gravwell

CASE STUDY

UNLOCKING FULL VISIBILITY AND OPERATIONAL AGILITY WITH GRAVWELL

Before Gravwell: Costly Constraints and Operational Headaches

Summary: The customer's previous SIEM solution was holding them back. Data collection was limited by cost, system performance was unreliable, and infrastructure demands drained internal resources The previous SIEM's pricing model penalized increased data ingestion, forcing the organization to make difficult decisions about what telemetry they could afford to ingest. Key sources, including authentication logs, device data, and security events, were excluded to stay within budget.

Performance issues compounded the problem. Searches were frequently skipped or delayed due to resource contention, introducing blind spots and eroding confidence in the system's reliability. Security investigations took longer, and teams were forced to work around the tool instead of with it. Maintenance overhead also became a pain point. Managing infrastructure, keeping the application stable, and troubleshooting ingest pipelines consumed significant engineering time. Operational energy was spent keeping the system afloat rather than improving security outcomes or supporting cross-team visibility.

The result was an environment shaped by compromise. Decisions were based on cost constraints, not data relevance. Teams had to choose between visibility and affordability, weakening the organization's overall security and operational readiness.

Choosing Gravwell: An SDP Approach

When the customer began evaluating alternatives to their existing SIEM, they weren't just looking for more features—they needed a solution that directly addressed the operational pain points holding them back. Their priorities were shaped by years of working around cost-based ingestion limits, unreliable search performance, and an overburdened infrastructure.

They needed a platform that would eliminate data-related trade-offs, provide dependable performance under load, and significantly reduce the engineering effort required to maintain and troubleshoot the system. In short, they were looking for a tool that empowered rather than restricted them.

gravwell

CASE STUDY

UNLOCKING FULL VISIBILITY AND OPERATIONAL AGILITY WITH GRAVWELL

A traditional SIEM was no longer capable of meeting the customer's evolving operational demands. They had outgrown the rigid, ingestion-first architecture that prioritized cost control over data fidelity. Licensing constraints forced them to omit critical telemetry, while search performance issues and infrastructure overhead created unnecessary friction across teams.

What they needed wasn't just another SIEM—they needed a fundamentally different approach to security data: one that prioritized scalability, flexibility, and operational efficiency without punitive pricing. That's where Gravwell's Security Data Platform stood out.

As an SDP, Gravwell addressed each of these challenges head-on. Unlike SIEMs that require predefined schemas and structured data at ingestion, Gravwell enabled structure-on-read—allowing the customer to retain raw data and query it dynamically based on need. This unlocked deeper threat hunting, broader telemetry coverage, and faster operational insight. Its scalable architecture supported massive data volumes without performance degradation, and its piped query language empowered analysts to create advanced analytics and automation pipelines.

Crucially, Gravwell's pricing model removed the data volume tax, aligning cost with capability and enabling the customer to finally make decisions based on relevance—not budget. For a modern, high-scale environment, an SDP wasn't just a better option—it was the only option that made sense.

The Migration: A Collaborative, Customized Path to Success

Summary: As part of the mission support program, Gravwell partnered closely with the customer to build a tailored migration plan. Every phase, from planning to deployment, was driven by transparency, collaboration, and technical validation.

THE MISSION SUPPORT PROGRAM IS INCLUDED FOR ALL GRAVWELL CUSTOMERS

Gravwell's migration strategy began with one key principle: understand before acting. Our architects conducted structured interviews with stakeholders across departments to gather insights on data requirements, use cases, and pain points. The result was a comprehensive, cross-functional migration plan aligned with real operational needs.

We provided tools to extract and catalog all existing assets from the legacy system, including searches, dashboards, macros, and automations. This inventory became the foundation for a clean, trackable transition.

gravwell

CASE STUDY

UNLOCKING FULL VISIBILITY AND OPERATIONAL AGILITY WITH GRAVWELL

The first technical milestone was data onboarding. Gravwell engineers worked hand-in-hand with the customer to configure new ingesters, validate timestamps, and confirm volume expectations. Each data source was tracked, verified, and checked off the migration list with precision.

With ingestion underway, our team rebuilt over **250 saved searches, dashboards, and automation rules**. Each asset underwent acceptance testing, with customer feedback integrated at every step. Teams were encouraged to test and explore, surfacing discrepancies early and helping us tune the system in real time.

Training was built into the process. Gravwell led targeted sessions using the customer's own data and scenarios to ensure that teams could confidently operate the platform from day one. By the time the migration was complete, end users and administrators were already fluent in Gravwell's tools and workflows.

As a final step, the customer was transitioned into our long-term maintenance phase. We outlined SLAs, provided escalation procedures, and ensured they had access to our technical team for ongoing support and continued growth.

Current State: Gravwell Powers Mission-Critical Operations

Summary: Gravwell now serves as a foundational part of the customer's operational stack. It drives automation, search at scale, and real-time infrastructure visibility across the organization.

Today, Gravwell is fully embedded into the customer's ecosystem. It supports a wide range of departments and use cases, from security and compliance to infrastructure monitoring and identity management. Because Gravwell licenses by indexer, not by data volume, the customer now ingests everything they need without compromise.

Search scale is no longer a concern. ***The customer runs more than 3.5 million searches every day with no performance issues. Teams can confidently build, automate, and explore without worrying about concurrency limits or hidden usage penalties.***

Automation has become a cornerstone of operations. Gravwell is tightly integrated with the customer's authentication systems, device and identity platforms, and orchestration tools. ***Automated searches and workflows run thousands of times per minute, powering everything from real-time access audits to compliance checks and change validation.***

gravwell

CASE STUDY

UNLOCKING FULL VISIBILITY AND OPERATIONAL AGILITY WITH GRAVWELL

Equally important is the visibility Gravwell provides into infrastructure health. The customer has built a robust suite of live dashboards that track ingestion completeness, log freshness, system performance, and telemetry coverage. These dashboards enable engineering and operations teams to catch issues before they escalate, monitor pipeline integrity, and quickly validate changes across their environment.

Gravwell's scheduled searches and alerting capabilities support proactive maintenance and fast response. Whether onboarding a new data source, tuning an ingest configuration, or rolling out a new detection strategy, the platform provides clear, immediate feedback.

Ongoing collaboration with Gravwell's support team has also proven critical. The customer engages regularly with our architects for search optimization, complex content builds, and secondary administrative support. Gravwell is more than just a tool in their stack, it's a trusted partner helping them stay ahead of what's next.

2025, Gravwell Inc.