Introducing DOBUS™ our trusted content delivery system.

DOBUS is a high-availability, trusted content delivery system that can help reduce risk of your eco-system being compromised when you need to reach out for new content. Housed in a secure vault to offer you the highest levels of MoD accredited protection, the DOBUS platform sources content direct from the publisher, fully vets and cleanses the package and transfer via a one-way diode to a high security area. From here you can access the content directly, greatly reducing the risk of contamination as everything comes from a single reliable source. It works without an internet connection or even when you're under attack. This enables you to protect and rebuild your system if compromised.

Benefits of using DOBUS™

- Trusted and secure procedure for procuring and verifying online content from almost any vendor.
- Independent, secure system off the internet, creating a safe and accredited environment.
- Secure storage for data classified as Official/Official sensitive up to Top Secret.
- Robust network design for reliable delivery of content.

How DOBUS™ works

DOBUS™ gathers data, patches, updates and bug fixes direct from publishers, manufacturers and approved online vendors via secure links. It carries out thorough checks for viruses, malware, suspicious coding and any other faults or indicators of compromise. Once we are certain the patches and updates are clean and authentic, they are made available for distribution to relevant parts of your organisation through one of three options:

- DOBUS™ REMOTE – Physical delivery of updates and content direct via a hard copy on an external drive.
- DOBUS™ CONNECT – Delivery of updates and content via secure VPN tunnel
- DOBUS™ CORE Bespoke – Delivery of updates and content through a direct fixed line.

How DOBUS™ can be used

DOBUS™ can be used in a multitude of ways, here are a few examples of how it can become part of your security playbook:

Secure Patch Delivery: We gather patches, updates, and bug fixes direct from any publishers and manufacturers so that you can keep up to date with your patch management program, protecting and optimising your software, systems, and applications.

Firmware Provision: Just like patching we can securely source firmware updates, ensuring you can continually optimise your hardware.

DevOps Enablement: DevOps helps you to achieve digital business transformation and rapid delivery of high-quality software and IT solutions. However, a crucial part of this process is building an artefact repository software development process. Accessing your artefacts through DOBUS™ gives you a safe, secure alternative to remote repositories. Such as Python & Github.

Deployment tool integration: Integrate with existing deployment tools such as IBM Bigfix providing patches directly into your systems ready for deployment.

Critical Vulnerability Response: All modern software contains vulnerabilities, normally the risk of these are low and can be resolved as part of a normal patch management cycle. However, in some instances the impact of the risk is so high that work is required immediately to resolve the issue. DOBUS can give you access to critical patches in order for you to minimise the risk of them being exploited.

Secure Digital Library: Sometimes you need to be able to access content such as technical specs or schematics anywhere in the world, even without an internet connection. DOBUS can be used as a secure storage area for important documentation without exposing it to the internet.