

**CLAVISTER®**

# NetWall

Clavister NetWall is our family of AI-powered Next-Generation Firewalls – designed and developed in Sweden – ideal for cyber-protecting mission-critical infrastructure, including datacentres, remote sites and harsh industrial environments.





## 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 NetWall is designed to support the most complex network setups.

## APPLICATION-BASED ROUTING

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

## VIRTUAL & DYNAMIC ROUTING

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

## ALWAYS-UP PHILOSOPHY

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



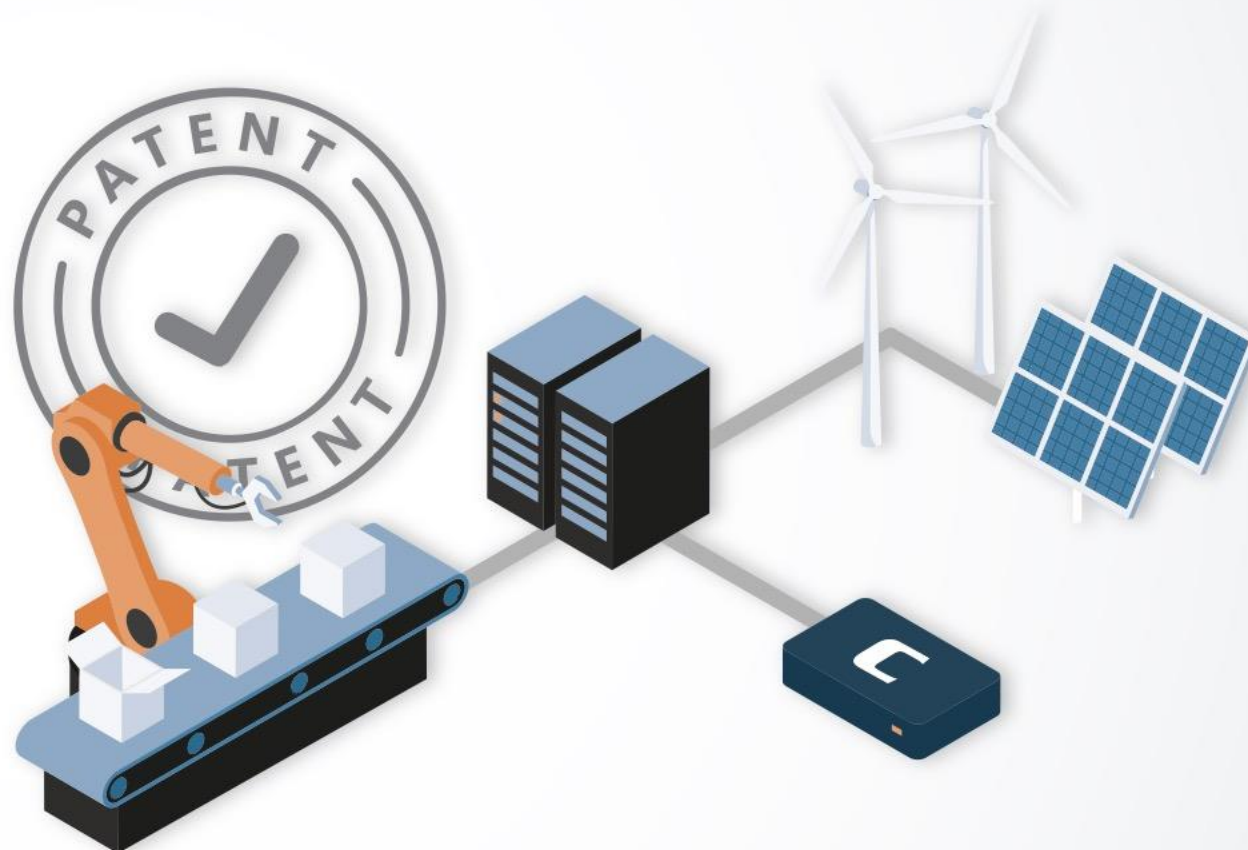
## Patented AI-Power

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  
ON-DEVICE  
TRAINING

No  
CLOUD  
PROCESSING

Instant  
ANOMALY  
DETECTION







# Simple Secure Remote Working

Clavister OneConnect is our VPN client that offers a simple and easy to use solution for remote access. Connecting securely is as easy as downloading and installing from common marketplaces or distributing using a device management software. Complement with the Clavister IAM solution to benefit from strong authentication and single sign-on capabilities.

 Windows

 chromeOS

Android 

macOS

iPadOS

iOS





## Highly Resilient

We appreciate the mission-criticality of your network. That is why Clavister NetWall 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 NetWall device itself but also on links, routes, gateways and even third-party hosts, cater for prompt resolution in case of degradation.

## 7+ Years

AVERAGE NUMBER OF YEARS  
OF UNINTERRUPTED PROTECTION







## Actionable Security Analytics

All Clavister NetWall products come with powerful security analytics capabilities. A single pane of glass console provides clear, actionable, and comprehensive evaluation of your organisation'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 business secure.





# Central Management and Control

The Clavister InControl centralised management console, included in all Clavister NetWall licensing plans, makes managing Clavister NetWall firewalls easy and efficient, 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.

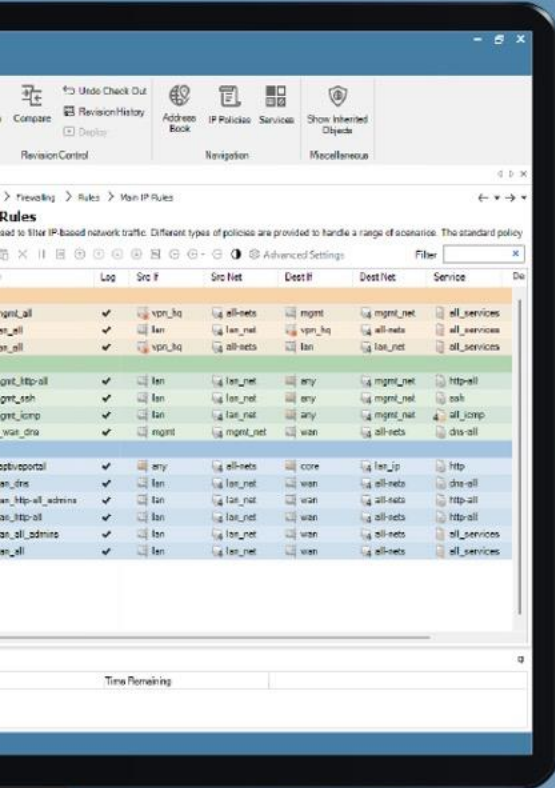
With tools for firewall configuration, troubleshooting, firewall backups, and remote access, Clavister InControl is designed to save time and reduce complexity while keeping your network running smoothly.

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







## Traffic Management

The advanced traffic management capability in Clavister NetWall ensures optimised bandwidth usage, enabling smoother network performance even during peak loads. With granular control and intelligent traffic prioritisation, businesses can secure critical applications while maintaining consistent service quality across their infrastructure.



# Deep Application Awareness

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

## SELECTED APPLICATION-BASED CAPABILITIES

- Inspection of, and policies for, granular application attributes.
- Ensure consistent quality-of-service with effective bandwidth management.
- Block or limit undesired or risky applications.
- Extensive logging for analytics and auditing.
- Apply routing decisions to achieve local internet break-out scenarios.







## Flexible Deployment Options

Clavister NetWall is available in a number of models ranging from small desktop versions to large datacentre appliances. Clavister NetWall is also available on virtualised versions for deployment in public and private cloud environments. Turnkey appliances to fit all your needs.

ORACLE  
CLOUD

Azure

Google Cloud

aws

openstack.

KVM

Microsoft  
Hyper-V

vmware  
vSphere





# Always-Up VPN

Clavister NetWall delivers reliable and secure site-to-site VPN capabilities, designed to connect remote locations seamlessly.

Built on industry-standard encryption protocols, it ensures excellent interoperability with other VPN solutions, providing secure data transmission across networks.

With Clavister's robust IPsec implementation, businesses can count on high performance, ease of configuration, and strong protection for their critical communications.

Whether connecting branch offices or integrating with partner networks, Clavister NetWall simplifies secure connectivity while maintaining top-tier security and reliability.



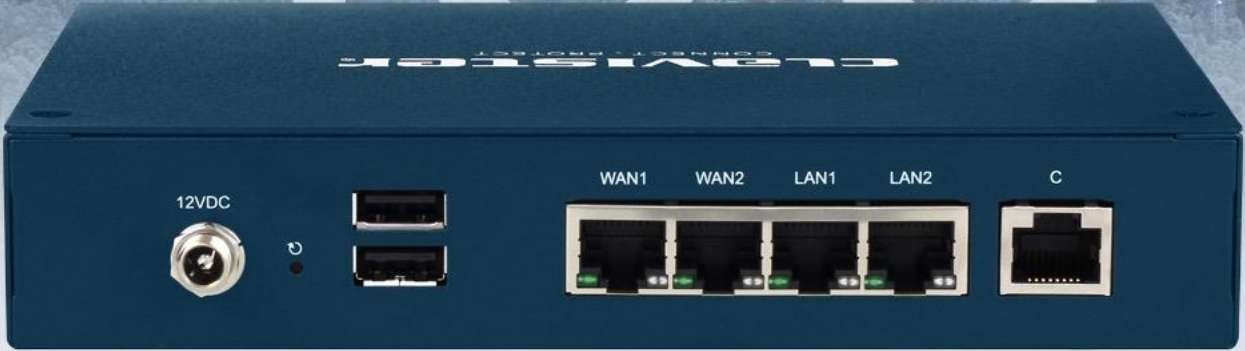


# Threat Prevention

Clavister NetWall 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.



100





# 300





500



6000





# 200R





# Virtual



# Licensing Plans

	ESSENTIALS ★	ENHANCED ★★	PREMIUM ★★★
<b>Support and Maintenance</b>			
Standard Support	●	●	●
Software Maintenance	●	●	●
Hardware Replacement	●	●	●
<b>Networking Capabilities</b>			
Routing	●	●	●
Always-Up VPN	●	●	●
Traffic Management	●	●	●
Simple Secure Remote Networking	●	●	●
High Availability	●	●	●
Reverse Proxy		●	●
<b>Management and Analytics</b>			
Centralised Management	●	●	●
Security Analytics	●	●	●

	ESSENTIALS ★	ENHANCED ★★	PREMIUM ★★★
<b>Threat Prevention</b>			
Firewalling	●	●	●
Deep Application Awareness	●	●	●
Geo-fencing	●	●	●
Intrusion Prevention		●	●
Anti Malware		●	●
Web Content Filtering		●	●
IP Reputation		●	●
<b>SSL Inspection</b>			
SSL Inspection with Clavister NetEye			●
Cloud Sandboxing			●



# NetShield

Clavister NetShield is our family of High-capacity Next-Generation Firewalls – designed and developed in Sweden – ideal for cyberprotecting datacentres and providing secure remote networking.







## 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.

CLAVISTER

NetShield



## Always-Up VPN

Clavister NetShield delivers reliable and secure site-to-site VPN capabilities, designed to connect remote locations seamlessly.

Built on industry-standard encryption protocols, it ensures excellent interoperability with other VPN solutions, providing secure data transmission across networks.

With Clavister's robust IPsec implementation, businesses can count on high performance, ease of configuration, and strong protection for their critical communications.

Whether connecting branch offices or integrating with partner networks, Clavister NetShield simplifies secure connectivity while maintaining top-tier security and reliability.





## Built for Modern Infrastructures

Deploy Clavister NetShield as a container for maximum agility and scalability – perfect for cloud-native and microservice environments.

### **LIGHTWEIGHT & FLEXIBLE**

Run Clavister NetShield directly in Kubernetes or Docker, spinning up instances on demand. Scale security alongside your applications without the overhead of physical appliances.

### **SECURE ANYWHERE, ANYTIME**

Deploy firewalls at the edge, in multi-cloud environments, or within isolated workloads.





# The Swiss Army Knife of Routing

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

## **VIRTUAL & DYNAMIC ROUTING**

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

## **ALWAYS-UP PHILOSOPHY**

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

## **BGP & HIGH-SPEED FAILOVER**

Seamlessly handle large, distributed networks with BGP for intelligent path selection. BFD (Bidirectional Forwarding Detection) ensures ultra-fast link failure detection, minimising downtime and keeping connections stable.



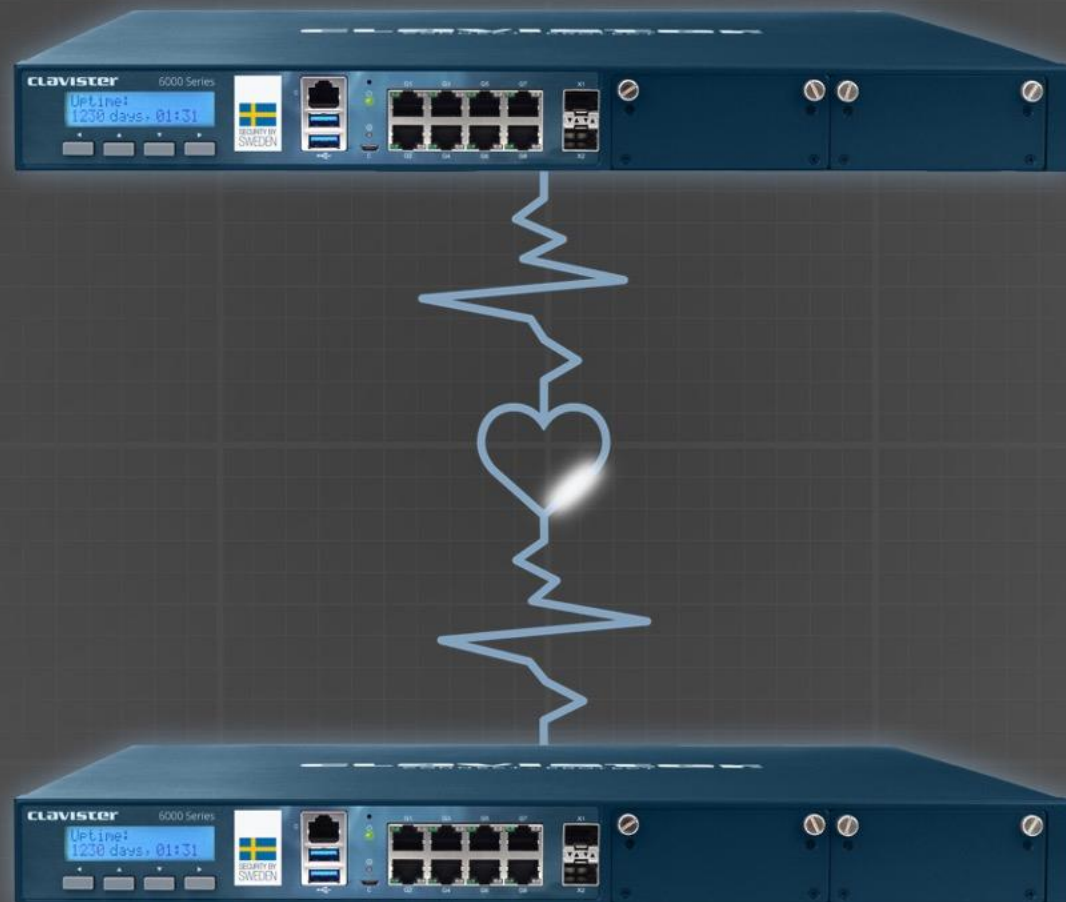
## Highly Resilient

We appreciate the mission-criticality of your network.

That is why Clavister NetShield 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 NetShield device itself but also on links, routes, gateways and even third-party hosts, cater for prompt resolution in case of degradation.

## 7+ Years

AVERAGE NUMBER OF YEARS  
OF UNINTERRUPTED PROTECTION



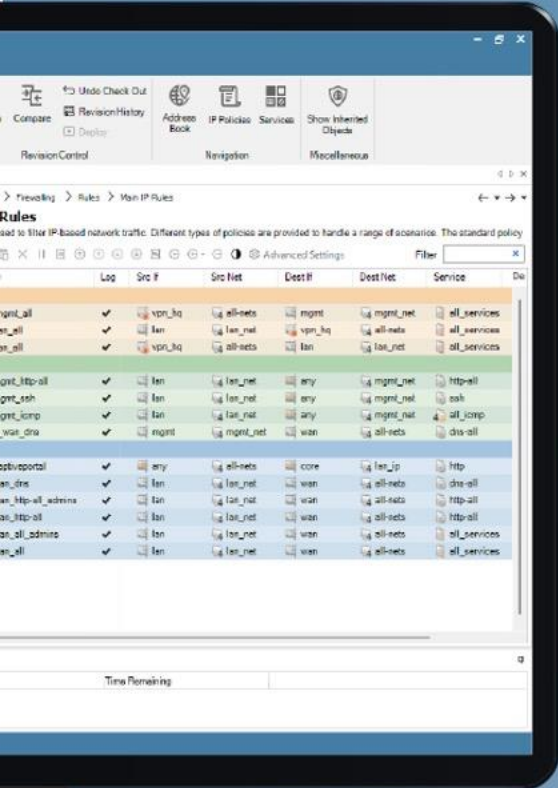




## Actionable Security Analytics

All Clavister NetShield products come with powerful security analytics capabilities. A single pane of glass console provides clear, actionable, and comprehensive evaluation of your organisation'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 business secure.





# Central Management and Control

The Clavister InControl centralised management console, included in all Clavister NetShield licensing plans, makes managing Clavister NetShield firewalls easy and efficient, even for large networks.

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

Batch  
FIRMWARE  
UPGRADES





## Traffic Management

The advanced traffic management capability in Clavister NetShield ensures optimised bandwidth usage, enabling smoother network performance even during peak loads. With granular control and intelligent traffic prioritisation, businesses can secure critical applications while maintaining consistent service quality across their infrastructure.



# Deep Application Awareness

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

## SELECTED APPLICATION-BASED CAPABILITIES

- Inspection of, and policies for, granular application attributes.
  - Extensive logging for analytics and auditing.







## Built for Massive-Scale VPN

Power your network with Clavister NetShield's high-performance VPN capabilities – designed to handle secure, large-scale connectivity with ease.

### **UNMATCHED TUNNEL CAPACITY**

Support thousands of simultaneous VPN tunnels, making it easy to connect remote sites, branch offices, and remote users – all without compromising performance.

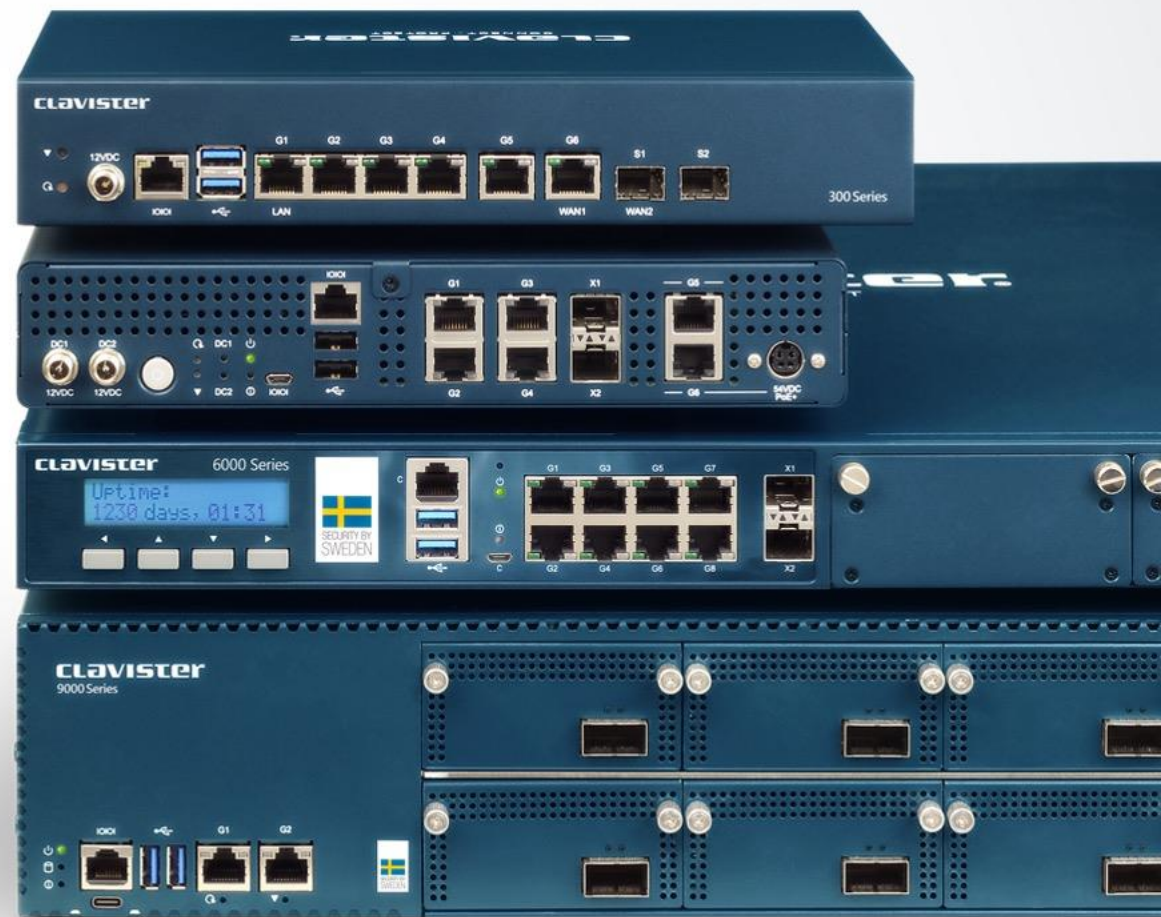
### **HIGH-PERFORMANCE ENCRYPTION**

Leverage hardware-accelerated encryption and optimised packet handling for blazing-fast, ultra-secure VPN traffic, even under heavy loads.



## Flexible Deployment Options

Clavister NetShield is available in a number of models ranging from small desktop versions to large datacentre appliances. Clavister NetShield is also available on virtualised versions for deployment in public and private cloud environments. Turnkey appliances to fit all your needs.





# 300



500





6000





9000



# Virtual





# Licensing Plans

	ESSENTIALS ★	ENHANCED ★★	PREMIUM ★★★
<b>Support and Maintenance</b>			
Standard Support	●	●	●
Software Maintenance	●	●	●
Hardware Replacement	●	●	●
<b>Networking Capabilities</b>			
Advanced Routing	●	●	●
High Availability	●	●	●
Border Gateway Protocol (BGPv4)	●	●	●
Open Shortest Path First (OSPFv2)	●	●	●
<b>Management and Analytics</b>			
Centralised Management	●	●	●

	ESSENTIALS ★	ENHANCED ★★	PREMIUM ★★★
<b>Threat Prevention</b>			
DoS Protection	●	●	●
Intrusion Prevention		●	●
Application Visibility		●	●
SIP ALG			●
SCTP Inspection			●
GTP Inspection			●
Carrier Grade NAT			●
Deterministic NAT			●
<b>SSL Inspection</b>			
SSL Inspection		●	●





# CyberArmour

AI-POWERED CYBERSECURITY  
FOR MILITARY PLATFORMS

# Military-grade AI-powered Next-Generation Firewalls

FOR DEFENCE APPLICATIONS

Clavister CyberArmour 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.





# 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 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.



### 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 the SOTAS system and can detect and block cyberattacks in real time.

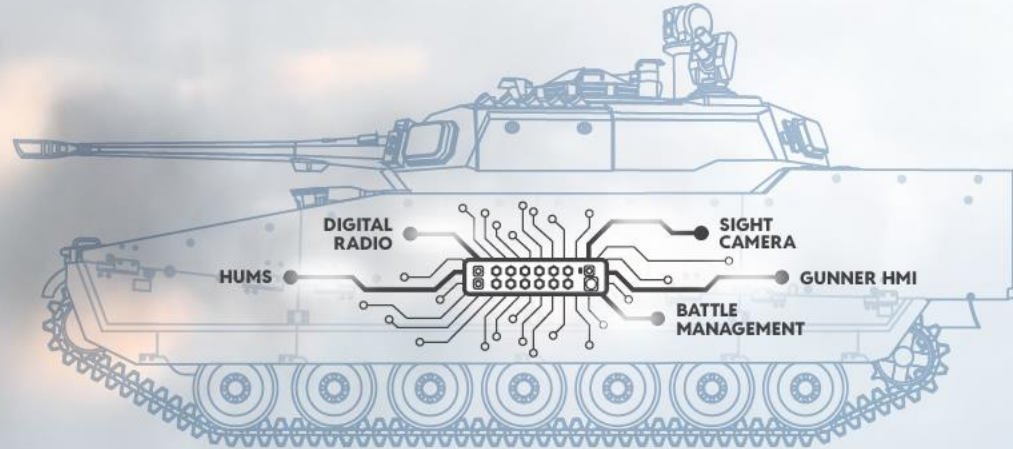


### WEAPON SYSTEMS

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.

## 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.



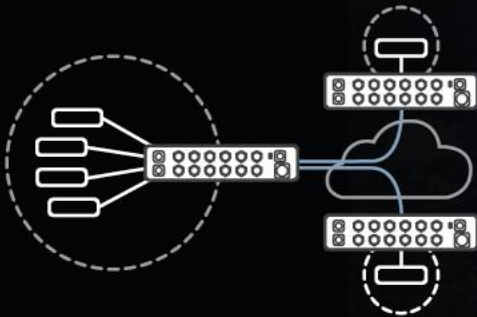


**A CLAVISTER SOLUTION**

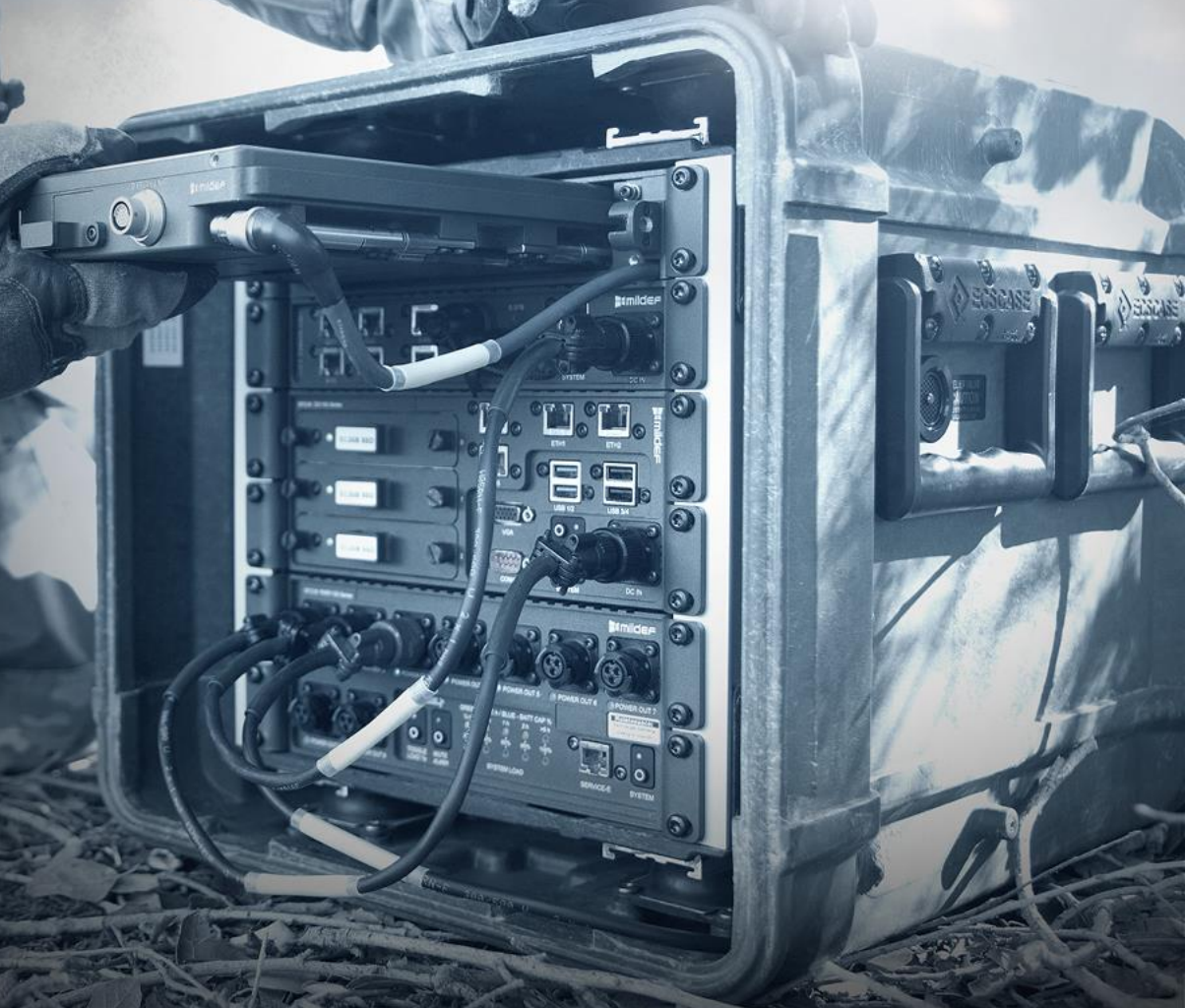
# Securing Tactical IT Systems

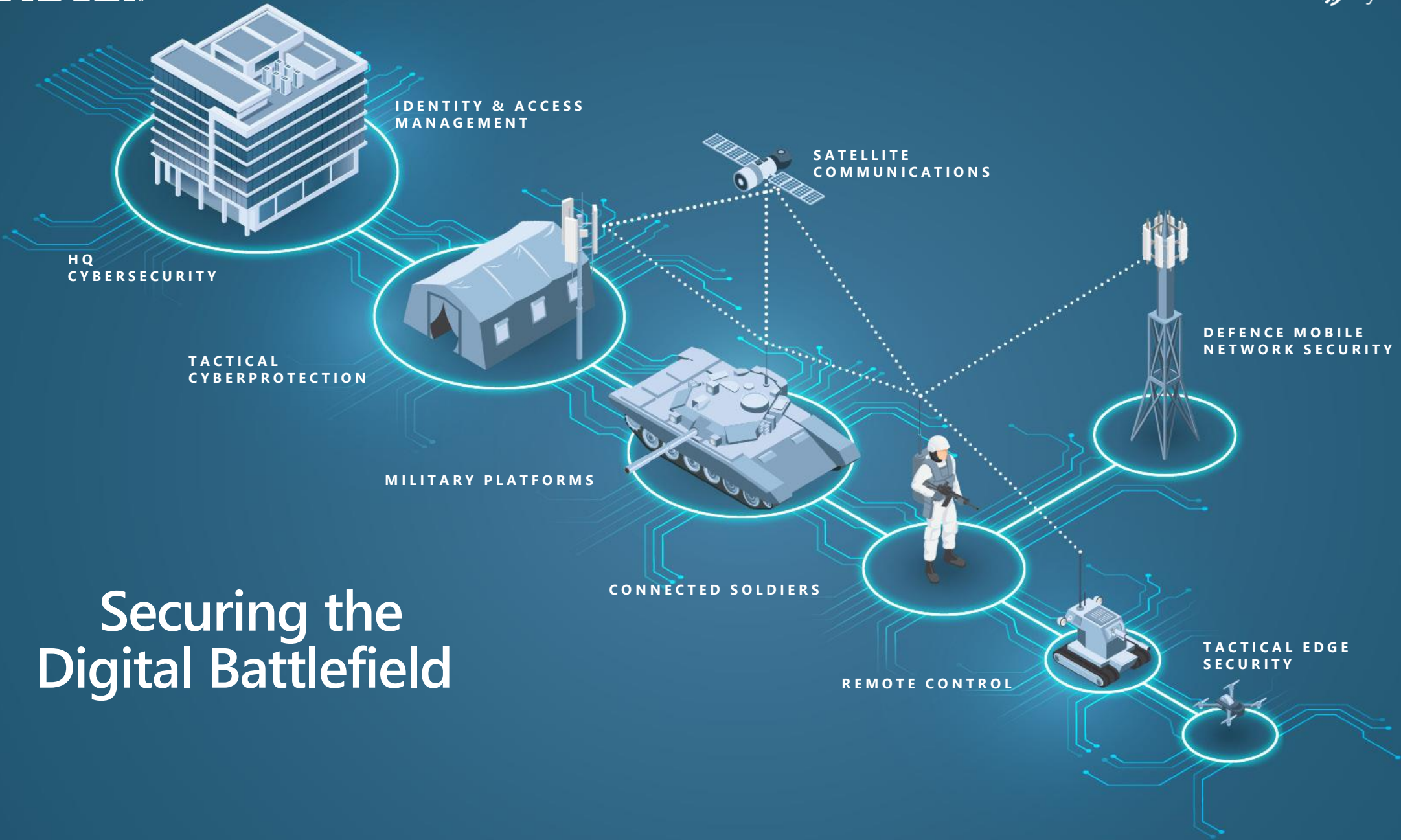
With increased digitalisation, tactical IT infrastructure and networks are expanding, introducing new types of vulnerabilities. Enhancing cybersecurity is crucial for tactical communication, battle management systems, sensors, counter-UAS solutions, and other mission-critical technologies.

**PROTECTING SYSTEMS  
FROM EXTERNAL  
THREATS**



**REDUCING RISK  
BY SEGMENTING  
COMMUNICATION**





# Securing the Digital Battlefield





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.

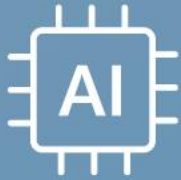
### **VIRTUAL & DYNAMIC ROUTING**

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

ON-DEVICE  
TRAINING

No

CLOUD  
PROCESSING

Instant

ANOMALY  
DETECTION





## MILITARY-GRADED 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.

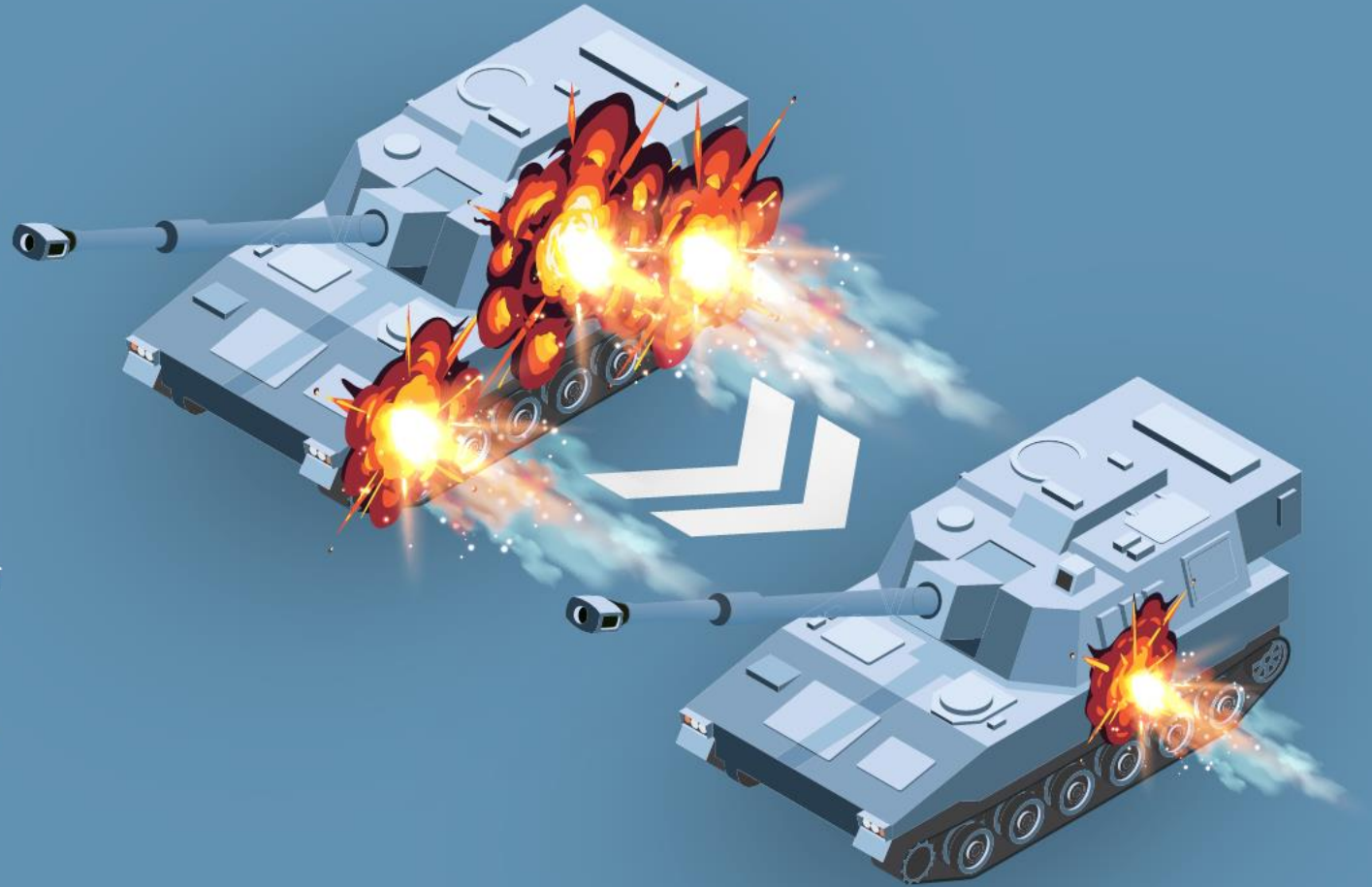




## NETWORK SEGMENTATION

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

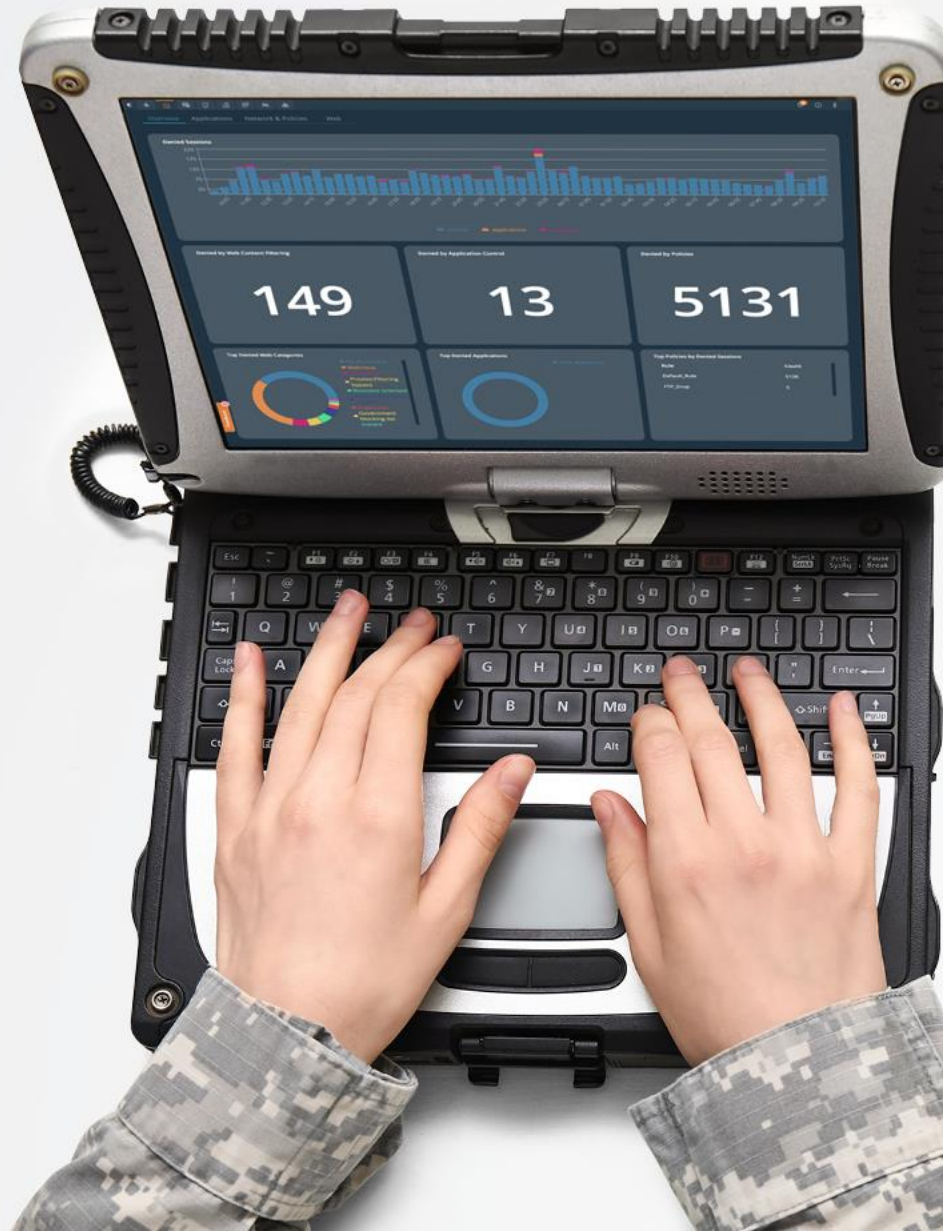
By restricting access between network segments, the blast radius is significantly reduced in the event of a cyberattack.





## 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

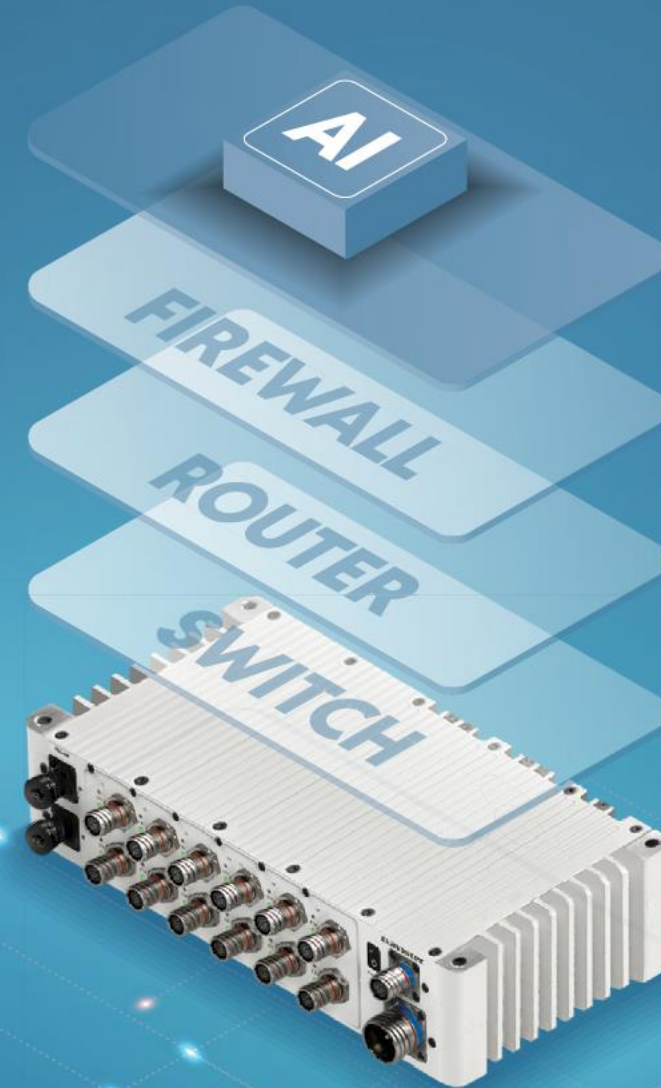
Batch  
FIRMWARE  
UPGRADES



## 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



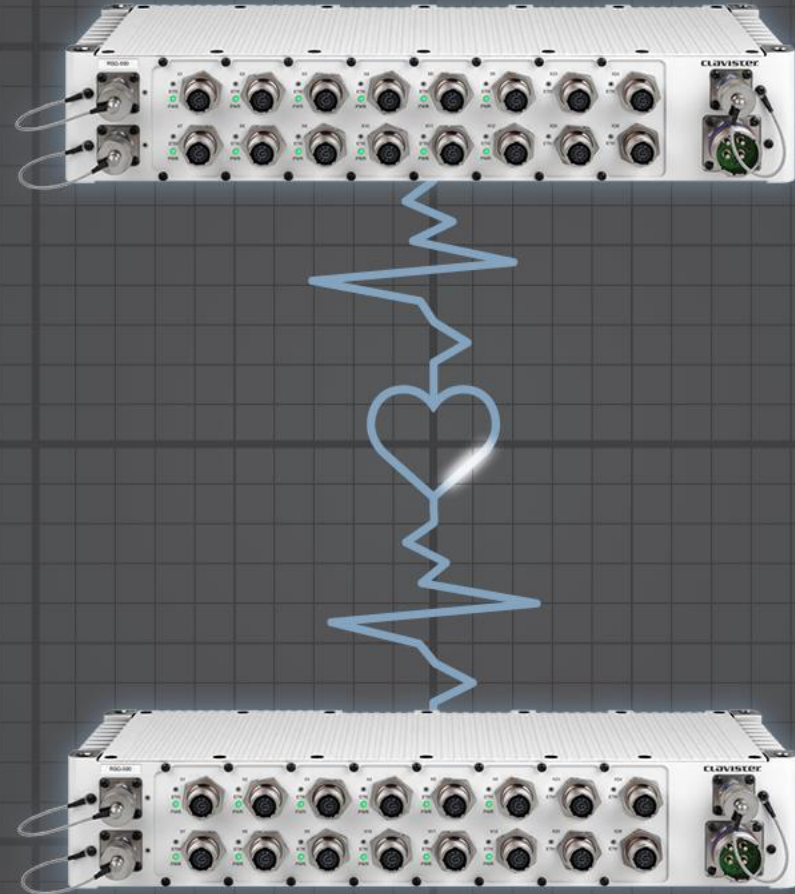


## HIGHLY RESILIENT

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.







# RSG-200



FIREWALL



# RSG-400



**FIREWALL (RSG-400) / SWITCH (RSW-400)**



# RSG-500



FIREWALL



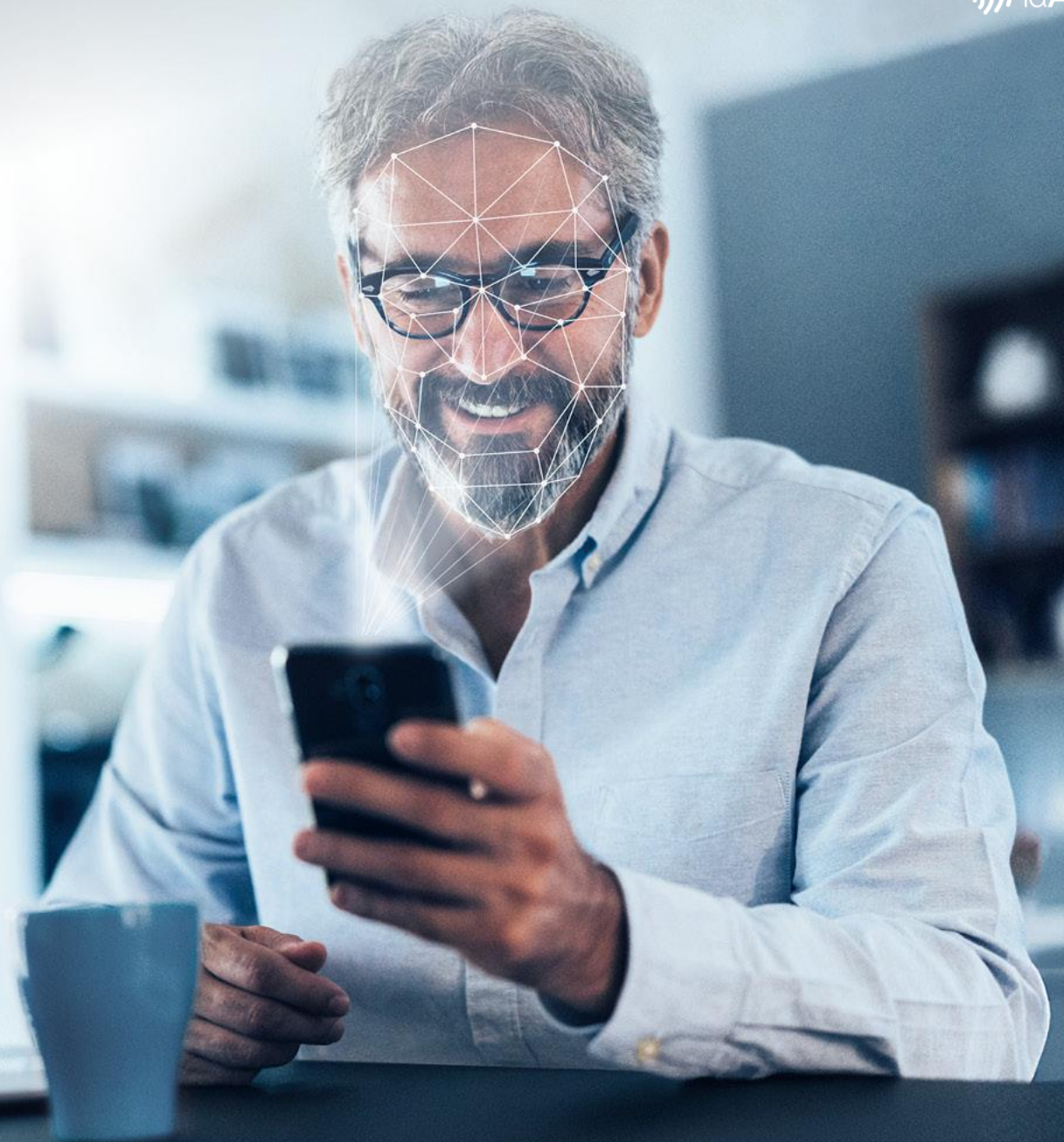
WHERE IDENTITY  
IS KEY



IdAuth

# Where Identity is Key

Clavister IdAuth is a modern Identity Provider (IdP) platform that combines simple, user-friendly authentication with powerful security. It protects against phishing, identity theft, and unauthorised access, while giving administrators the full flexibility to configure advanced authentication flows and integrations.







## 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.





## ON A MISSION TO CYBER-PROTECT EUROPE

Clavister provides top-tier cybersecurity solutions made in Sweden, trusted by organisations with mission-critical applications. With a tradition deeply rooted in Swedish engineering, we are known for reliability, quality and cutting-edge innovation.

**We are committed to strengthening  
Europe's digital sovereignty.**





## **YOUR DIGITAL IDENTITY – OUR PRIORITY**

In today's digital landscape, security and efficiency are crucial for protecting sensitive data while enabling employees and partners to work productively. Clavister IdAuth puts identity at the centre of security, defining who is allowed in, under what conditions, and through which methods. This ensures strong security and full compliance across the entire environment.





## EVERYTHING INTEGRATED – SECURITY PERFECTED

With Clavister IdAuth, you can seamlessly connect your existing services, applications and authentication methods. Acting as a central hub for secure identity verification, Clavister IdAuth ensures a cohesive and streamlined authentication process across your organisation. Enhance security, improve efficiency and simplify identity management with a fully integrated authentication solution. Clavister IdAuth ensures smooth and secure integration with more than 300 external services.

300+ **EXTERNAL  
SERVICES**



Inera

Google

FREJA

SITHS

FIDO2



eIDAS



Microsoft  
AD



Microsoft  
Entra ID



France  
Connect



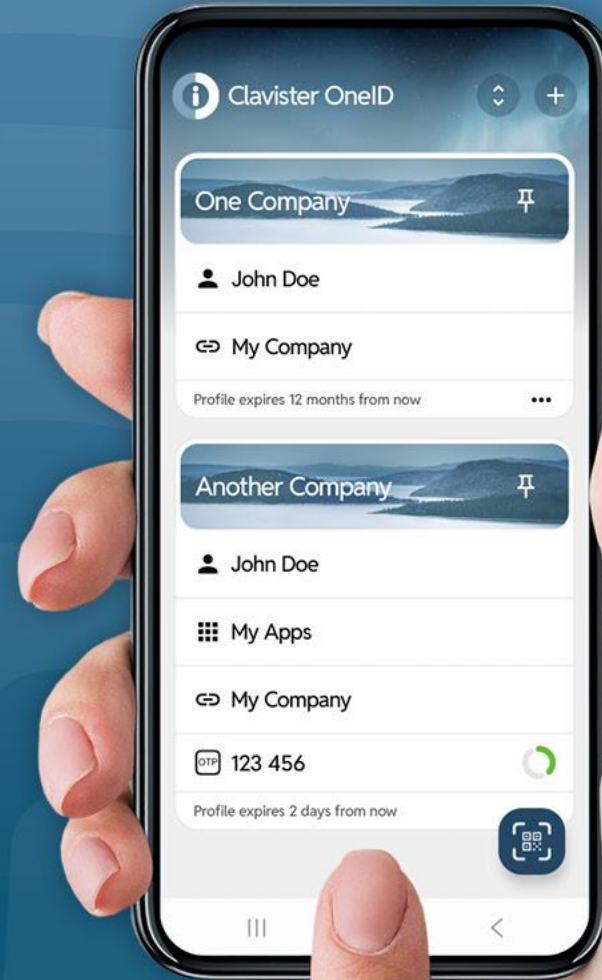




## MFA IN YOUR POCKET with Clavister OneID

Multi-Factor Authentication (MFA) adds an extra layer of protection by requiring more than one method of verification. With our own mobile application Clavister OneID, we enable tailored, fast and secure access while reducing the risk of unauthorised entry.

Through the self-enrollment portal, users can quickly activate their preferred authentication method. Secure, accessible and easy to use, MFA powered by biometrics and modern authentication standards provides your organisation with a secure identification method for all employees and customers in no time.





## MULTIFACTOR AUTHENTICATION

Enhance security and flexibility by offering users a choice of multiple authentication methods, ensuring a seamless login experience for both on-premises and cloud environments. MFA is the safest and easiest way to access your applications and is crucial to ensure safety in every organisation.





## CONDITIONAL ACCESS

Make better and tailored security decisions with richer context. Clavister IdAuth can evaluate a wide range of factors, from user network and device state, to time of day and risk signals, before granting access.



# ACCESS GRANTED



## SINGLE SIGN-ON

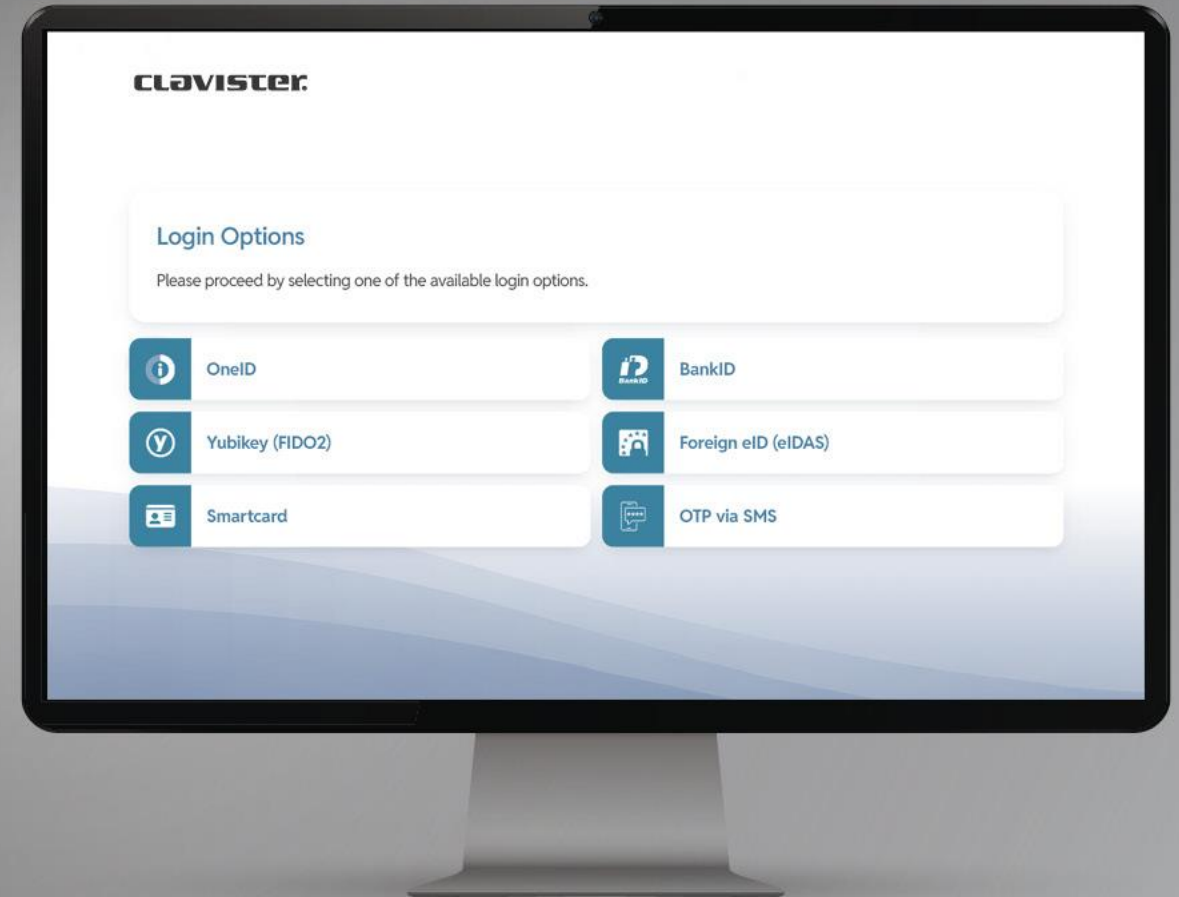
Log in once and access all your services effortlessly. Single sign-on saves time while keeping your accounts secure with centralised authentication across your digital ecosystems.





## ACCESSIBLE FOR ALL USERS

At Clavister, accessibility isn't an afterthought, it's a core principle that we deeply integrate into the development of our products. While laws and regulations set important accessibility requirements, including the widely recognised WCAG standards, our goal goes beyond compliance: No user, regardless of ability, should face obstacles when accessing our services.





## ONE IDENTITY – ENDLESS POSSIBILITIES

Federated authentication empowers users to access multiple platforms with a single, secure login. Supporting industry-standard protocols such as SAML2, OIDC and OAuth, not only enhancing user experience, but also strengthening security by centralising the authentication flow to your organisation's control.





The image displays three smartphones side-by-side, each showing the Clavister Password reset interface. The interface includes a header with the Clavister logo and a user profile icon (A). Below the header, the title "Password reset" is displayed. A list of requirements is shown, each with a checkbox and a description:

- Must be at least 8 characters long
- Must be a maximum of 32 characters long
- Must contain at least one digit
- Must contain at least one uppercase letter
- Must contain at least one lowercase letter
- Must contain at least one special character

Below the requirements, there is a text input field labeled "Enter new password" with a toggle icon. At the bottom, there is a "CHANGE PASSWORD" button.

The first phone shows the initial screen with empty password fields. The second phone shows the same screen with the password "abc123" entered. The third phone shows the same screen with the password "abc123DFG#" entered, which meets all requirements.



## PASSWORD SELF-SERVICE

In many environments, passwords remain essential. With password self-service, organisations save time and money by reducing help desk workload, while improving productivity, user convenience and overall security.



**CONNECT EFFORTLESSLY  
TO ANY SYSTEM**

Take smart access decisions based  
on data or attributes found in external  
or internal systems, on-premises  
or cloud.





## GAIN INSIGHTS - BE PROACTIVE

Monitor authentication trends across your organisation to detect suspicious activity and uncover weak points before they cause harm. Insight-driven visibility transforms authentication from a routine process into an intelligent layer of protection.



## AVAILABLE AS ON-PREM OR IN CLOUD

Select delivery based on your specific needs. Keep your identities close by deploying your authentication system on-prem and centralised, or empower your organisation quickly and simply with authentication delivered in the cloud.







## TWO STEPS TO PEACE

When full MFA isn't an option, one-time Password (OTP) is a powerful stopgap – better protection compared to passwords while keeping friction low for users.

### Two-Factor Authentication



USERNAME

\*\*\*\*\*

PASSWORD

\*\*\*\*\*



ONE-TIME PASSWORD

\* \* \* \* \*

# User Value



## END USER: TIFFANY

*Tiffany is a non-technical end user who values efficiency and simplicity. She wants secure solutions that make her digital work life easier and more secure.*

### HOW TIFFANY BENEFITS



## MANAGER: ANDERS

*Anders is a manager with broad responsibility across different areas within the company. He values solutions that improve efficiency while ensuring strong security and compliance.*

### HOW ANDERS BENEFITS



## CIO: ANNA

*Anna is an experienced CIO, responsible for cybersecurity across the organisation. She manages both IAM and NGFW solutions, ensuring a secure and compliant environment.*

### HOW ANNA BENEFITS





# User Value



**END USER:**  
**TIFFANY**

## Seamless Login

Access all services with a single, effortless sign-on.

## Activate Your Way

Choose your preferred authentication method with ease.

## Familiar Integrations

Use trusted services such as BankID and Freja eID.

## Multi-Factor Authentication

Secure login with user-friendly MFA.

## Intuitive Interface

Benefit from a design that is simple and accessible.

## Authenticate Once

Reach every application from one secure starting point.

# User Value



**MANAGER:  
ANDERS**

## **Easy On- and Off-boarding**

Add or remove users quickly while keeping security intact.

## **Password Protection**

Prevent risks from password reuse and weak credentials.

## **Streamline Organisation**

Reduce workload and costs with password self-service

## **Compliance with Accessibility Laws**

Ensure to meet WCAG and accessibility requirement.

## **Strengthen Defences**

Safeguard the organisation against phishing and brute-force attacks.



# User Value



**CIO:**  
**ANNA**

## Full Control

Manage data, infrastructure and security policies.

## Proactive Insights

Gain visibility into users and systems to stay ahead of risks.

## Take Access Decisions

Based access control on data and attributes from external system.

## Simple Access Management

Provide users with secure access while keeping control.

## Reduce Workload

Empower users to reset their own passwords.

# Licensing Plan



## ALL-INCLUSIVE FUNCTIONALITY

One plan for all features.



## PRICE MODEL BASED ON USERS

Scale only on number of users,  
not the number of instances.



## UNLIMITED INSTANCES

Deploy as many instances  
you need at no extra charge.



## VOLUME DISCOUNTS

Reduced per-user cost  
as you grow.



## INTEGRATIONS INCLUDED

No extra cost for integrations  
or SAML/OIDC connections.



## DESIGNED FOR MODERN SECURITY

Stay compliant with a license model made  
for tomorrow's identity challenges.