gravwell

Case Study

BRIDGING THE OT AND IT GAP

This customer case study is based on a global materials science company with a long history of developing materials that are critical to the defense of the United States.They pride themselves on their ability to take on difficult technical challenges and solve them in a way that delivers the highest quality products to their customers throughout the military and defense supply chain.

This research and manufacturing organization has tens of thousands of employees and works with thousands of vendors around the world. Their suppliers range from raw materials and commodities brokers to speciality engineering consulting firms which help assure that the company provides the highest quality materials and products to their customers.

Customer At-A-Glance

Industry: Chemical Manufacturing

80,000+
Global Employees

10,000+
Suppliers

$25B
2019 Revenues

CUSTOMER CHALLENGES

Many of the chemical formulas and manufacturing processes involved in the creation and production of the materials that this company delivers are governed by strict export control regulations.These laws, established by the US Department of Commerce and enforced in partnership with the Departments of State and Justice, restrict how specific technologies must be protected from both intentional and unintentional exports.

As with many multinational enterprises that are facing IT integration and modernization challenges, the specific physical infrastructure, legacy devices, personalities, and data center capacities and capabilities required an extremely flexible platform that could provide a solution unique to their facility. As this industrial conglomerate worked to modernize and expand its manufacturing and technology operations the gap in their level of cybersecurity maturity became clear.

Gravwell partnered with this customer to develop a solution which solved both the regulatory and intellectual property protection risks. The enterprise wanted to deploy a system which would give visibility into network anomalies, new devices on a network, and the potential attempted access or transfer of intellectual property, whether it be a physical onsite threat from within a plant, or a cyber threat. As an added benefit, this solution was able to view network data (such as process logic changes) to validate the integrity of the manufacturing process itself.

By choosing the Gravwell's platform, the organization was able mature their cyber security efforts. With all their data in one place they now have more visibility than ever before and have greatly reduced the risk of intellectual property theft and other malicious intents.

GRAVWELL HIGHLIGHTED FEATURES

+ Ability for deployment in cloud, on-premises, hybrid, and even in an isolated on-premises network lacking outside network connectivity.
+ Capable of collecting disparate unstructured time-series data sources into a queryable data lake.
+ Unlimited data ingestion and retention.
+ Enable data scientists to create custom algorithms and machine learning to be executed in the search pipeline.
+ Analysts and data scientists have access to raw entry records for retroactive analysis and application of machine learning that did not exist at the time of collection.
+ Capable of data separation and fine-grained access controls for multi-tenancy.
+ Data collectors or agents are modifiable by the customer to enable processing, filtering, or enrichment before forwarding to the central store.
+ Massive scalability. The customer is currently expanding the program to include additional manufacturing sites across the globe.

By using Gravwell, the company has improved the protection of their critical intellectual property. With a focus on the log correlation, auditing, and incident response readiness Gravwell has significantly increased visibility into network and plant machinery activity. These goals have been accomplished while simultaneously giving users greater access and flexibility to their time critical logs.

By providing a single unified source of all their disparate data sources, from IT events to OT sensors, team members for the first time have a full 360 degree view of what is happening on their networks and the plant floor. Gravwell's granular user access control means the right teams and individuals get access to the right data at the right time. Combined with compliance logging functions, Gravwell has significantly reduced the overhead associated with regulatory reporting and other compliance tasks.

All of these improvements and enhanced capabilities have been delivered to the company by Gravwell at a fraction of the cost of competing offerings. Gravwell's ability to be deployed in the cloud, on-premises, and on an isolated on-premises network that is lacking outside network connectivity, combined with ease-of-use, has been a game changer. Gravwell enhanced the organization's efficiency at identifying and resolving threats, significantly reducing the likelihood of the loss of critical intellectual property and/or any future regulatory compliance problems.

> **For the first time in my 30 years working here, we have a reliable and simple way to access all of our OT and IT logs. With easy to read dashboards for auditing and automated alerts that let us know when something is wrong we're always up to speed with what's happening. We're more confident than ever that we're doing everything necessary to protect our intellectual property and meet regulatory compliance.**

Director Research and Development IT
at a global science company