clavister
CONNECT . PROTECT

Clavister Endpoint Security Client

Intelligent and Proactive

CYBER CRIME

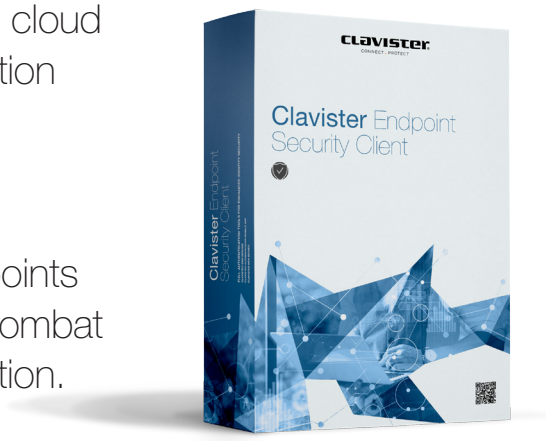
The year of 2016 was the year of cyber crime. Crimeware such as ransomware grew with 400% in a single year. Looking forward, into 2017 and beyond, there are clear signs of an evolution where these tools become more sophisticated and evasive to traditional security products.

Zero-day attacks are growing steadily and ransom-wares are evolving to target Point of Sales systems, IoT Devices and other sensitive infrastructure.

Clavister Endpoint Security Client

The Clavister Endpoint Security Client – with its cloud based management console and Next Generation technology – delivers award winning protection against known and unknown threats.

Global threat intelligence from 500 million endpoints combined with Artificial Intelligence helps you combat ransomware and other threats to your organization.



THE RISE OF ZERO DAY ATTACKS

Each day, there're more than 300,000 new malwares created, each designed to attack your endpoints, create havoc in your network, encrypt your files or to steal your data and even money. Zero day attacks are growing exponentially which renders most antivirus solutions useless.

To ensure your privacy, integrity and avoid costly security breaches you need advanced threat prevention tools that are capable of detecting zero day and evasive malware.

THE SOLUTION

The Clavister Endpoint Security Client (ESC) is a Next-Gen antimalware product featuring award winning technology, powered by Bitdefender, rated best in class year after year due to its security effectivness. Combining classic signature based protection with modern Next-Generation technologies such as behavior based intelligence ensures highest level of security for your endpoints.

The cloud based management console makes it easy to deploy, able to manage hundreds or even thousands of clients simultaneously and effectively.

"Enterprises spend more than USD4 billion every year on endpoint security solutions*, but are still loosing ground to cyber criminals."

* IDC Endpoint Security Market Prediction

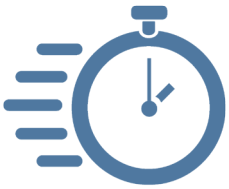
Feature Highlights

CLOUD MANAGED

The cloud based management console provides a powerful and centralized interface for all your endpoints and doesn't require any installation or maintenance. No management or configuration on the actual client is necessary.

Benefits:
- No additional hardware needed
- No cost for additional Operating Systems
- No cost for time-consuming maintenance
- Easy-to-use and requires minimal support

RAPID DEPLOYMENT



Deploy the Endpoint Client to your devices fast and easy. With the local relayer you can also detect new devices and provision the client in minutes, even if another endpoint client is already installed.

Benefits:
- No interaction needed from the end user
- Lowered costs for deployment

BANDWIDTH EFFICIENT

By using the relay feature you will only need to download signatures and new software packages once, all other client will download the files on your local area network (LAN), thus helping you save bandwidth and provide faster updates.

Benefits:
- Faster software updates and upgrades
- Avoids wasting bandwidth
- Improved Quality of Experience

THREAT INTELLIGENCE ECOSYSTEM

+500 MIL

The Clavister Endpoint Security Client is part of an integrated eco system with more than 500 million other endpoint clients. Anytime one of the endpoints discovers a new malware, the information is shared across all clients in minutes.

Benefits:
- Improved security
- Minimal time exposed to zero-day malware
- Reduced costs related to security incidents

ZERO DAY PROTECTION

0 DAYS

Artificial Intelligence and fourth generation machine learning looks at the behavior of files rather than trying to simply recognize if it's a known malware; a highly proactive and effective strategy against zero day attacks.

Benefits:
- Improved security
- Reduced risk of infections for clients not updated
- Reduced costs related to security breaches
- Reduced urgency of patch management

RANSOMWARE PROTECTION

The Clavister Endpoint Security Client is highly effective in preventing ransomwares from encrypting your valuable data. Using a combination of behavior based and signature based protection ensures that both known and unknown ransomwares are eliminated.

Benefits:
- Improved security
- Avoid having to pay ransom to criminals
- Reduced Costs / TCO

DATA LOSS PREVENTION

Data Leakage Prevention avoids sensitive data such as credit card numbers, social security numbers and similar from being leaked from your endpoints.

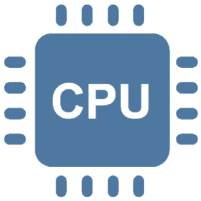
Benefits:
- Achieve regulatory compliance (e.g. GDPR)
- Avoid intentional or un-intentional data leakage

APPLICATION CONTROL

By using the application control feature, with policy scheduling, you can decide what applications are allowed to run and communicate on your endpoint devices.

Benefits:
- Reduced risk for data leakage and breaches
- Maintenance free, no signatures to be updated

RESOURCE EFFICIENT



The Clavister Endpoint Security Client is one of the most resource efficient clients on the market, requiring only a minimal amount of CPU and RAM, allowing you to maximise the use of your devices.

Benefits:
- Minimal impact on performance
- Increased Quality of Experience for End Users

DEVICE CONTROL

Control how USB ports, printers, removable media and similar may be used on your endpoint devices using granular and powerful policies.

Benefits:
- Improved security
- Minimal time exposed to zero-day malware
- Reduced costs related to security incidents

INTEGRATED REPORTING

Pre-defined and customizable reports helps you see and understand what is happening with your endpoint devices. Reports can easily be scheduled and distributed to different recipients of your choice.

Benefits:
- Increased Security / Lowered Risk
- Faster Incident Responses
- Achieve Policy Compliance
- Reduced Costs / TCO

HOST BASED IDS/IPS

Detect and block network based intrusions by using the host-based intrusion detection and prevention feature. This feature also help identify if a malware has managed to infect your devices and are trying to communicate with Command and Control servers.

Benefits:
- Improved security
- Reduced costs of security incidents
- Identify attempted intrusion and hacking campaigns

Clavister Endpoint Security Client (ESC) | 7

Specifications

Management and Provisioning	
Cloud based management console	Yes
Integration with Microsoft Active Directory	Yes
Intelligent Deployment (Relaying)	Yes
Software Updates from Local Relayer	Yes
Network discovery and automated deployment	Yes
Pre-Defined and Custom Reports	Yes
Scheduled Report Generation and Distribution	Yes
Custom Report Distribution Lists	Yes
Pre-Defined Monitoring Dashboards and Widgets	Yes
Custom Monitoring Dashboards and Widgets	Yes
Alarms Center	Yes
Alarm Distribution via Email	Yes
Antimalware	
Antivirus / antimalware / antiransomware / antispyware / antiphishing	Yes
Trojan and rootkit detection	Yes
Behavioral Monitoring and Active Protection	Yes
Firewall / IPS	
Fully featured two-way (directions) firewall	Yes
Host Based Intrusion Detection and Prevention (H-IDS / H-IPS)	Yes
Content Control	
Scan SSL Encrypted Traffic	Yes
Scan Web, Mail (outgoing and incoming)	Yes
Policy based web category filtering (time/schedule and web category)	Yes
Manual black-/whitelisting	Yes
Fraud and phishing protection	Yes
Device Control	
Policy-based port / device control (USBs, printers, scanners, network adapters, scsi, internal/external storage), etc.	Yes
Application Control	
Policy-based Application Control (application name, path, user, time/schedule)	Yes
Host-based solution, agnostic to evasive traffic patterns)	Yes
Location Based Policies	
Create policies based on device location and network	Yes
Supported Operating Systems	
Windows 7, 8, 8.1, 10, Vista (SP1, SP2), XP (SP3)	Yes
Windows Embedded Standard, POSReady, 2009, 7	Yes
Windows Embedded Enterprise 7	Yes
Windows XP Embedded (SP 2), Tablet PC Edition	Yes
Windows Server 2012, 2012 R2	Yes
Windows Small Business Server (SBS) 2003, 2008, 2011	Yes
Windows Server 2003 (SP 1), 2003 R2, 2008, 2008 R2	Yes
Windows Home Server	Yes
Mac OS X Lion (10.7.x), Mountain Lion (10.8.x), Mavericks (10.9.x), Yosemite (10.10.x), El Capitan (10.11.x)	Yes
Red Hat Enterprise Linux / CentOS 5.6 or higher, Ubuntu 10.04 LTS or higher, SUSE	Yes
Linux Enterprise Server 11 or higher, OpenSUSE 11 or higher, Fedora 15 or higher,	Yes
Debian 5.0 or higher, Oracle Solaris 11, 10 (only in VMware vShield environments)	Yes

clavister®
CONNECT . PROTECT

CONTACT

Phone: +46 (0)660 29 92 00
Email: sales@clavister.com
Web: www.clavister.com

Sjögatan 6J
SE-891 60 Örnsköldsvik
Sweden

About Clavister
Clavister (NASDAQ: CLAV) is a leading security provider for fixed, mobile and virtual network environments. Its award-winning solutions give enterprises, cloud service providers and telecoms operators the highest levels of protection against threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the Product Quality Leadership Award from Frost & Sullivan. The company was founded in Sweden in 1997, with its solutions available globally through its network of channel partners. To learn more, visit www.clavister.com.

Where to Buy
www.clavister.com/partners

Contact
www.clavister.com/contact