



NEXOR PROTEAN

Secure, Scalable Information Exchange for Modern Defence Operations

A Modern Gateway for Modern Missions

Nexor Protean is an agile software-defined gateway designed to secure information sharing across complex and sensitive environments. Built for the flexibility of today's cloud-first defence architecture, it ensures secure, reliable data transfer between departments, contractors, and allied partners.

With defence operations increasingly requiring collaborative working environments (CWEs) and agile infrastructure, Protean offers the performance and adaptability needed to keep pace, without compromising on assurance.

Flexible, Cloud-Native Design

Nexor Protean has been purpose-built to thrive in dynamic, high-tempo environments. It is:

- Software-defined, allowing rapid deployment and reconfiguration;
- Cloud-native, integrating smoothly with hybrid or fully cloud-based systems;
- Scalable on demand, managing varying data volumes without performance loss.

This makes it ideal for both planned deployments and urgent mission rollouts, where speed and adaptability are critical.



Built-In Security That Evolves With You

Security is embedded at the core of Nexor Protean. It performs deep content inspection and automates security checks to protect data as it moves between domains. Its capabilities include:

- Text and schema validation;
- Malware and anti-virus scanning;
- Content, Disarm, Reconstruct (CDR);
- Quarantining of suspicious content.

These automated controls reduce risk across all trust boundaries, ensuring high-trust networks remain uncompromised even in collaborative or multi-party settings. Protean is fully aligned with zero-trust principles, applying policy controls based on content, context, and configuration, not assumption.



Supporting Complex Collaborative Environments

Defence projects today are rarely carried out in isolation. Secure collaboration between multiple parties, each with distinct policies and trust levels, is increasingly the norm.

Nexor Protean supports Collaborative Working Environments (CWEs) by enforcing tailored security policies for each organisation, verifying every file and message against agreed standards. This allows data to be uploaded, worked on, and exchanged securely across departments, nations, or tiers of command.

No manual handling is needed. Protean automates this process with:

- Configurable rule sets per domain or organisation;
- Deep inspection of files and metadata;
- Enforcement of custom clearance and sanitisation policies.

This makes it easier to manage “many-to-many” data flows across complex partnerships, without sacrificing control or accountability.



Where Protean Delivers Value

Whether part of a long-term programme or a rapid deployment, Nexor Protean delivers measurable impact in several key defence scenarios:

- Joint operations and multinational CWEs;
- Cross domain DevSecOps pipelines;
- Secure transfer of classified software artefacts;
- High-assurance communication between trusted and less-trusted domains.

Why Choose Nexor Protean?

Nexor Protean brings together the three capabilities strategic defence operations need most:

- Security – Trusted, automated controls based on proven SIXA® architecture;
- Agility – Fast to deploy, simple to scale, and easily reconfigured;
- Reliability – Built and supported by Nexor, a long-standing provider of trusted cross-domain solutions.

In an era where secure collaboration and cloud integration are critical to defence success, Nexor Protean offers a powerful, future-proofed solution. It ensures that information flows where it needs to safely, securely, and with complete control, no matter how complex the environment.



Programmable, Automated and Future-Ready

What sets Nexor Protean apart is its adaptability. As operational needs evolve, so too can the system:

- Rules-based configuration means policies can be adapted without system redesign;
- Infrastructure-as-Code (IaC) and Policy-as-Code integration streamlines setup, compliance, and audit;
- Open APIs enable orchestration with existing defence platforms and workflows;
- New filters and checks can be added to support emerging threats or novel file types.

This flexibility allows organisations to stay one step ahead, adapting their security posture without overhauling their technology stack.



Speak to Nexor about your secure information exchange problem.