network. Enterasys NAC provides access control based on user identity, role, time, and access location. Identity and role information can be leverage from existing Identify management databases.

(2) Secure access control measures that:	
(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and	Enterasys SIEM provides an important alerting function as a result of log and event correlation. The solution provides detailed auditing of user access to systems that store protected information. Enterasys policy based switches provide identity and role based least privilege control at the access ports of the network. Enterasys NAC provides access control based on user identity, role, time, and access location. Identity and role information can be leveraged from existing identity management databases.
(b) assign a unique identification plus a password, which is not vendor supplied, to each person with computer access;	Not directly applicable to Enterasys SIEM, however Enterasys SIEM does collect and process events from systems that manage user access and identity. The solution does provide a level of passive inspection of network traffic to flag applications that transmit usernames and passwords unencrypted.
(3) Encryption of all transmitted records and files containing personal information, including those in wireless environments, that will travel across public networks.	Enterasys SIEM's layer 7 network activity monitoring capability detects the transmission of personal information in non-encrypted format.
(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information.	Enterasys SIEM provides constant monitoring of networks and systems. Through broad surveillance and event/log aggregation Enterasys SIEM provides a comprehensive audit trail of user activity (not just IP address activity) in a network. Enterasys SIEM provides flexible logging, searching, alerting and reporting across all data types and system types within an organization.
(5) Encryption of all personal information stored on laptops or other portable devices.	Enterasys SIEM provides centralized collection and analysis of events from end point security products that facilitate encryption on portable devices.
(6) For files containing personal information on a system that is connected to the Internet, there must be firewall protection with up-to-date patches, including operating system security patches. A firewall must, at a minimum, protect devices containing personal information from access by or connections from unauthorized users.	Enterasys SIEM plays an important role monitoring events from multiple firewalls, as well as monitoring and alerting on the vulnerability level of system assets and hosts. Enterasys IPS provides deep packet inspection placed behind the firewall in provides a second layer of defense
(7) Reasonably up-to-date versions of system security software	Not directly applicable to Enterasys SIEM as a policy enforcement mechanism, however the solution does manage events from a wide spectrum of system security software, including anti-virus.
(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.	Not directly applicable to Enterasys SIEM as a policy enforcement mechanism, however the product does provide a centralized knowledge base for staff tasked with managing the information security program.

ⁱ 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth regulation that implements the provisions of M.G.L.c.93H.

ⁱⁱ M.G.L.c.93H:Section 6. Enforcement chapter references section 4 of chapter 93A, <http://www.mass.gov/legis/laws/mgl/93a-4.htm>

ⁱⁱⁱ 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth, <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>

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.

