Protect your secrets and safeguard availability and integrity of critical assets

Ruggedized DataDIODE™ solutions

Confidential information needs to stay confidential. There's no question about that. However, high levels of security often hamper your productivity. On the other hand, loosening the reins on security for a more fluent workflow means putting your data at risk.

FOX IT
part of nccgroup

NEXOR®

fox-it.com/datadiode

With the Fox-IT & Nexor Ruggedized DataDIODE™ solutions you can solve this dilemma. Its one-way network connection offers the highest certified level of security and prevents unwanted access to business assets and critical systems, while facilitating a free flow of information. Thanks to its ruggedized design it can be used in demanding environments with extreme high or low temperature and humidity levels, dust, movement etc. Take the nuclear, power, oil and gas industry and/or other critical infrastructure areas, for example. These environments require equipment that can operate reliably under even the most severe circumstances.

CC EAL7+ certified

The Ruggedized DataDIODE™ Hardware ensures that state and company secrets remain secure and that critical systems cannot be manipulated. The Ruggedized DataDIODE™ is the only one-way solution worldwide that has received widespread independent confirmation of its security claims and is classified with the highest level of Common Criteria Evaluation: EAL7+. Moreover, it is the only device that makes use of light emitting diodes and receivers within the hardware, providing a 100 percent guarantee of a unidirectional flow of data at a physical level: it does not have software, firmware, or FPGAs. Hence, it cannot be exploited or misconfigured.

The Ruggedized DataDIODE™s come in a 1G and 10G version and provide the following **key features**:

- Industry standard fiber optic lc connectors
- Rugged coated steel and anodized aluminum casing
- Extended temperature and humidity range
- TEMPEST level-A compliant by default
- Suitable for transport
- Shock and vibration resistant: Truck, Rail, Air (non-operational) ASMT D 4728

Nexor and Fox-IT – a solid partnership

Nexor specializes in secure information exchange and cross-domain applications for the UK government, defense and critical national infrastructure and has been an OEM (original equipment manufacturer) partner of Fox-IT since 2009. Together, we established an excellent working relationship which led to Nexor becoming a Fox-IT OEM partner. Today, we continue to collaborate closely to develop solutions for our chosen markets. As shown in the cases laid out in this document where Nexor spearheaded both projects.

Importing patches to a secure network

In this case a UK government agency needed to install system update files or patches on its closed classified network (Impact Level 5/IL5) that has no connection to the internet or any other internal system. Automating this process is essential to ensure operational efficiency, but importing these files poses significant security risks that need to be mitigated. These risks included an unauthorized data flow back to the other networks and potentially the outside world and denial of service caused by for instance forcing a component malfunction. A new solution was needed that would tackle these issues.

The solution

This solution provided a means to import the patches whilst ensuring data only flows one way, thereby reducing risks of data loss and back communication channels. As part of the agency's patch ingest system, all the different patches from Microsoft, Java, anti-virus software packages and other software vendors are placed into a staging area. A Proxy (upstream) is connected to the staging area to capture the files and send them on to the DataDIODE™, which transfers the patch files. In doing so it provides a 100 percent guarantee of a one-way communication as its physical construction only allows data to flow in one direction. A second Proxy (downstream) is connected and delivers the files into the agency's closed secure network.

Thus, the agency reduced risk of data loss from its closed (IL5) network, improved business efficiency as network users were able to use the latest software features distributed by the update mechanisms and lowered maintenance costs due to the removal of the manual update procedures.

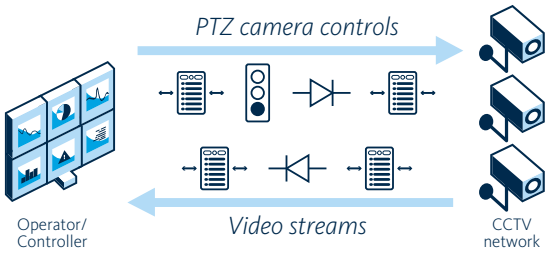
Secure remote camera control

Secure Remote Camera Control

Security cameras are increasingly part of today's society; however, these cameras are typically located in insecure public areas, but feed the vital imagery back to secure control rooms. Civil authorities often use cameras to protect public spaces, police for law enforcement and the military for force protection. In the control rooms operations staff and intelligence officers monitor the images for signs of wrong-doing. This often involves the desire to pan, tilt or zoom (PTZ) the camera to take a close look at a suspected security event.

A simple networking configuration is often used, which introduces vulnerabilities into the control system network: can an adversary supply false imagery, use the network to mount a denial of service attack, launch malware or even access the intelligence information?

The Nexor Secure Remote Camera Control Solution mitigates these risks. The solution package includes DataDIODE™ and content checking software, to ensure only video images flow into the secure network and to ensure only PTZ data can flow out. A recent implementation has been accredited and deployed in a high assurance environment, to provide robust protection of a classified network.



Set-Up: DataDIODE™s in High Assurance set-up, Nexor Guardian content checker software.

DataDIODE™ Content Checking

Nexor have used their experience of deploying cross domain solutions incorporating DataDIODE™ and guards to develop a shrink-wrapped content checker data diode appliance.

The Nexor DataDIODE™ Appliance Content Checker provides the ability to deploy an integrated file validation capability together with the DataDIODE™ to further protect themselves in high threat environments.

The reason behind adding extra functionality to the Nexor DataDIODE™ Appliance, it now provides the customer with the extremely useful capability to identify, inspect and validate a wide range of files as they are transferred between domains.

The Nexor content checker recognizes that different file types introduce unique threats; File Foundation Pack enables administrators to build individual security policy rules on configurable groups of content types using the management GUI. This means that specific rules can be created to mitigate against the unique threats in each file type. The available content filters include:

File Foundation Pack, which provides the following filter capabilities:

- File type whitelist/blacklist
- Dirty work searching
- XML & text schema validation

	Content Types Group	Rule	Virus Scan	Deep Scan	Dirty Words	Work-flow	Verification Filters	
	Associated Metadata	Allow			✓			+
+ −	XML Documents	Allow				✓	+ − ✓ XML Filter	+
+ −	Plain Text Files	Allow	✓		✓	✓	+ − ✓ Text Content Patterns	+
+ −	PDF Documents	Allow	✓	✓	✓	✓		+
+ −	MS Office Documents Old	Deny	✓			✓		+
+ −	MS Office Documents Macro-Enabled	Deny	✓			✓		+
+ −	MS Office Documents Current	Allow	✓	✓	✓	✓		+
+ −	Image Files	Deny	✓	✓		✓		+
	Other Identified Content Types	Deny				✓		+
	Unidentified Content Types	Deny				✓		+

Groups Policy: set content types group specific configuration and toggle which checks should be done for each.

Manual Release Workflow:
The Manual Release Workflow quarantines all submitted files for a human-in-the-loop validation check. Once the file is submitted to the DataDIODE™, authorizers are notified who can then view the file in their browser to inspect its content if necessary. Authorizers can either approve individual or multiple files for release depending on their review. Once authorized, users are notified when files have been released. To simplify authorization, Active Directory integration enforces access control on users' quarantined files so that it can only be accessed and authorized by their line manager or authorizer group.

Third Party Filters:
- Sophos AV
- PuriFile DLP

Additional third-party AVs and filters can be integrated upon demand.

The Nexor DataDIODE™ Appliance Content Checker provides a secure, simple to configure content checking capability along with the proven data diode functionality.

Fox-IT
Fox-IT prevents, solves and mitigates the most serious threats caused by cyber-attacks, data leaks, or fraud with innovative solutions for governments, defense agencies, law enforcement, critical infrastructure and banking and commercial enterprise clients worldwide. Fox-IT combines smart ideas with advanced technology to create solutions that contribute to a more secure society. We develop products and custom solutions for our clients to guarantee the safety of sensitive and critical government systems, to protect industrial networks, to defend online banking systems, and to secure confidential data.

Nexor
For over twenty five years Nexor has specialized in developing its secure information exchange (or cross domain) solutions for defense, government and critical national infrastructure organizations. This enables organizations to perform more efficiently and effectively. The connection of secure networks is achieved by using people, process and technologies that align to best cyber security practice established by national authorities.

For more information about any of the solution cases provided in this document please consult the Fox-IT or Nexor website.

FOX IT
part of nccgroup

fox-it.com/datadiode

Fox-IT B.V.
Olof Palmestraat 6, Delft
P.O. Box 638, 2600 AP Delft
The Netherlands

T +31 (0)15 284 7999
F +31 (0)15 284 7990
fox@fox-it.com

Fox-IT is part of NCC Group.

NEXOR®

European Office
Nexor Limited
8 The Triangle
Enterprise Way
ng2 Business Park
Nottingham
NG2 1AE
UK

T +44 (0) 115 952 0500
F +44 (0) 115 952 0519
info@nexor.com