

# Corero's IPS Keeps Business Flowing Securely at Laclede Gas

## Summary

**Industry:** Natural gas distribution

**Challenge:** Protect Laclede Gas Company's Supervisory Control and Data Acquisition (SCADA) systems against malicious external threats that endanger critical infrastructure as well as corporate networks.

**Solution:** Corero's IPS

**Results:** The system cost-effectively protects Laclede's networks against the latest threats with minimal management overhead while transparently allowing legitimate production traffic to flow without impediment.

## Key Benefits

- Stops advanced threats out of the box
- Outstanding performance; lowest latency, superior throughput
- Reliable, purpose-built hardware
- Fast, easy deployment
- Blocks, malware, spyware, viruses and botnets
- Compatible with distributed network architecture

*Laclede Gas Company is the largest natural gas distribution utility in Missouri, serving 625,000 residential, commercial and industrial customers in St. Louis and 10 other counties. Laclede operates 31 locations, including its corporate office in St. Louis and a disaster recovery site. The company also operates an underground natural gas storage field, a propane storage cavern and propane vaporization facilities. Securing this critical infrastructure is a key to enhancing Laclede's position as a prominent gas distribution utility in the competitive national energy market.*

## The Challenge

As an energy provider in the 21st Century, Laclede Gas Company operates under the continuous threat of criminally or politically motivated attack. The computerized Supervisory Control and Data Acquisition (SCADA) systems used to monitor and control the physical processes to distribute natural gas through pipelines are no longer isolated from spreading Ethernet networks and the outside world. Once secure in their isolation, these proprietary and closed systems have gradually become more exposed as SCADA vendors began migrating to applications built on commodity hardware and software, communicating via TCP/IP across Ethernet networks.

"Today, SCADA is just as vulnerable to exploit as any other system," says Gary Kay, Laclede Director, Infrastructure and Security Services. "We've lost the security of being a closed system."

As the person responsible for Laclede's security, Kay is acutely aware of the cyber security threats that have been escalating "on an exponential basis" over the last couple of years. Stuxnet demonstrated how an attack could penetrate even isolated SCADA networks and exploit zero-day vulnerabilities. As far back as 2006, engineers at Idaho National Labs demonstrated how they could cripple a generator by remotely exploiting a vulnerability over an Internet connection. In addition to potential targeted attacks, all Internet-connected networks are exposed to botnets and automated mass reconnaissance scans and attacks.

What's more, the data generated in SCADA systems have become an integral part of the information fabric so vital to business. For years, SCADA data produced information that was consumed solely by the engineering group, Kay notes. That data has become more valuable and has to be integrated into business processes.

"You can't close these systems off," says Kay. "You have to find ways to allow some communication securely, which increases the exposure and requires increased levels of mitigating security." Laclede's SCADA system relies on a dedicated Internet connection through firewalls to the remote terminal units (RTU) and programmable logic controllers (PLC), which perform local field control and feed data from readings back to the SCADA network. Additional Internet connections through the main corporate network and disaster recovery provide redundancy.

Kay was very concerned about threats to the security of the SCADA environment, web exposure in the company's DMZs, and his inability to effectively detect malicious behavior inside from bots, "owned" computers, malware, and improper insider behavior, whether malicious or simply in ignorance of policy.

## The Solution

Kay decided that Laclede needed a strong commercial-grade intrusion prevention system (IPS) to secure the connections into the company's potentially vulnerable SCADA systems. A proprietary open-source IPS solution had failed before he came to Laclede. The company was making do with a cobbled-together Snort-based intrusion detection system (IDS) that monitored traffic but could not block potential attacks. Managing the box and maintaining signatures was a drain on Kay and his staff.

Making his case to management, Kay secured authorization and budget and began the search that culminated in the purchase and deployment of Corero Network Security's Intrusion Prevention System to protect Laclede's networks from dangerous activity while allowing business operations to continue unimpeded.

Kay wanted an active IPS, as opposed to IDS, to automatically control the application layer as Laclede's firewalls control the network layer. Among other requirements, Corero met his insistence on a solution that provides timely automated updates in response to the latest threats, so that he and his staff know their networks are secure, without draining resources.

"I wanted to know that this was one piece I could trust the vendor was taking care of so we can concentrate on day-to-day operation and security of the network," he says. He also wanted an IPS that was effective without generating too many false positives, which can result in blocking legitimate traffic and undermining confidence in the IPS' detection capabilities.

Kay's search was eventually narrowed to IPS products from Corero, TippingPoint and Sourcefire IPS. TippingPoint's cost was prohibitive, and "we really didn't see any justification for the price", he says. He was also concerned about the roadmap for TippingPoint following its acquisition by HP. Sourcefire performed well, he says, but its functionality seemed to indicate some question of focus over product direction. "These capabilities are cool but do not necessarily have to do with core IPS functionality."

And, after a negative experience with performance and latency issues with a UTM vendor, Kay was pleased to note that Corero's IPS "proved to be transparent on the network."

Kay has been well satisfied with the pre- and post-sales support he has received from Corero, and was impressed with the ease of deployment. "Everything has been exceedingly easy." Corero is highly flexible, and Kay found that rules could easily be adapted to match the applications and traffic flows unique to Laclede.

"We were able to put the devices in place without dropping more than a packet or two," he recalls.

Corero also met his requirement to seamlessly pipe its logs into Laclede's security information and event management system (SIEM), because "we don't want to devote resources to a number of dashboards and reporting tools."

## The Results

Today, Laclede's networks are secure behind Corero's IPS.

"Corero's detection capabilities have picked up a lot of things we weren't aware were going through our network," he declares. "Its protocol analysis (Corero's unique Protocol Validation Modules and file format-specific Data Validation Modules, which evaluate payloads as well the protocols themselves) does an effective job and tips me off when things aren't right. Supplemented by signature-based detection, Corero's PVM/DVM technology enables its IPS to detect most potentially malicious traffic, including zero-day exploits."

In addition to threat detection, the visibility Corero's IPS provides into Laclede networks helps from an operational perspective.

"What we see in a lot of cases are helpful troubleshooting network issues," he observes. "Behavior detected and noted as possibly risky is also often indicative of network misbehavior in general."

Similarly, Kay appreciates the visibility inside Laclede's networks that enables him to observe not only suspicious outbound traffic that may indicate an owned computer or bot, but traffic between workstations and between workstations and servers that may also indicate anomalous activity.

And, Kay is fully satisfied with the IPS' reliability (the appliance has a documented mean time between failures of 20 to 30 years and dual power supplies) and high availability features through its ProtectionCluster capability. "I don't believe I have even rebooted the appliance once."

Kay is selective about the products he endorses, "but very good about expressing my disappointment" when a product fails to live up to its claims. He has no such qualms about Corero's IPS.

"I've spent 12 years in security and dealt with a lot of platforms and technologies," he declares. "When a product does what it's supposed to do and does it well, doesn't cause me trouble or phone calls in the middle of the night, and I can feel confident it is doing exactly what I bought it for, I will volunteer to inform and enlighten people as to the benefit of that product."

## About Corero Network Security

Corero Network Security (CNS:LN) is a leading global provider of Network Intrusion Prevention Systems (IPS) and Distributed Denial of Service (DDoS) defense solutions. Enterprise organizations rely on Corero to protect their critical online assets against risks associated with network-borne cyber threats. Corero, formerly Top Layer Security, is headquartered in Massachusetts, U.S. with offices worldwide. [www.corero.com](http://www.corero.com).

---

### Corporate Headquarters

1 Cabot Road  
Hudson, MA 01749  
Phone: +1.978.212.1500  
Fax: +1.978.212.1600  
[www.corero.com](http://www.corero.com)

### EMEA Headquarters

No.1 Cornhill  
London  
EC3V 3ND  
Phone: +44 (0) 203 427 3407

To purchase Corero Network Security solutions, please contact your Corero representative at **1.978.212.1500** or authorized reseller.