ARCTIC WOLF

ROPER PUMPS

PERSONAL | PREDICTABLE | PROTECTION

CASE STUDY

Company at a Glance

Roper Pump (roperpumps.com) is recognized worldwide as a leading provider of innovative fluid handling solutions, including external gear Pump and flow dividers, and progressing cavity power sections and pumps.

Challenges

- Lack of visibility into a diverse and distributed network
- Constrained IT resources
- Satisfying risk management questionnaires from strategic customers

Results

- Security visibility across the entire environment, both on-premises and in the cloud
- Monitoring AWS infrastructure, including EC2 instance and S3 storage activity
- Improved security posture through ongoing advice and partnership

Roper Pump Enhances Security Posture with Arctic Wolf's SOC-as-a-Service

> "Arctic Wolf has been one of the best decisions I have ever made. It is the most cost-effective and impactful way to monitor our security."
>
> — **Phillip Partin,** Director of Information Technology, Roper Pump

The Need to Secure Intellectual Property

Founded in 1857, Roper Pump leverages unsurpassed fluid dynamics expertise to deliver superior engineering offerings for the most challenging applications. Roper Pump and its sister company have over 260 employees with offices in Commerce Georgia, Houston Texas and Chicago Illinois.

The Roper Pump IT team manages, secures, and monitors a diverse infrastructure that includes over 300 workstations, 125 servers, networking infrastructure comprised of switches, routers, and wi-fi access points, along with Amazon Web Services (AWS) cloud infrastructure.

The firm differentiates itself in the fluid dynamics marketplace through superior technology. It spends considerable time ensuring the security of its valuable intellectual property, which includes patented processes and products. As Phillip Partin, the company's director of information technology, described, "We are typically first to market with new fluid dynamics technologies, and that is a competitive barrier. It also paints a bullseye on us. We need to safeguard that information."

The Challenges of a Fluid Cybersecurity Environment

Prior to considering a managed detection and response solution, Roper Pump had no comprehensive approach to holistically monitor infrastructure or gather security insights from log data generated by its various IT systems. According to Partin, "Given the threat environment and how aggressive the bad guys can be, you ideally need a dedicated security team to handle this. Mid-sized companies like Roper Pump cannot afford to go out and hire a cybersecurity team and put in place the necessary infrastructure. We needed a solution operating 24/7 that included people we could depend and rely on that could become a part of our team."

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Confidential

The Roper Pump team had multiple reasons to ramp up cybersecurity. A strategic customer required the company to complete a vendor risk management questionnaire that included security monitoring and external vulnerability assessment, the corporate parent updated its cybersecurity mandate, and a deluge of ransomware news motivated the IT team to ensure it had a strong cybersecurity posture. Commented Partin, "We had the eyes and ears of the executive leadership behind us. That made a huge difference when you consider something like security that doesn't make a profit."

The team considered multiple options. Eventually, Roper Pump determined that Arctic Wolf's MDR offering provided the best option to meet its ongoing monitoring and compliance requirements. "We were not satisfied with other options. The relationship piece was a huge part of the equation—I wanted a force multiplier for my team to generate outcomes, not a computer program that would spit out more false positive alerts. The Arctic Wolf™ team is sort of like a security heart monitor—when that security heartbeat increases or decreases, they can help tell you why. They know my environment and can distinguish normal from not normal."

Arctic Wolf SOC-as-a-Service Elevates Roper Pump Cybersecurity

The Arctic Wolf SOC-as-a-service featuring Arctic Wolf™ Managed Detection and Response was initially deployed in early 2017 across Roper Pump on-premises environment and subsequently rolled out across the AWS deployment. Since then, Arctic Wolf has helped uncover a number of issues, including:

- Malware and adware beaconing on endpoints
- Questionable administrative account activity
- Users visiting known malicious websites
- Quickly identifying causes behind account lockouts to facilitate unlock processes
- AWS identity and access management (IAM) hygiene deficiencies

"Users sometimes take a path of least resistance, which can be an issue from a security perspective," Partin said. "Arctic Wolf watches our environment and quickly notifies me when things appear to go sideways. This lets our IT team to immediately make improvements."

Arctic Wolf monitors the Roper Pump AWS environment that includes Amazon EC2 instances and S3 storage buckets. Telemetry from those AWS services goes into the Arctic Wolf SOC-as-a-service where Arctic Wolf's Concierge Security™ Team ensures everything is properly configured, locked down, and monitored on an ongoing basis.

Roper Pump has progressively increased the number of log sources that Arctic Wolf MDR ingests. "We've started directing more and more log sources to Arctic Wolf," Partin said. "An approach that ingests log sources at no additional cost helps deliver better security."

Arctic Wolf also monitors administrative accounts and provides visibility into previously unwatched activity. "That visibility provides us with confidence that we are maintaining appropriate security," Partin said.

Arctic Wolf MDR has the ability to contain threats on endpoints, a function that Partin finds to be quite useful. "Containing threats on our endpoints helps make our IT team more efficient and effective. When something malicious is identified on an endpoint, Arctic Wolf can lock it down so we can then remediate it based on our schedule."

As part of the Arctic Wolf MDR service, Roper Pump has regular review meetings with the Concierge Security Team to improve its security posture, receiving feedback on necessary steps to take to stay better protected. "The Arctic Wolf team has visibility and lessons learned from a bunch of different environments, and I benefit from that experience," said Partin. "And when we meet with our corporate parent, I am one of the few people who has no significant security incidents. We have avoided catastrophic breaches because Arctic Wolf helps slam shut the window of vulnerability. Small security incidents do not grow into catastrophic breaches. Within moments of anything happening, Arctic Wolf notifies us, and we can address it."

ARCTIC WOLF

©2020 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.

SOC2 Type II Certified

Contact Us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com