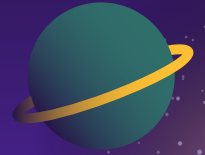


VISIBILITY INTO IT AND OT DATA, WITH NO INSIGHTS LEFT UNCOVERED

Large Southeastern U.S. utility turns to Gravwell to unify data across operational units, reducing costs and improving security monitoring, compliance, and efficiency.



COMPANY:

LARGE SOUTHEASTERN U.S. UTILITY

INDUSTRY:

UTILITIES/ENERGY

Operating a utility is a tremendous operational challenge, thanks to numerous legacy and holdover systems from acquisitions or previous owners, dispersed operations, and enormous customer data stores. Disparate and siloed systems add to the complications of gaining a high-level view from every source – especially now that smart meters and new technologies for transmission measurement are generating exponentially more valuable data.

As a large utility in the Southeastern United States discovered, data from separate business units is housed in systems and applications that were never intended to communicate with each other. That meant monitoring network data for security awareness was difficult, particularly in an era where dedicated attackers have their sights set on disrupting public services.

To bring together data from many operational units for analysis and compliance, the utility chose Gravwell for its unlimited data lake, integration with security tools, technology agnostic approach to ingestion and aggregation – and the ability to manage its own data, without ceding ownership to a vendor.

OBJECTIVES



Improve data integrity.

With previous solutions, the utility discovered problematic gaps in data collection, which raised concerns about the completeness of the data picture.



Share data easily.

Breaking down silos between data, and ensuring data was technology and user-agnostic, would allow any business unit to benefit from everyone's data.



Maintain ownership and control over data.

With highly sensitive, critical infrastructure data onsite, the utility did not want to give control of its data to a cloud-only vendor.



Improve archiving practices for security and compliance.

Detecting adversaries who exploit systems over time demands data that spans long timeframes – but gathering and storing such data is costly.



Whether it comes from a network, factory, or siloed legacy system on the plant floor – Gravwell enables investigation, collaboration and analysis of data from ANY source, all with unlimited collection and retention.

“Gravwell has become the single solution for solving many of our data challenges – even the ones we’d almost given up on. They’re a partner, not just a vendor.”

Security Architect, Large Southeastern U.S. Utility

Solution

- Gravwell’s unlimited volume pricing and its “the more data, the better” approach ensured that none of the utility’s data was left behind at the ingestion stage.
- Since Gravwell doesn’t discriminate between technologies, applications, or languages, the utility company could bring every type of data to the table.
- Ingesting, analyzing, and archiving log data helped the utility keep an eye on system events and anomalies that could indicate the presence of bad actors.
- Gravwell abides by its mission, “It’s your data, not ours,” allowing the utility to control and manage its own data.



Results

Cost savings

With Gravwell’s unlimited data collection and retention, as well as pre-filtering of data, the utility avoided the cost spikes and data ingestion limitations of its previous data platform – saving a potential **31% in future costs**.

Simplified Architecture

The savings went beyond the data platform costs: Gravwell helped the utility simplify its architecture.



Improved Operations

Gravwell’s expert customer success team helped the utility improve operations for other solutions and even replace them entirely.

Easy Rollout, Fast ROI

The utility was able to deploy Gravwell quickly and self-manage the rollout, allowing for faster return on investment.