

Distributed infrastructure. One operating model.

Connect, protect and understand critical infrastructure through one secure infrastructure operating platform, run as an assured and accountable managed service.

SINCE 2017

Your estate has changed. So have we.

For years, Cloud Gateway has been trusted to connect and secure the services that critical UK organisations cannot afford to fail. Technology moves, threats change and estates grow more distributed. In response, we now offer a richer portfolio of connectivity, security and observability solutions, underpinned by one secure infrastructure operating platform - with a single point of accountability.

Orchestration

Services designed, provisioned and changed as one, not stitched together after the fact.

Service Intelligence

Telemetry and service context connected across the estate, so signals become understanding.

Assurance

Evidence that proves control and performance, rather than asking you to take it on trust.

THE PROBLEM WE EXIST TO SOLVE

The harder the boundary, the clearer the case.

Your infrastructure is distributed by design: multiple networks, clouds, security controls and suppliers, often bought as separate point solutions through separate contracts.

Most providers run their own part well, but services rarely fail inside one neat technology silo. They fail where responsibility is fragmented, in the space between suppliers, where no single party owns the end-to-end route, the policy, telemetry and the operational authority together.

As the estate changes, the gap between how each service is meant to run and how it actually runs keeps widening. That accumulating gap is **governance debt**. The space in between is where we hear the same problems:

“ Five suppliers, and none of them own the full picture. Every incident turns into a blame game.

“ When an auditor asks which system caused an outage, I have to go back to three different teams.

“ Our security team is drowning in alerts. We need to act, not just look at dashboards.

“ The board keeps asking when we'll modernise. Right now the estate is too fragile to touch.

WHAT WE DO

Connect. Protect. Observe. Operated as one.

One service, integrated through one Unified Control Plane and delivered by one UK-based team, with a single point of accountability. Each pillar carries the specific services your environment needs.

CONNECT

Managed paths between sites, users, data centres, cloud, HSCN & PSN - routing, resilience and supplier hand-offs designed in.

- SD-WAN
- Public cloud
- HSCN & PSN
- Remote Users
- Data Centres

PROTECT

Firewall, secure access and application security applied across trust boundaries in scope, governed as one consistent policy intent.

- Secure Internet Access (SWG)
- Secure Private Access (ZTNA)
- Managed Firewall
- Application Security (WAF)

OBSERVE

Service health, incidents, changes and source coverage for in-scope services, turning telemetry into assurance you can evidence.

- Service health & intelligence
- Incident & change context
- Source coverage
- Assurance reporting

HOW WE MEASURE SUCCESS

The outcomes we design for.

- Incidents can be resolved faster, because one team sees across the boundary instead of triaging between suppliers.
- New technology capabilities can be delivered sooner, through supported standardised patterns rather than bespoke builds each time.
- Disparate operations are simplified, with blind spots and duplicated tooling identified and removed to eliminate running costs.
- Shared services are properly leveraged and integrated, both within your organisation and with your peers.



WHY CLOUD GATEWAY

Built for the spaces between suppliers.

Engineering ownership.

Network, security, cloud and service engineers shape the offer, qualify the dependencies and stay connected to how it runs.

Regulated-sector depth.

Our experience across health, public sector, policing and other critical environments informs architecture, posture, and supplier decisions.

Service discipline.

Service definitions, supported patterns, readiness checks, run-books and lifecycle governance turn capability into repeatable delivery.

Observability included.

Telemetry, source coverage and service context are treated as design inputs as part of the service, not an afterthought after go-live.

Transparent sovereignty

Customer service management and engineering are UK-based, with any non-UK platform, support or data documented clearly.

Selective partnerships.

Proven carrier, cloud and security providers used where they fit, designed around your estate with a coherent responsibility model.

PROOF

Trusted where failure is not an option.

We work with organisations that cannot afford to fail: NHS trusts, central government, local authorities and police forces, plus tech innovators who serve them. Delivery is fully managed or co-managed with guardrails, backed by a 24/7 UK-based Network Operations Centre.

ISO 27001

ISO 9001

ISO 14001

Cyber Essentials Plus



Maritime and Coastguard Agency



Essex County Council



Department for Environment Food & Rural Affairs



START HERE

Book an architecture session.

Bring one critical service that crosses networks, clouds or suppliers. We'll map who is accountable for what today, where the gaps sit, and how a single operating model could transform the way your infrastructure works.

cloudgateway.co.uk

sales@cloudgateway.co.uk

(+44) 0 203 870 2444