PROLINX

› Secure, Simplify, Collaborate

PROLINX SECURE MANAGED SERVICES CATALOGUE

DEPLOYED BEARER OF OPPORTUNITY (DBOO)

Suited For - Customers that require a secure compute and communications platform that is easily and rapidly deployable to support remote operations but is also scalable and can interface, where required, with headquarters/backend systems.
Available/Accredited at - OFFICIAL SENSITIVE and SECRET levels.
Connectivity to - MOD Core Network (Official Sensitive) (MCN(OS)), MOD Core Network (Secret) (MCN(S)).

The Overview

The Prolinx Deployed Bearer of Opportunity (DBoO) is a validated capability in support of mission critical systems, complying to MoD connectivity doctrine and HMG security standards. The Low Weight Size and Power (SWaP) specifications ensures it is fully transportable as on-board cabin luggage guaranteeing deployed personnel can provide connectivity on immediate arrival in Theatre through its plug and play configuration. With additional ancillaries of a broadband router and high gain antennae, the DBoO provides connectivity options including but not limited to MoD Sat Systems, locally provided Internet Service Provider or 3G/4G LTE.

DBoO provides a resilient service that is able to meet the most challenging of operational requirements. A fully managed service, supported by the Prolinx ISO/IEC 20000 accredited 24/7/365 service desk. The DBoO ports are remotely configurable by our Technical Experts to satisfy the specific deployment requirements with the ability to accommodate a compendium of differing systems such as Ground Support Systems – secure UADs and other connected services.

INFRASTRUCTURE AS A SERVICE (IAAS)

Suited For - Customers who have an engineering capability around the design, develop, deploy and support aspects of virtual workloads and wish to maintain that level of control in addition to the application layer.
Available/Accredited at - OFFICIAL SENSITIVE and SECRET levels.
Connectivity to - MOD Core Network (Official Sensitive) (MCN(OS)), Public Sector Network (PSN) and Public Sector Network Police (PSN-P), MOD Core Network (Secret) (MCN(S)).

The Overview

Prolinx offer customers the option of an Infrastructure as a Service capability. Provided via a self-service portal, users can select pre-built or customer imported machine templates and deploy them onto Production, Pre-Production or Development platforms.

The makeup of the virtual workload (storage, RAM, CPU, network, OSE) is configurable by the customer and the workloads can be deployed either vanilla or fully secured and hardened using Prolinx accredited templates. Workloads can also be auto-enrolled into Prolinx fully managed Active Directory solutions to support an IDAM capability and additional layers of security.

The target platforms can be Public Cloud, Private Cloud or Community Cloud across many different levels of security.

CORPORATE OFFICE 365 (O365)

Suited For - Customers who need to communicate or exchange data with official government platforms from their private commercial networks and devices.
Available/Accredited at - OFFICIAL SENSITIVE level.
Connectivity to -MOD Core Network (Official Sensitive) (MCN(OS)) through SMI2 Gateway.

The Overview

Prolinx Corporate Secure O365 is a suite of cloud-based productivity and collaboration applications that integrates all Microsoft's existing applications. It is offered to enable MoD industry partners to collaborate with government organisations and for them to communicate directly into the MoD. It provides a capability for customers who have daily business to guarantee contract deliverables and in flight projects but do not have the requirement to purchase a fully hosted environment connected to MOD Core Network (MCN). Industry partners and enterprises of all sizes are finding Prolinx Corporate Secure O365 collaboration drives productivity, ROI and corporate success. Prolinx further offers a complimentary User Access Device with fully managed services to enhance this offering.

PLATFORM AS A SERVICE (PAAS)

Suited For - Customers whose business value is at the application and service level and have limited resources available to provide the design, develop, deploy and support of the virtual workloads up to and including the operating system and/or development platform.
Available/Accredited at - OFFICIAL, OFFICIAL SENSITIVE AND SECRET levels.
Connectivity to - MOD Core Network (Official Sensitive) (MCN(OS)), Public Sector Network (PSN) and Public Sector Network Police (PSN-P), MOD Core Network (Secret) (MCN(S)).

The Overview

The Prolinx Platform as a Service (PaaS) provides Operating Systems Environment (OSE) on top of the base layer Infrastructure as a Service (IaaS) offering. This includes the configuration, hardening and support of the full OSE which includes anti-virus, patching, monitoring, identify and many other services. This means the customer only has to be concerned about the application layer and will get full support from the Prolinx engineering team to on board, configure and integrate their applications. This also includes fully managed container capabilities ensuring customers can fully embrace DevOps approaches without worrying about the underlying platforms.

SOFTWARE AS A SERVICE (SAAS)

Suited For - Customers that require a secure compute and comms platform that is easily and rapidly deployable to support remote operations but is also scalable and can interface, where required, with headquarters/backend systems.
Available/Accredited at - OFFICIAL SENSITIVE levels.
Connectivity to - MOD Core Network (Official Sensitive) (MCN(OS)).

The Overview

Prolinx recognises that not all data and services are applicable or even permitted to be deployed onto Public Cloud solutions. However many Prolinx customers have a desire to leverage some of the fantastic solutions available in that space.

Working with Software Development houses, Prolinx also host a number of enterprise applications, traditionally only available in the Public Cloud space, at the higher security tiers. This enables organisations to leverage leading edge capabilities from inside their secure networks and using their real data sets.

SECURE EARLY ENTRY DEPLOYMENT SERVICES

Suited For - Customers that require a secure compute and comms platform that is easily and rapidly deployable to support remote operations but is also scalable and can interface, where required, with headquarters/backend systems.
Available/Accredited at - OFFICIAL SENSITIVE levels.
Connectivity to - MOD Core Network (Official Sensitive) (MCN(OS)).

The Overview

Secure Early Entry Deployed Service (SEEDS) is designed to support a small number of forward operating personnel and provides rapid delivery of information in a secure collaboration environment. SEEDS is a resilient service able to meet the most challenging operational requirements, whilst being fully compliant with the MOD's strict security regime.
SEEDS could be classed as your mini datacentre in a box, it's a Deployed Bearer of Opportunity (DBoO) that includes compute, storage and network. SEEDS can be utilised immediately at a deployed Forward Operating Base (FOB) in any building or tent satisfying the needs of the initial troop deployment. A smart function of the SEEDS is it gets over traditional performance challenges especially when sharing large amounts of data hungry files, such as video and images and allows all deployed personnel to collaborate locally without the need to reach back via the UK.

HYBRID CLOUD

Suited For - Customers that have capabilities split across multiple platforms/security zones but want end to end control and visibility through a central toolset or resource.
Available/Accredited at - OFFICIAL, OFFICIAL SENSITIVE AND SECRET levels.
Connectivity to -Internet-based Public Cloud, MOD Core Network (Official Sensitive) (MCN(OS)), Public Sector Network (PSN) and Public Sector Network Police (PSN-P), MOD Core Network (Secret) (MCN(S)).

The Overview

As described above Prolinx offers IaaS, PaaS and SaaS at multiple security tiers. Therefore because of this Prolinx is in a unique position to offer customers, who wish to leverage capabilities across multiple clouds and security tiers, a single entry point for both commercial and technical aspects.

The Prolinx provisioning toolsets, monitoring dashboards and billing engines can consolidate the data from all environments and, where applicable/permitted, provide our customers with a single engagement model. This could mean a single and predictable bill for workloads split across Amazon, Azure and the Prolinx secure datacentres, or could mean an end to end performance and availability dashboard for a service that has nodes in Public cloud and the Prolinx secure datacentres.