

Feature Brief



Using Clavister InSight™ for Compliance

Clavister SSP™ Security Services Platform

firewall • VPN termination • intrusion prevention • anti-virus
anti-spam • content filtering • traffic shaping • authentication

CLAVISTER®

Protecting Values

Introduction

Clavister Security Services Platform (SSP™) is our proven, feature-rich, service-oriented framework for providing best-in-class security solutions. Clavister SSP™ consists of **Clavister Network Security Elements**, **Clavister Lifecycle Systems**, and **Clavister Lifecycle Services**. Clavister SSP™ combines precise control, fine-granular administration, and seamless scalability making it easy to provision the perfect solution for any customer; be it a small organization, a large Internet Service Provider, a Managed Security Service Provider, or a multimedia-ready telecommunication operator.

Clavister Network Security Elements

These are the physical building blocks that you install in your network. Clavister SSP™ currently offers two network security elements; Clavister Security Gateway Series and Clavister Secure Access Gateway. The Clavister Security Gateway is available both as a pre-packaged turnkey appliance solution for fast and easy deployment or as a distributed software-only solution for your preferred hardware platform. The Clavister Secure Access Gateway Series is available as a pre-package turnkey appliance solution only and offers SSL VPN, Single Sign-On (SSO) and multi-factor authentication (MFA).

Clavister Lifecycle Systems

The Clavister Lifecycle Systems is a set of software components enabling true network security management throughout the entire lifecycle, including deployment, monitoring and reporting, configuration and integration, as well as analysis, optimization and troubleshooting. Clavister FineTune™ and the Web-based administration user interface enable you to manage a large set of Clavister Network Security Elements. Clavister InSight™ is our premium Security Event and Information Management (SEIM) system, which does not only support Clavister security network elements, but also a majority of other network devices. By correlating data from all network elements, you get a complete log of all activities in your network. Clavister PinPoint™ completes the Clavister Lifecycle Systems suite with accurate and precise real-time information packaged in a convenient dashboard-style application.

Clavister Lifecycle Services

The Clavister Lifecycle Services empowers you and your products with tools, services, and resources that help maximize benefits and eliminate problems, including planning, deployment, optimization, operations and maintenance. The Clavister Lifecycle Services include the Clavister Service Provisioning Network (CSPN) for automated signature updates, the Clavister xPansion Lines™ license upgrade framework and Clavister's award-winning Technical Support.

The Clavister SSP™ service-oriented framework provides you with a secure environment for your business; either as a service provided to you by a Managed Security Service Provider (MSSP) or as systems and services integrated in your own network.

For more information about Clavister products and services, please visit us at: www.clavister.com.

Introduction

There are numerous regulations for organizations to adhere to, especially if your organization is a publicly held financial institution or healthcare organization. Solutions from Clavister InSight™ provide a comprehensive solution to assist meeting the demanding monitoring, reporting and alerting requirements of the GLBA, HIPAA and Sarbanes-Oxley regulations. This document discusses the solution and how Clavister InSight™ can provide insight into meeting compliance for GLBA, HIPAA and Sarbanes-Oxley regulations.

For information on how Clavister InSight™ can provide insight into meeting compliance for Payment Card Industry (PCI) compliance, please read **Feature Brief: Using Clavister InSight™ for PCI Compliance** available from www.clavister.com.

GLBA Compliance

The Gramm-Leach-Bliley Act (GLBA) has widespread impact on financial institutions including banks, mortgage brokers, lenders, credit unions, insurance and real-estate companies. The regulations are complex and require significant reporting on the processes in place that guarantee the integrity of customer data.

Section 501 of the GLBA documents specific regulations required for financial institutions to protect "non-public personal information". The overall requirements of the regulations can be summarized as the development of "administrative, technical, and physical safeguards:

1. To insure the security and confidentiality of customer records and information;
2. To protect against any anticipated threats or hazards to the security or integrity of such records; and
3. To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

There are many aspects of GLBA that are beyond the scope of this document; however, it does cover monitoring and reporting features from Clavister InSight™ that help meeting some of the documentation requirements of the regulation.

Documentation Requirements

As part of the GLBA requirements, it is necessary that a security management process exists in order to protect against attempted or successful unauthorized access, use, disclosure, modification, or interference of customer records. In other words being able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive customer information. Breaking this requirement down further an organization should be able to assess the following types of "security events":

- Failed system level login attempts
- Failed application level login attempts
- Exploitation of a system by a virus or worm
- Exploitation of a system by unauthorized individuals (i.e. hacking)
- Failed access attempts to files or application data
- Correlating multiple system events to illicit data access

HIPAA Compliance

HIPAA regulations have widespread impact on healthcare providers and insurance companies. The regulations are complex and require significant bookkeeping.

HIPAA regulations impact those in healthcare that exchange patient information electronically. This information exchange includes many types of information such as patient records, prescriptions, health insurance claims, x-rays, doctor referrals, and financial records. HIPAA regulations were established to protect the integrity and security of health information, including protecting against unauthorized use or disclosure of the information.

There are many aspects of HIPAA that are beyond the scope of this document; however, it does cover the parts of the regulation where solutions from Clavister InSight™ can help in meeting some of the bookkeeping requirements of the regulation.

Bookkeeping Requirements

As part of the requirements, HIPAA states that a security management process must exist in order to protect against "attempted or successful unauthorized access, use, disclosure, modification, or interference with system operations". In other words being able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive patient information. Breaking this requirement down further an organization should be able to assess the following types of "security events":

- Failed system level login attempts
- Failed application level login attempts
- Exploitation of a system by a virus or worm
- Exploitation of a system by unauthorized individuals (i.e. hacking)
- Failed access attempts to files or application data
- Correlating multiple system events to illicit data access

Sarbanes-Oxley Compliance

Sarbanes-Oxley regulations have a widespread impact on publicly held companies. The regulations are complex and require significant reporting on the processes in place that guarantee the integrity of financial reporting data.

Section 404 of the Sarbanes-Oxley act documents specific regulations required for publicly traded companies to document the Management's "Assessment of Internal Controls" over security processes. The overall requirements of the regulations can be summarized as: (1) documenting commitment to a process, (2) documenting the effectiveness of the process that's in place, and (3) documenting an auditor's assessment of the company's assessment of the process that's in place.

There are many aspects of Sarbanes-Oxley that are beyond the scope of this document; however, it does cover monitoring and reporting processes from Clavister InSight™ that help meeting some of the documentation requirements of the regulation.

Documentation Requirements

In general, the actual process requirements of Sarbanes-Oxley regulations are vague. It generally states that it requires that a process is in place and that the process is shown to be effective by management, but it does not define the process itself. As part of the requirements, it can be assumed that a security management process must exist in order to protect against attempted or successful unauthorized access, use, disclosure, modification, or interference with system operations. In other words, being able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive financial information. Breaking this requirement down further, an organization should be able to assess the following types of "security events":

- Failed system level login attempts
- Failed application level login attempts
- Exploitation of a system by a virus or worm
- Exploitation of a system by unauthorized individuals (i.e. hacking)
- Failed access attempts to files or application data
- Correlating multiple system events to illicit data access

How to Proceed

The good news is that both firewall and server systems provide sufficient data for assessing these types of security events. The data is reported by these systems in various audit trails called log files. At first these log files seem insurmountable because they are often very large without any consistent format across different systems and applications. However, Clavister InSight™ provide advanced collection, monitoring, reporting and event generation across the most popular firewall, server and application systems. The following sections show some of the advanced reporting to help comply with GLBA, HIPAA and Sarbanes-Oxley regulations.

An important attribute of Clavister InSight™ is the ability to "Normalize" the information across multiple, possibly disparate, systems. Clavister InSight™ is capable of collecting and correlating information from multiple, often times different, systems.

Breaking It Down Further

Clavister InSight™ provides the following information for GLBA, HIPAA, Sarbanes-Oxley reporting:

- Failed Login Attempts (system and application)
- Account Misuse
- Changed Passwords
- Account Lockouts
- Deleted/Disabled Accounts
- Security Group Modification
- Loading and Unloading of Drivers
- File and Directory Ownership Changes
- Log File Modification

In addition, Clavister InSight™ provides the following reports:

- Virus activity on the network
- Network intrusion attempts

Clavister InSight™ provides you all the information needed and has the ability to generate reports stated above that are necessary for GLBA, HIPAA and Sarbanes-Oxley. Being compliant to regulations is often-times complex. There are usually 2 sides to meeting a regulation: (1) showing that a procedure is in place to guarantee the integrity and access to information and (2) processes are in place to audit these policies. Clavister InSight™ can help a company put in place a process to audit and report on the integrity and access to protected information required under several regulations, such as GLBA, HIPAA and Sarbanes-Oxley.

Conclusion

This Feature Brief describes how to use Clavister InSight™ to help you with GLBA, HIPAA and Sarbanes-Oxley compliance. Below are some key customer benefits:

Clavister SSP™ Key Benefits

- **Robust Security**
The purpose-built security offering from Clavister provides a complete set of security features, including Stateful Packet Inspection (SPI) firewall with DoS and DDoS protection, VPN with strong encryption, and User Authentication.
- **Rapid Deployment**
The Clavister Security Gateway provides effortless and rapid deployment. A trained technician can easily deploy and configure new network security elements within minutes, even across continents.
- **Flexible Traffic Control**
The highly sophisticated bandwidth management capabilities in the Clavister Security Gateway make it possible to not only guarantee bandwidth for business critical applications or server, but also to optimize the entire traffic flow in your network and avoid inefficient bandwidth usage.
- **Lowered Costs for Administration**
The powerful administration system that comes with Clavister Security Gateway enables organizations to lower the costs for administration through centralized management. The administration system makes it possible to deploy and configure all devices across the network, no matter if they are located next door or across the globe.
- **High Performance**
Scalable performance with unsurpassed maximum bandwidth, concurrent connections and simultaneous VPN tunnels makes the Clavister Security Gateway the ideal choice even in the most demanding environments like Internet Service Provider Networks, Data Centers, and telecom operators.
- **Low Total Cost of Ownership (TCO)**
Clavister's goal is to provide complete security solutions more cost efficiently than any competitor. Clavister SSP™ with its unique combination of integrated features, world-class service and support, and powerful administration system provide the lowest TCO and the best price/performance ratio possible.

Clavister InSight™ Key Benefits

- Security-based topology and threat visualization
- Real-time monitoring and event correlation
- Comprehensive reporting
- Log management
- Audit and forensics capabilities

Feedback

Clavister Product Marketing is always interested in feedback from our readers. Please direct suggestions, comments or questions regarding this document to product-marketing@clavister.com. Please include the title of the document in your email.

About Clavister

Clavister - a Swedish privately owned company developing IT security products, including its award-winning Clavister Security Services Platform (SSP™). This service-oriented framework enables organizations to monitor network traffic, protecting critical business assets and blocking undesirable surfing. It will also protect you against intrusion, viruses, worms, Trojans, and overload attacks. It requires minimal servicing, with central administration, and has exceptionally flexible configuration possibilities. Its seamless scalability makes it easy to provision the perfect solution for any customer; be it small organizations, large Internet Service Providers, Managed Security Service Providers, or multimedia-ready telecom operators.

Clavister was founded 1997 in Sweden, with R&D and headquarters based in Örnköldsvik and Sales and Marketing based in Stockholm. Its solutions are marketed and sold through International sales offices, distributors, and resellers throughout EMEA and Asia. Clavister also offers its technology to OEM manufacturers.

For more information, please visit us at www.clavister.com.

Limitation of Responsibilities

The information in this document represents the current view of Clavister AB on the issues discussed as of the date of publication. Because Clavister must respond to changing conditions, it should not be considered to be a commitment for Clavister, and Clavister cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. CLAVISTER MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the written permission of Clavister. Clavister may have trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Clavister, the furnishing of this document does not give you any license to these trademarks, copyrights, or other intellectual property.

Part Number: [clavister-fbr-insight_compliance \(0801\)](#)