

Feature Brief



Using Clavister InSight™ for PCI 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.

Using Clavister InSight™ for PCI Compliance

Overview

Visa Cardholder Information Security Program (CISP) has widespread impact on most any organization that is involved in Visa credit card transactions. The CISP requirements were incorporated into an industry standard known as Payment Card Industry (PCI) Data Security Standard resulting from collaboration between Visa and MasterCard to create common industry security requirements. This standard was developed to protect customer information by facilitating the adoption of data security measures worldwide. Today American Express, Discover, MasterCard, Visa and other credit card associations mandate that all online and brick-and-mortar merchants and service providers meet certain security standards when they store, process and transmit cardholder information. The regulations are complex and require significant reporting to guarantee the privacy and integrity of customer data. While there are many PCI aspects that are beyond the scope of this document, a key component necessary to meet such mandates is having an effective security audit process in place. Clavister InSight™ provides comprehensive solutions that help organizations meet PCI monitoring, reporting, auditing and alerting requirements.

Regulation compliance is often a timely and complex process that requires the establishment of:

- Policies and procedures to guarantee the integrity and access to specific information
- Processes to audit specific policies and procedures

Clavister InSight™ can help organizations and credit card agents implement security processes to audit and report on the integrity and access to protected information required under PCI.

PCI Documentation Requirements

The PCI requirements, as defined by the mandate, include twelve data security standard (DSS) requirements that are organized as follows:

- Build and maintain a secure network
 - Requirement #1: Install and maintain a firewall configuration to protect cardholder data
 - Requirement #2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect cardholder data
 - Requirement #3: Protect stored cardholder data
 - Requirement #4: Encrypt transmission of cardholder data across open, public networks
- Maintain a vulnerability management program
 - Requirement #5: Use and regularly update anti-virus software
 - Requirement #6: Develop and maintain secure systems and applications
- Implement strong access control measures
 - Requirement #7: Restrict access to cardholder data by business need-to-know
 - Requirement #8: Assign a unique ID to each person with computer access
 - Requirement #9: Restrict physical access to cardholder data
- Regulatory monitor and test networks
 - Requirement #10: Track and monitor all access to network resources and cardholder data
 - Requirement #11: Regularly test security systems and processes
- Maintain an information security process
 - Requirement #12: Maintain a policy that addresses information security

Core to these requirements are strict safeguards to protect any system that stores, processes or transmits sensitive cardholder data. Any system is defined to be any network component, server or application that possesses or processes cardholder data, which may include firewalls, switches, routers, wireless access points, network appliances, security appliances, Web, database, authentication, mail, proxy and DNS systems.

First Steps: Monitor, Report and Alert

As part of the PCI requirements, it is necessary that an information security policy be established, published, maintained and disseminated. This policy must:

- Address all mandates
- Include an annual process that identifies threats and vulnerabilities, and assesses risks
- Includes a formal annual review and updates when the environment changes

Therefore, it is necessary that organizations processing credit card transactions are able to monitor, report, audit and alert on attempted or successful access to systems and applications that contain sensitive cardholder information.

To effectively do this, credit card processing agents should have a process in place 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

Similar to most regulations, there is no single solution that ensures PCI compliance. What is required is the implementation of both a physical infrastructure to meet the data protection requirements of the standard, and the implementation of a security management framework (e.g., network, systems and security management tools) to meet PCI monitoring, auditing and reporting requirements.

A challenge for many organizations is determining how to best meet PCI requirements across the entire computing environment. Often times, an organization may try to leverage point solutions from specific vendors or deploy a management solution that only meets specific requirements. Unfortunately these solutions typically are not comprehensive enough to meet the breadth and depth of the PCI requirements across all systems.

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. However, the log files may seem insurmountable because they are often very large without any consistent format across different systems and applications so many organizations seek solutions to better manage, interpret and audit the data. Clavister InSight™ provides comprehensive solutions for advanced collection, monitoring, reporting, auditing and correlation across the most popular firewall, server and application systems.

Breaking it Down Further: Manage, Interpret and Audit

Clavister InSight™ enables organizations to better manage, interpret and audit security processes by collecting and correlating information across numerous systems. Delivering both Security Information Management (SIM) and Security Event Management (SEM) capabilities, Clavister InSight™ also helps organizations gain enterprisewide security intelligence via:

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

Clavister InSight™ provides security administrators with all the features necessary to not only simplify day-to-day security operations, but to also satisfy management reporting requirements, including security audits required by government regulations.

With a highly flexible and scalable multi-tier and agent-less architecture, Clavister InSight™ enables the easy collection, storage and collection of the following:

- Security events
- Network events
- System events
- Application events

Once collected, these events are normalized across all devices, aggregated, compressed and archived in an encrypted log file. The real-time event data is then sent to monitoring, correlated alerting and topology threat visualization modules for real-time threat management. At the same time, the aggregated log data is analyzed and stored in a database for reporting and security auditing purposes. This enables organizations to easily comply with assorted government mandates.

How Clavister InSight™ Supports PCI Compliance

Clavister InSight™ helps organizations maintain a security, monitoring and testing process to comply with PCI Requirements 10-12. PCI Requirements 10-12, as detailed in the chart that follows, provide specific guidelines in the areas of monitoring and testing networks (#10), testing of security systems and processes (#11) and maintaining an information security policy (#12).

PCI REQUIREMENT	CLAVISTER'S SOLUTION
#10: Track and monitor all access to network resources and cardholder data	<ul style="list-style-type: none"> • Log collection across systems and applications impacted by PCI • Secure log file archive to protect from inappropriate access to log data • Log archival for extended time (1 year for PCI) • Provide audit trails of access to physical systems including firewalls, IDS, IPS, routers, switches and application servers • Provide audit trails of access to leading credit card processing data systems, including Oracle and MS-SQL • Monitor, alert and report on failed access to systems and applications • Monitor access system for all users including employees and contractors • Provide role-based access to security event data • Create baselines of "normal" activity and define alerts to acknowledge "abnormal" activity • Monitor access to critical server resources including systems, files, and database records, and applications • Log file backup capability
#11: Regularly test security systems and processes	<ul style="list-style-type: none"> • Integrate leading vulnerability scan data • Monitor, alert and report on vulnerabilities as reported from vulnerability scanners • Integrate leading IDS/IPS log data • Monitor, alert and report on vulnerabilities as reported from IDS/IPS systems • Provide role-based access to security event data • Service-oriented architecture for implementation of required event management services • Provide security event management best practices as part of overall PCI strategy • Integrate with third-party incident response solutions
#12: Maintain a policy that addresses information security for employees and contractors	<ul style="list-style-type: none"> • Provide role-based access to security event data • Service-oriented architecture for implementation of required event management services • Provide security event management best practices as part of overall PCI strategy • Integrate with third-party incident response solutions

Table 1: PCI Requirements and Clavister's Solutions

Conclusion

This Feature Brief describes how to use Clavister InSight™ to help you with PCI 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_pci \(0801\)](#)