Case Study

ASAVIE

# Private IoT Network Connectivity & Controls Shield Critical Mining Infrastructure from Cyberattacks

Since deploying Asavie SD IoT™, Howard Energy Partners (HEP) has re-defined how it manages and protects its Sierra Wireless routers used to monitor its distributed oil and gas mining assets. By moving all data traffic off the public internet, HEP is shielding its devices and data from the rising threat of Distributed Denial of Service (DDoS), malware, and ransomware attacks. They are also seeing significant cost savings in their cellular data bills on the back of the ability to efficiently manage data consumption and block unsolicited requests to their router infrastructure.

## CHALLENGES

HEP utilizes Airlink®RV50X routers from Sierra Wireless to monitor their infrastructure across a geographically remote and diverse network of oil and gas assets. They manage these assets from a command control center via LTE on both AT&T and Verizon Wireless. The main challenge encountered by the team was the need to protect these mission critical routers from the potential of attack from an increasing volume of DDoS and ransomware threats from rogue actors targeting critical national infrastructure such as oil and gas fields.

Coupled with this was the desire to optimize how they could manage the software updating and security patching of these devices in a cost-effective manner. With the increasing sophistication of cyberattacks, the information network team was regularly called on to manually perform security patch updates, which was time consuming and costly to HEP.

> ***Asavie SD IoT™ allowed us to immediately take our estate of IoT monitoring devices out of the line of fire and simplify the process for performing security patch updates through a single command & control console. Now we won't deploy any new kit without ensuring it is running on Asavie SD IoT™ first.***
>
> *Chris Isbell, I&E Technician, Howard Energy Partners*

## SOLUTION DEPLOYED

HEP deployed the Asavie SD IoT™ solution on both Verizon and AT&T. With Asavie their Sierra Wireless routers were instantly communicating on a private network and from this vantage point HEP could implement policies to enforce security, visibility and control across all their Verizon and AT&T LTE networks.

Leveraging the cellular connectivity backbone, Asavie also assists HEP by enabling remote connection to the gateway and devices behind it to perform remote patch updates. This addresses the challenge of ensuring that the network team is able to quickly and cost-effectively manage the dispersed network of monitoring equipment without costly truck-rolls.

HOWARD ENERGY PARTNERS

San Antonio-based Howard Energy Partners, is an independent midstream energy company, owning and operating natural gas gathering and transportation pipelines, natural gas processing plants, rail facilities, liquid storage terminals, deep-water port facilities and other related midstream assets in Texas, Pennsylvania and Mexico. They offer an integrated platform of midstream infrastructure and services from wellhead to market to ensure the smooth running of oil and gas plants throughout the region.

## RESULTS

The Asavie SD IoT™ private network connectivity and security controls have benefitted Howard Energy Partners in several ways in a very short timeframe.

- Increased security levels through a private network IoT connectivity solution that eliminates the vulnerabilities of the public internet. Furthermore, Asavie provides zero-day defense protection from malicious websites and blocking of unsolicited requests.
- It has quickly brought data consumption costs into line with business objectives, ensuring that the finance department can forecast with confidence its monthly and quarterly cellular data expenditures.
- Asavie enables remote connection to the gateway and devices behind it to perform remote patch updates.

## TOUGHENED SECURITY

By putting their Airlink®RV50X on a private network with an IP Subnet that HEP defined on the Asavie SD IoT™ portal, HEP immediately removed themselves from the line of fire of DDoS attacks such as IoTroop/Reaper.

> ***We have confidence that our router network is protected from unsolicited requests and we're on target to hit less then 2GB of data per month across our entire network monitoring estate.***
>
> *Chris Isbell, I&E Technician,*
> *Howard Energy Partners*

## BLOCK UNSOLICITED TRAFFIC

HEP further leveraged the reports of Asavie SD IoT™ to audit the type of traffic that their Airlink®RV50X were using and implemented network security policies that on a monthly average blocks 50,000 unsolicited requests per router.

Asavie makes secure connectivity simple for any size of mobility or IoT deployment in a hyper-connected world.

ASAVIE