

capability statement

Nexor Capability Statement

Guards, Gateways and Diodes

October 2010

connect transform protect

NEXOR[®]

www.nexor.com



Nexor Overview

The Company

Recognised for its high assurance guard and gateway expertise and in-depth domain knowledge, Nexor is a leading technology integrator of Information Assurance (IA) solutions for defence and government agencies. Nexor's solutions ensure that sensitive information is accessed, controlled and shared in accordance with prevailing security policies by managing the connection, transformation and protection of that information as it flows between individuals and domains.

Established in 1990, Nexor's links to defence and intelligence date back to the company's earliest years, resulting in Nexor becoming one of the best known niche players in its field. The company's business profile and expertise lend it to be viewed as a strong, yet independent, contributor, capable of providing objective advice and guidance as well as executing to exacting standards.

Headquartered in Nottingham, Nexor is a privately-owned UK SME employing over 40 staff. As such, Nexor represents an important UK sovereign capability. Nexor's management play important roles in the wider community of security and resilience, not least through representation in leading UK forums including RISC (the Security and Resilience Industry Suppliers Council), SITC (the Science and Innovation Technology Council), IACG (Information Assurance Collaboration Group) and Intellect, as well as several UK and NATO defence working groups.

Nexor is proud to count amongst its customers some of the world's largest government and military organisations, including the UK MoD and other UK Government departments, Australian, US and Canadian military and intelligence agencies, and several European defence departments. In these organisations, Nexor technology underpins many mission critical communications and interoperability systems.



Technology

Guards and Gateways

Nexor appreciates that the terms guard and gateway are used inconsistently across the industry. Nexor uses the term ‘guard’ to refer to technology used to enforce a security policy, whereas ‘gateway’ refers to technology that transforms content, protocol or security information from one format to another to enable interoperability.

Nexor has long been recognised for its cross domain security solutions. The company’s role in the industry has been to provide end customer and systems integrators with Commercial of the Shelf (COTS) products, Modified off the Shelf (MOTS) products, bespoke applications and interfaces through our secure development facility in Nottingham. Nexor’s heritage is developing high grade messaging components that have subsequently been used in SECRET and TOP SECRET guard and gateway projects worldwide. The Nexor family of data and mail guards draws on this mature, proven, robust technology as well as new architectural guidelines and frameworks, including those from the UK National Technical Authority, CESG.

History of Guard and Gateway Development

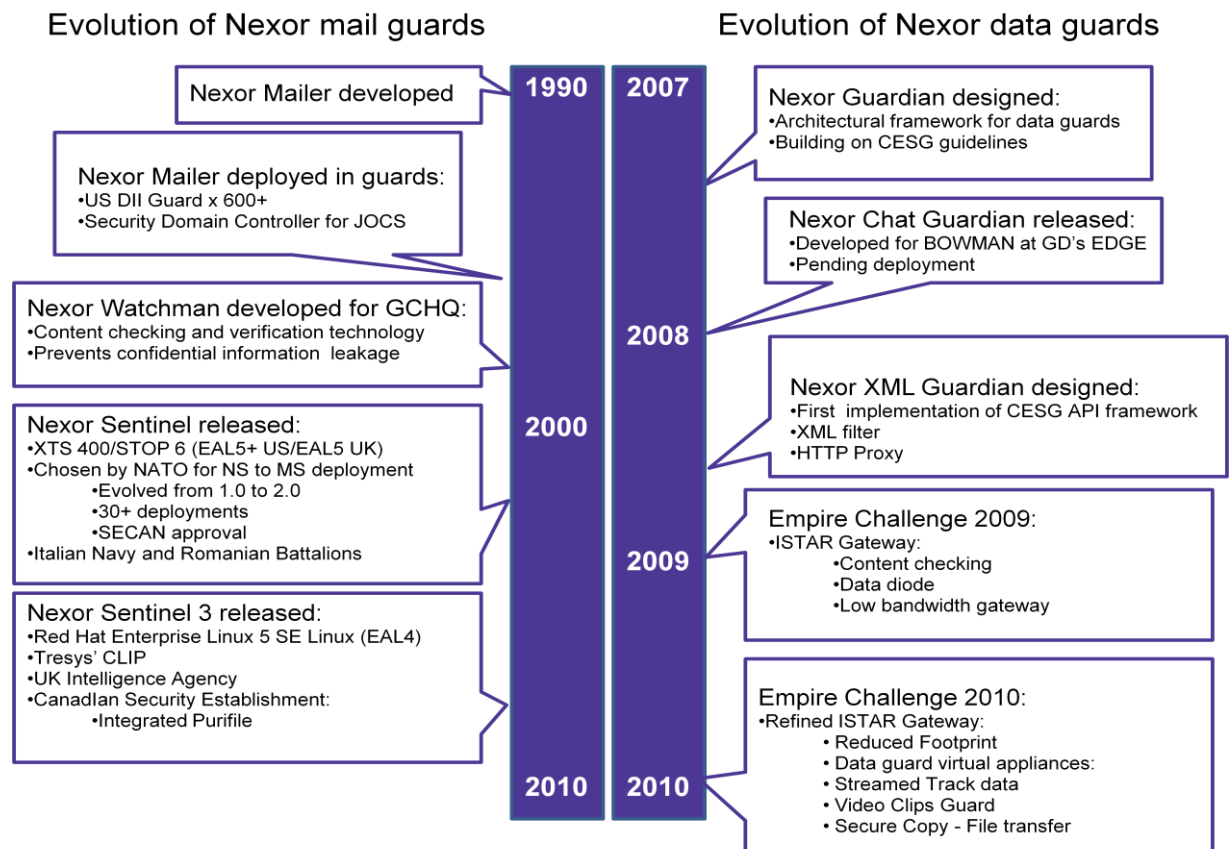


Figure 1: Nexor’s Guard Development Timeline
Demonstrating the breadth and depth of capability and track record



Nexor was recognised very early for having developed important security technology. As well as its own secure messaging offerings, Nexor technology was incorporated into the US DII guard in the 1990's by BAE Systems (formerly DigitalNet and Wang), which now has over 600 deployments. The same Nexor technology has been deployed by many third parties to create gateways, for example, ACP127 gateways, profilers and to create guards, for example security domain controllers.

In 2004, Nexor decided to capitalise on its secure development capability and the suitability of its technology for guard and gateway solutions and added these to its market strategy. Nexor became the exclusive European reseller of BAE Systems' XTS400/STOP 6.4 guard – branded Nexor Sentinel - a non-ITAR restricted product built for the Canadian market. Nexor has developed a leading UK capability in this product and undertaken onward development to meet the demanding requirements on NATO, resulting in Sentinel being the preferred guard of choice for NATO Secret to Mission Secret deployment.

In 2009, Nexor launched Sentinel 3, the SELinux variant of Sentinel. In building Sentinel 3, Nexor drew on the expertise of leading SELinux authority and host of the SELinux open source repository, Tresys Technology, to ensure the robustness of the security policies.

One of the key components of Nexor's guard and gateway technology is Nexor Watchman which was built specifically for a UK agency customer to address the need to prevent accidental data leakage. Watchman provides content checking and verification technology to prevent confidential information being transferred by unauthorised parties between specified domains. Watchman is deployed on Trusted Solaris at the original customer site, but is now also used inside Sentinel on both SELinux and STOP and as a standalone gateway element on Windows.

Nexor Filters

Nexor is experienced in handling various data formats and building filters to process different data types. Nexor's solutions incorporate proven filter technology based on the original EAL4 Military Message Handling System (MMHS) filter design from BAE Systems and on Nexor's own Watchman product. Specifically, Nexor filters handle validation of the structure and content of data in:

- X.400 interpersonal and military messages
- SMTP/MIME
- XMPP
- XML



The filters also validate the policy by checking:

- Signatures and encryption
- Security labels in multiple locations and formats including label dominance
- Senders and recipients
- Attachment types
- Military message precedence
- Prohibited words / phrases
- Viruses and malware called by calling a 3rd party virus scanner.

Deep Content Filters

Nexor incorporates other filters into its solutions. In particular, Nexor collaborated on the following projects:

- Above Secret Guard: in conjunction with QinetiQ and BAE Systems Insyte, as part of the CWID ISTAR demonstration in 2006, Nexor provided guard technology and expertise that included checking for steganographic content
- DII - BOWMAN Guard / Gateway: in partnership with QinetiQ, Nexor developed a guard demonstrator to provide the gateway between strategic CWID core DII infrastructure and the tactical BOWMAN community. This included the Sybard filters working with Sentinel
- Government Agency: to address the specific needs on one customer, Nexor integrated the Purifile deep content checker with Sentinel 3 mailguard.

Depending on project requirements, Nexor can use its Secure Development capability to modify its own filters, develop new filters or integrate third party filters.

Data Guards

Nexor has been working on a generic design and has produced data guard solutions since 2008. Nexor data guards are built on a common framework to allow support for multiple different transport protocols and multiple different content filters. As of October 2010, multiple different instances of the data guard have been built to be used in demonstrations and for user trials in exercises. Figure 2 below shows the current state of the guard architecture with proxies supporting HTTP, XMPP, SCP, and UDP transports.

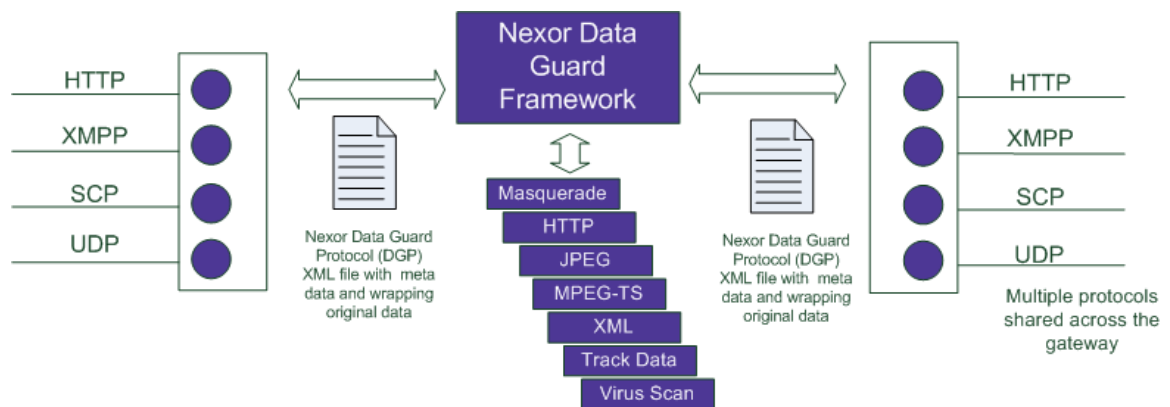
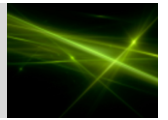


Figure 2: Nexor Data Guard

Designed to be secure, modular and scalable

The Masquerade filter identifies the content being transferred across the guard and schedules the content specific filters to be run. A number of filters have been prototyped to show checking of:

- HTTP protocol
- JPEG images - validating the meta data added to the EXIF field by sensors
- MPEG-TS video clips - validating that the correct video format (H.264) is present and checking the associated meta data added by the sensors
- XML - validating the XML schema with the ability to further validate specific XML content such as Cursor on Target track data by plugging in extensions to the XML filter
- Virus Scan - using Sophos Anti-Virus to check the content for malicious code
- Multiple Domain Support - the Nexor Data Guard has been designed with a Routing Engine component; this sits between the proxies and the guard framework to inspect the data envelope and make the appropriate routing decisions based on the domains that are supported. This capability will allow the data guard to support multiple domains for any protocol that contains routing information
- Scalability - the modular design of the Nexor Data Guard allows for scalability to meet increased traffic volumes. The filters run in separate processes and can be run in parallel to scale up as traffic volumes increase. Additionally, a number of instances of the guard can be run in parallel either to separate traffic by protocol or to load balance the data across data guard.



Data Guard Evolution

The Data Guard solutions are developed using an Agile approach, which has enabled the rapid evolution of the technology in line with a number of different customer scenarios for technical demonstration and proof of concept situations. Nexor’s product lifecycle methodology allows accreditation, deployment and productisation aspects to be built in from the start. Figure 3 shows the components required to reach full product release.

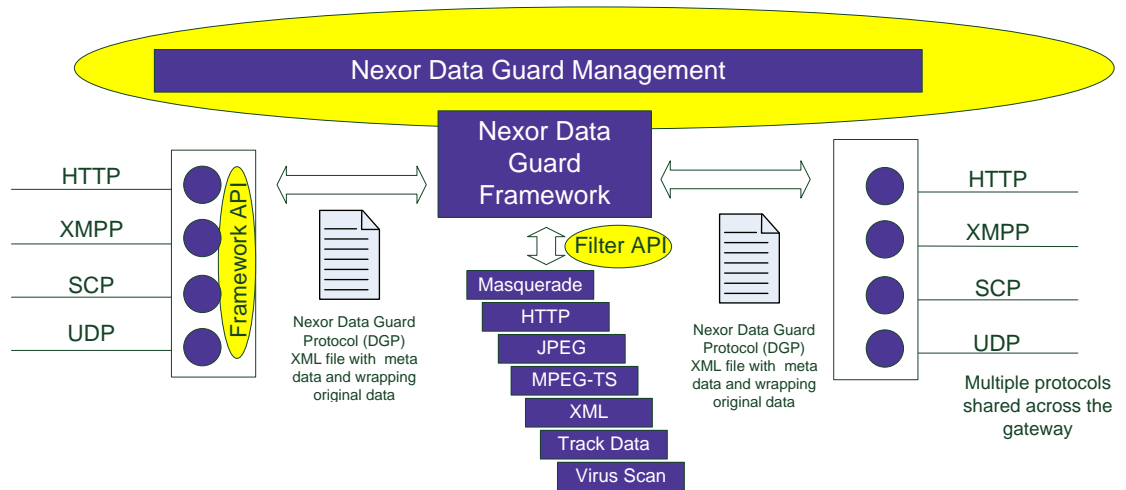


Figure 3: Nexor Data Guard Development Areas
An extensible architecture which can be quickly enhanced to respond to ever changing threats

Proxies

Additional proxies will support new transport protocols. The proxies will need to extract additional information from the content and place it in the meta data as required by the agreed interface to the guard. This could include, for example, XML security labels.

Filters

The XML filter will validate the meta data passed to it from the proxies. Additional filters may need to be developed dependent on the actual content being transferred and the level of checking required.

APIs

Currently, the Nexor Data Guard uses internal unpublished APIs between the proxies and the guard framework and between the guard framework and the filters. These APIs could be made publicly available to allow customers to develop their own filters and proxies as different applications are shared.



Guard Management

Management of the Nexor Data Guard will be in line with the overall Nexor guard management strategy, which will allow for management of multiple devices from a single workstation. As shown in Figure 4, the management workstation supports connection over a network using SSH to configure the devices. If a network connection is not possible or not allowed from a security perspective, then the configuration can be written to removable media, such as a CD and loaded directly onto the device. Alternatively, the management workstation could be directly connected to the device to allow local configuration. This approach will allow for consistent policies to be applied to multiple different devices.

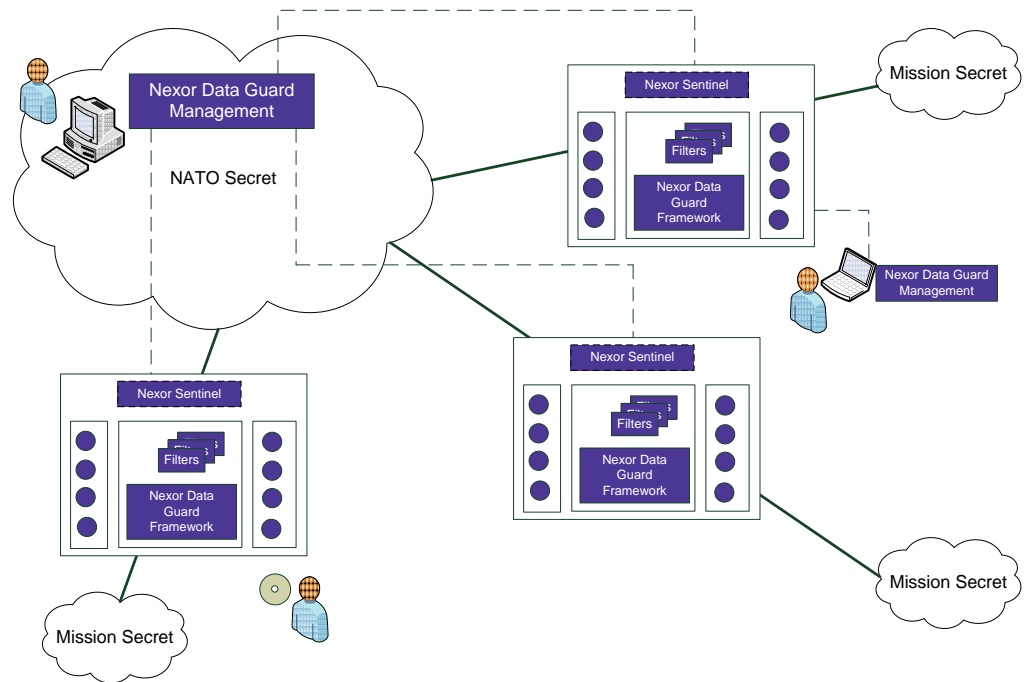


Figure 4: Nexor Management Workstation
Supporting local and centralised remote web based management



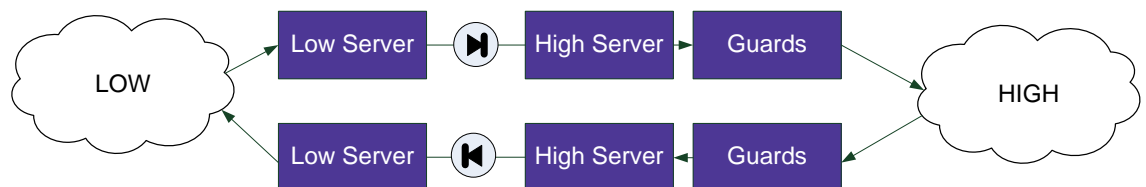
Diodes

The Nexor Data Diode is an EAL7+¹ evaluated product that provides one way data transfer for a wide range of applications and data protocols. A Nexor Data Diode solution consists of the hardware data diode (a 19", 1U rack mounted server) and two servers. A low side server receives the data to be transferred across the diode and converts it as necessary to allow one way transfer. The high side server receives the data from the diode and converts it back to the original protocol to forward it on to the destination.

The Nexor Data Diode supports a number of protocols out of the box, but can also be modified to support further protocols as required. As standard, the Nexor Data Diode supports:

- SMTP
- UDP (including SNMP, syslog, NTP, video streaming)
- CIFS
- FTP/FTPS
- SCP

A Nexor Data Diode solution can be used in conjunction with Nexor guard products to provide either one way transfer with integrated content checking or two way transfer using a data diode for each direction as shown in Figure 5.



**Figure 5: Two way content checking using data diodes
Combining content checking and diode technology for enhanced security**

Future work on the Data Diode solution includes the ability to perform the content checking on the high and low side servers to reduce the overall footprint of solutions.

¹ EAL7 certificate issued by TNO in The Netherlands



CyberShield Secure™ Development

Introduction

Nexor's CyberShield Secure™ Development facility provides a UK sovereign capability to produce high assurance software. Nexor offers a full outsourcing service to build, enhance, integrate, port or productise secure solutions for customers. The CyberShield Secure™ Lifecycle can be applied in both Agile and Waterfall projects. In either case, Nexor ensures that security objectives are established and developed throughout the lifecycle. Threats and security requirements are analysed alongside the functional requirements; both are captured in Unified Modelling Language (UML), a standardised methodology for modelling the structure, behaviour and interactions of system elements. Security objectives and requirements are identified from both physical, platform and software perspectives.

Nexor keeps a constant eye on new industry trends and best practice. CESG guidance, specifically that found in its assurance guidance model, is a primary influence. Other inputs to best practice and procedure include CERT (from the US Software Engineering Institute), "Build Security In" initiatives and Microsoft's Secure Development Lifecycle. Feedback loops are built in throughout the CyberShield Secure™ Lifecycle to ensure early capture and rectification of issues. Completed code passes through the CyberShield Secure™ verification suite where it is thoroughly tested by ISEB qualified testers. During this phase, accreditation document sets are written ready for delivery with the final software and manuals.

Development Approach

Nexor's philosophy is that secure solutions should be developed using secure operating systems, so we have adopted the technical approach of using Common Criteria evaluated operating systems as the basis for developing applications. The operating systems are used to enforce the network separation and the applications are designed to exploit the Security Enforcing Functions of the underlying operating system. The resulting applications and appliances may be deployed as part of a wider system and accredited within that context. This approach speeds the initial system build and enables rapid adaptation of the solution to meet changing needs.



Technical challenges

Examples of the challenges and resolutions during the design and build of guards include:

- **Management interfaces:** there is a growing desire for centralised management of distributed guards, leading to a demand for sophisticated management GUIs. Secure operating systems have not typically offered this. Nexor has developed a new approach to this including the ability to manage multiple different appliances from one console. This design allows Nexor's guards to be managed either centrally or remotely.
- **Deployability:** the footprint and performance of guards is a regular challenge; the demand is for scalable, transportable, rugged solutions. Nexor's architectures are modular and the newest designs fit onto a 1U system and may be virtualised. Integrated solutions are built into transportable flightcases.
- **Accreditation:** building systems that are acceptable to accreditors is always a challenge. Experience has shown that early and open engagement with the accreditors is essential, combined with a pragmatic approach to adopting suggestions and adapting solutions dynamically.
- **Tracking and preventing vulnerabilities:** this constant challenge is tackled by regular and diligent monitoring of known vulnerability sources and by designing systems to make optimum use of operating system security features. For example, by using Tresys' Certifiable Linux Integration Platform (CLIP), which provides a security hardened operating system platform to host secure applications, we mitigated against both the Proc Filesystem Race Condition and the SMM Cache Poisoning Vulnerability, and any zero-day exploits based on them, without any system changes.
- **Unclear requirements:** requirements were not always documented at a detailed level, resulting in several iterations of the revised software. This has led us to implement an Agile approach to software development to allow multiple iterations with customer input at regular intervals.



Testimonial

The success of Nexor's solutions is summed up by our customers:

- Awarded a framework contract and appointed as supplier of choice for the provision of high assurance mailguards for operational use by NATO Maintenance and Supply Agency (NAMSA) (<http://www.namsa.nato.int>)
- "Nexor exceeded our expectations by producing an exemplary beta and an excellent product on time and to budget", spokesperson for GCHQ regarding Nexor Watchman
- "Exemplary performance at Empire Challenge 2010", John Dickinson, DES PTG-TD-C4ISTAR2.

Methodologies

Nexor has its own CyberShield Secure™ methodology which can work with a traditional waterfall development approach, but to address the market need for better value for money and uncertain or changing requirements, Nexor has added the Agile approach to its capability. Agile works on the basis of setting objectives, then working iteratively and interactively with the customer, using time-boxing to maintain control and impetus in the project.

Platforms

Secure and high assurance environments require the highest standards of robustness and resilience. On top of this, there is a balance to be achieved relating to performance, speed, functionality and accreditation. Nexor has focused on building expertise in a range of platforms and operating systems to cater for many circumstances, including:

- Trusted Solaris
- STOP 6
- SELinux

Nexor has also investigated innovative approaches to address the performance needs of real time data guards.

APIs

In addition to its own software development capability, Nexor makes a set of Software Development Kits (SDKs) available to its customers. The SDKs provide a series of Application Programme Interfaces (APIs) that enable an open method of accessing messaging, directory and security services conforming to international standards. Over the last 20 years, Nexor APIs have been used to make specific, specialist products such as data profilers and ACP127 gateways.



Services

Project Management

Nexor has a track record of delivering on time and to budget. Nexor has undertaken a business improvement programme to review and revise its processes in accordance with Lean techniques and in compliance with Capability Maturity Model integration (CMMi). This initiative extended through the development department including project management. All Nexor assignments are managed using a proven and comprehensive service delivery methodology as shown below.

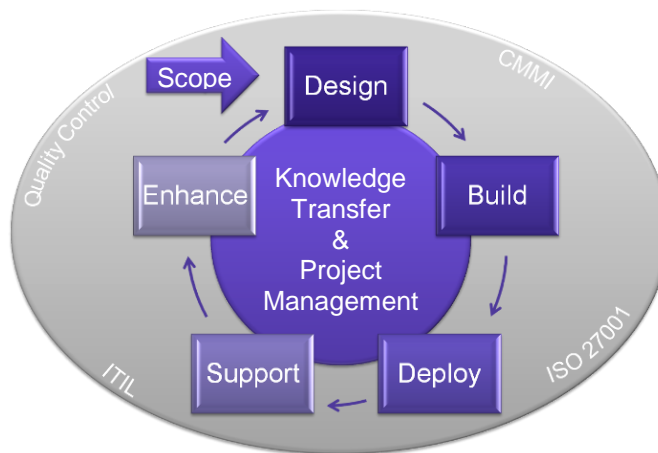


Figure 6: Nexor Delivery Process
Proven service delivery methodology

Nexor is always pragmatic in its approach ensuring efficient and effective application of all policies and procedures. This means the delivery approach for each project will be appropriate, to ensure quality and consistency of delivery is maintained without being overly onerous.

Integration Support

Nexor technical consultants, architects and engineers are amongst the best in this field of specialisation and they may be called upon to provide expert advice and guidance. Many years' experience, combined with Certified IT Professionals (CITP), Certified Information Systems Security Professional (CISSP) and Certified Secure Software Lifecycle Professional (CSSLP) status and relevant clearances, lead Nexor's staff to understand the wider business and technology context of information assurance and interoperability as well as the detailed policy, architecture and solution options available.



IA/Accreditation

Philosophy

Nexor's experience of creating software for accreditation and evaluation has been built into the development process over many years. Nexor holds the philosophy that application software should be suitable for tailoring to suit each customer's requirements, so has designed a development approach to support this. Nexor uses Common Criteria evaluated operating systems as the basis for developing its applications, which are designed and built to exploit the Security Enforcing Functions of the underlying operating system. The resulting applications and appliances can then be deployed as part of a wider system and accredited within that context.

This approach speeds the initial system build and enables rapid adaptation of the solution to meet the ever changing needs of the projects in which Nexor technology is deployed. By working in this way, Nexor believes it is possible to support the model of dynamic reaccreditation of systems by being able to quickly assess the risk that introducing a change in any one element of a solution may have on the system as a whole.

At a practical level, Nexor's core technology underpins numerous accredited systems deployed in the defence and intelligence communities and Nexor has directly assisted a number of projects in this process. The projects below evidence Nexor's experience in supporting accreditations.

- Sentinel 2 was developed as an enhancement to Sentinel 1, an EAL4 application running on an EAL5+ platform. Nexor engaged with SECAN, NATO's accreditation authority, from the beginning of the project, providing analysis and design documentation at every stage.
- Nexor's demonstration at CWID 2006 (see Deep Content Filters below) was assessed at ARL8, one of a small number of demonstrations to achieve this level.
- Nexor participated in Empire Challenge 2009 with a fully integrated demonstration solution that was accredited by both the US and the UK within weeks.
- Nexor developed customised Security Label Mapping (SLM) software for a major operational system. Nexor was engaged to provide validation testing services and code review support to achieve security accreditation of the overall solution.
- Working with a Lead System Integrator, Nexor designed and developed its Nexor Oracle Gateway for a UK Government agency and produced all of the evidence to support the system accreditation of the resulting gateway solution.



Future Roadmap

Nexor expects the demand for guards and gateways to grow significantly over the coming years due to numerous factors:

- Continued multi-national defence cooperation in support of military and peace-keeping action that requires increased interoperability
- Use of new and different technologies and standards, such as instant messaging, VOIP and XML, increasing the variety of interoperation required
- The trend towards “need to share” versus “need to know”, which encourages wider access to data and information with a view to improving the intelligence picture, thereby supporting better counter terrorism measures
- The response to increased occurrences of data loss and leakage, whether accidental or malicious
- The continued growth of collaboration between defence, other government departments (OGDs) and non-government departments (NGOs) to provide a concerted response to the threat of terrorism and national disaster.

In the past, guard and gateway technology had been the preserve of the defence and intelligence communities, operating typically at the high assurance end of data classification. With increased focus on the impact of poor data management across many industries the appeal of this technology is growing. Nexor will therefore continue to develop its families of guards and gateways. Examples of current area of research and development are:

- Policy and process for data labelling, including aggregation and association. Investigation and trialling solutions to facilitate the sharing of outputs, while preserving the security classification
- The role of guards and gateways in the automation of governance, risk and compliance policies and procedures
- The use of tracking software to assist in data management within an organisation and beyond the organisational boundary
- The role and influence of human factors in enforcing security policy and whether and how this affects the design and implementation of technology
- Assessing differing architectural approaches to support the needs of high performance real time data guards.



Track Record

Below is a range of projects that show Nexor's guard and gateway technology in action. These examples show both Nexor as a COTS provider and Nexor as a software house and technology integrator.

Operational Projects

MOTS Project

In 2006, Nexor was awarded a framework contract and appointed as supplier of choice for the provision of high assurance mailguards for operational use by NATO Maintenance and Supply Agency (NAMSA) (<http://www.namsa.nato.int>). In advance of this award, Nexor worked in close collaboration with NAMSA to enhance Nexor Sentinel to offer boundary protection services for NATO mission systems. This project has been hailed a successful example of industry's flexibility and responsiveness to the customer's needs.

Custom Project

When a UK agency recognised a requirement to prevent accidental data leakage, Nexor developed Nexor Watchman specifically to address this need. Watchman provides content checking and verification technology to prevent confidential information being transferred by unauthorised parties between specified domains. Watchman is standards-based and supports X.400 and SMTP.

COTS Project

After a thorough evaluation of the market, Nexor Sentinel 3 was selected by a North American Government agency to fulfil its cross domain guarding requirements. The customer onward recommended this solution to another agency that is using it in conjunction with Nexor gateway technology to provide a complete border solution.

Custom Project

In 2005, Nexor was selected to participate in a major UK ABOVE SECRET intelligence programme, which included the brief to enable the secure transfer of information between standards-based X.400 and SMTP messaging and an Oracle database. Nexor developed the Nexor Oracle Gateway to fulfil this requirement. This project was delivered on time and to budget.

OEM Projects

Nexor's APIs have been used by a number of leading System Integrators over the years to complement their own defence solutions, including:

- Selex Communications for its ACP127 naval messaging solution
- Fujitsu for its Security Domain Controller in AMRAD and JOCS
- EADS for its security features in the NATO Messaging System (NMS).



Demonstrators

Guard/Gateway Project

In 2009, Nexor created an ISTAR Security Gateway for a major international demonstration. The gateway provided a mechanism to transfer ISTAR information between security domains. The gateway allowed one way transfer of information from a low domain into a high domain to provide critical information to that domain. To create the solution, Nexor integrated its own and third party technology including an email generation server, an email content checking server, high side and low side data diodes and a low bandwidth email gateway with all the relevant infrastructure components into robust flight cases for use in an extremely harsh environment. This project was taken from concept to delivery in four weeks and accredited by the UK and the US for use at the event.



Figure 7: Nexor Secure ISTAR Gateway

Integrated Gateway

For Empire Challenge 2010, Nexor developed the ISTAR Gateway further and conducted further successful trials – see separate Case Study for details.

Integration Project

Nexor completed a successful contribution to General Dynamics UK's (GDUK) BCIP6 Technical Demonstration Programme (TDP) by showing both domain and multi-protocol guarding in a tactical environment. The TDP required GDUK, in partnership with the MoD DE&S BATCIS IPT, to provide a view of potential capabilities available in BCIP6. It was designed to inform options for capability enhancements for battlespace information management, improved interoperability with UK and allied systems, and improved resilience through advanced system management. A specific requirement of the TDP was to show a mechanism to control the flow of information based on security policy, thereby proving the ability to enable and appropriately protect connections between domains of different security classifications.



Nexor deployed the Watchman component of its Border Gateway COTS suite to validate the security policy on the domain boundary and to implement dirty word checking. Nexor also deployed military extensions to commercial instant messaging products to show additional security measures and tracking features in an instant messaging environment. Nexor extended the XMPP protocol to include security labelling of chat sessions. These enhancements demonstrated how increased security and assurance can be incorporated into an instant messaging system by validating security policies between domains, in this case between an appropriate UK representative domain (created for the TDP) and the BOWMAN domain.

A second demonstration utilised the Mailer and Watchman components of the Nexor Border Gateway, running on the Linux operating system, to validate security labels and control the flow of information based on security policy. This was implemented on the border between two domains containing Microsoft Exchange Servers utilising the SMTP protocol.

The TDP provided MoD with a clear insight of the benefits of an open architecture utilising industry standards to accelerate time to field, whilst maximising industry technological advances.

As a result of this successful work, Nexor joined GD's EDGE initiative and built its new Chat Guardian product to demonstrate to MoD the potential for guarding instant messaging in the BOWMAN environment.

For further information on Nexor or our Guard, Gateway and Data Diode capabilities, please contact info@nexor.com