

A Proven Data Security Methodology for Modern Regulatory Compliance

Key Benefits

**Reduce cost & complexity
of compliance**

**Meet regulatory
requirements across
multiple mandates**

**Easily prove compliance
to auditors**

Today's enterprises face an overwhelming and constantly growing array of compliance mandates that regulate the management and protection of sensitive data against disclosure, theft, and misuse. Mandates such as PCI DSS, Sarbanes Oxley, HIPAA, state privacy laws and European Privacy Legislation introduce civil and criminal penalties for data leaks, creating pressure to disclose leaks and protect the brand image of the enterprise from negative public scrutiny. For example, PCI DSS, the Payment Card Industry's security mandate, requires merchants, banks and other organizations handling credit card data to encrypt cardholder data transmitted over networks.

Today's remote sites and datacenters usually store all of an organization's business critical information as well as sensitive information about employees and customers that are subject to government and industry regulation. Every compliance initiative must therefore address the issue of protecting sensitive data streaming over the WAN against interception or modification to maintain compliance with regulatory mandates. Experts agree that encryption is the most robust method for protecting sensitive data in transit. Even if encrypted data is intercepted, it is essentially useless to the attacker.

By encrypting sensitive data at the network link layer (layer 2), companies ensure robust compliance with mandates because all data traversing the network is encrypted without exception, thereby dramatically reducing proof requirements and cost of compliance efforts. This adds another robust layer of protection to complement data at rest security solutions such as SafeNet DataSecure which encrypts sensitive data in databases and files.

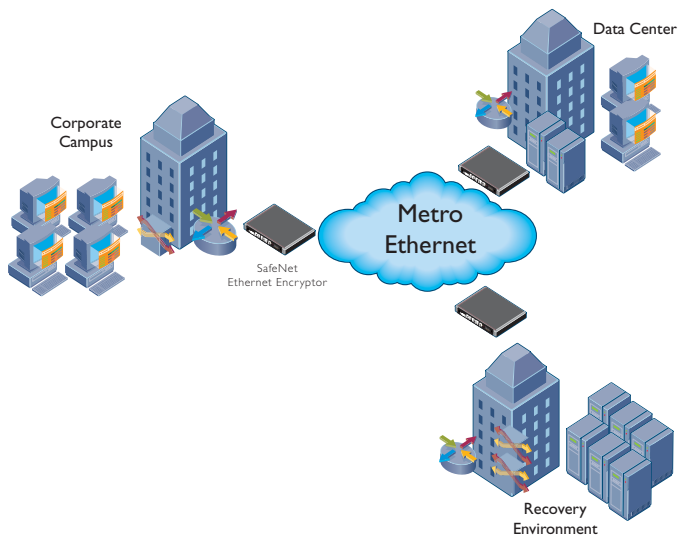
Data Explosion and Compliance Drive Need for WAN Encryption

Financial institutions, government agencies, and telecommunications companies transmit large volumes of sensitive data over high-speed Ethernet WANs that connect offices and data centers with disaster recovery sites. The consolidation of datacenters and rise of bandwidth intensive applications such as voice, video, virtualization, and cloud computing, and the consolidation of datacenters are causing exploding data volumes transmitted over ultra high-speed wide area networks. Because of its high overhead and other technical limitations, traditional router-based encryption often does not scale cost-efficiently to the levels of throughput required to protect data sent over such high-bandwidth networks.

Eliminate Cost & Complexity of Compliance

SafeNet network encryption solutions provide easy to deploy compliance solution for data transmitted to disaster recovery sites and offsite data storage facilities while preserving full network performance, latency requirements, and service level agreements.

In the current economic environment, companies are looking to cut cost and complexity of compliance. Instead of purchasing costly bandwidth upgrades with high monthly recurring charges, companies deploy the Gigabit Ethernet encryptor in place of their legacy IPSec encryption and effectively double their available bandwidth in addition to the 10-fold latency improvement.



Centralized Policy Management

Through central policy management, SafeNet further eliminates cost. SafeNet's Network Security Management Center allows network administrators to centrally configure, monitor and manage network encryption policy from a single web-based console. It helps companies define granular security policies that can be distributed across multiple devices, thereby not only lowering policy management cost but also easily generating data security audit trails to meet compliance auditing requirements.

Ease of Integration

SafeNet's purpose-built appliances easily integrate into existing networks in a matter of minutes. In contrast to traditional IPsec routers, there are no error-prone, complex routing tables to configure and maintain, thereby reducing maintenance cost and opportunities for misconfiguration. Once installed, SafeNet WAN encryptors require virtually no ongoing configuration and maintenance.

Most Secure Layer 2 Encryption Solution

The SafeNet Ethernet Encryptor 10G provides a FIPS 140-2 Level 3 and Common Criteria EAL-4 certified network security solution that enables companies to utilize all available network bandwidth and eliminate complex administration. Designed to overcome the technological limitations of IPsec, the SafeNet Ethernet Encryptor moves sensitive data faster and more efficiently at network layer 2, thereby lowering the cost of network security and compliance.

Layer 2 network encryption is the superior, low latency solution to protecting data in transit over the WAN. Instead of costly bandwidth upgrades with high monthly recurring costs, companies deploy high-speed Ethernet Encryptors to immediately double encrypted bandwidth over IPsec.

Complete Portfolio of Encryptors

SafeNet's complete family of high-speed network encryptors for all network protocols provide the fastest and easiest way to integrate robust network security to protect mission-critical data for Enterprise and Government organizations. Multi-Gigabit throughput and lowest latency make SafeNet's encryptors the ideal solution for protecting massive amounts of data in motion, including time-sensitive voice and video streams. With solutions for ETHERNET, SONET, LINK, ATM, FRAME and IPsec encryption, SafeNet offers the world's only complete suite of high-speed WAN encryption for every topology, performance range and network design requirement.

Enterprise Data Protection

SafeNet Ethernet Encryptors are a key component of SafeNet's comprehensive enterprise data protection solution to reduce the cost and complexity of regulatory compliance, data privacy, and information risk management. SafeNet Enterprise Data Protection (EDP) is the only solution that secures data across the connected enterprise, from core to edge, with 360-degree protection of data at rest, data in transit, and data in use. Unlike disparate, multi-vendor point solutions that can create limited "islands" of security, SafeNet EDP provides an integrated security platform with centralized policy management and reporting for seamless, cost-efficient management of encrypted data across databases, applications, networks, and endpoint devices. For more information, visit www.safenet-inc.com/EDP



www.safenet-inc.com

Corporate Headquarters:

4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524,
Email: info@safenet-inc.com

EMEA Headquarters:

Tel.: +44 (0) 1276 608 000, Email: info.emea@safenet-inc.com

APAC Headquarters:

Tel.: +852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit www.safenet-inc.com/company/contact.asp

©2009 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. SB-Compliance Data In Transit-07.20.09