

Managed Private Cloud - Networks

Service description

This service provides planning and delivery support for public sector organizations building or migrating networks to private cloud network platforms. It focuses on defining a structured build or migration approach, managing risks, and supporting delivery to ensure networks are built or migrated in a controlled and secure manner.

Service features

- End-to-end system design and assurance for managed private cloud environments.
- Expert implementation of multi-vendor software-defined networking fabrics. Using Cisco ACI or NDFC technology, or Extreme Networks Fabric Connect or IP fabric technology
- Integrated next-generation security using industry approved firewall solutions. Palo Alto NGFW or Fortinet NGFW products & services.
- High-availability application delivery and load balancing. F5 BIGIP or VMWare NSX Advanced Load Balancer technologies.
- Cloud-managed networking and SD-WAN connectivity via multi-vendor integration. Cisco Viptela or Meraki SD-WAN, or Fortinet Secure SD-WAN technology.
- Comprehensive 24/7 proactive monitoring and incident management for cloud infrastructure.
- Automated network provisioning and orchestration to streamline infrastructure management.
- Strategic vendor selection and hardware procurement for private cloud deployments.
- Secure hybrid-cloud connectivity and multi-site networking architecture and support.
- Robust compliance alignment including Cyber Essentials Plus and ISO27001 standards.

Service benefits

- Reduces deployment times through automated software-defined networking and orchestration.
- Enhances organizational security posture with integrated multi-vendor firewall protection.
- Minimizes operational downtime using high-availability application delivery and load balancing.
- Decreases management complexity with centralized dashboards. Cisco Nexus Dashboard, Extreme Platform ONE, Palo Alto Panorama.
- Optimizes infrastructure performance through continuous 24/7 proactive system monitoring.
- Accelerates digital transformation by streamlining private and hybrid cloud migrations.
- Improves workforce productivity with reliable, high-performance remote access solutions.
- Simplifies governance using comprehensive audit trails and automated reporting tools.

Scope of the service

Services can included

- Discovery & Prerequisites workshops
- Review of current network solution, if required
- Design workshops to define new build
- Project planning & management
- Design validation, including hardware, software, licensing, subscription & integration requirements
- Hands-on implementation & deployment services related to new build

- X Level Design documentation (HLD, LLD)
- Post build validations & support
- Operational Handover Documentation (OHD)
- Migration planning workshops
- Migration plan and supporting documentation
- Hands-on delivery support during migration activities
- Post-migration review and validation support

Not included

- Purchase of hardware, software, licenses, subscriptions
- Legacy network support
- EOL network support
- Third-party tooling or services

Onboarding

Service initiation is via a kick-off meeting to confirm scope, assumptions and delivery approach. We will then prepare a Statement of Work for your approval before beginning service delivery.

Offboarding

Service completion includes delivery of migration documentation and a close-out review meeting.

Service constraints

Key constraints include:

- **On-boarding:** 15-30 day lead time from contract signature. Requires timely access to relevant stakeholders and documentation review.
- **Version Support:** Limited to vendor-supported, non-EoL software.
- **Prerequisites:** Buyers must provide necessary power, cooling, and rack space for physical components.
- **Scope:** Changes are subject to agreed maintenance windows.
- On-site support and management of legacy systems are excluded from the standard service scope.
- Standard delivery is remote via secure VPN/Jump box during business hours, unless 24/7 support is specifically contracted
- Assessment is based on information provided by the customer

Data handling and security

- No customer data is hosted or retained beyond the engagement
- Any access to systems is agreed in advance and limited to what is required
- All information is handled in accordance with UK data protection requirements and customer security policies

Service levels

Service delivery timescales are agreed at engagement start. No ongoing support or SLA is included.