


**CLAVISTER®**



CONNECT  
PROTECT  
PREVENT

ENTERPRISE SECURITY  
USE-CASE GUIDE



An all communicating world,  
based on trust and security.

*Clavister's Vision*

# SECURING BUSINESS CONTINUITY



## Clavister secures and protects enterprise and service provider networks, enabling business continuity with a multi use-case product suite

Cybersecurity is now seen as one of the main threats to the world economy and will cost the an estimated 6 trillion USD annually by 2021 (source: Cybersecurity ventures). Clavister provides distributed enterprises with security solutions that protect and connect their business securely. The products are engineered in Sweden — guaranteed free from back-doors and not based on any conventional operating systems.

The solutions provides multiple use-cases in the same setup providing secure connectivity and protection from threats . It also enables to take preventative measures to restrict inappropriate usage from inside the network. They run on appliances suitable for small to large offices but also virtualised to protect the cloud resources. Clavister's solutions can be managed in-house by IT departments or can be operated by local specialized managed services partners.



**Headquartered in Örnköldsvik, Sweden, with offices in Nordics, Germany, Japan and South East Asia, Clavister has more than 200.000 installations with customers in 154 countries. Solutions are sold under OEM by Nokia, D-Link and others.**

## The Clavister package

Clavister's Next Generation Firewall has a very simple licensing model that waives user licenses, software-blades, add-on packages or similar. Instead two subscription models are available enabling basic or advanced functionalities empowering use-cases. Likewise, central management is supplied with both packages, ensuring minimal maintenance and flexible configuration options.

This packaging makes it possible to equip small as well as large companies with a turnkey, highly efficient Next Generation Firewall solution, without having to give up the tried-and-tested universal threat management functionality or have to deploy another appliance for it. With Clavister you deploy a security solution that provides peace of mind with reduced cost.

### Ecosystem

Clavister collaborates with and includes technologies from leading suppliers in their field. The Clavister ecosystem focuses on including the best-of-breed solutions and include:

- **McAfee for Intrusion Prevention System signatures**
- **Bitdefender for Anti-virus signatures**
- **Webroot for IP Reputation feeds**
- **ContentKeeper for Web Content Filtering**
- **Qosmos by ENEA to enable Application Control with Deep Packet Inspection (DPI)**
- **Bitdefender providing Endpoint Protection client technology**



### The two subscription packages available are:

#### Clavister Product Subscription — CPS

This is the basic subscription with 24/7 support and next business day hardware replacement. Firewall upgrades are included and the software is enabled to support major use-cases including Perimeter Protection, Routing — Redundancy & Load Balancing, Reliable Secure Virtual Private Networking, Secure Network Zones, Server, Load Balancing and Active Traffic Optimisation.

#### Clavister Security Subscription — CSS

Same as the CPS plus subscription services enabling the following use-cases: Network/Server Attack Protection, Advanced Threat Protection, Web Content Blocking and Application Visibility & Control.

Clavister products are used for a wide set of security solutions and use-cases. In this book we present a sample of the most popular and describe their benefits.



Connecting business locations to each other and to the internet with focus on security and reliability ensuring business continuity.

<b>Reliable Secure Virtual Private Networking</b>	<b>6-7</b>
<b>Routing — Redundancy &amp; Load Balancing</b>	<b>8</b>
<b>Secure Network Zones</b>	<b>9</b>
<b>Server Load Balancing</b>	<b>10</b>
<b>Flexible Remote Access</b>	<b>11</b>



Use-cases inspecting traffic and behavior of traffic for threats in order to protect your digital assets.

<b>Perimeter Protection</b>	<b>12</b>
<b>Network/Server Attack Protection</b>	<b>13</b>
<b>Advanced Threat Protection</b>	<b>14-15</b>
<b>End-User Protection</b>	<b>16</b>



With preventative security measures and rules these use-cases reduce the risk of users making mistakes to threaten or compromise the digital perimeter of your business.

<b>Web Content Blocking</b>	<b>17</b>
<b>Application Visibility &amp; Control</b>	<b>18-19</b>
<b>Multi Factor Authentication (MFA/2FA)</b>	<b>20-21</b>
<b>Active Traffic Optimisation</b>	<b>22-23</b>



“By 2020, more than 50% of WAN edge infrastructure refresh initiatives will be based on SD-WAN versus traditional routers (up from less than 2% today).“ - *Gartner*



### Reliable Secure Virtual Private Networking

## Connecting branch offices and remote locations securely and cost effectively

Enterprises depend on their inter-office connectivity and need therefore a solution that is robust, reliable and secure. In a distributed office environment real-time communication between systems is key for business intelligence and enablement. In the past companies rented private leased lines or used MPLS solutions. These solution proved to be limiting

and costly and often with a lock-in to a single telecom provider. Requirements for flexibility and reduced costs have resulted in usage of virtual private networking setup over common internet connections on each site. Advances in cloud enablement have introduced packaged solutions called Software Defined — Wide Area Networks — or SD-WAN.



## Solution

Clavister's Secure SD-WAN solution combines the Reliable Secure VPN use-case and other use-cases such as Perimeter Protection and Routing — Redundancy & Load Balancing. It offers them in a software-only virtualised solution for deployment in the cloud or on a range of hardware appliances. A virtual network between your locations is setup easily with management tools allowing for secure communication between the sites and the cloud.

**Clavister's smallest setup is just between two locations while the largest installation connects over 3.000 different locations with close to 10.000 unique VPN tunnels. With holistic management capabilities and Policy-based Routing the solution is both flexible and scalable as well as easy to manage.**

## Results

Companies using SD-WAN VPN solutions save significant operational costs compared to leased lines or MPLS solutions. Also, unlike with MPLS, the internet service provider can differ on each location. A wide choice of Internet transports (such as Cable, DSL, Fibre and 4G) may be used furthering empowering with flexibility and cost reduction.

**Check here to learn more about Clavister's SD-WAN solution:**

[www.clavister.com/sd-wan](http://www.clavister.com/sd-wan)





## Routing — Redundancy & Load Balancing

### Avoid downtime and secure business continuity

Businesses are dependent on their communication infrastructure to keep operations efficient. The slightest amount of downtime of a connection can hurt productivity—or make a critical remote site unreachable. With the entire business being more dependent on connectivity the entire workforce risks becoming unproductive.



**Clavister's routing functionality was named as state of the art and easy to setup and use in every customer survey done since 1997.**

## Solution

With the right infrastructure, businesses can utilize lower cost second connections (such as Cable, DSL, and 3G) to serve as a backup route when needed. In larger setups, the Firewall can act as a traffic router and make complex decisions with easy setup.

## Results

Built in advanced routing and load balancing functionality secures business continuity utilizing cost efficient paths. It also eases maintenance and migration paths for IT technicians—eliminating the need for additional 3rd party equipment.

**Check here to learn more about Clavister's Routing and Load Balancing functionality:**

[www.clavister.com/routing](http://www.clavister.com/routing)







**“Only 3% of enterprises surveyed by Gartner have anti-malware protection on mobile Android devices and only 1% on iOS devices.” - Gartner**



## Secure Network Zones

# Network segmentation to protect company's digital assets

Employees expect to be able to bring their own devices (BYOD) to the office and connect them to the infrastructure. Often however these devices are not managed by the administrator and do not come with the same level of protection as corporate issued devices. This poses a risk towards internal systems from inside the secure perimeter.

## Solution

The solution is to segment your network into several zones and control the traffic allowed between them tightly. A complementary way is to setup an internal secure perimeter in front of the most critical business applications such as databases, file servers and collaboration servers.

## Results

By protecting each of your digital assets with a virtualised dedicated firewall, you gain full control of the traffic even from inside your network. Due to Clavister's small footprint, this takes very limited extra resources and can be run on the same virtualisation infrastructure.

**Check here to learn more about Clavister's secure network zones:**

[www.clavister.com/zones](http://www.clavister.com/zones)





## Server Load Balancing

# Simplifying scaling and allowing preventive maintenance

Every IT infrastructure has components that are critical and need a setup to provide redundancy and scalability. Both to guarantee service uptime when something happens to one of the servers unexpectedly, but also to enable pro-active maintenance in an easy way. Redundancy can be built into the application layer or be setup with DNS round-robin, but this adds complexity and does not always provide control to the service owner.

## Solution

Built into the firewall that protects the hosted service is a server load balancing function can provide high availability with control. Without rewriting packets contents the solution can load balance protocol traffic including HTTP(S), DNS and LDAP and can utilize connection-rate and resource-usage based strategies. It can receive information through an API to dynamically change ratio of load distribution to the servers so that this can be decided by 3rd party process externally. This could be, mail queue, disk space, CPU usage etc.

## Results

With an integrated Server Load Balancing function the IT administrator saves on specialized solutions to achieve their high availability requirements. It also eases their work to enable pro-active maintenance during normal hours and enables for cost efficient scaling of the service infrastructure.

**The Clavister firewall solution provides several ways to check the availability of the server. A basic ping ICMP message checks if the server responds. TCP monitoring validates if specific services respond on their ports and HTTP monitoring can be configured to poll a specific URL and with that validate an expected response. In combination with scripts on the server this can also check through if a backend database works and triggers failover based on the results.**

**Check here to learn more about Clavister's load balancing functionality:**

[www.clavister.com/slb](http://www.clavister.com/slb)





### Flexible Remote Access

## Empowering remote workers securely

How we work has changed dramatically: we're now more mobile and global; we use BYOD, we access our workflow across complex and unsecured connections such as WiFi hotspots and other access points. Regardless of location or connection, an easy to manage and configure secure remote working solution is a key driver of organizational success and data protection. Nowadays a diverse number of different devices need to be supported.

### Solution

A flexible remote access solution supports a range of technologies including IPsec, SSL or L2TP enabling secure connectivity even in the most restricted remote environments. Compatibility with VPN clients with support for Windows, Mac and mobile operating systems allows all devices to get connected and purpose built Clavister SSL VPN client provide easy of use for both the end user and IT administrator.



### Results

Clavister remote access VPN solutions are quick to set-up on any and all of your devices without the need for IT administrators. You will have the confidence to know that all data is being shared confidentially and without malicious code inserted as it passes through your network. Clavister's solution does this all without latency to allow your network (and employees) to perform at their best and works both in appliance and virtualised installations.

**Check here to learn more about Clavister's VPN solutions:**

[www.clavister.com/vpn](http://www.clavister.com/vpn)





## Perimeter Protection

# Network firewall securing IT resources and users

Hackers, viruses, ransomware, data theft, industrial espionage and even government sponsored attacks. The list of cyber threats that could put your business at risk goes on and on. The World Economic Forum has declared Cyberattacks the 3rd most likely to occur and 6th most impactful. But the challenge isn't just to make the network secure but also to make it efficient and productive at the same time.

## Solution

What is needed is a firewall that monitors and controls incoming and outgoing network traffic based on intelligent security rules. For ideal protection it is critical to be very specific of what

type of traffic to allow and block everything else. While the internet border to your network is the obvious place for a firewall, deployment within the corporate network can increase the security levels for specific segments as well.

## Results

With both virtualised and appliance based versions, Clavister provides peace of mind for every corner of your network. All enterprise class versions include options to run in high-availability mode to secure business continuity even during maintenance periods.

**Clavister Next Generation Firewalls are Made in Sweden and based on a proprietary operating system. Because of this they are guaranteed without backdoors and not vulnerable to the flaws periodically found in operating systems like Windows and Linux. The firewalls include a range of networking services including network address translation, dynamic address allocation and user-awareness through integration with Microsoft Active Directory.**

**Check here to learn more about Clavister's perimeter protection solution:**

[www.clavister.com/firewall](http://www.clavister.com/firewall)







## Network/Server Attack Protection

# Intrusion detection and prevention systems plus denial of service protection

Distributed Denial of Services (DDoS) attacks are one of the easiest and most accessible ways for an entry level hacker to cause trouble. Using one of the many pre-made tools available it's easy to mount an assault from hundreds or even thousands of computers overwhelming just about any system or firewall, causing them to go off-line or operate at a crawl. It's not just web-shops falling victim but whole enterprises with carrier grade security systems becoming subject of ransom schemes. Most scenarios end up with companies paying the ransom fee that is demanded to get rid of the threat. Far from optimal but still a lot cheaper than days of downtime causing irreputable damage to the brand name.

## Solution

Clavister provides a protection tailored for your business. Creating a defence that doesn't just stop the traffic but remains evasive and flexible. Even during a massive DoS attack that shuts everything down, the Clavister Next Generation Firewall makes sure the internal network and backup internet links remain operational. DoS attacks to server services behind the firewall can be mitigated through traffic management and rate limiting.



## Results

The Clavister Next Generation Firewall not only enables a multi-set of strategies to mitigate and reduce the impact of an DoS attack on a server hosted behind the firewall. The solution also secures that internal business is unaffected during a DoS attack and your employees can focus on business continuity.

**Check here to learn more about Clavister's DoS protection functionality:**

[www.clavister.com/server-protection](http://www.clavister.com/server-protection)





**"4% of people will click on any given phishing campaign."**  
- Verizon's 2018 Data Breach Investigations Report (DBIR)

**AV-TEST Institute registers over 250,000  
new malicious programs every day.**



## Advanced Threat Protection

# Integrated Intrusion Prevention System with anti-virus & malware screening

Cybercriminals with malicious intent will try to send pieces of code or links through the firewall in order to persuade the users to create a pinhole from the inside. This often enables cybercriminals to take control of a piece of the user's equipment and provides the them with a

platform to explore the digital assets inside your company. Attacks are often very well covered and even the most careful user can make the mistake to aid the cybercriminal unintentionally.

## Solution

Next Generation Firewalls provide integrated threat protection in several forms. Untrusted traffic can be scanned for viruses and malware based on multiple signature databases, artificial intelligence and behavior detection. All email and web traffic specifically gets thoroughly screened for known threats or suspicious behaviour. For example attachments must be screened as well as links in emails checked if their destination is the same as the domain the mail is sent from.

IP addresses are unique and information about their reputation on how trusted they are is collected centrally. Based on this reputation the Next Generation Firewall can add policies to block traffic from less reputable sites.

**Clavister firewalls include anti-virus and anti-malware scanning with signature databases from Kaspersky and McAfee that scans Web, FTP and Mail content in real-time. In addition connections are screened by an IP Reputation database with feeds from Webroot. All suppliers are world leaders in their niche space.**

## Results

With a Next Generation Firewall from Clavister in place you protect your network and users from cybercriminals and intruders. Malicious content will be stopped and traffic from sites with questionable reputation can be avoided. Users can focus adding value to the business and stop worrying about suspicious looking emails and web content.

**Check here to learn more about Clavister's advanced threat protection functionality:**

[www.clavister.com/threat-protection](http://www.clavister.com/threat-protection)





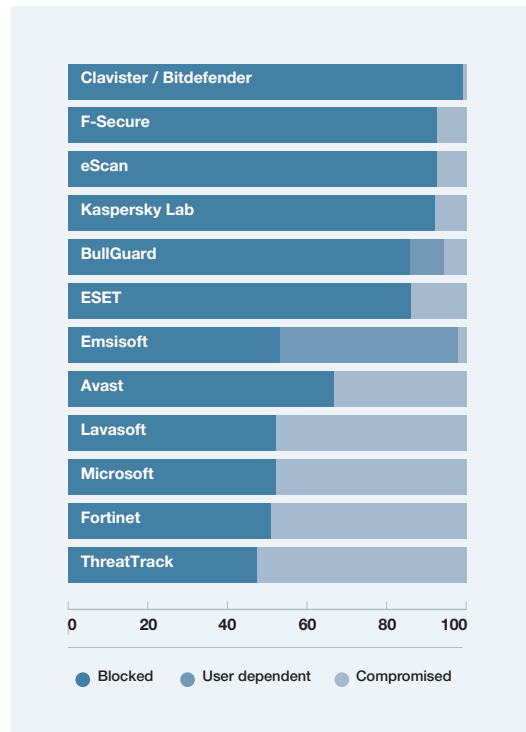
## End-User Protection

# Blocking threats and detecting data loss at endpoint devices

As laptop devices move outside your secure perimeter they will become exposed while being connected to other open networks. While being away, these laptops risk becoming infected—and in the worst scenario this stays undetected until the laptop returns to the corporate network again. The virus or malware will have unrestricted access to the internal environment creating a very undesirable and risky situation.

## Solution

Clavister's endpoint solution is based on industry leader Bitdefender who provides artificial intelligence and behavior detection software together with signature databases to detect viruses and malware. The software also has built-in data leakage prevention (DLP) ensuring GDPR policy compliance and that sensitive data does not get compromised. The solution is cloud managed, easy to deploy and proven in major independent tests year over year to be the best performing solution on the market.



Source: AV-Comparatives, Heuristic/Behavior Test

**Check here to learn more about Clavister's end-user protection:**

[www.clavister.com/endpoint](http://www.clavister.com/endpoint)







## Web Content Blocking

# Restrict access to inappropriate content and comply with regulations

Specific locations on public networks, office policies on private networks, or general government regulations there may be many reasons on why certain type of web sites might have to be restricted.

## Solution

With a web content classification engine the URL and server hostname are in real-time matched to a database with content categories — then labelling the traffic flow with what kind of content it is. Policies in the engine can then take appropriate action or just log this information for statistical purposes. In this way administrators can easily restrict access to X-rated material or block social media sites during specific times in the day. In addition the system can screen the traffic and block if malicious content is detected. The database is refreshed several times a day



*If 100 employees save 1 hour a week by restricting their usage of non-business related web browsing, the opportunity for savings amounts to over 100.000 EUR per year easily.*

to ensure new sites are added continuously and secure accurate actions. In addition, for unencrypted traffic the Next Generation Firewall can screen the traffic and block if malicious content is detected.

## Results

When implemented the results will not only avoid embarrassing situations but also help increase productivity to secure that business resources are used for the right purposes.

**Check here to learn more about Clavister's web content filtering:**

[www.clavister.com/filtering](http://www.clavister.com/filtering)



### ***Best-of-breed by ENEA / Qosmos***

**Clavister integrates Qosmos' ixEngine by ENEA who leads the market for IP traffic classification and network intelligence technology. Just like finding a birch tree in a pine forest based on the trees characteristics, Qosmos identifies 3000+ unique applications out of network traffic. The definitions are updated continuously with every release of our software scheduled on a monthly basis. For more information visit [www.qosmos.com](http://www.qosmos.com)**



### **Application Visibility & Control**

## **Control applications and user behaviour**

Enterprise IT administrators need to control the usage of their network to ensure it's used for business applications. Some of these applications may even deserve priority while others should be pro-actively blocked—as they are known to carry higher risks and compromise security. An example is BitTorrent clients for peer-to-peer file downloading or Tor, an application to browse the dark-web and commonly used by malware to exfiltrate data from your network. Another example is unauthorized excessive usage of server resources for BitCoin mining, spiking up a company's electricity bill. These applications should be blocked.

Not all traffic is web traffic—a lot of traffic runs on separate ports and uses custom protocols to communicate with its servers and peers. Therefore an Application Identification (also called deep packet inspection/DPI) engine is required to detect the application or service accurately. An application like WebEx and Skype can be identified and its traffic can be prioritized to aid in the quality of the conversations. Application control is essential to improve the user's experience.

To manage in a controlled way the traffic from your users, Clavister's Next Generation Firewall includes the world's best deep packet inspection technology to do application identification. In addition, Clavister has classified each application with a risk level from very low to very high, making configuration of blocking risky applications a breeze.

### ***YES! Encrypted traffic can be classified***

**The majority of the traffic nowadays is encrypted. But by reading the Server Name Indication (SNI) in the SSL/TLS certificate, doing Statistical Protocol Identification (SPID) or search for binary patterns in traffic flows the deep packet inspection engine in Clavister's Next Generation Firewall can still detect what application it is with 90-100% accuracy.**

## **Internet of Things (IoT)**

Specifically for IoT devices, application visibility provides the perfect means to control what the devices are doing. With advanced policies you can restrict them only to be allowed to do what they are support to do on the network. So that even if an IoT device is hacked it cannot be used as a springboard to reach other resources.

## **Results**

Application control provides the means to be very specific on what you want to allow on your network. This increases the security levels and enables you to use new technologies early without taking unnecessary risks.

**Check here to learn more about Clavister's application visibility & control use-case go here:**

[www.clavister.com/dpi](http://www.clavister.com/dpi)







***“63% of confirmed data breaches involved weak, default or stolen passwords.” - Verizon’s 2016 Data Breach Investigations Report (DBIR)***



## **Multi Factor Authentication**

### **Ensuring authenticity of end-users**

Users are typically not careful enough with passwords, they often use simple passwords. This makes for an easy path for cybercriminals to compromise an account. Even if your system is secure—if the user-account information is obtained elsewhere—it is likely that your

infrastructure is in danger as well. This is because in many cases users reuse the same password on different services. A second layer of security should be created to identify and authorize the user's identity.



## Solution

Multi Factor Authentication or 2-Factor Authentication provides easy and secure way for your users to login. Several out of band methods can be used to confirm the identity of the user. These may include One Time Password solutions via SMS, mobile app or HW tokens or/and certificates.

**Multi Factor Authentication (MFA) from Clavister is used by the most critical government institutions in Sweden. The product includes multiple and flexible MFA delivery methods such as One Time Password SMS, email, mobile app one-touch confirmation and hardware tokens, x.509 certificates etc. It's redundant and scalable for high availability and provides with it's ease of use a given increased level of security protection that your company needs.**

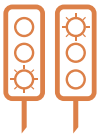
## Results

With a Multi Factor Authentication solution security is improved and it's easy for an administrator to know who is logged-in is actually authenticated as the intended user. With integration to the Flexible Remote Access use-case users are empowered to work from anywhere in a secure manner.

**Check here to learn more about Clavister's Multi Factor Authentication solution:**

[www.clavister.com/mfa](http://www.clavister.com/mfa)





### Active Traffic Optimisation

## Traffic prioritisation securing preferred use of resources

It's common that network links reach their limit and become congested due to the way applications are designed to utilize bandwidth availability. Typically this occurs with file-sharing / syncing or through usage of other applications that create multiple TCP sessions in parallel, aiming for maximum bandwidth utilization.

The result is that capacity is unable to be allocated fairly to other users, causing service degradation and typically impacting vulnerable applications like VoIP and Conferencing Apps. The result is poor conversation quality and network induced disconnects hurting productivity.

## Solution

At the border of the network the Next Generation Firewall acts as a policy gatekeeper to treat different types of traffic—or traffic from different users—with different priority. Service level agreements can be set up to guarantee a portion of the available bandwidth to specific applications or users as well.

**Clavister's Next Generation Firewalls are extensively configurable to differentiate traffic. Different virtual pipes can be created to manage traffic sets within sets and can utilize both application detection as well as user-identification in order to make decisions what traffic pipe a particular session belongs too.**

## Results

Implementing smart traffic optimisation and prioritisation has a significant impact on the traffic when capacity limits are reached. Voice and video conferencing calls will be higher quality and have less interruptions—while file syncing applications like dropbox will just take a second or so longer to sync the files in the background—but will continue to operate as normal.

**To learn more about how to differentiate different types of traffic from each other check this whitepaper:**

[www.clavister.com/optimisation](http://www.clavister.com/optimisation)





## The importance of being pro-active

Advanced perimeter protection and secure connectivity between sites are the basis of a solid security infrastructure. But more often than not, users play an unintended key role in why cybercriminals anyway succeed in gaining access to the enterprises' digital assets and resources.

Multi factor authentication helps solve the problem of inferior passwords in a way that can also provide improved ease of use to connect to companies' systems. But for IT administrators, there is another key opportunity to help the user prevent from doing the wrong things by controlling access to safe applications and sites. Restricting malicious sites based on their global reputation and blocking dark-web, bitcoin mining and other specific applications reduces exposure to risks and secures that the company resources are used as intended. Controlling the traffic flows intimately can also provide an improved customer experience by differentiating real-time critical applications from background traffic and with that increasing the quality for web conferencing applications.

It's time to think pro-actively and implement preventative measures in order to avoid security incidents. Clavister provides the advanced technologies for preventative use-cases that does not require you to be an expert to implement and experience instant results.





The background of the entire page is a photograph of a wind farm. Numerous white wind turbines are visible, their blades blurred by motion, suggesting they are spinning. The turbines are situated in a body of water, and the scene is captured during sunset or sunrise, with a warm, orange and yellow glow on the horizon and a blue sky with scattered clouds above.

**CLAVISTER®**



# Industry Vertical Specifics & Global Cybersecurity Trends

ENTERPRISE SECURITY  
USE-CASE GUIDE

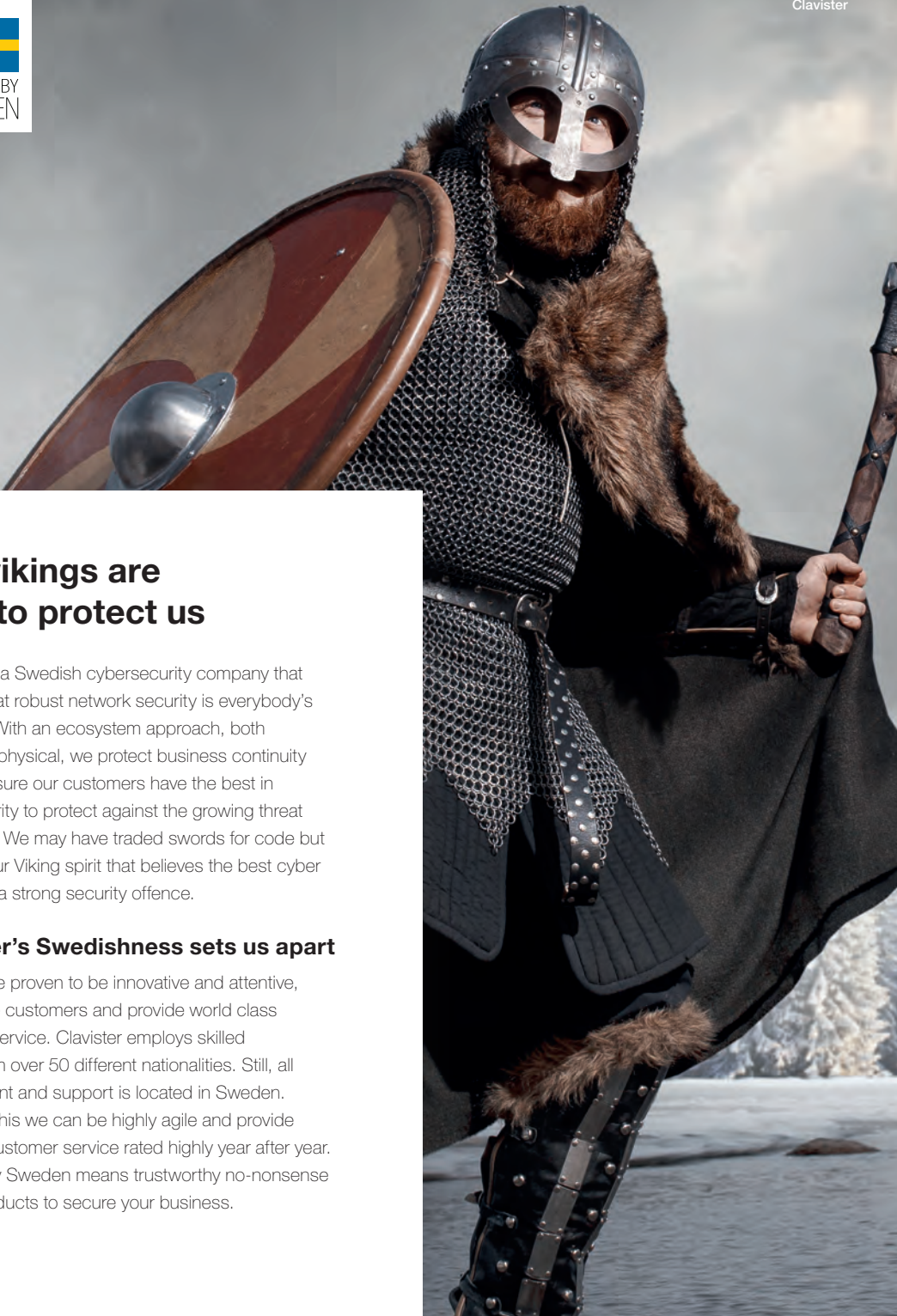


## The vikings are here to protect us

Clavister is a Swedish cybersecurity company that believes that robust network security is everybody's business. With an ecosystem approach, both virtual and physical, we protect business continuity and make sure our customers have the best in class security to protect against the growing threat landscape. We may have traded swords for code but still keep our Viking spirit that believes the best cyber defence is a strong security offence.

### Clavister's Swedishness sets us apart

Swedes are proven to be innovative and attentive, listen to the customers and provide world class customer service. Clavister employs skilled people from over 50 different nationalities. Still, all development and support is located in Sweden. Thanks to this we can be highly agile and provide excellent customer service rated highly year after year. Security By Sweden means trustworthy no-nonsense flexible products to secure your business.



# #NoBackDoors

All Clavister appliances are delivered with the operating system cOS Core developed by Clavister. This completely in-house developed software in Sweden is build on it's own propriatary operating system. This full control enables Clavister to guarantee that it's Next Generation Firewalls are 100% backdoor-free.

Likewise vulnerabilities such as "Heartbleed", "Shellshock / Bash", "Ghost" or "FREAK", as well as open source bugs still to be discovered are not possible in Clavister solutions due to use of propriatary operating system. Many alternative security solution providers have been affected in the past (see table below).

Uniform software on all systems ensures that there are no functional differences between the platforms—both appliance based and virtualised.

	Heartbleed	Shellshock/Bash	Ghost	Freak
<b>Barracuda</b>	●	●	●	●
<b>Checkpoint</b>	●	●	●	●
<b>Cisco</b>	●	●	●	●
<b>Clavister</b>	●	●	●	●
<b>Cyberoam</b>	●	●	—	●
<b>Fortinet</b>	●	●	●	●
<b>Juniper</b>	●	●	●	●
<b>Palo Alto Networks</b>	●	●	●	●
<b>Securepoint</b>	●	●	●	—
<b>Sophos</b>	●	●	●	●
<b>Watchguard</b>	●	●	●	●

● No firewall affected   ● All firewalls affected   ● Some firewalls affected  
 ● All firewalls affected but cannot be attacked according to vendor  
 — No information

*Disclaimer: Statement valid at time of attack publication. Vendors might have patched their products since.*

Contact Clavister - HQ: Sjögatan 6J, SE-891 60, Örnsköldsvik, Sweden. Phone: +46 660-29 92 00  
 For more information visit [www.clavister.com](http://www.clavister.com) or follow on Twitter @Clavister

© 2018 Clavister - v0824. All rights reserved. All other trademarks are property of their respective owners.

# Global Cybersecurity Trends

There are many security topics discussed in every-day press nowadays. In the Global Risks Report 2018 by the World Economic Forum, cyberattacks are listed the 3rd most likely and 6th most impactful. This is compared to other disasters like extreme weather events and terrorist attacks!

## Top 10 risks in terms of Likelihood

- 1 Extreme weather events
- 2 Natural disasters
- 3 **Cyberattacks**
- 4 **Data fraud or theft**
- 5 Failure of climate-change mitigation and adaption
- 6 Large-scale involuntary migration
- 7 Man-made environmental disasters
- 8 Terrorist attacks
- 9 Illicit trade
- 10 Asset bubbles in a major economy

## Top 10 risks in terms of Impact

- 1 Weapons of mass destruction
- 2 Extreme weather events
- 3 Natural disaster
- 4 Failure of climate-change mitigation and adaption
- 5 Water crises
- 6 **Cyberattacks**
- 7 Food crises
- 8 Biodiversity loss and ecosystem collapse
- 9 Large-scale involuntary migration
- 10 Spread of infectious diseases

Source: Global Risks Report 2018 by the World Economic Forum  
[www.weforum.org/reports/the-global-risks-report-2018](http://www.weforum.org/reports/the-global-risks-report-2018)

To learn more about specific security topic check the these pages:

<b>Ransomware</b>	<b>6</b>
<b>Botnets, Zero Days Threats</b>	<b>7</b>
<b>Distributed Denial of Service Attacks</b>	<b>8-9</b>
<b>General Data Protection Regulation</b>	<b>10</b>
<b>NIS-Directive</b>	<b>11</b>





## Industry Vertical Specifics

Each industry is different and specific requirements and regulations need to be met with solutions. Grouping on common requirements this use-case book outlines the following specific verticals:

<b>Retail &amp; Distributed offices</b>	<b>12-13</b>
<b>Industrial IoT &amp; Transportation</b>	<b>14-15</b>
<b>Critical Infrastructures</b>	<b>16-17</b>
<b>Education &amp; Public Sector</b>	<b>18-19</b>
<b>Managed Security Service Providers</b>	<b>20-21</b>
<b>Product Portfolio Overview</b>	<b>22</b>



## Ransomware

# Malware encrypting systems causing them to malfunction

Ransomware is the newest cyber threat whereby a cybercriminal takes control of your files by encrypting them and forcing you to pay to get them back.

First the computer gets infected through a virus or malware installed on the system. Often these get installed because a user is tricked to click an unsecured link or add unauthorized software on their system outside the security perimeter.

If infected, the cybercriminal will display a message on your computer like "Your computer files have been encrypted and are inaccessible.

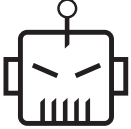
Your photos, videos, documents etc. are under our control. But don't worry, we have not deleted them yet. You have 24 hours to pay 500 USD in bitcoins". Just to show you he/she can do it, he destroys a few files and then starts exponentially destroying more and more, by the hour. Try to restart your computer and he'll destroy the hard drive; not paying within 72 hours, the same.

Experts have been working on a fix, using anti-ransomware protection through your firewall and keeping backups is preventative. Once you are hit, you can only pay up or destroy your drive and recover from an off-line backup.

**Check here to learn more about ransomware:**

[www.clavister.com/ransomware](http://www.clavister.com/ransomware)





## Botnets, Zero Days Threats

### Malicious code on your device providing access and control to 3rd party

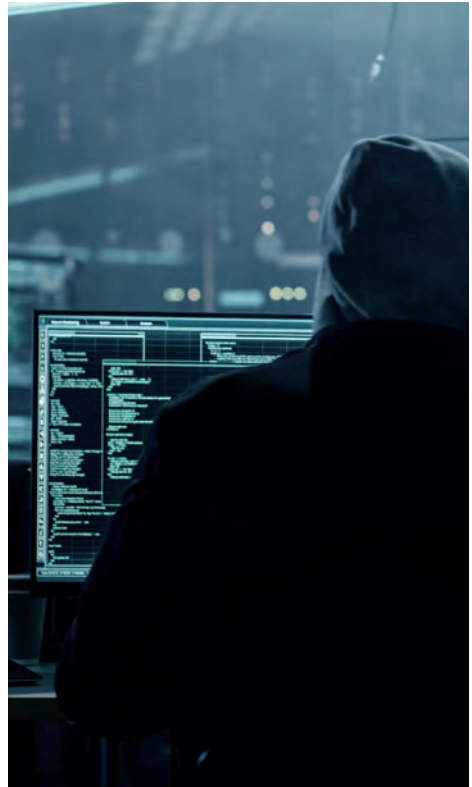
A botnet is a number of Internet-connected systems, each of which is running one or more bots.

A bot is a small program that can be controlled remotely to perform certain task—it comes from the word—"robot". Botnets are usually referred to in a negative context and can be used to perform a distributed denial-of-service attack (DDoS attack), steal data, send spam, and allows the attacker

to access the device and its connection.

For the cybercriminal, the bot is a tool to perform malicious tasks either to use local resources or function as a springboard to penetrate a network or IT system deeper.

A zero day exploit is a vulnerability unknown or newly known to the developer/vendor without an official released patch or fix. "Zero-day" or 0-day refers to the time developers got to fix it = zero days. At that point, it can be exploited before a fix becomes available and are therefore often used by cybercriminals to install sleeping bots on systems, to be used in an attack another time.



**Check here to learn more about protection  
against Botnets and Zero-Day Threats:**

[www.clavister.com/ipreputation](http://www.clavister.com/ipreputation)





## **Distributed Denial of Service Attacks**

### **Internationally targeted overload of server or network resources**

A denial-of-service attack (DoS attack) is a cyber attack in which the initiator seeks to make a service or network unavailable to its intended users. It does this either by flooding the service with requests overloading the service or network capacity or exploiting vulnerabilities in the service applications.

A Distributed DoS attacks is utilizing a wide range of sources for these requests in order to initiate a flood from all directions simultaneously.

DDoS attacks are illegal in many countries but it can be hard to identify who initiated the attack. As attack tools are becoming more

widely available and easy to use, the number of organisations that are attacked has increased dramatically.

Attacks come in many variations and therefore it requires a combination of different features to provide good protection. Defense techniques include rate limiting, traffic shaping and access control. Critical for security infrastructure is to operate in a segmented mode, meaning that if one interface get's overloaded the other interfaces do not become unaffected. In this way businesses can continue to operate their internal infrastructure utilizing backup links. Even during a live DDoS attack in progress - fully utilizing their primary internet connection.



## Slow DDoS

Not all systems overloads are intentionally created by hackers or cyber terrorists. Malfunctioning devices such as mobile phones with older operating systems or internet of things connected devices with poor connectivity implementations can send repeated requests to the same service—often at very low intervals. While this may start unnoticed with tens or even hundreds of these devices, when thousands have the same behavior this will cause problems for the server's capacity. In this scenario, patterns need to be detected in traffic to identifying malfunctioning devices. Thereafter isolate them from the rest of the traffic to avoid service degradation.



## Protection and business continuity

Clavister's products have comprehensive protection against DoS and DDoS attacks and can either be deployed as a central protection or retro-fitted into an existing network as a separate layer. Instead of costly niche products Clavister adds good protection without

significantly increasing administration and cost. Even during a massive DDoS attack targeting your public web services Clavister's multi-wan-link technologies ensure that internal business is unaffected.

**Check here to learn more about DDoS and Clavister's solutions go here:**

[www.clavister.com/ddos](http://www.clavister.com/ddos)



**“The EU General Data Protection Regulation (GDPR) has created renewed interest and will drive 65 percent of data loss prevention buying decisions today through 2018.” - Gartner Inc.**



## **General Data Protection Regulation (GDPR)**

# **The EU law on data protection and privacy**

GDPR is a regulation in EU law on data protection and privacy for all individuals within the European Union. It became enforceable on May 25 2018 and because it is a regulation, not a directive, it does not require national governments to pass any enabling legislation and is directly binding and applicable. GDPR requires adoption of improved data security practices, technology and policies for most companies. It broadly classifies personal data as any information that can be directly or indirectly attributed to an individual. GDPR instructs companies to add new procedures and processes, reporting and communication, as well as improved network security to the latest technology that provides “situational awareness of risks” and “enables preventative, corrective and mitigating action”.

The term “Situational Awareness” is central to the GDPR directives and talks about the requirements of routines and capabilities to detect if you had a breach where sensitive information might have been compromised. Data controllers are required to report a breach and data loss with 72 hours. Failure to either having adequate situational awareness or reporting within the 72 hours deadline can result in significant fines.

A critical component enabling this is Data Loss Prevention technology and Multi Factor Authentication strategies to ensure that who is logged on is authenticated and authorized and attempts to move data out of the secure perimeter is detected and alerted upon.

**Check here to learn more about GDPR and Clavister's solutions:**

[www.clavister.com/gdpr](http://www.clavister.com/gdpr)





## NIS-Directive

# The EU directive on security of network and information systems

The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU and is specifically for operator of critical infrastructure. These include digital service providers and operators of essential services including power, water heating and waste management.

## Solution

The proposal has been adopted since mid 2016. By the end of 2018 all member states must have identified operators of essential services. They are then held accountable for reporting major security incidents to incident response teams. Operators not located in the EU but still operate in the EU still face regulations. Also, when outsourcing the maintenance of their information systems to third parties, the NIS Directive still holds them accountable for any security incidents.



## Results

Security requirements include technical measures that manage the risks of cybersecurity breaches in a preventative manner. The Directive will increase the security of network and information systems within the EU and ensure protection of our society against hackers and cyberterrorist.

**Check here to learn more about the NIS-Directive and Clavister's solutions for critical infrastructures:**

[www.clavister.com/nis](http://www.clavister.com/nis)



**“Finance and Retail are the 2 largest industries suffering Distributed Denial of Service (DDoS) attacks.”**

*– Verizon 2017 Data Breach Investigations Report*



## Securing branch infrastructures Retail & Distributed Offices

A modern retailer is heavily reliant on IT in order to reach their goals of operational efficiency, lowered costs and better customer experience. Companies with many small branches or shops are often faced with the challenge of having to guarantee uninterrupted connections without local administrators in the field offices, so that the merchandise management system, SAP or the cash register system function properly. With more in-store technology like WiFi based Point-of-Sale terminals, complimentary WiFi access for customers, Smart Beacons, self-service checkouts, in-store advertisement screens and internal administrative networks, the complexity is only increasing. Although IT does a fantastic job at all these points it also leaves the companies vulnerable to security breaches that threaten their business continuity and therefore their profit.

Companies with many small branches or shops but also companies with several branches have a lot in common. You need a centrally administrable and at the same time inexpensive solution for the connection of the field offices, without having to compromise on functionality and security. This not only includes classic perimeter detection firewall functionalities, but also so-called Next Generation Firewall functions, which make it possible to regulate communication on the basis of protocols and applications with more advanced use-cases.

Solutions from Clavister offer the latest technologies and functions even in the smallest appliances. These provide an effective and cost-effective protection and optimal solution for IT security in distributed networks, always including centralised management.





**Key ingredients and use-cases that make Clavister the ideal choice for retail companies and companies with distributed offices:**

- Reliable Secure Virtual Private Networking ensures that confidential data remain private and that branch offices can communicate with each other and the headquarters in a secure way.
- Routing — Redundancy & Load Balancing making it possible to build a reliable and fault-tolerant infrastructure using low cost broadband services instead of costly leased lines.
- Network/Server Attack Protection—integrated Intrusion Detection and Prevention Systems and DDoS protection to enable protection for digital front ends—but also provide protection mechanism to ensure business continuity while such overload scenarios are in progress.
- Reports that are completely customizable and can also display the desired information graphically. Likewise, a finely scalable live monitoring via a customizable dashboard is included and ensures that, for example, VPN tunnels or Internet connections can be permanently monitored.

**Check here to learn more about Clavister's solutions for retail and distributed offices:**

[www.clavister.com/retail](http://www.clavister.com/retail)





### Securing business continuity

## Industrial Internet of Things (IoT) & Transportation

Almost all machines and industrial systems today offer the convenient option of remote maintenance and centralised analysis of collected statistics measurement data. This requires secured external access that can't be abused by unauthorised persons. At the same time accesses must also be resiliently protected in places with fluctuating environmental influences. This may be common in industrial environments when machines that are moving.

Networks should be segmented into zones to allow for different security and traffic management policies. Ensuring that access to industrial sensors is tightly controlled with limited external access. Other policies must be put in place to provide certain amount of guaranteed bandwidth to ensure highly availability. This is especially relevant when using industrial connected robots.

## Case Study: Securing the remote maintenance network in machines and plants

Whether the ship's diesel on a cruise ship is being monitored and maintained by the manufacturer or a manufacturing robot receives a software update, the remote access is indispensable in large machines nowadays. Since there's often only a narrow time window for this, besides the necessary protection against the misuse by unauthorized persons, the speed and the high availability of important points is critical. With solutions from Clavister, this can be achieved easily and cost-efficiently, while also significantly increasing the overall IT security level.



### Key ingredients that make Clavister the ideal choice for Industrial IIoT and Transportation:

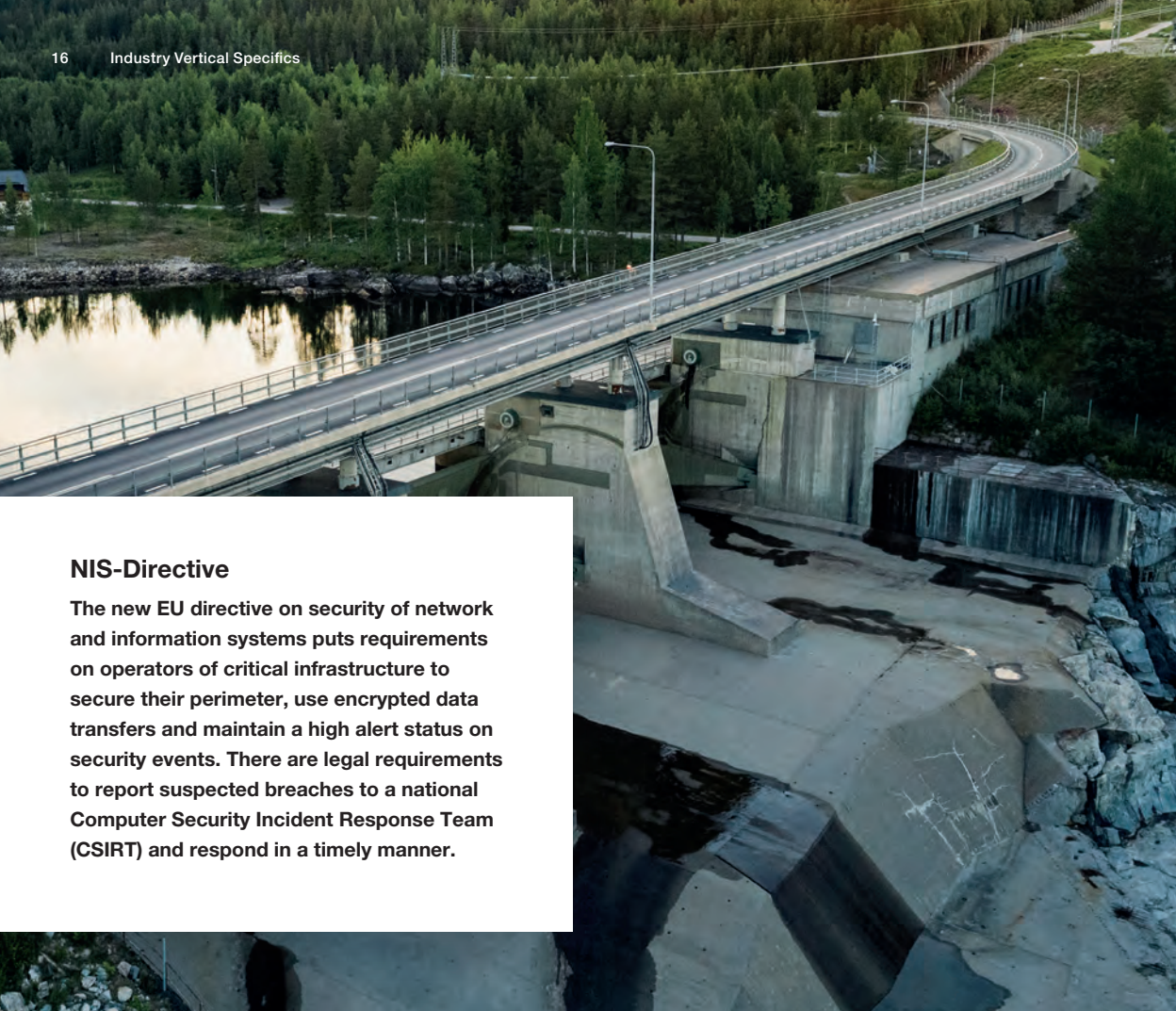
- Reliable Secure Virtual Private Networking ensures that confidential data remain private and that branch offices can communicate with each other and the headquarters in a secure way.
- Routing — Redundancy & Load Balancing making it possible to build a reliable and fault-tolerant infrastructure using low cost broadband services instead of costly leased lines.
- Secure Network Zones to allow for network segmentation and applying different security and quality policies to provide the right machines with good network resources.
- Centralised remote management empowering the IT administrator to control and see everything and actions are taken in real-time.
- The virtualised Clavister Next Generation Firewall provides all use-cases and features in an extremely small footprint, capable of being installed in practically any virtualised environment.

**Check here to learn more about Clavister's solutions for industrial IIoT & transportation:**

[www.clavister.com/iiot](http://www.clavister.com/iiot)







## NIS-Directive

The new EU directive on security of network and information systems puts requirements on operators of critical infrastructure to secure their perimeter, use encrypted data transfers and maintain a high alert status on security events. There are legal requirements to report suspected breaches to a national Computer Security Incident Response Team (CSIRT) and respond in a timely manner.



## Full compliance with a low footprint solution Critical Infrastructures

Energy suppliers, municipal utilities and grid operators have much in common — they are all operating critical infrastructure for life to function normally. This infrastructure needs a solid security infrastructure that provides full control from headquarters, allows for real-time data collection for intelligence purposes and provides secure remote access to provide control. Specific for critical infrastructures is that physical space can be scarce and a solution may need to be hosted together with other functions such as sensor data collection processes.



## Case Study: Connection of solar and wind farms

A Next Generation Firewall deployed as a direct maintenance component, for example in the turbine of a wind turbine, provides perimeter security and can limit external access from a special remote network. It can even be configured to allow access only at specific times or for a special maintenance program. In addition it can ensure and encrypt the data transmission of a complete wind farm ensuring that the data on the amount of electricity generated can easily reach the central data centre. To save physical space, the Next Generation Firewall can operate on the same infrastructure as other components — in any common virtualised environment.



### Key ingredients and use-cases that make Clavister the ideal choice for critical infrastructures:

- Fully featured next generation firewall providing a strong and resilient network perimeter protection.
- VPN with strong encryption guaranteeing that your sensitive information remains confidential
- Centralised Management and Operation ensuring that the IT Security Administrators are alerted in a timely manner about incidents and possible breaches.
- As a virtualised Next Generation Firewall, it provides all features leaving an extremely small footprint in resources. Capable of being installed in practically any virtualised environment.

**Check here to learn more about Clavister's solutions for critical infrastructure:**

[www.clavister.com/critical](http://www.clavister.com/critical)





## Central individual control with secure identification Education & Public Sector

New networking technologies like eLearning, online collaboration and devices have in many educational institutions improved the learning experience. But with these new technologies and ever-increasing numbers of devices comes the need to scale networks. At the same time providing additional security to protect sensitive systems and information. In addition, the public sector works with particularly sensitive and valuable data and with sensitive and expensive equipment that requires special protection. In public places, such as in on school property, strict

regulations may need to be applied controlling what content can be seen and internet services can be used.

Educational institutes and local governments need a flexible security solution providing them with the power to control access at a very granular level—while at the same time have full insights in what is happening when to be able to audit and backtrack on incidents.



### Case Study: WiFi in classrooms with teacher control

All students and teachers are connected to and authenticated on the school's WiFi network. Students not in class have access to the internet while teachers have the power to block access to the internet temporarily to get the students' attention for those sitting in class. Temporarily access can be provided to let the students find information about a subject or application filtering can be used to block non educational usage—like social media—for a limited period of time. The firewall secures the network and provides web content filtering policies to secure that no unwanted material is consumed on the school yard.

#### Key ingredients and use-cases that make Clavister the ideal choice for schools and the public sector:

- Identity awareness functions transparently integrated to any connected network, enables individual and group based policies on the WiFi network.
- Web content and application identification empowers teachers to steer how time is used.
- Centralised management and role based access providing teachers with the tools to control the internet access in the classroom.



**Check here to learn more about Clavister's solutions for education and public sector:**

[www.clavister.com/schools](http://www.clavister.com/schools)





## Secure cloud utilizing minimal resources Managed Security Service Provider

Because of the criticality and increased complexity of the security infrastructure an increasing number of enterprises chooses to outsource the operations and maintenance to a 3rd party. System integrators and local resellers are innovating their offerings to provide security as a managed services.

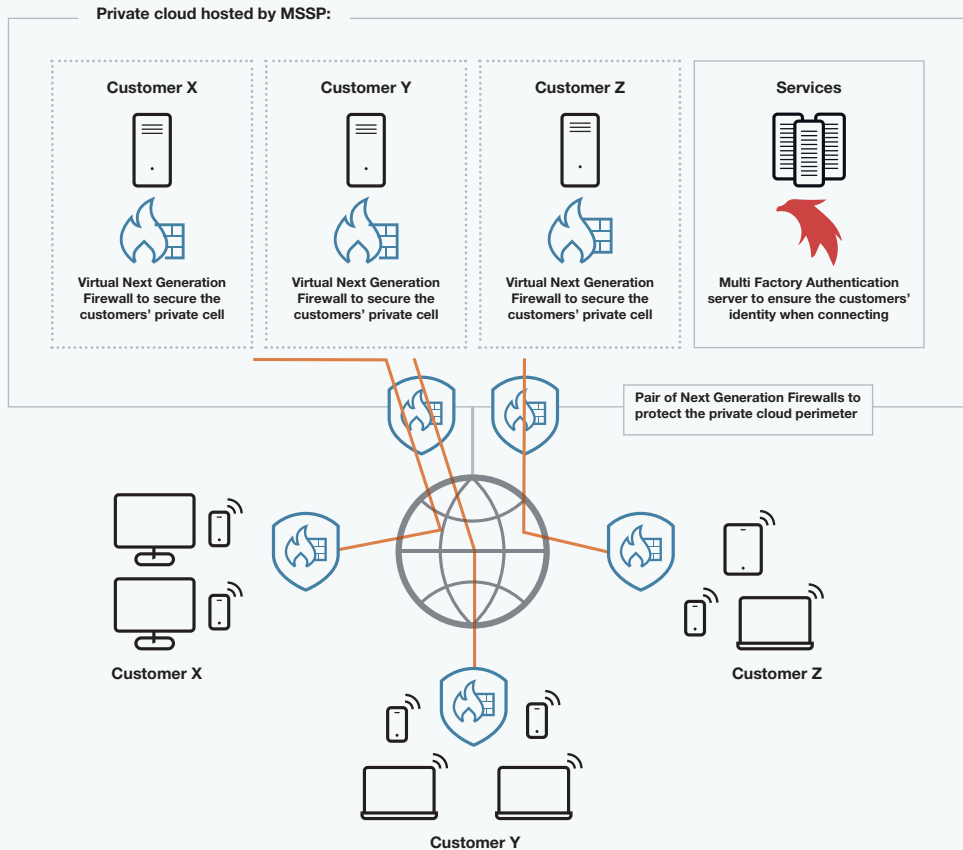
Clavister's solutions are ideal for use by Managed Security Services Providers (MSSP) and can be offered in combination with other hosted services. This is because the software is available both in appliance as well as virtualised format and can be used in the datacentre protecting the cloud resources as well as on premises.



### Case Study: Micro-Segmentation using Secure Virtual Cells

IT Services such as Remote Desktop, Backup and Fileserver are offered by the service provider to small and medium enterprises. The services are produced in dedicated virtual machines hosted in a private cloud environment. The cloud infrastructure is protected by a dedicated pair of Next Generation Firewalls performing perimeter protection while the customer's virtual machines are each protected by dedicated virtualised Next Generation Firewalls. A secure SD-WAN is setup to connect the customers network directly with the virtual machines providing a virtual secure cell with end-to-end security and full privacy of data.





### Key ingredients that make Clavister the ideal choice for Managed Security Service Providers:

- As a virtualised Next Generation Firewall, it provides all features with an extremely small footprint in resources. Capable of being installed in practically any virtualised environment.
- Centralised management with multitenancy support enabling large deployments for multiple customers to be managed holistically and efficiently (thousands of virtual images).

**Check here to learn more about Clavister's MSSP solutions:**

[www.clavister.com/mssp](http://www.clavister.com/mssp)









## Next Generation Firewalls — appliances and virtual for cloud

### Product portfolio

Clavister provides a full range of appliances from desktop models for small offices to rack mountable models for server rooms for medium enterprises. Datacenter models for larger enterprises and service providers include redundant & hot-swappable power supplies and support a range of interface modules that enables you to customize port configuration. The use-cases are available on all platforms including the virtualised software that runs on all modern hypervisors and can be used to secure the perimeter of your virtual machines as well.

clavister		 Desktop	 Server Room	 Data Center	 Virtual – Cloud
Model		E10 – E80	W20 – W30	W40 – W50	V2 – V10
Capacity	Firewall	1 – 4 Gbps	4 – 10 Gbps	10 – 55 Gbps	300 Mbps – 10 Gbps*
	VPN	100 Mbps – 1 Gbps	1 – 2 Gbps	2 – 8 Gbps	150 Mbps – 5 Gbps*
Interfaces		4-6 x 1GbE	6 – 9 1GigE W30 supports a interface module	8 GigE or 4 x 10GbE per interface modules	3 – 10 interfaces supported
Supported Hypervisors		n/a			VMware vSphere, KVM, Microsoft Hyper-V, OpenStack
Resource Requirements		n/a			256 MB – 4 GB or RAM, 256 MB storage, 1 vCPU
High Availability		Optional	Active-Passive, Active-Active and Active-Passive-Active		Yes
Estimated number of users		10 - 25	100 - 200	n/a	n/a
Technologies		All platforms include support for Universal Treat Management (UTM) and Next Generation Firewall (NGFW) technologies including IDS/IPS, Antivirus, Anti-Spam, IP Reputation, Geo Fencing, Application Control/DPI and Web Content Filtering – depending on support subscription type.			
Use Cases		All	All	All	All

\* Actual performance depends on host/server-hardware, hypervisor and similar.



## Configuration management and operations software

### Holistic end-to-end control



The Clavister Next Generation Firewalls provide multiple interfaces for configuration and management. A modern Web GUI with wizards for quick setup is included, but also direct CLI access and APIs for configuration automation are available.

Included with the license for the software is a central administration software that can be used for all installed security gateways called InControl. All methods allow the administrator to make changes during operation without interrupting connections. The generated reports are completely customizable

and can also display the desired information graphically. Likewise, a finely scalable live monitoring via a customizable dashboard is included and ensures that, for example, VPN tunnels or Internet connections can be permanently monitored.

Of course, Clavister solutions can also be integrated into existing monitoring, such as Nagios-based systems. The logs can also be used for further evaluation on alternative platforms such as syslog or Splunk. The necessary settings can be easily and conveniently made.

**Check here to learn more about Clavister's product portfolio:**

[www.clavister.com/product-models](http://www.clavister.com/product-models)



## Network automation opportunity

In a fast moving world where new threats occur on an hourly or more frequent basis IT administrators need to constantly be on their guard to protect the company's digital assets.

The increase in the number of connected internet — of things devices — also in corporate networks— further drives the need to respond quickly.

In order to facilitate this cost efficiently advanced technologies including machine learning and artificial intelligence are required to see patterns, detect deviations and alert about abnormalities. Clavister doesn't stop there — the solution shall take automated action where appropriate in order to neutralize a threat before it impacts your business.

You do not need to become a security expert — the Clavister self learning solution will protect you 24/7.

