

Product Data Sheet



Clavister Security Services Platform and PCI Compliance

Clavister SSP™ Security Services Platform

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

CLAVISTER®

Protecting Values

- Turnkey appliance solution or software-only solution
- Stateful Packet Inspection (SPI) Firewall
- DoS and DDoS protection
- Anti-Virus
- Intrusion Detection & Prevention
- Zero-Day Signature Updates
- SSL/IPsec VPN
- Multi-Factor Authentication
- Comprehensive Security Reports
- Regulation Support: SOX, GLBA, HIPPA, PCI and FISMA
- Real-time Monitoring and Correlated Alerting
- Reporting Portal with Powerful Drilldown
- Access over 1,000 Interactive Reports and Pre-Defined Compliance Reports

Clavister Security Services Platform and PCI Compliance

Overview

The world is processing billions of credit card transactions each day. Everywhere in the world, from the local dry cleaner on the street corner to the Apple Store in San Francisco, USA. The commonality between the local dry cleaner and the Apple Store is that they must comply with the Payment Card Industry Data Security Standard (PCI DSS). This is a requirement they share with anyone that processes credit or debit card information, including merchants and third-party service providers that store, process or transmit credit card/debit card data.

Background

The PCI 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 framework comprising firewall, anti-virus, encryption and security auditing processes. Clavister Security Services Platform (SSP™) provides a comprehensive solution that helps organizations meet PCI requirements.

PCI Regulation Compliance

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

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

Clavister SSP™ can help organizations and credit card agents implement security mechanisms and required processes to secure transactions, audit and report on the integrity and access to protected information required by the PCI regulation.

Clavister Security Services Platform

Clavister Security Services Platform (SSP™) is a proven, feature-rich, service-oriented framework for providing best-in-class security solutions. Clavister SSP™ comprises of **Clavister Network Security Elements**, **Clavister Lifecycle Systems**, and **Clavister Lifecycle Services**. Its combination of precise control, fine-granular administration, and seamless scalability makes 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 telecom operator.

Clavister Network Security Elements

The network security elements are the physical building blocks installed in the network. Clavister SSP™ currently offers two network security elements; Clavister Security Gateway Series, available both as a pre-packaged turnkey appliance solution for easy deployment or software-only format for your preferred hardware platform, and the Clavister Secure Access Gateway Series offering SSL VPN and multi-factor authentication.

"Being PCI compliant is a smart business decision."

Aaron Biddar, President ControlScan

Clavister Lifecycle Systems™

The Clavister Lifecycle Systems™ is a set of software components enabling true network security management throughout the entire lifecycle, including deployment, configuration and integration, monitoring, reporting, and analysis, optimization and troubleshooting.

The Clavister InSight™ is our premium Security Event and Information Management (SEIM) system. Clavister InSight™ 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 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.

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

Clavister and Selected PCI Compliance Partners

Clavister are working in close collaboration with a number of selected partners to offer customers a full PCI compliance package, including products, services and support. For more information about PCI compliance and partners, please contact your local Clavister Sales Representative. For more information about Clavister products and services, please visit us at: www.clavister.com.

Clavister SSP™ Highlights

Robust Security

Clavister Security Gateway is a comprehensive and purpose-built security offering from Clavister, which 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.

The Clavister Secure Access Gateway delivers cost-efficient and high-performing SSL VPN access for any organization. Support for multi-factor authentication, Single Sign-On (SSO), Clavister Remote Assistance™ are only a few of the features included with Clavister Secure Access Gateway.

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.

PCI Documentation Requirements

The PCI requirements, as defined by the mandate, include twelve (12) data security standard (DSS) requirements that are organized as follows:

PCI DSS Requirements	Clavister Security Services Platform (SSP™)
Build and maintain a secure network	
R1: Install and maintain a firewall configuration to protect cardholder data	Clavister SSP™ offers one of the most powerful, fast and versatile firewall in the security industry, including Stateful Packet Inspection, DoS and DDoS protection, access control and quality of service (QoS) functionality.
R2: Do not use vendor-supplied defaults for system passwords and other security parameters	This requirement should be handled by carefully crafted policies and routines. A selected Clavister partner will be able to help you with this requirement.
Protect cardholder data	
R3: Protect stored cardholder data	Encryption is a critical component of cardholder data protection. Clavister SSP™ supports all major encryption standards, such as AES, 3DES, DES, Blowfish and CAST-128.
R4: Encrypt transmission of cardholder data across open, public networks	Sensitive information must be encrypted during transmission across networks. Clavister SSP™ supports all major encryption standards, such as AES, 3DES, DES, Blowfish and CAST-128. Clavister SSP™ also supports SSL VPN, enabling organizations to use clientless VPN connectivity with support for DES, 3DES, RC4 and AES.
Maintain a vulnerability management program	
R5: Use and regularly update anti-virus software	Many vulnerabilities and malicious viruses enter the network via employees email activities. An anti-virus system must be in place on all systems commonly affected by viruses. Clavister SSP™ supports both anti-virus system using powerful stream-based signatures, Intrusion Detection & Prevention (IDP) system with more than 9,000 signatures and anti-spam functionality. All signature-based functions has the capability of using an automated update process.
R6: Develop and maintain secure systems and applications	Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. Clavister SSP™ is updated regularly under strict quality control. This extra layer of defense enhances the overall security of your IT infrastructure.
Implement strong access control measures	
R7: Restrict access to cardholder data by business need-to-know	It is important to restrict access to cardholder data to authorized personnel. Clavister SSP™ supports a number of authentication mechanisms, such as multiple RADIUS servers, CHAP, PAP. This will ensure that only authenticated personnel are allowed to log in. Access policies can be set up both for external as well as internal users.
R8: Assign a unique ID to each person with computer access	Clavister SSP™ can easily communicate with external RADIUS servers, making it easy to authenticate unique users.
R9: Restrict physical access to cardholder data	This requirement should be handled by carefully crafted policies and routines. A selected Clavister partner will be able to help you with this requirement.
Regulatory monitor and test networks	
R10: Track and monitor all access to network resources and cardholder data	Logging mechanisms and the ability to track user activities are critical. Clavister SSP™ includes Clavister InSight™ - the premium Security Event and Information Management (SEIM) system. Clavister InSight™ 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.
R11: Regularly test security systems and processes	This requirement should be handled by carefully crafted policies and routines. A selected Clavister partner will be able to help you with this requirement.
Maintain an information security process	
R12: Maintain a policy that addresses information security	This requirement should be handled by carefully crafted policies and routines. A selected Clavister partner will be able to help you with this requirement.

Core to these requirements are strict safeguards to protect any system that stores, processes or transmits sensitive cardholder data.

The term *any system* above 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.

For more information about PCI DSS compliance, please visit: www.pcicomplianceguide.org.



Clavister AB, Torggatan 10, SE-891 28 Örnköldsvik, Sweden
 Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com | Email: info@clavister.com