

How CloudGo.ai Revealed Hidden Security, Cost, and Architecture Risks in a Production IoT Platform

About Berner International

Industry: Industrial Manufacturing

Platform: Connected IoT Device Platform

Cloud Environment: AWS

Architecture: Serverless APIs, IoT device fleet, Lambda-based processing, DynamoDB storage, and supporting compute infrastructure

Founded in 1956, Berner International is a leading manufacturer of commercial and industrial air curtain systems, sometimes referred to as air doors. These systems create a controlled stream of air across an opening, forming an invisible barrier that separates indoor and outdoor environments while allowing people, vehicles, and goods to move freely through doorways.

Berner's products are widely used in facilities such as warehouses, manufacturing plants, retail entrances, restaurants, and transportation hubs to maintain indoor climate conditions, improve comfort, reduce energy loss, and prevent outside contaminants such as insects, dust, and fumes from entering buildings.

Headquartered in New Castle, Pennsylvania, Berner has spent more than six decades engineering air curtain solutions that help organizations create energy-efficient and comfortable environments while maintaining open access through facility entrances.

As the company expanded its product capabilities and introduced more advanced digital controls and connected management features across its systems, the supporting cloud infrastructure behind these capabilities became increasingly important. To ensure the reliability, security, and efficiency of this infrastructure, Berner partnered with CloudGo.ai to conduct a comprehensive cloud infrastructure audit and identify opportunities to strengthen governance, modernize architecture, and optimize operational efficiency.

The Challenge

The organization's cloud platform was stable and supporting production workloads, but several common challenges had begun to emerge as the environment scaled.

Infrastructure Governance Drift

As cloud environments grow, infrastructure decisions are often made quickly to support product delivery. Over time this can lead to configuration drift where the current state of infrastructure gradually diverges from best practices.

Increasing Security Complexity

A connected device platform introduces multiple security boundaries, including:

- device authentication
- API access control
- certificate management
- network access policies

Maintaining consistent security governance across these layers becomes increasingly complex as device fleets and services expand.

Runtime and Platform Modernization

Serverless platforms evolve rapidly. As new runtimes and platform capabilities become available, older functions and shared dependencies can unintentionally block modernization efforts if upgrade paths are not carefully managed.

Hidden Cost Drivers

Many cloud cost drivers exist deep within service-level usage patterns rather than in compute or storage resources. These cost contributors are often difficult to identify through standard billing reviews.

The company needed a **holistic understanding of how its infrastructure actually operated** in order to identify improvement opportunities without disrupting production systems.

Before CloudGo.ai

Like many growing cloud environments, the organization already relied on standard cloud tooling including monitoring dashboards, security scanning tools, and cost reporting systems.

However, these tools evaluated infrastructure **service-by-service**, producing fragmented insights rather than a holistic understanding of how the platform functioned as a whole.

As a result:

- security signals existed but were not connected across services
- modernization blockers were difficult to diagnose
- cost drivers were buried within service-level usage patterns

The company needed a way to analyze the cloud environment **as a system rather than a collection of independent services**.

The CloudGo.ai Approach

CloudGo.ai performed a comprehensive **read-only audit of the AWS environment**, connecting through a secure role to analyze infrastructure configuration, resource relationships, and service usage patterns.

Unlike traditional scanning tools that evaluate services independently, CloudGo.ai performs **context-aware analysis across the entire infrastructure graph**.

The system collects and correlates infrastructure data across services including:

- device fleet configuration
- API infrastructure
- serverless runtime dependencies
- networking policies
- service usage and billing dimensions
- infrastructure governance controls

By analyzing how these services interact, CloudGo.ai is able to identify compound issues that traditional tools often miss.

The result is not just a list of alerts, but a **structured understanding of the architecture and how it evolves over time**.

Key Insights

The audit surfaced several important areas where improvements could strengthen the platform's long-term reliability and governance.

Device Fleet Security Governance

Connected device platforms rely on certificate-based authentication and policy controls to secure communication between devices and cloud services.

CloudGo.ai identified opportunities to strengthen device security governance by improving credential lifecycle management and tightening permission scopes for device operations.

These changes reduce unnecessary access privileges across large device fleets and ensure credentials are actively managed throughout the lifecycle of deployed hardware.

API Layer Authentication

The audit also identified opportunities to standardize authentication across the API layer supporting the platform's mobile and web applications.

Implementing centralized identity and authorization controls ensures all API requests are validated through a consistent security framework. This approach strengthens security posture while simplifying long-term maintenance as new services and endpoints are introduced.

Serverless Runtime Modernization

CloudGo.ai analyzed the full serverless architecture and identified a dependency pattern that prevented many functions from upgrading to modern runtimes.

Rather than requiring a coordinated migration across the entire system, CloudGo.ai determined that a small number of shared components were blocking upgrades for a large portion of the platform.

By modernizing those shared components first, the organization could unlock incremental runtime upgrades across the broader system without operational disruption.

This approach significantly reduces the complexity of large-scale runtime modernization efforts.

Infrastructure Governance and Network Hardening

The analysis also surfaced opportunities to strengthen infrastructure governance and network configuration.

These included tightening network access policies, standardizing operational access patterns, and cleaning up unused resources that accumulated as the platform evolved.

Implementing these improvements reduces operational risk while simplifying long-term infrastructure management.

Service-Level Cost Visibility

One of the most impactful insights involved cloud cost composition.

CloudGo.ai identified a significant cost driver embedded within a specific service-level usage pattern that was not visible through traditional cost summaries.

By understanding the operational workflow responsible for this usage, the organization could implement governance controls to reduce unnecessary usage without making architectural changes to the platform.

Measurable Outcomes

Within days of the audit, CloudGo.ai provided a clear roadmap for strengthening and optimizing the cloud environment.

The analysis identified opportunities to:

- significantly reduce unnecessary cloud spend driven by service-level usage patterns
- strengthen security controls across device authentication and API access
- unlock modernization for a large portion of the serverless architecture
- eliminate infrastructure drift accumulated during years of rapid product growth

Most importantly, the organization gained **a structured implementation plan that allowed improvements to be introduced safely without disrupting production systems.**

Remediation Roadmap

CloudGo.ai translated the audit findings into a phased implementation roadmap designed to minimize operational risk.

Phase 1: Security Hardening

Immediate configuration improvements to strengthen authentication, device policies, and network access controls.

Phase 2: Platform Governance

Implement credential lifecycle management, deploy infrastructure monitoring controls, and modernize shared runtime dependencies.

Phase 3: Optimization and Hygiene

Address cost drivers, remove unused infrastructure resources, and establish recurring infrastructure review processes to prevent future drift.

Because many of these improvements involve configuration changes rather than architectural redesigns, they can be implemented incrementally while maintaining platform availability.

Why Traditional Tools Miss These Problems

Most cloud tools analyze infrastructure **one service at a time**.

They can flag misconfigurations or surface usage metrics, but they struggle to answer deeper architectural questions such as:

- Which dependencies are blocking platform upgrades?
- Where does a security policy affect an entire device fleet?
- Which operational workflow is driving unexpected cloud costs?

Answering these questions requires **cross-service reasoning across thousands of resources**.

CloudGo.ai builds a **context graph of the entire cloud environment** and analyzes how infrastructure components interact.

This allows the system to:

- detect hidden dependencies between services
- surface compound security risks
- identify root causes of cost drivers
- generate step-by-step remediation strategies

Instead of producing alerts, CloudGo.ai produces **architectural insight**.

Business Impact

Following the audit, the organization gained:

Stronger security posture

Improved governance across device authentication, APIs, and network access.

A clear modernization strategy

A structured plan for upgrading serverless runtimes without disrupting production workloads.

Improved infrastructure visibility

A comprehensive understanding of how cloud services interact across the environment.

Significant cost optimization opportunities

Identification of operational patterns driving unnecessary cloud spend.

CloudGo.ai

Context-Aware Infrastructure Intelligence

Cloud environments evolve rapidly as organizations scale. Over time, infrastructure complexity grows faster than most teams can manually analyze.

CloudGo.ai provides organizations with **continuous, context-aware infrastructure intelligence**, enabling engineering teams to:

- identify hidden security risks
- modernize architectures safely
- uncover cost drivers
- prevent infrastructure drift

By transforming infrastructure analysis into a repeatable system, CloudGo.ai helps companies operate their cloud environments with the insight and discipline typically associated with the most experienced cloud architecture teams.