

BestPath- Cisco Unified Network Infrastructure as a Service

Service overview

Cisco Unified Network Infrastructure as a Service provides a managed network service built on Cisco networking and security technologies, delivered and operated by BestPath. The service delivers secure, resilient, and scalable network connectivity across on-premises, cloud, hybrid, and remote user environments.

The service integrates WAN connectivity, cloud-delivered security, and network protection into a unified, centrally managed offering, supporting modern public sector requirements such as hybrid working, cloud adoption, and security by design.

Service features

- Secure WAN and site-to-site connectivity
- Cloud-delivered security and access controls
- Integrated network and security management
- Centralised policy and configuration control
- Monitoring, alerting, and reporting
- Scalable service design supporting growth or reduction

Service benefits

- Improved network reliability and resilience
- Consistent security across users, devices, and locations
- Reduced operational complexity through managed delivery
- Improved visibility into network performance and health
- Support for hybrid and remote working models

Service delivery and onboarding

The service is delivered as a fully managed or co-managed service. Onboarding includes requirements confirmation, service design, configuration using standard Cisco capabilities, and transition into operational support. Onboarding can be phased to minimise disruption.

Management, monitoring, and support

The service includes proactive monitoring of availability, performance, and security. Alerts are generated when thresholds are exceeded, enabling timely investigation and response. Monitoring data is reviewed to support optimisation and capacity planning.

Incident management follows documented processes aligned with Cyber Essentials and ISO/IEC 27001, with incidents logged, prioritised, investigated, and resolved in a controlled manner.

Security governance and vulnerability management

Security governance is underpinned by policies and processes aligned with Cyber Essentials and ISO/IEC 27001. Vulnerability management uses vendor advisories, recognised vulnerability sources, and operational monitoring. Critical vulnerabilities are prioritised and patched promptly, with lower-risk changes managed through controlled change processes.

Access to management and support channels is restricted to authorised personnel using role-based access controls, with logging and regular access reviews.

Scalability, resilience, and independence

The service scales through configuration rather than redesign, allowing users, sites, and capacity to increase or reduce as required. Customer resources are logically separated to ensure independence. Resilience is achieved through redundancy, distributed architectures, and continuous monitoring to avoid single points of failure.

Data export, exit, and end-of-contract support

The service supports data export using standard platform capabilities, including configuration information, reports, and operational data. At contract end, BestPath supports structured handover to a new supplier or internal team, including documentation, knowledge transfer, access changes, and secure withdrawal of operational access.