clavister

CyberArmour

MILITARY-GRADE AI-POWERED NEXT-GENERATION FIREWALLS FOR DEFENCE APPLICATIONS

SECURITY BY SWEDEN

clavister

CyberArmour

TABLE OF CONTENTS

COMMON CRITERIA CERTIFIED EAL4+

QUALITY SYSTEM CERTIFICATION DNV ISO 9001

SOFF Säkerhets- och försvarsföretagen

SECURITY BY SWEDEN

Military-grade AI-powered Next-Generation Firewalls

FOR DEFENCE APPLICATIONS

In an era of escalating conflicts and geopolitical tensions, digital warfare has become an integral part of the modern battlefield. Challenges that were once countered with thicker armor now demand advanced cybersecurity solutions.

The Clavister CyberArmour product family offers state-of-the-art, AI-driven protection tailored for military applications. Designed to secure vehicles and tactical communications, it ensures operational resilience and mission success.

intel Network Builders

CYBERSECURITY MADE IN EUROPE

Defense Innovation Sweden

SECURITY BY SWEDEN

There is an Ongoing Cyberwar

A cyberwar is raging alongside armed conflicts worldwide, operating in the shadows. As military platforms and weapon systems become increasingly digital and interconnected, they are exposed to a growing range of cyberthreats that could compromise their effectiveness and security.

The sophistication and the amount of cyberattacks on defence platforms is increasing by the day. Here are a few real-world examples that illustrate the severe consequences of successful attacks:

North Korean Hackers Target South Korean Military
In mid-2024, North Korean hackers allegedly infiltrated South Korea's defence networks, stealing sensitive data on key military assets. Technical specifications and operational details of the K2 Black Panther tank were compromised, potentially undermining the tank's battlefield effectiveness. In addition, information on the Baekdu and Geumgang reconnaissance aircraft, crucial for monitoring North Korean activities, was exfiltrated.

GPS Jamming and Spoofing in Eastern Europe
Between 2022 and 2024, incidents of GPS signal interference, suspected to be orchestrated by Russian actors, increased in Eastern Europe. NATO military drills experienced navigation disruptions, potentially compromising operational readiness and safety. The jamming also affected civilian aviation and maritime operations, highlighting vulnerabilities in navigation systems used by both military and civilian platforms.

Ukrainian Artillery App Compromise
In 2016, Russian hackers, identified as the group Fancy Bear, distributed a malicious version of an Android application used by Ukrainian artillery units. This malware, known as X-Agent, infiltrated the app designed to improve the efficiency of D-30 howitzer operations. The compromised app reportedly transmitted the artillery units' locations to Russian forces, leading to significant losses.

"The next Pearl Harbor may not come as bombs destroying ships, but as keystrokes and hidden malware idling a fleet in home port or already at sea."

US DEPARTMENT OF DEFENSE, JANUARY 2022

BATTLE PROVEN CYBERPROTECTION

Clavister's technology protects a variety of military platforms, weapon systems and tactical communication systems which are in operation across multiple NATO countries and has been proven in battle.

WEAPON SYSTEMS

There are examples of successful air raids where the opponent's air defence system was rendered blind through cyberattacks. To mitigate this threat and ensure a fully operational air defence, Clavister protects multiple types of advanced air defence systems across Europe.

ARMOURED VEHICLES

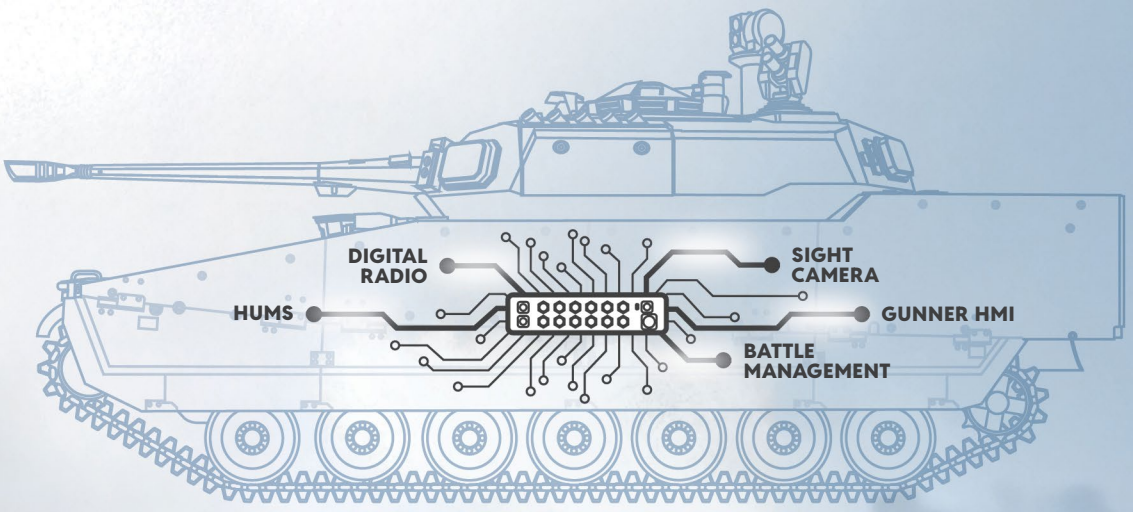
The CV90 infantry fighting vehicle from BAE Systems is a highly digitalised combat vehicle, where a cyberattack could have caused the vehicle to malfunction and in worst case lead to fatalities on the battlefield. Close to 1,000 vehicles of the CV90 family, in operation and production, are protected by Clavister CyberArmour.

TACTICAL COMMUNICATION

Thales SOTAS is a leading military vehicle communication and data network solution in use across many countries and vehicle types. With the introduction of the server node opening for more applications and 3pp components such as sensors, the need for more advanced cyberprotection is high. Clavister CyberArmour in the SOTAS system can detect and block cyberattacks in real time.

A CLAVISTER SOLUTION

Cyberprotection for Military Platforms



Hardening and extensive testing do not guarantee protection. Always assume that a cyberattack is possible – but ensure you can detect it, withstand it, and continue operating to fulfill your military mission.

Clavister CyberArmour protects military platforms, such as armoured vehicles and ships, against cyberattacks. This continuously evolving solution adapts to emerging cyber-risks, maintaining a high level of protection through a multitude of threat prevention capabilities. CyberArmour can be integrated from the start or incorporated into upgrade and modernisation programs, with hardware tailored and optimised for military environments.

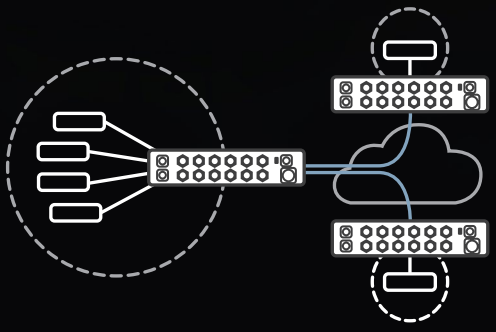
A CLAVISTER SOLUTION

Securing Tactical IT Systems

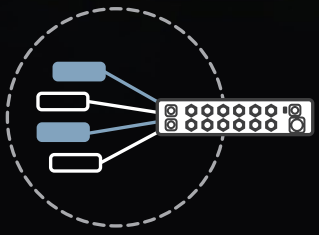
With increased digitalisation, tactical IT infrastructure and networks are expanding, introducing new types of vulnerabilities. Enhancing cybersecurity is crucial for tactical communication, battle management systems, sensors, counter-UAS solutions, and other mission-critical technologies.

Clavister provides military-grade firewalls that strengthen the cybersecurity of both new and existing systems. These firewalls enhance protection for tactical communication solutions through advanced firewalling, encrypted communication (VPN), and AI-powered intrusion detection.

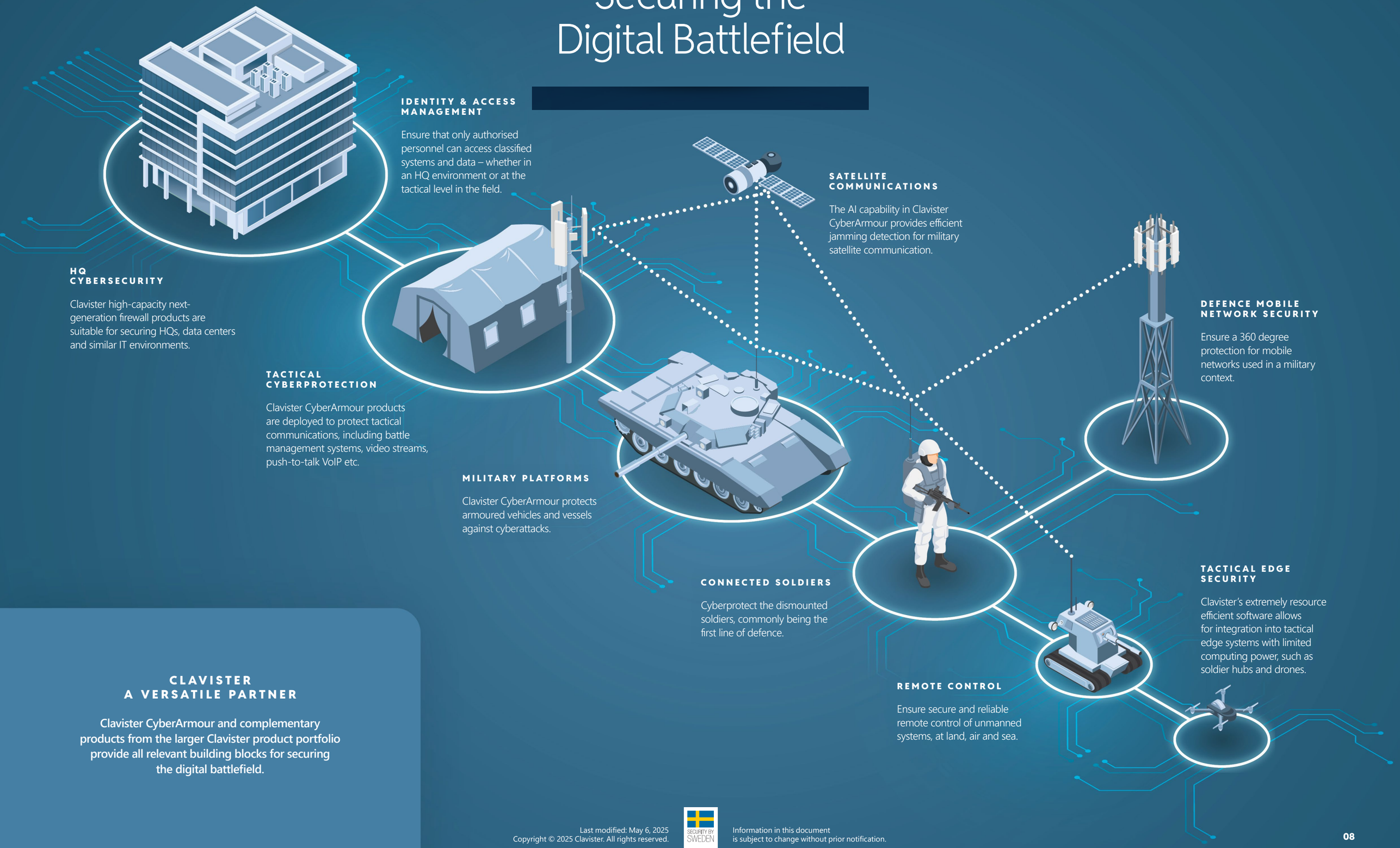
PROTECTING SYSTEMS FROM EXTERNAL THREATS



REDUCING RISK BY SEGMENTING COMMUNICATION



Securing the Digital Battlefield



HQ CYBERSECURITY

Clavister high-capacity next-generation firewall products are suitable for securing HQs, data centers and similar IT environments.

IDENTITY & ACCESS MANAGEMENT

Ensure that only authorised personnel can access classified systems and data – whether in an HQ environment or at the tactical level in the field.

TACTICAL CYBERPROTECTION

Clavister CyberArmour products are deployed to protect tactical communications, including battle management systems, video streams, push-to-talk VoIP etc.

SATELLITE COMMUNICATIONS

The AI capability in Clavister CyberArmour provides efficient jamming detection for military satellite communication.

DEFENCE MOBILE NETWORK SECURITY

Ensure a 360 degree protection for mobile networks used in a military context.

MILITARY PLATFORMS

Clavister CyberArmour protects armoured vehicles and vessels against cyberattacks.

CONNECTED SOLDIERS

Cyberprotect the dismounted soldiers, commonly being the first line of defence.

TACTICAL EDGE SECURITY

Clavister's extremely resource efficient software allows for integration into tactical edge systems with limited computing power, such as soldier hubs and drones.

REMOTE CONTROL

Ensure secure and reliable remote control of unmanned systems, at land, air and sea.

CLAVISTER A VERSATILE PARTNER

Clavister CyberArmour and complementary products from the larger Clavister product portfolio provide all relevant building blocks for securing the digital battlefield.

Product Highlights

SECURITY BY DESIGN

We believe we offer the most robust cybersecurity solutions ever built. We build on 25 years of security track record – the result of a proven secure development lifecycle. The result? Record-few vulnerabilities and unparalleled uptime.

THE SWISS ARMY KNIFE OF ROUTING

With incredibly flexible routing capabilities, Clavister CyberArmour is designed to support the most complex network setups.

ALWAYS-UP PHILOSOPHY

Through a vast range of health monitors, balancing and fail-over methods, network traffic is guaranteed to reach its destination at all times.

VIRTUAL & DYNAMIC ROUTING

Deploy multiple virtual routers with powerful policy flows. Dynamic routing protocols ensure interoperability with existing network equipment.

APPLICATION-BASED ROUTING

Efficient routing-decisions made by identification of applications. Allow mission-critical application to use the best routes available.

AI-BASED THREAT DETECTION

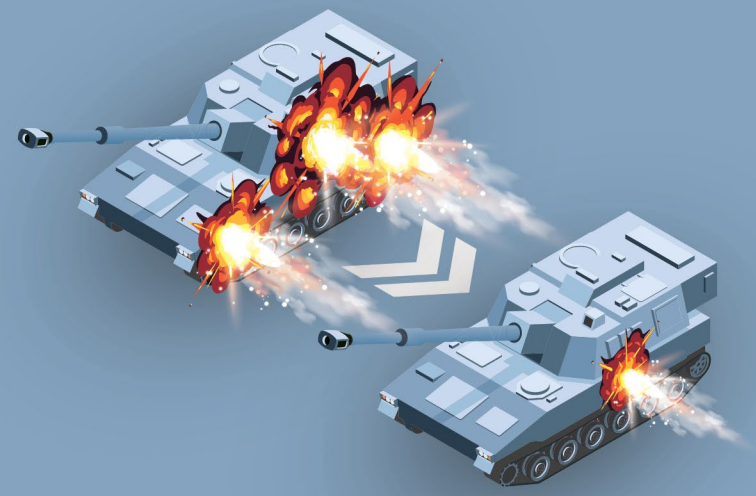
Clavister AI capability, the result of years of scientific research, provides instant on-device anomaly detection. Without any cloud dependency, the privacy and confidentiality of your data are preserved.

<15 min	No	Instant
ON-DEVICE TRAINING	CLOUD PROCESSING	ANOMALY DETECTION

NETWORK SEGMENTATION

A fundamental capability of Clavister CyberArmour is the ability to create proper segmentations of networks.

By restricting access between network segments, the blast radius is significantly reduced in the event of a cyberattack.



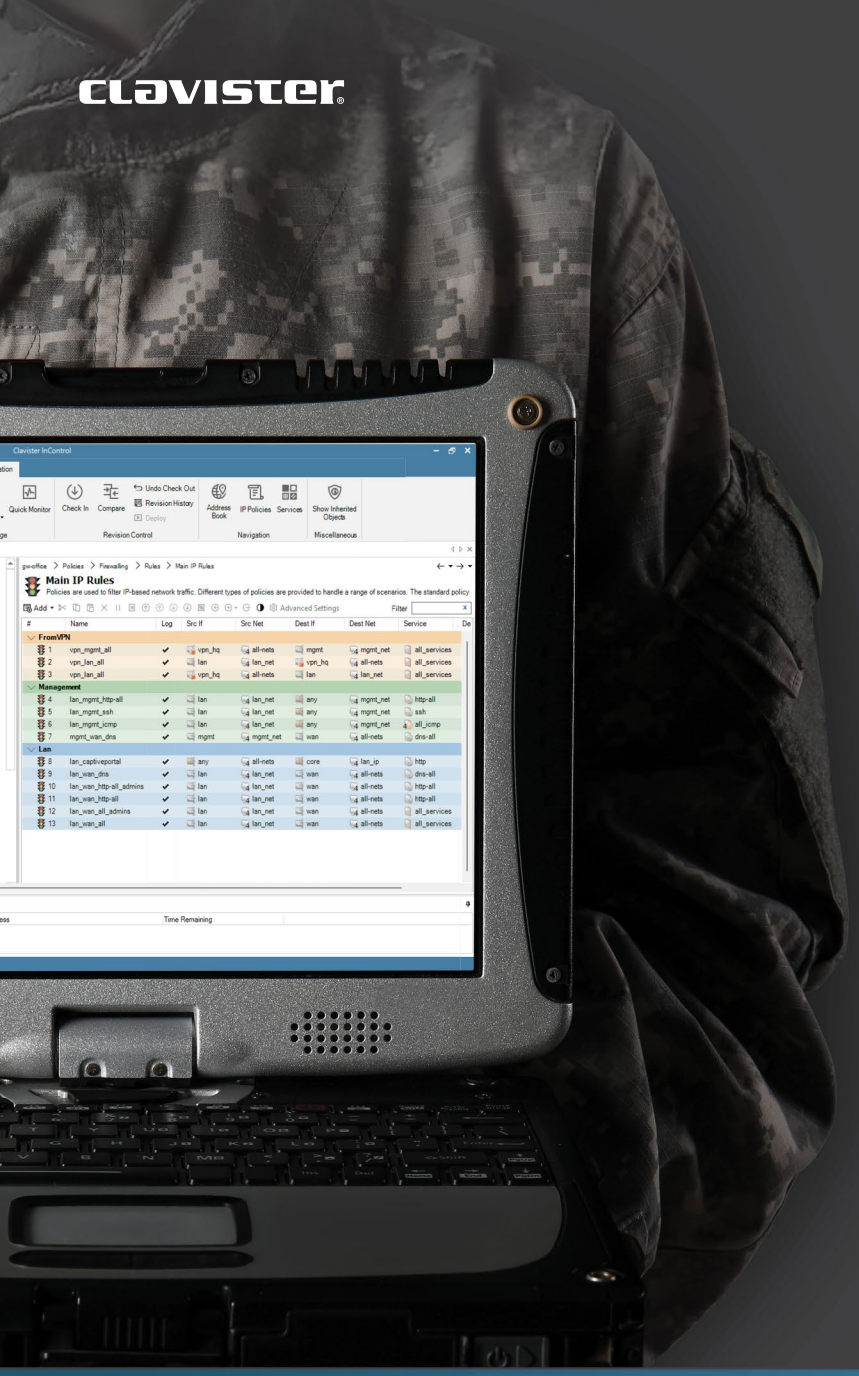
MILITARY-GRADE DESIGN

The products in the Clavister CyberArmour product family are designed to withstand the most harsh conditions.

Compliance with MIL-STD-810 and similar standards ensures operational resilience at all times.

ACTIONABLE SECURITY ANALYTICS

Clavister CyberArmour integrates seamlessly with Clavister's powerful security analytics capabilities. A single pane of glass console provides clear, actionable, and comprehensive evaluation of your operation's cybersecurity readiness. Through a blend of sophisticated algorithms and real-time insights, the system pinpoints vulnerabilities, prioritises risks, and offers tailored recommendations to keep your operations secure.



CENTRAL MANAGEMENT AND CONTROL

The Clavister InControl centralised management console provides for easy and efficient management of Clavister CyberArmour products, even for large networks.

Its intuitive interface simplifies administration through features like zero-touch deployment, shared policy sets, and scheduled firmware updates to simplify day-to-day tasks.

With tools for firewall configuration, troubleshooting, firewall backups, and remote access, Clavister InControl is designed to save time and reduce complexity while keeping your network running smoothly.

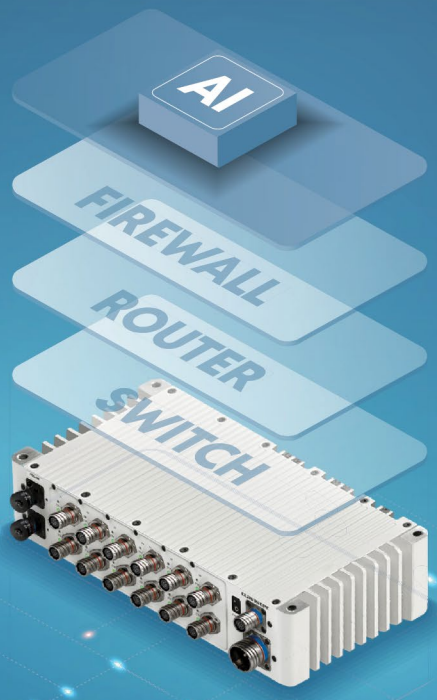
Through a granular role and permission structure, Clavister InControl integrates well with your security policy framework.

Full REVISION CONTROL | **Zero Touch** DEPLOYMENT | **Batch** FIRMWARE UPGRADES

COMPLETE COMMUNICATION HUB

The products in the Clavister CyberArmour product family are highly versatile and capable of acting as complete communication hubs in a defence platform or system.

From high-capacity Ethernet switching, through advanced IP routing and full Next-Generation Firewall capabilities, all the way to AI-based threat protection – Clavister CyberArmour can literally assume all roles in a communication network.



DEEP PROTOCOL AND APPLICATION AWARENESS

In-depth recognition, inspection and control of several thousands of protocols and applications allow for the most powerful and granular enforcement of security policies.

SELECTED CAPABILITIES

Detect and block stealth communication over common protocols.

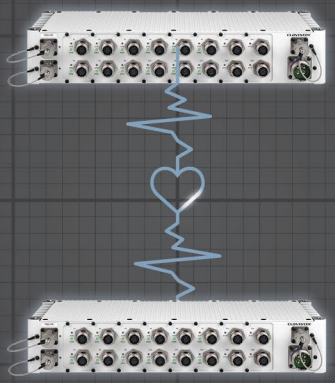
Ensure consistent quality-of-service with effective bandwidth management.

Extensive logging for analytics and auditing.

Inspection of, and policies for, granular application attributes.

Apply routing decisions to achieve local internet break-out scenarios.

4,500+
IDENTIFIED APPLICATIONS AND PROTOCOLS



HIGHLY RESILIENT

Network communication in a tactical environment is highly mission-critical. That is why Clavister CyberArmour is built to provide the highest level of resiliency. Through our state-of-the-art high availability capability, seamless switch-over to a secondary device happens within milliseconds, without any interruption of traffic. Extensive health checks, not only on the Clavister CyberArmour product itself but also on links, routes, gateways and even third-party hosts, cater for prompt resolution in case of degradation.

~750 ms
TYPICAL FAIL-OVER TIME

RELIABLE VPN WITH QUANTUM-RESISTANT* ENCRYPTION

Clavister CyberArmour delivers reliable and secure site-to-site VPN capabilities, providing encrypted data transmission across networks.

Using the strongest available encryption standards, privacy, integrity and authenticity of sensitive information in transit is maintained at all times.

** Available in upcoming software release.*

QUALITY OF SERVICE

The advanced quality-of-service capabilities in Clavister CyberArmour ensures optimised bandwidth usage, enabling smoother network performance even during peak loads.

With granular control and intelligent traffic prioritisation, critical communication is secured while maintaining consistent service quality across the full infrastructure.

THREAT PREVENTION

Clavister CyberArmour employs a wide array of sophisticated threat prevention capabilities, all seamlessly integrated with each other, working in concert to provide the most efficient mitigation for a vast range of cyberattacks.

SUPPLY CHAIN ATTACKS

Rogue actors can attack systems by infecting components from vendors further down the supply chain. The cyberattack stays dormant until the system is used on the war theatre, exposing the users to lethal risks. Clavister CyberArmour actively monitors communication and detects and blocks anomalies before they cause an incident.

REMOTE HIJACKING

In times of autonomous and remote controlled defence platforms, adversaries gaining unauthorised control poses a significant battlefield threat. Clavister CyberArmour safeguards communication with the strongest encryption standards and ensures access is granted exclusively to legitimate users through multi-layered authentication schemes.

UNAUTHORISED ACCESS

Defense systems and platforms require strict access control to subsystems and data to prevent unauthorised control or manipulation of high-risk system components. Clavister CyberArmour employs a comprehensive range of segmentation and authentication capabilities to enforce robust access policies effectively.

VULNERABILITIES AND EXPLOITS

Hackers commonly abuse poorly written software – both on an application and operating system level – to gain unauthorised access to systems, or to simply cause disruptions. Clavister CyberArmour detects and automatically blocks attempts to exploit known vulnerabilities.

DENIAL-OF-SERVICE (DoS)

A DoS cyberattack aims at disrupting the normal functioning of a network by overwhelming it with a flood of malicious traffic. The goal is to make the targeted resource unavailable, causing downtime, inconvenience, and/or financial loss. Clavister CyberArmour reduces the impact of DoS attacks using a combination of mitigation technologies.

VIRUSES AND OTHER MALWARE

Malware, such as viruses, worms, ransomware and trojans, pose a constant threat to all organisations and can be extremely costly to address once they have gained foothold and begun spreading within a network. Clavister CyberArmour restricts access to websites known for hosting malware, and can furthermore detect malware in transit to reduce the risk of infection.

THE HUMAN FACTOR

Even trusted users can inadvertently introduce malicious content through seemingly harmless activities. Clavister CyberArmour mitigates this risk by restricting communication to a carefully controlled set of subsystems, permitting only safe protocols, applications, and content.

clavister

CyberArmour

RSG-200

FIREWALL

DIMENSIONS & POWER	
Form Factor	Rugged
Dimensions *(H x W x D)*	67.5 x 140 x 205 mm (2.66 x 5.51 x 8.07 in)
Hardware Weight	1.9 kg (4.19 lb)
Volume	1.94 l
System Typical Power Consumption	<15 W
Power Supply *(DC)*	16 to 36V DC

INTERFACES & MODULES	
Ethernet Interfaces	2 x 10/100/1000 Base-T (MIL-DTL-38999)
Switch	N/A
Power Delivery Ports	N/A
Console Port	1x Serial Console – RS232
Number of Expansion Slots	Four (4)

OPERATING ENVIRONMENT & CERTIFICATIONS	
Safety	EN 62368-1
EMC	MIL-STD-461F
Environmental	IP 67
Operating and Storage Humidity	Operates at full performance under high humidity conditions in accordance with DO-160, tested up to 95% RH at 65°C and 85% RH at 38°C
Cooling	Passive cooling, no moving parts
Operating Temperature	-40°C to 71°C (-40°F to 159°F)
Designed to meet MIL-STD-810	Yes
Designed to meet MIL-STD-461F	Yes
Designed to meet MIL-STD-1275	Yes

SYSTEM PERFORMANCE & CAPACITY	
Firewall Throughput[1] *(1518 / 512 / 64 byte, UDP)*	2 / 2 / 0.441 Gbps
Firewall Throughput[1] *(Packets per Second)*	742 Kpps
Concurrent Connections	128,000
IPsec VPN Throughput[2] *(1420 / 512 / 64 byte, UDP)*	300 / 180 / 42 Mbps
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	100
OneConnect VPN Tunnels	100
VLANs	128
Virtual Routers	10

[1] Firewall Throughput tested according to RFC2544 [2] IPsec VPN performance test uses AES-CGM-128 ICV16

SECURITY BY SWEDEN

RSG-400

FIREWALL

DIMENSIONS & POWER	
Form Factor	Rugged
Dimensions *(H x W x D)*	88 x 390 x 193 mm (3.46 x 15.35 x 7.6 in)
Hardware Weight	6 kg (13.3 lb)
Volume	6 l
System Typical Power Consumption	36 W
Power Supply *(DC)*	16 to 32V DC
System Maximum Current Rating *(Power Delivery Ports)*	40 A
Hot-swappable Power Supplies	1,440 W

INTERFACES & MODULES	
Ethernet Interfaces	2 x 10GBase-KR internal to Switch
Switch	12 x 1000Base-T 2 x 10GBase-LR (D38999)
Power Delivery Ports	12 x 1GbE (D38999) (X1-X12)
Console Port	3x Serial Console – RS232 (Service, Firewall and Switch)

OPERATING ENVIRONMENT & CERTIFICATIONS	
Safety	EN62368-1
EMC	MIL-STD-461G
Environmental	IP 65
Operating and Storage Humidity	Operate at full performance under high humidity conditions in accordance with AECTP 230, A1 through C2
Cooling	Passive cooling, no moving parts
Operating Temperature	-40°C to 65°C (-41°F to 149°F)
Designed to meet MIL-STD-810G	Yes
Designed to meet MIL-STD-461G	Yes
Designed to meet MIL-STD-1275E/1275F	Yes

SYSTEM PERFORMANCE & CAPACITY	
Firewall Throughput[1] *(1518 / 512 / 64 byte, UDP)*	5 / 4.8 / 0.6 Gbps
Firewall Throughput[1] *(Packets per Second)*	1.2 Mpps
Concurrent Connections	128,000
IPsec VPN Throughput[2] *(1420 / 512 / 64 byte, UDP)*	1 / 1 / 0.2 Gbps
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	25
OneConnect VPN Tunnels	25
VLANs	128
Virtual Routers	50

[1] Firewall Throughput tested according to RFC2544 [2] IPsec VPN performance test uses AES-CGM-128 ICV16

RSW-400

SWITCH

DIMENSIONS & POWER	
Form Factor	Rugged
Dimensions *(H x W x D)*	88 x 390 x 193 mm (3.46 x 15.35 x 7.6 in)
Hardware Weight	6 kg (13.3 lb)
Volume	6 l
System Typical Power Consumption	36 W
Power Supply *(DC)*	16 to 32V DC
System Maximum Current Rating *(Power Delivery Ports)*	40 A
Hot-swappable Power Supplies	1,440 W

INTERFACES & MODULES	
Ethernet Interfaces	N/A
Switch	12 x 1000Base-T 2 x 10GBase-LR (D38999)
Power Delivery Ports	12 x 1GbE (D38999) (X1-X12)
Console Port	3x Serial Console – RS232 (Service, Firewall and Switch)

OPERATING ENVIRONMENT & CERTIFICATIONS	
Safety	EN62368-1
EMC	MIL-STD-461G
Environmental	IP 65
Operating and Storage Humidity	Operate at full performance under high humidity conditions in accordance with AECTP 230, A1 through C2
Cooling	Passive cooling, no moving parts
Operating Temperature	-40°C to 65°C (-41°F to 149°F)
Designed to meet MIL-STD-810G	Yes
Designed to meet MIL-STD-461G	Yes
Designed to meet MIL-STD-1275E/1275F	Yes

SYSTEM PERFORMANCE & CAPACITY	
Firewall Throughput *(1518 / 512 / 64 byte, UDP)*	N/A
Firewall Throughput *(Packets per Second)*	N/A
Concurrent Connections	N/A
IPsec VPN Throughput *(1420 / 512 / 64 byte, UDP)*	N/A
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	N/A
OneConnect VPN Tunnels	N/A
VLANs	N/A
Virtual Routers	N/A

RSG-500

FIREWALL

DIMENSIONS & POWER	
Form Factor	Rugged
Dimensions *(H x W x D)*	88 x 470 x 193 mm (3.46 x 18.5 x 7.6 in)
Hardware Weight	7.2 kg (15.9 lb)
Volume	8 l
System Typical Power Consumption	38 W
Power Supply *(DC)*	16 to 32V DC
System Maximum Current Rating *(Power Delivery Ports)*	40 A
Hot-swappable Power Supplies	1,440 W

INTERFACES & MODULES	
Ethernet Interfaces	2 x 10GBase-KR internal to Switch
Switch	16 x 1000Base-T 2 x 10GBase-LR (D38999)
Power Delivery Ports	12 x 1GbE (D38999) (X1-X12)
Console Port	3x Serial Console – RS232 (Service, Firewall and Switch)

OPERATING ENVIRONMENT & CERTIFICATIONS	
Safety	EN62368-1
EMC	MIL-STD-461G
Environmental	IP 67
Operating and Storage Humidity	Operate at full performance under high humidity conditions in accordance with AECTP 230, A1 through C2
Cooling	Passive cooling, no moving parts
Operating Temperature	-40°C to 65°C (-41°F to 149°F)
Designed to meet MIL-STD-810G	Yes
Designed to meet MIL-STD-461G	Yes
Designed to meet MIL-STD-1275E/1275F	Yes

SYSTEM PERFORMANCE & CAPACITY	
Firewall Throughput[1] *(1518 / 512 / 64 byte, UDP)*	10 / 4.8 / 0.6 Gbps
Firewall Throughput[1] *(Packets per Second)*	1.2 Mpps
Concurrent Connections	128,000
IPsec VPN Throughput[2] *(1420 / 512 / 64 byte, UDP)*	2 / 1.2 / 0.2 Gbps
Gateway-to-Gateway or Roaming IPsec VPN Tunnels	100
OneConnect VPN Tunnels	100
VLANs	256
Virtual Routers	50

[1] Firewall Throughput tested according to RFC2544 [2] IPsec VPN performance test uses AES-CGM-128 ICV16

Technical Specifications

FIREWALL	
Stateful Firewall / Deep Packet Inspection	Yes / Yes
IP Policies	ALLOW, DROP and REJECT
Security Zones	Yes
Multiple IP Rule-sets	Yes
User- and Group-based Filter in Policies	Yes
Time- and Date-based Scheduled Policies	Yes
DoS and DDoS Detection and Prevention	Yes
Threshold Rules (Connection Count and Rate Limits) for IPv4	Yes
IP Blacklisting / Whitelisting for IPv4	Yes / Yes
TCP Sequence Number Tracking	Yes
FQDN- and Wildcard FQDN Address Filter in IP Policies	Yes
IP Geolocation Filter in IP Policies	Yes
DOS Protection based on IP Geolocation Filter for IPv4	Yes
Ingress Filtering / IP Spoofing Protection	
Access Rules	Yes
Strict Reverse Path Forwarding (RPF)	Yes
Feasible RPF by using Interface Equivalence	Yes
Address and Port Translation for IPv4	
Policy-Based	Yes
Dynamic NAT (Source)	Yes
Symmetric NAT	Yes
NAT Pools	Yes
Static Source Translation	Yes
Static Destination Translation (Virtual IP/ Port forward)	Yes
NAT Hairpinning	Yes
Reverse Proxy for IPv4	
Protocol	HTTP, HTTPS
IP Blacklisting	Yes

SERVER LOAD BALANCING (SLB) FOR IPv4	
SLB Distribution Methods	Round-Robin, Connection-Rate, Strict, Server Resource-Usage over REST API
SLB Monitoring Methods	ICMP Echo, Custom TCP Port, HTTP Request/Response
SLB Server Stickiness	State, IP Address, Network
SLB Maintenance Mode	Yes
SLB Server Fallback	Yes

CONNECTIVITY	
Ethernet Interfaces	1GbE, 2.5GbE, 10GbE, 25GbE, 40GbE
Link Aggregation IEEE 802.1AX-2008 (Static / LACP)	Yes
VLAN Interfaces IEEE 802.1Q	Yes
Service-VLAN Interfaces IEEE 802.1ad (Q-in-Q)	Yes

Disclaimer: This is a general overview of all the features, for an updated feature list always refer to the latest CyberArmour documentation for your product

MODES OF OPERATIONS	
Transparent Mode (Layer 2)	Yes
Routing Mode (Layer 3)	Yes
Mixed Transparent and Routing Mode	Yes

ROUTING	
Static Routing	Yes
Policy-Based Routing (PBR)	Yes
Scheduled Policy-Based Routing	Yes
Virtual Routing	Yes
Multiple Routing Tables	Yes
Loopback Interfaces	Yes
Route Load Balancing (Equal-Cost Multipath)	Yes
Route Failover	Yes
Route Monitoring Methods	ARP, ICMP Echo, Custom TCP Port, HTTP Request / Response
Source-Based Routing	Yes
Path MTU Discovery	Yes
Dynamic Routing	
Policy-Based Dynamic Routes	Yes
OSPFv2 Routing Process (RFC2328)	Yes, Multiple
OSPFv2 RFC1583 Compatibility Mode	Yes
OSPFv2 over VPN	Yes
Application-based Routing	
Routing based on application	Yes
Multicast for IPv4	
Multicast Forwarding	Yes
IGMPv2 Compatibility Mode (RFC2236)	Yes
IGMPv3 (RFC3376)	Yes
IGMP Proxy Mode	Yes
IGMP Snoop Mode	Yes
Transparent Mode (L2 Bridge Mode)	
Policy-Based	Yes
MPLS Pass-through	Yes
DHCP Pass-through	Yes
Layer 2 Pass-through of Non-IP Protocols	Yes
Spanning Tree BPDU Relaying	Normal (STP), Rapid (RSTP), Multiple (MSTP), Per VLAN Spanning Tree Plus (PVST+)

INTERFACE IP ADDRESS ASSIGNMENT	
Static IPv4 Address Assignment	Yes
Static IPv6 Address Assignment	Yes
DHCPv4 Client	Ethernet, VLAN, Link-Aggregation
DHCPv6 Client	Ethernet, VLAN, Link-Aggregation
IPv6 Prefix Delegation	Ethernet, VLAN, Link-Aggregation
PPPoE IPv4 Client	Ethernet, VLAN, Link-Aggregation
PPPoE IPv6 Client	Ethernet, VLAN, Link-Aggregation
Stateless IPv6 Address Auto-configuration	Yes
IPv6 Router Solicitation	Yes
PPTP / L2TP IPv4 Client	Yes

SPECIFIC IPv6 PROTOCOL FEATURES	
IPv6 Ready Certification	Core Protocols, Phase-2 Router
Neighbor Discovery	Yes
Proxy Neighbor Discovery	Yes
IPv6 Router Advertisement	Yes

NETWORK SERVICES	
DHCPv4 Server	Yes, Multiple
DHCPv4 Server Custom Options	Yes
DHCPv4 Relay	Yes, Multiple
DHCPv6 Server	Yes, Multiple
IP Pool	Yes
Proxy ARP	Yes
Dynamic DNS Services for IPv4	Dyn.com, Dyns.cx, DuckDNS.org
Custom HTTP Poster for IPv4	Yes

BANDWIDTH MANAGEMENT FOR IPv4	
Policy-Based Bandwidth Management	Yes
Scheduled Policies	Yes
Bandwidth Guarantees	Yes
Bandwidth Limits	Yes
Bandwidth Prioritization	Yes
DSCP-based / ToS-based	Yes
Bandwidth Management per Group	Yes
Dynamic Bandwidth Balancing between Groups	Yes
Packet Rate Limits	Yes
DSCP Forwarding	Yes
DSCP Copy to Outer Header	VLAN, IPsec

APPLICATION CONTROL	
Recognizable Applications	4,500+
Application Content Control	5,700+
Policy-Based	Yes
Policy Matching on Application	Yes
Policy Matching on Application Content (Metadata)	Yes
Policy Actions	Audit, DROP, Bandwidth Management

Disclaimer: This is a general overview of all the features, for an updated feature list always refer to the latest CyberArmour documentation for your product

INTRUSION DETECTION AND PREVENTION (IDS / IPS)	
Policy-Based	Yes
Signature Selection per Policy	Yes
Policy Actions	Audit, DROP, Bandwidth Management
Stateful Pattern Matching	Yes
Protocol and Rate Anomaly Detection	Yes
Insertion and Evasion Protection	Yes
Dynamic IP Blacklisting for IPv4	Yes
Automatic Signature Updates	Yes

IP REPUTATION FOR IPv4	
Real-Time DoS Protection	Yes
Real-Time Botnet Protection	Yes
Real-Time Phishing Protection	Yes
Real-Time Scanner Protection	Yes
Real-Time SPAM Protection	Yes
Real-Time IP Reputation Scores	Yes

CONTENT SECURITY	
Policy-Based	Yes
IPv4 Protocol Validation	HTTP, HTTPS, FTP, SMTP, POP3, IMAP, TFTP, SIP, H.323, PPTP, TLS/SSL, DNS, Syslog
IPv6 Protocol Validation	HTTP, HTTPS
Web Content Filtering	
HTTP / HTTPS	Yes / Yes
Audit / Blocking Mode	Yes / Yes
Classification Categories	86
URL Whitelisting / Blacklisting	Yes / Yes
Customizable Restriction Pages	Yes
Cloud-Based URL Classification Source	Yes
User-Agent Filter	Yes
Anti-Virus	
Supported Protocols	HTTP, FTP, SMTP, POP3, IMAP
Stream-Based Scanning	Yes
File Type Whitelisting	Yes
Scanning of Files in Archives (ZIP / GZIP)	Yes
Nested Archives Support (ZIP / GZIP)	Yes, Up to 10 Levels
Automatic Signature Updates	Yes
Anti-Spam	
Supported Protocols	SMTP, POP3, IMAP
Anti-Spam Detection Mechanisms	
Reply Address Domain Verification	SMTP, POP3, IMAP
Malicious Link Protection	SMTP, POP3, IMAP
Distributed Checksum Clearinghouses (DCC)	SMTP, POP3, IMAP
DNS Blacklisting	SMTP, POP3, IMAP

Disclaimer: This is a general overview of all the features, for an updated feature list always refer to the latest CyberArmour documentation for your product

Anti-Spam Actions	
Strip Malicious Links	SMTP, POP3, IMAP
Tag Subject and Headers	SMTP, POP3, IMAP
Send to Quarantine E-mail Address	SMTP
E-mail Rate Limiting	SMTP
Reject Email Reception	SMTP

File Integrity	
Supported Protocols	HTTP, FTP, SMTP, POP3, IMAP
File Type Whitelisting / Blacklisting	Yes / Yes
File Extension and MIME Type Verification	Yes

Update Center	
Scheduled Signature Updates	Hourly / Daily / Weekly / Monthly
Manual Signature Updates	Yes
HTTP / HTTPS Proxy Support	Yes

APPLICATION LAYER GATEWAY	
HTTP / HTTPS (Content Security)	Yes
FTP (Content Security, NAT / SAT)	Yes
TFTP (NAT / SAT)	Yes
SIP (NAT / SAT)	Yes
Syslog	Yes
H.323 / H.323 Gatekeeper (NAT / SAT)	Yes
SMTP (Content Security)	Yes
POP3 (Content Security)	Yes
IMAP (Content Security)	Yes, Using Email Control Profile
SSL / TLS (Offloading)	Yes
PPTP (Passthrough, NAT / SAT)	Yes
DNS	Yes

VPN TUNNELS	
IPsec VPN	
Internet Key Exchange	IKEv1, IKEv2
IKEv1 Phase 1	Main Mode, Aggressive Mode
IKEv1 Phase 2	Quick Mode
IPsec Modes	Tunnel, Transport (IKEv1 Only)
IKE Encryption	AES-GCM, AES, 3DES, DES, Blowfish, Twofish, Cast-128
IPsec Encryption	AES-GCM, AES, 3DES, DES, Blowfish, Twofish, Cast-128, NULL
AES Key Size	128, 192, 256
IKE / IPsec Authentication	SHA-1, SHA-256, SHA-512, MD-5, AES-XCBC (IKEv2 Only)
Perfect Forward Secrecy (DH Groups)	1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 28, 29, 30, 31
IKE Config Mode	Yes, Static Pool and RADIUS Assigned IP
IKE DSCP Assignment	Static
Dead Peer Detection (DPD)	Yes
Pre-Shared Keys (PSK)	Yes
X.509 Certificates	Yes
XAuth (IKEv1)	Yes, Client and Server
EAP (IKEv2)	Client (EAP-MSCHAPv2, EAP-MD5) Server (EAP-MSCHAPv2, EAP-MD5, RADIUS)
PKI Certificate Requests	PKCS#1, PKCS#3, PKCS#7, PKCS#10
Self-Signed Certificates	Yes

Certificate Authority Issued Certificates	Yes, VeriSign, Entrust etc.
Certificate Revocation List (CRL) Protocols	LDAP, HTTP
CRL Fail-Mode Behaviour	Conditional, Enforced
IKE Identity	IP, FQDN, E-mail, X.500 Distinguished-Name
Security Association Granularity	Net, Host, Port
Replay Attack Prevention	Yes
Policy-Based Routing	Yes
Virtual Routing	Yes
Roaming Client Tunnels	Yes
NAT Traversal (NAT-T)	Yes
MOBIKE	Yes
IPsec Dial-on-Demand	Yes
IPsec Tunnel Selection Through	Firewall Rule Set, Routing, Policy-Based Routing
Redundant VPN Tunnels	Yes
IPsec Passthrough	Yes
Tunneling of IPv4 in IPv4 IPsec Tunnel	Yes
Tunneling of IPv4 in IPv6 IPsec Tunnel	Yes
Tunneling of IPv6 in IPv4 IPsec Tunnel	Yes
Tunneling of IPv6 in IPv6 IPsec Tunnel	Yes

OneConnect SSL VPN

TLS (TCP) Support	Yes
DTLS (UDP) Support	Yes
One-Time Client Installation	Yes
Multi-factor Authentication (MFA/2FA) Support	OpenID Connect (OIDC), RADIUS
Browser Independent	Yes
VPN Policy Selection Through	Firewall Rule Set, Routing, Policy-Based Routing
Split Tunneling	Yes
SSL VPN Client IPv4 Provisioning	IP Pool, Static
Client OS Support	Windows, macOS, iPadOS, iOS, Android

L2TP VPN

L2TPv2 Client (LAC)	Yes
L2TPv2 Server (LNS)	Yes
L2TPv3 Client (LAC)	Yes
L2TPv3 Server (LNS)	Yes
L2TP over IPsec	Yes
L2TP Tunnel Selection Through	Firewall Rule Set, Routing, Policy-Based Routing
L2TP Client Dial-on-Demand	Yes
L2TPv2 Server IPv4 Provisioning	IP Pool, Static

Other Tunnels

PPPoE IPv4 Client	Yes
PPPoE IPv6 Client	Yes
Unnumbered PPPoE	Yes
PPPoE Client Dial-on-Demand	Yes
PPTP Client (PAC)	Yes
PPTP Client Dial-on-Demand	Yes
PPTP Server (PNS)	Yes
PPTP Server IP Provisioning	IP Pool, Static
MPPE Encryption (PPTP / L2TP)	RC4-40, RC4-56, RC4-128
Generic Routing Encapsulation, GRE (RFC2784, RFC2890)	Yes
6in4 Tunneling (RFC4213)	Yes
Tunnel Selection Through	Firewall Rule Set, Routing, Policy-Based Routing

Disclaimer: This is a general overview of all the features, for an updated feature list always refer to the latest CyberArmour documentation for your product

DEVICE AUTHENTICATION (802.1x)	
RADIUS Server	Yes, Multiple
EAT-TLS	Yes

USER AUTHENTICATION	
Local User Database	Yes, Multiple
OpenID Connect (OIDC) Authentication	Yes, Multiple Servers, for OneConnect
RADIUS Authentication	Yes, IPv4 / IPv6, Multiple Servers
RADIUS Accounting	Yes, IPv4 / IPv6, Multiple Servers
LDAP Authentication	Yes, Multiple Servers
RADIUS Authentication Protocols	PAP, CHAP, MS-CHAPv1, MS-CHAPv2
XAUTH IKEv1 / IPsec Authentication	Yes
EAP IKEv2 / IPsec Authentication	Yes
Web-Based HTTP / HTTPS Authentication	Yes
Customizable HTTP / HTTPS Portal	Yes
L2TP / PPTP / OneConnect / SSL VPN Authentication	Yes
Identity Awareness	
Device-Based Authentication (MAC Address)	Yes
ARP Authentication	Yes
RADIUS Relay	Yes
Active Directory Integration	Microsoft Windows Server
Client-less Deployment	Yes

MANAGEMENT	
Centralized Management	Clavister InControl
Web User Interface (WebUI)	HTTP and HTTPS
SSH Management	Yes
Command Line Interface (CLI)	Yes
REST API	User Authentication, SLB, Blacklist Control
Management Authentication	Local User Database, RADIUS
Management Brute Force Protection	Yes
Remote Fail-Safe Configuration	Yes
Local Console (RS-232)	Yes
Traffic Simulation (CLI)	ICMP, TCP, UDP
Scripting Support	CLI, WebUI
Packet Capture (PCAP)	Yes
Packet Capture (PCAP)	WebUI, InControl, SCP
System and Configuration Backup	WebUI, InControl, SCP
SNTP Time Sync	Yes

Disclaimer: This is a general overview of all the features, for an updated feature list always refer to the latest CyberArmour documentation for your product

SECURITY BY SWEDEN

MONITORING AND LOGGING	
Syslog	Yes, Multiple Servers
Clavister InControl Log	Yes, Multiple Servers
Real-Time Log	CLI, WebUI, InControl
Memory Log	CLI, WebUI
Mail Alerting	Yes, SMTP
Log Settings per Policy	Yes
Log Export via WebUI	Yes
SNMPv2c Polling / Traps	Yes / Yes
SNMPv3 Polling / Traps	Yes / Yes
Real-Time Monitor Alerts (Log action)	Yes
Real-Time Performance Monitoring	WebUI, InControl
Hardware Key Metrics Monitoring	CPU Load, CPU Temperature, Voltage, Memory, Fan etc

HIGH AVAILABILITY	
Active Node with Passive Backup	Yes
Firewall Connection State Synchronization	Yes
IKE / IPsec State Synchronization	Yes / Yes
User and Accounting State Synchronization	Yes
DHCP Server and Relayer State Synchronization	Yes
DHCP Client	Yes
Synchronization of Dynamic Routes	Yes
IGMP State Synchronization	Yes
Server Load Balancing (SLB) State Synchronization	Yes
Configuration Synchronization	Yes
Device Failure Detection	Yes
Dead Link / Gateway / Interface Detection	Yes / Yes / Yes
Average Failover Time	< 800 ms

HYPERVISOR SUPPORT	
VMware	Yes
KVM	Yes
Hyper-V	Yes

SECURE BOOT	
UEFI Secure Boot	Yes

EASY DEPLOYMENT	
Clavister Zero Touch	Yes
Cloud Init	Yes, Network Based

ACME (AUTOMATIC CERTIFICATE MANAGEMENT ENVIRONMENT)	
Let´s Encrypt	Yes
Buypass	Yes
Custom Server	Yes

Disclaimer: This is a general overview of all the features, for an updated feature list always refer to the latest CyberArmour documentation for your product

SECURITY BY SWEDEN

CLAVISTER CYBERARMOUR

An Embedded Software Component in your Solution

The lineup of products in the Clavister CyberAmour family is able to meet the demands from a wide range of customer applications. Still, we acknowledge the fact that there are scenarios where the existing Clavister CyberArmour products do not meet your precise requirements.

In addition, there might be situations where your application is already using a specific line of hardware for compliance or procurement reasons.

In these scenarios, Clavister is able to provide the full CyberArmour capabilities as a pure software offering for embedding onto your choice of hardware platform. The software supports the most common CPU architectures and can be used either as "bare metal" deployment, or as a virtual machine on frequently used hypervisors. As a consequence of the unique software design of Clavister CyberArmour, you do not need to sacrifice neither capacity nor functionality when opting for a software-based deployment.

Following Clavister's engagement model, we are able to support you throughout the entire journey, from initial requirements mapping, through proof-of-concept deployment and complete system validation to full lifecycle support.

Contact us for more info on how we can support you with your specific scenario!

SECURITY BY SWEDEN

On a Mission to Cyber-Protect Europe

Clavister provides top-tier cybersecurity solutions made in Sweden. For over 25 years, we are the trusted partner for customers with mission-critical applications.

YOUR TRUSTED PARTNER

In today's rapidly evolving cyberthreat environment, everyone needs all the help they can get – but who do you trust? With over 20,000 satisfied customers and 25 years of innovation, Clavister has proven itself as the reliable choice, trusted by major brands and recognised for our strong partnerships.

SWEDISH ENGINEERING AT HEART

Clavister's solutions are rooted in the strong tradition of Swedish engineering, known for reliability, quality, and cutting-edge innovation. We believe we offer the most robust cybersecurity solutions, built on long-standing security expertise, resulting in record-low vulnerabilities and unparalleled uptime. Our commitment to innovation keeps us at the forefront of the industry.

A CARING RELATIONSHIP

At Clavister, cybersecurity is a team game. That's why we focus on building long-term relationships where you engage directly with our domain experts. Our presence in Europe includes a dedicated team and a strong reseller network, ready to support you.
We've got you covered!

TRUSTED BY MAJOR BRANDS

BAE SYSTEMS NOKIA THALES

SAAB ERICSSON

clavister

CLAVISTER.COM