
TactiGate XD
Secure tomorrow.
Stay ahead of
cyber threats.
Cross-domain solution
clavister
SAAB

Military-grade cross-domain solution

for land applications

The TactiGate XD is a next-generation product designed for secure, real-time communication across multiple classified domains – including NATO Restricted and NATO Secret environments.

By seamlessly integrating Saab's TactiGuard XD cross-domain capability with Clavister's CyberArmour firewall, the system ensures strict policy enforcement, rigid access control, and advanced network security.

Integrated on a rugged, compact hardware platform, it is purpose-built for tactical and mobile environments, meeting critical requirements for size, weight and power efficiency.

This integrated solution offers full bi-directional, policy-controlled data exchange, with deep protocol inspection, dynamic routing, and secure tunneling capabilities.

The result is a highly flexible product that enables mission-critical information sharing across domains – without compromising security. With unified control, reduced hardware complexity, and NATO-aligned interoperability, the TactiGate XD sets a new standard for cross-domain communication in defence and national security networks.

Battle Proven Cyber Protection

Clavister's and Saab's technologies protect 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 platform, where a cyberattack could compromise critical functions and, in the worst case, lead to battlefield fatalities. Nearly 1,000 CV90 vehicles – both in service and in production – are protected by Clavister. As other vehicle manufacturers follow a similar path toward digitalisation, both Clavister and Saab are trusted partners in addressing their evolving cybersecurity needs.

Tactical communication

Saab's TactiGuard Cross domain solution has been successfully deployed in military vehicles integrating the unclassified vehicle platform, sensors and weapons systems with the classified tactical networks and Battle Management System.

Product Highlights

A NEW FIRST:
MULTI-DOMAIN CAPABILITY

TactiGate XD uniquely enables simultaneous, policy-controlled communication across different security domains – handling integrated communication between multiple sub-systems.

This capability is essential for emerging battlefield concepts, such as dismounted soldiers requiring access to selected, mission-relevant classified information.

FLEXIBLE AND CONFIGURABLE DATA FILTERING

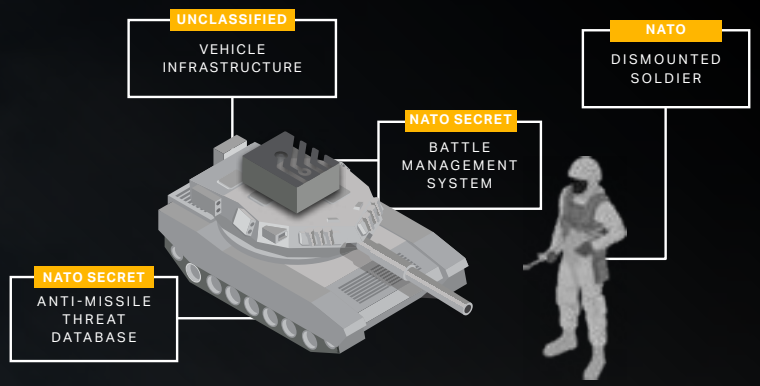
TactiGate XD applies comprehensive format, syntax and semantic validation to incoming and outgoing data. Only well-formed, policy-compliant content is permitted to cross classification boundaries.

Administrators can define custom whitelist-based filters, and updates to filtering policies do not require system re-certification – maintaining agility and compliance.

CERTIFIED TO DEFEND

Key components of TactiGate XD are certified according to Common Criteria.

Included in the NATO Information Assurance Product Catalogue (NIAPC), supporting accreditation for deployments in NATO environments or other classified networks.



SUPPORT FOR DYNAMIC NETWORKING

TactiGate XD offers a broad range of networking capabilities, ensuring seamless integration even in highly complex environments.

Termination of IPsec tunnels provides additional transport security to other nodes without the need to add additional devices.

Traffic shaping and Quality of Service optimise bandwidth usage, delivering smoother network performance even under during peak load conditions.

TIGHTER POLICY ENFORCEMENT AND REDUCED ATTACK SURFACE

Unified policy logic ensures tight coordination between domain separation (cross-domain guard) and traffic filtering (firewall), reducing the risk of configuration mismatches or security blind spots.

Running on a hardened microkernel, TactiGate XD minimises system dependencies and dramatically reduces the trusted compute base (TCB).

TAILORED FOR NATO AND EU JOINT MISSIONS

Purpose-built to meet European defence requirements, TactiGate XD aligns with NATO interoperability standards and supports classified domains, including NATO Restricted and NATO Secret.

It enables secure, policy-controlled data exchange, with dynamic control and secure routing across multiple domain classifications.

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.

COMPACT MILITARY -GRADE DESIGN

TactiGate XD are built to endure the harshest operational environments.

Designed in compliance with MIL-STD-810 that ensure reliable performance at all times.

By combining multiple critical functions into a single device, TactiGate XD reduces hardware footprint, power consumption, cabling, and installation complexity – where size, weight and power constraints are mission-critical.

Threat prevention

TactiGate XD 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.

REMOTE HIJACKING

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

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.
TactiGate XD actively monitors communication and detects and blocks anomalies before they cause an incident.

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. TactiGate XD detects and automatically blocks attempts to exploit known vulnerabilities.

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. TactiGate XD employs a comprehensive range of segmentation and authentication capabilities to enforce robust access policies effectively.

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. TactiGate XD restricts access to websites known for hosting malware, and can furthermore detect malware in transit to reduce the risk of infection.

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. TactiGate XD reduces the impact of DoS attacks using a combination of mitigation technologies.

THE HUMAN FACTOR

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

Cross-Domain Solutions

Clavister and Saab have joined forces to deliver a next-generation cross-domain product tailored for the evolving needs of modern defence and national security.

This collaboration brings together Clavister's deep expertise in next-generation firewall technology with Saab's trusted leadership in defence systems and secure information exchange.

The result is a unified, certified, and mission-ready product that bridges classified domains with unprecedented agility and assurance.

Clavister and Saab partnership delivers a solution that meets the highest security standards and adapts to the demands of coalition operations, mobile warfare, and zero-trust architectures. Together, we are shaping the future of trusted multi-domain communication.

CLAVISTER is a specialised Swedish cybersecurity company, protecting customers with mission-critical applications for more than two decades. Founded and headquartered in Örnsköldsvik, Sweden, Clavister pioneered one of the first firewalls and continues to build robust and adaptive cybersecurity solutions since. Empowering a growing ecosystem of partners and resellers, we are serving customers in more than 100 countries with deployments across the public sector, energy, telecom and defence sectors.

CLAVISTER.COM

SAAB is a leading defence and security company with an enduring mission, to help nations keep their people and society safe. Empowered by its 25,000 talented people, Saab constantly pushes the boundaries of technology to create a safer and more sustainable world. Saab designs, manufactures and maintains advanced systems in aeronautics, weapons, command and control, sensors and underwater systems. Saab is headquartered in Sweden. It has major operations all over the world and is part of the domestic defence capability of several nations.

SAAB.COM