NEXOR

IMPORTING PATCHES TO A SECURE NETWORK

Often you need to transfer patches or system updates from one network to another that have different levels of security. In order to maintain the confidentiality of the downstream server you need to be able to control the flow of data in a secure manner.

THE CLIENT

A UK Government Agency

THE CHALLENGE

A UK Government Agency needed to install system update files or patches to 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:

- Unauthorised data flow back to the other networks and potentially the outside world;
- Denial of service caused by forcing a component malfunction.

Traditional security solutions, such as air-gaps, where there is no physical connection, and firewalls, are no longer secure or efficient enough:

- Air-gaps are labour intensive and prone to poor operational practice, which together introduce vulnerabilities;
- Firewalls cannot be demonstrated to prevent all risk of data flows from the secure network and are therefore not suitable on their own in environments where the impact or threat is high.

A new solution was required that would tackle these issues.

THE SOLUTION

The Nexor solution provides 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 Nexor Proxy (upstream) is connected to the staging area to capture the files and sends them on to the data diode;

- A Nexor Data Diode transfers the patch files, in doing so it provides a 100% guarantee of a one-way communication as its physical construction only allows data to flow in one direction;
- A second Nexor Proxy (downstream) is connected and delivers the files into the Agency's closed secure network.

The solution was built, configured and tested off-site before delivery to a secure location for the client.

TRUSTING THE SOLUTION

The Nexor solution was developed through a combination of our accredited professionals, CyberShield Secure® processes and industry-leading SIXA® technology portfolio.

Critical to any security solution is gaining the confidence that it meets the security claim. The Nexor solution was designed to meet business critical customer requirements.

Specific measures that supported this were:

- The Nexor Data Diode is assured to Common Criteria EAL7+;
- All the appliances used were Common Criteria certified to Common Criteria EAL 4+;
- Software was developed using our CyberShield Secure® development process that conforms to Microsoft SDLC, CMMI and TickITplus standards;
- Use of threat modelling during development;
- Delivered using cyber security professionals with industry-recognised accreditations;
- A three-year support and maintenance package was included in the solution.

THE IMPACT

The automation of the patches to the segregated network meant that the UK Government 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;
- Reduced maintenance costs due to the removal of the manual update procedures and reduced clean-up costs of a malware infection.

NEXOR CAPABILITIES

Nexor provides solutions to get information in to and out of secure networks. This enables organisations 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.