controlplane

Cloud-Native Transformation and Security Enablement

Service Overview

This service supports organisations adopting and operating cloud-native platforms where security, compliance, and resilience are non-negotiable. It enables the secure transformation of containerised and Kubernetes-based environments from fragmented, high-risk estates into dependable, verifiable platforms of trust. The service is delivered as Cloud Support and focuses on security-by-design, operational assurance, and sustainable platform enablement rather than standalone tooling.

Service Objectives

- Enable secure, compliant adoption of Kubernetes and cloud-native technologies
- Embed security, governance, and resilience into platform design and operations
- Reduce operational risk, configuration drift, and regulatory uncertainty
- Support scalable, vendor-neutral cloud-native platforms
- Challenges Addressed
- Regulatory non-compliance caused by limited auditability and declarative controls
- Security fragmentation and tooling sprawl across cloud-native environments
- Inconsistent configuration and visibility across multi-cloud estates
- Shortage of internal Kubernetes and cloud-native security expertise

Challenges Addressed

- Regulatory non-compliance caused by limited auditability and declarative controls
- Security fragmentation and tooling sprawl across cloud-native environments
- Inconsistent configuration and visibility across multi-cloud estates
- Shortage of internal Kubernetes and cloud-native security expertise

Service Scope

The service applies to Kubernetes-based, cloud-native environments operating in public, private, or hybrid cloud models. It focuses on platform security, configuration assurance, and delivery governance, and does not provide underlying cloud infrastructure or hosted software services.

Key Capabilities

Security-by-Design Platforms

Platforms are engineered with embedded security controls, declarative configuration, and vendor-neutral architectures to support consistent, repeatable compliance.

Policy-as-Code and Governance

Automated guardrails enforce approved configurations, segregation of duties, and known-good states across environments.

Auditability and Assurance

Immutable configuration, traceability, and cryptographic audit signals are embedded into cluster operations, supporting verifiable regulatory alignment.

Resilience and Operational Stability

Guardrails eliminate ad-hoc changes and configuration drift, improving platform stability and recovery while enabling safe change at scale.

Threat Assurance Enablement

Threat modelling, configuration assurance, and integration with industry-standard security tooling help identify and reduce real-world exposure.

Service Components

- Cloud-native maturity assessments
- Security health checks with prioritised recommendations
- Threat modelling workshops and risk analysis
- Secure platform design and implementation support
- Kubernetes operations and security training

Delivery Model

Services are delivered through a combination of fixed-scope engagements, bespoke projects, and enablement services. Delivery is aligned to recognised frameworks including NIST and NCSC Cloud Security Principles, and integrates with customer operating models and governance structures.

Accessibility

The service does not provide end-user applications. Any customer-facing interfaces supplied as part of delivery are designed to meet WCAG 2.2 Level AA requirements.

Service Constraints

The service is limited to cloud-native and Kubernetes environments. It relies on customer access to cloud platforms, Kubernetes clusters, and version-controlled repositories. Availability and resilience depend on the underlying cloud provider and platform configuration. Monitoring, SOC, and incident response services are not provided unless explicitly contracted.

Outcomes and Value

- Reduced security and compliance risk
- Improved audit readiness and operational confidence
- Increased platform resilience and consistency
- Accelerated cloud-native adoption with reduced reliance on scarce expertise

About the Supplier

The service is delivered by a specialist cloud-native security consultancy with deep expertise in Kubernetes, DevSecOps, and regulated environments. The team actively contributes to industry standards and open-source security initiatives and has supported complex, high-trust organisations globally.