Clavister IDP System

Clavister SSP™ Security Services Platform

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

clavister™

Control Freaks

- Zero-day attack prevention
- Signature Based Detection
- Stateful Signatures
- Component Based Signatures
- Traffic Anomaly Detection
- Protocol Anomaly Detection
- Dynamic IP Blacklisting
- Application Blocking
- High Performance
- Granular configuration
- Automated signature updates

Clavister IDP – The Route to Multi-Layered Security

The Clavister Intrusion Detection & Prevention System (Clavister IDP) is an in-line subsystem of the award-winning Clavister Security Gateway Series, designed to protect critical environments such as the telecom operator, service provider and enterprise networks. Thanks to the unique combination of security functions, high-performance and timely updated signatures, Clavister IDP provides a multi-layered security solution capable of stopping Internet threats before they can harm your business. By blocking the attacks before they can enter your network, Clavister IDP assures maximum network uptime, minimized administrator involvement and ultimately it frees up IT resources which can be used for other critical projects.

Efficient Network Protection

Today when new threats arise every day and the time between a documented vulnerability and a released attack is getting shorter, it is no longer possible for organizations to protect their network by only patching their applications.

Even if it was possible to keep all servers updated it would be a very cumbersome, time-consuming and often reactive task. Clavister IDP provides a pro-active and centralized protection against most sorts of attacks and eliminates the need to have administrators patch the servers 24/7.

Additionally, Clavister IDP provides application blocking capabilities which makes it possible to prevent Peer-to-Peer applications from consuming costly bandwidth and causing productivity loss.

This means that Clavister IDP not only ensures the highest level of security, it also delivers unparalleled Return On Investment and the lowest Total Cost of Ownership possible.

Features and Benefits

Continuous Signature Updates
Signatures are continuously updated and made available through Clavisters Update Servers.

A global network of sensors detects new threats on the internet and makes it possible for Clavister to provide customers with new signatures before a possible outbreak or attack.

Hardware Acceleration
Maximizes throughput while still performing deep packet inspection.

Dynamic Black-listing
Protects the network from further attack attempts when an attack is detected.

Protocol Anomaly Detection
Protects the system against new attacks by detecting and blocking protocol anomalies.

Backdoor detection
Protects the network against backdoor attacks such as Sub7, BackOrifice etc.

NOP Sled Detection
Detection of NOP sled's in text based protocols will protect the system against new and/or undocumented buffer overflow attacks.

Virtual Patch Capabilities
Vulnerability signatures work as virtual patches for servers before they have been updated with the latest patches.

Efficient Signature set

Clavister IDP uses a set of highly unique, auto-generated, and component based signatures which detect attacks based on attack components such as the NOP sleeds, attack payload and shell code.

This is very efficient since many hackers are releasing their new attacks based on old components as they strive to beat the application vendors from coming out with vulnerability patches.

Component based signatures make it possible for Clavister IDP to protect your network against variations of attacks thus making it far more efficient than traditional signatures which uses exact fingerprints for each attack. At the same time as this makes Clavister IDP capable of providing "zero-day" prevention for attack variations it also decreases the number of false positive alarms, thus minimizing administration needs.

The Clavister IDP signature-set efficiently captures:

- Hostile Probings: port scans, backdoor probes, host sweeps and other inappropriate network and application interrogations.
- Exploits of vulnerabilities in: DNS, FTP, HTTP, ICMP, SMTP, POP3, RPC and other network protocols.
- Attacks on vulnerabilities in popular and custom applications such as: IIS, Oracle, MySQL, SQL server, Internet Explorer, Apache and more.
- Social engineering attacks related to popular Instant Messaging, Chat and Peer-to-Peer applications

About Clavister

Clavister is a leading developer of high-performance IT/IP security. The products, based on unique technology, include carrier-class firewalls and VPN solutions. They have been awarded preferred choice by the international press and are in use today by thousands of satisfied customers. In short; In a world where people depend on information, Clavister provides complete security solutions more cost-efficiently than any competitor, always with Your business in mind.

Clavister was founded 1997 in Sweden. Its R&D and headquarters is situated in Örnsköldsvik, Sweden and its solutions are marketed and sold through sales offices, distributors and resellers in Europe and Asia. Clavister also offers its technology to OEM manufacturers.

Clavister IDP – One step ahead!

By using highly advanced and unique technology such as auto-generated and component based signatures, Clavister IDP is capable of catching both new and un-known attacks as well as variations and combinations of known attacks. This makes Clavister IDP one of the most secure and efficient solutions available to companies who no longer want to spend time and money on maintaining a re-active organization or recovering from disasters.

Feature List

Detection Methods
- Protocol Anomaly Detection
- Traffic Anomaly Detection
- Backdoor Detection
- IP Spoofing Detection
- Layer 2 Detection
- Worm Protection
- Trojan Protection
- Spyware Protection
- Buffer overrun Protection
- VoIP Protection

Signatures
- Component Based Signatures
- Stateful Signatures

Traffic interpretation
- Reassembly
- Normalization

Response Method
- Drop Connection
- Dynamic IP Blacklisting (Hosts & Networks)

Application Awareness
- Layer 7 - Application awareness
- Layer 2-4 Network Layer awareness

Auditing
- Clavister Logger
- SNMP traps
- SYSLOG
- Detailed attack Descriptions
- Threat analysis portal

The security service platform techies love

Clavister SSP™ Security Services Platform

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

clavister™

Control Freaks

Part number: CLA-IDP-DTS rev A01

www.clavister.com