Cloudcore Networks

Technology Landscape and Resource Assessment

Table of contents

Purpose of This Document

This document provides a snapshot of Cloudcore's current technology environment, resource availability, and change history. It is intended to support realistic implementation planning by grounding AI ambitions in the constraints of what exists today.

Current Technology Stack

The following table summarises the major systems in Cloudcore's environment. Systems are grouped by function.

Infrastructure and Operations

System	Purpose	Deployed	Vendor/Platform	Integration Status
VMware vSphere	Virtualisation (~2,500 VMs across client workloads)	~2014	VMware (Broadcom)	Core platform; well integrated with provisioning automation
AWS	Public cloud partner (hybrid workloads)	~2018	Amazon Web Services	Integrated via VPC peering and IAM federation; default region US-East (Ohio)
Azure	Public cloud partner (hybrid workloads)	~2019	Microsoft	Secondary cloud partner; less deeply integrated than AWS
Terraform	Infrastructure as code	~2020	HashiCorp	Covers ~70% of new deployments; legacy systems outside IaC
Ansible	Configuration automation and deployment	~2019	Red Hat	Used alongside Terraform for server provisioning; some overlap with Chef
Chef	Legacy configuration management	~2015	Progress Software	Being phased out in favour of Ansible; still manages some legacy hosts

System	Purpose	Deployed	Vendor/Platform	Integration Status
Salt	Configuration automation (secondary)	~2016	VMware	Limited use; retained for specific legacy workloads
Kubernetes	Container orchestration	~2022	Open source (CNCF)	Limited adoption; used for internal applications, not yet client-facing
Prometheus + Grafana	Infrastructure monitoring and alerting	~2020	Open source	Well integrated; feeds PagerDuty for on-call escalation

Security

System	Purpose	Deployed	Vendor/Platform	Integration Status
Splunk SIEM	Security log aggregation and correlation	~2021	Splunk	Central security platform; generates 500 to 800 daily alerts
CrowdStrike	Endpoint detection and response (EDR)	~2022	CrowdStrike	Deployed across endpoints; feeds into Splunk
Palo Alto firewalls	Network perimeter security	~2017	Palo Alto Networks	Load-balanced pair; rule base reviewed quarterly post-breach
Cisco switches	Network infrastructure (802.1x, segmentation)	~2014	Cisco	Core network; segmentation improved post-breach
Tenable.io	Vulnerability scanning	~2021	Tenable	Weekly scans; critical/high patching within 15 days
Auth0	Identity provider and SSO	Dec 2023	Okta (Auth0)	Migrated from Okta; some policies still reference old IdP

Business Applications

System	Purpose	Deployed	Vendor/Platform	Integration Status
HubSpot	CRM, email marketing, lead tracking	~2022	HubSpot	Marketing and sales use; limited integration with operational systems
ServiceNow	Change management (PRODCM project)	~2023	ServiceNow	Change management workflows; not yet integrated with monitoring
JupiterOne	IT asset management and CMDB	~2022	JupiterOne	AWS automated discovery; physical asset tracking via property tags
Atlassian (Jira, Confluence)	Project management and documentation	~2016	Atlassian	Widely used; ticket data not connected to analytics
Office 365	Email, productivity, collaboration	~2015	Microsoft	Core productivity platform
Slack	Team communication	~2018	Salesforce (Slack)	Primary internal communication; some alerting integrations

Development

System	Purpose	Deployed	Vendor/Platform	Integration Status
GitHub Actions	CI/CD pipeline	~2021	GitHub	SAST scanning integrated; ~70% test coverage
ArgoCD	GitOps deployment to Kubernetes	~2022	Open source (CNCF)	Used for internal microservices only

System	Purpose	Deployed	Vendor/Platform	Integration Status
PostgreSQL	Primary application database	~2015	Open source	Core data store; encrypted at rest and in transit
Python (FastAPI)	Backend API framework	~2021	Open source	15+ microservices in production
React	Frontend framework	~2021	Open source (Meta)	Client-facing dashboards and internal tools
Legacy PHP applications	Older application components	~2012	Open source	Technical debt; pre-dates current security standards

Analytics

System	Purpose	Deployed	Vendor/Platform	Integration Status
Power BI	Business intelligence dashboards	~2022	Microsoft	Used by data team; manual data imports from multiple sources
Excel	Ad-hoc analysis and reporting	N/A	Microsoft	Still heavily used for financial and operational reporting

Notable gaps: No data warehouse or data lake. No ML/AI platform (no SageMaker, Azure ML, or equivalent deployed). No MLOps or model management tooling. No real-time analytics pipeline. No dedicated ETL platform.

Data Flow Overview

Data moves through Cloudcore's environment primarily via manual processes and point-to-point integrations. There is no centralised data platform or integration layer.

How Data Currently Flows

```
Infrastructure Telemetry          Customer Interactions
(Prometheus, Grafana)             (Support tickets, CRM)
        |                                  |
        v                                  v
  Splunk SIEM  <-- Security logs     HubSpot CRM
  (security only)                   (marketing/sales only)
        |                                  |
        |        No integration            |
        |      <----- GAP ----->           |
        v                                  v
  Manual export                      Manual export
  to Excel/Power BI                  to Excel/Power BI
        |                                  |
        +----------> Analyst <-------------+
                   (Jamal's team)
                   Manual correlation
                        |
                        v
                   Static reports
                   (weekly/monthly)
```

Key Data Silos

Data Source	System	Owner	Connected To
Infrastructure metrics	Prometheus/Grafana	Infrastructure team (Martin Nguyen)	PagerDuty (alerting only)
Security events	Splunk SIEM	Security team (Sophia Martines)	CrowdStrike, firewall logs
Support tickets	Internal ticketing system	Support team (Samantha Wong)	Nothing; manual reporting
Customer records	HubSpot CRM	Marketing/Sales (Lisa Chen)	Email campaigns only
Billing and invoicing	Internal billing system	Finance (Aisha Rahman)	Manual reconciliation

Data Source	System	Owner	Connected To
Service usage	Provisioning and metering tools	Operations (Martin Nguyen)	Billing (batch, manual validation)
HR and access	Auth0 + Active Directory	HR/IT (Karen Lee, Raj Patel)	Partial RBAC; ~40% over-provisioned

Manual Processes and Gaps

- **Billing reconciliation:** Service usage data is manually validated against billing records. Errors are common and time-consuming to resolve.
- **Customer health reporting:** No automated way to correlate support tickets, usage patterns, and billing data for a single customer. Jamal's team builds reports manually in Power BI from exported CSVs.
- **Security-to-operations handoff:** Security alerts in Splunk are triaged manually. No automated ticket creation for operational follow-up.
- **Access provisioning:** Onboarding and role changes require manual coordination between HR, IT, and department managers. Quarterly access reviews found ~40% of employees have broader access than required.
- **Capacity planning:** Based on historical trends in spreadsheets. No predictive modelling or automated forecasting.

Resource Availability

Team Capacity

Team	Headcount	Current Commitments	Available for AI Work
Infrastructure engineering	12	Day-to-day operations, CSMP infrastructure, zero trust planning	Limited; 1 to 2 engineers could be partially allocated
Software development	7	CSMP development (primary focus), legacy maintenance, security remediation	Very limited; CSMP is consuming most capacity

Team	Headcount	Current Commitments	Available for AI Work
Security	8	Post-breach remediation, ongoing monitoring, compliance, zero trust planning	Minimal; team already needs 3+ additional hires
Customer support	8	500+ client support, 24/7 coverage	None; fully committed to operational support
Data and analytics	2	Operational reporting, ad-hoc analysis for all departments	Severely constrained; any AI data preparation would compete with BAU reporting
IT operations	4	Infrastructure maintenance, on-call rotation, patching, access management	Minimal; understaffed for current workload

Competing Commitments

Cloud Service Management Platform (CSMP): This is Cloudcore's largest active project, consuming the majority of development and a significant share of infrastructure team capacity. The CSMP aims to replace fragmented service provisioning, billing, and client management systems with an integrated platform. It is the primary pathway to enterprise market expansion. Any AI initiative will compete with CSMP for developer time, infrastructure resources, and management attention.

Post-breach security remediation: The security team is executing a multi-quarter programme including zero trust architecture planning, enhanced access controls, improved monitoring, and stricter third-party security assessments. This work is board-mandated and non-negotiable.

ISO 27001 surveillance audit: The certification achieved 18 months ago requires ongoing compliance activities. A surveillance audit is expected within the next 6 months.

SOC 2 Type II renewal: Annual recertification requires evidence collection and audit preparation, drawing on compliance, security, and IT teams.

Budget Envelope

Consistent with the AI Opportunity Evaluation Pack, the proposed initial AI investment is **$250,000 AUD** over 12 months. This must cover all costs including tooling, talent, data preparation, and governance development. No additional capital expenditure has been approved.

For context:

- A single ML engineer costs $180,000 to $250,000 AUD annually (market rate)
- Cloud AI platform licensing (e.g., SageMaker, Azure ML) typically runs $3,000 to $8,000 AUD per month for a modest deployment
- The $250,000 envelope is tight for any initiative that requires both a specialist hire and platform investment

Timeline Pressures

- **Board expectations:** The board wants a clear AI positioning statement and evidence-based investment plan. Competitors are already marketing "AI-powered" services.
- **CTO estimate:** 6 to 12 months of data engineering work before any ML model could be trained on production data.
- **Data analyst assessment:** Jamal Al-Sayed estimates the data is not "AI ready" and would need 6 to 12 months of preparation, including establishing consistent data definitions across systems.
- **CSMP delivery pressure:** Delays to CSMP would affect enterprise market expansion, Cloudcore's other strategic priority.

Existing Vendor Relationships

Cloudcore maintains relationships with the following approved vendors, as documented in DOC-COMP-007. Any AI vendor engagement would need to go through Cloudcore's third-party risk assessment process (strengthened post-breach).

Vendor	Category	Relevance to AI
AWS	Cloud infrastructure	Access to SageMaker, Bedrock, and other AI/ML services through existing partnership
Microsoft Azure	Cloud infrastructure	Access to Azure ML, Cognitive Services through existing partnership
Splunk	Security analytics	Has ML-powered analytics capabilities already licensed
CrowdStrike	Endpoint security	AI-driven threat detection already embedded in product
HubSpot	CRM	Has built-in lead scoring and predictive features in higher-tier plans
SecureHost Solutions	Hosting services	No AI relevance

Vendor	Category	Relevance to AI
Quantum Storage Technologies	Storage	No AI relevance
GlobalConnect Networks	Network services	No AI relevance
CyberSafe Security	Security services	Potential security AI advisory
ComplianceGuard	Compliance tools	Potential AI governance tooling

Key observation: Several existing vendor relationships include AI capabilities that Cloudcore is not currently using. AWS and Azure partnerships, in particular, provide access to managed AI/ML platforms without requiring new vendor onboarding or security vetting.

Previous Change Initiative Outcomes

Understanding how Cloudcore has handled significant change projects provides context for AI implementation planning.

Success: ISO 27001 Certification (2022 to 2024)

Scope: Enterprise-wide information security management system implementation and certification.

Outcome: Successfully certified, though the project took nearly two years against an initial 12-month target.

What went well:

- Strong executive sponsorship from the CEO and CISO
- Clear business driver (enterprise clients requiring certification)
- Dedicated project lead (Sophia Martines)
- External auditor engagement managed well

What was difficult:

- Scope underestimated; policy development took longer than expected
- Staff resistance to new processes (seen as bureaucratic)
- Resource contention with operational work
- Documentation burden strained a small team

Lessons for AI: Large-scale change takes longer than planned at Cloudcore. Executive sponsorship is essential. The team can deliver, but timelines should include realistic buffer. Policy and governance development is time-intensive and should not be an afterthought.

Partial Success: Identity Provider Migration, Okta to Auth0 (December 2023)

Scope: Migration of single sign-on and identity management from Okta to Auth0.

Outcome: Technical migration completed on schedule. However, internal documentation, security policies, and training materials were not updated. As of the most recent policy review, multiple security documents still reference Okta as the primary identity provider.

What went well:

- Technical execution was clean; minimal user disruption
- Auth0 integration with existing systems worked smoothly
- Project delivered on time and within budget

What went wrong:

- No change management plan for documentation and process updates
- Policy documents (POL-SECU-021 and others) still reference Okta months later
- Training materials not updated; staff unclear on new procedures
- Session timeout and MFA configuration differences between old and new systems created inconsistencies
- No post-migration review conducted

Lessons for AI: Cloudcore can execute technical changes competently but struggles with the organisational side of change: documentation, training, process alignment. Any AI initiative will need explicit change management planning, not just technical delivery.

Failure: CRM Consolidation Project (2021 to 2022)

Scope: Migration from a legacy contact management system and scattered spreadsheets to HubSpot as a unified CRM platform.

Outcome: HubSpot was deployed, but data migration was incomplete and the platform is underutilised. The project ran three months over schedule and 40% over budget.

What went well:

- HubSpot platform selection was sound; the tool meets Cloudcore's needs
- Marketing team adopted it fully for email campaigns and content management
- Integration with the website for lead capture works well

What went wrong:

- Historical customer data was migrated with significant quality issues: duplicate records, inconsistent formatting, missing fields
- Sales team adoption was low; many continued using spreadsheets for pipeline tracking
- No data quality standards were defined before migration
- Integration with billing and support systems was out of scope and never implemented
- Post-migration cleanup was never resourced, leaving data quality issues unresolved

Lessons for AI: Data migration and integration projects at Cloudcore have historically underestimated data quality challenges. The CRM project demonstrates that deploying a tool without addressing underlying data problems produces limited value. This pattern is directly relevant to AI readiness, where data quality is the foundation of any useful model.

Summary of Key Constraints

For implementation planning, the following constraints are the most significant:

1. **Data readiness is the primary bottleneck.** Siloed systems, no data warehouse, inconsistent data definitions, and a two-person analytics team mean that any AI initiative requiring cross-system data will face 6 to 12 months of preparation work.

2. **The CSMP project consumes most available development capacity.** AI work will need to either use different resources (external vendors, cloud-managed services) or accept a delayed timeline.

3. **The $250,000 budget is tight.** It cannot simultaneously fund a specialist hire and significant platform investment. Trade-offs will be necessary.

4. **Change management is a known weakness.** Technical execution is generally competent, but documentation, training, and process alignment consistently lag behind.

5. **Security governance must be addressed first.** The CISO has board-level backing to require governance frameworks before any AI system processes customer data.

Cross-References

For additional context, the following resources are available on the Cloudcore Networks website:

- **System and network documentation:** The support section at cloudcore.eduserver.au/docs/support/ includes network diagrams, the ERD, and the organisational chart
- **Security policies:** Current security and compliance policies are published at cloudcore.eduserver.au/docs/policies/, including the access control, change management, and data classification policies referenced in this document
- **Incident logs:** Detailed logs from the September 2024 breach, including VPN, database, firewall, and SIEM entries, are available at cloudcore.eduserver.au/docs/logs/

Cloudcore Networks is a fictional company created for educational purposes. Any resemblance to real organisations is coincidental.