CASE STUDY

Rural Electricity Co-op Fortifies Its IT and OT Networks With an MSP-delivered Security Fabric

The electric grid that spans nine counties in sparsely populated East Texas—distributing power over 5,000 miles of line to just under 25,000 members—does not seem like the kind of utility that would be taken down by a nation-state hacker or cyber criminal.

Shelby Vance wants to keep it that way. Vance, the IT director of the Houston County Electric Cooperative (HCEC), harbors no illusions about the reach of cyber threats. As a regional electric distribution cooperative, HCEC is owned by its customer-members. "We have member data—credit cards, Social Security numbers, phone numbers, street and email addresses, and other information that a lot of bad actors want to have," he explains.

HCEC also maintains an operational technology (OT) network, comprised of mainly unstaffed substations, with their switches and supervisory control and data acquisition (SCADA) systems, automatic metering infrastructure, and distributed generation systems (such as solar PV). "We are seeing large-scale attacks against the bulk electric system around the world," Vance says. "The fear is that somebody might get into substation equipment and shut down the power. Any unauthorized access to our system could have catastrophic results to our organization and communities. For us, the real challenge is to make sure that we protect all those resources."

A Big Security Load for a Small Utility

Guided by best practices such as those laid out in the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standard, Vance set out to upgrade HCEC's network security. The initiative had two main goals. First, the HCEC network needed to be segmented.

"Our network and infrastructure had never been designed with security in mind," he says. "We worked with the Department of Homeland Security to do a network evaluation and found that our network was very flat. So, traversing through the network would have been very easy." As part of the segmentation process, Vance wanted to create an air gap between the IT and OT networks, so that breaches on the IT side could not jump over to the OT systems and bring down the grid.

Second, Vance wanted to bring HCEC's security tools up to date. "All of our equipment was either end of life, or it was no longer receiving support," he explains.

HCEC
A Touchstone Energy® Cooperative

"Fortinet's product line, software, and support—combined with SkyHelm's skills, knowledge, expertise, and services—provide us with a great security benefit ensuring critical electric infrastructure is protected, monitored, and maintained in an efficient and cost-effective manner."

– *Shelby Vance, IT Director, Houston County Electric Cooperative*

Details

Customer: Houston County Electric Cooperative

Fortinet Partner: SkyHelm Technology

Industry: Power & Utilities

Location: Crockett, Texas

Business Impact

- For HCEC, significant improvement in security posture without increasing IT headcount
- For SkyHelm, a reliable roadmap to service growth by leveraging the Fortinet Security Fabric and through collaboration with Fortinet

Both of these objectives were laudable, but achieving them would require staff. Vance estimates he would need about double the IT headcount he has in order to manage the new security environment in-house. And if large metro areas across the country are facing a skills gap, consider how much harder security talent is to come by in rural East Texas. Vance himself has many roles at HCEC: PC support, server management, networking infrastructure, and all the planning and budgeting responsibilities. Bringing HCEC's network security in line with NERC CIP standards was not something he was able to tackle without help. "I really was looking for ease of use, ease of manageability, and being able to quickly see what was happening on the network," Vance explains. "I do not have time to spend sitting and looking at a console all day to try to figure out what is going on."

The Go-to MSP for Rural Electric Co-ops

Based on recommendations from peers in the industry, Vance reached out to SkyHelm Technology, a managed service provider (MSP) specializing in cybersecurity for electric distribution co-ops. SkyHelm's TITAN cybersecurity service is a comprehensive solution that relies heavily on the Fortinet Security Fabric. TITAN includes on-premises network security and LAN Edge technology, such as FortiGate next-generation firewalls (NGFWs) and FortiSwitch Ethernet switches. The MSP configures and manages the security tools from its U.S.-based 24×7 security operations center (SOC), using FortiManager and FortiAnalyzer solutions (known collectively as the Fabric Management Center). TITAN also leverages FortiSIEM security information and event management to alert its clients to potential threats and mount prompt, effective responses.

"We bundle those products with some of our own value-added services, and it is all managed and monitored by our team for a monthly service fee," explains SkyHelm Co-founder and CEO Jeremy Dreyer. "Small electric cooperatives often find that subscribing to TITAN is a more cost-effective way to achieve their security objectives than building all those capabilities themselves."

Solutions

- FortiGate
- FortiSwitch
- FortiManager
- FortiAnalyzer
- FortiSIEM

"One reason that I was so interested in the Fortinet suite was that we could get [updated equivalents to] a lot of the products that we were already using, packaged up as one. In doing so, we have eliminated several other vendors from our network."

– *Shelby Vance, IT Director, Houston County Electric Cooperative*

To prove that TITAN makes customers safer, SkyHelm uses the Rural Cooperative Cybersecurity Capabilities (RC3) assessment tool recently developed by the National Rural Electric Cooperative Association (NRECA) to gauge clients' security posture before and after subscribing to TITAN services. "Our customers who have done this have seen massive improvements—three to four times improvements—in their security posture," Dreyer says.

SkyHelm's specialization can also significantly reduce security infrastructure planning and deployment time for co-ops. "Based on our experiences from working with many cooperatives in the past, we recommend a standard configuration for everything from firewall rules and detection profiles to alerting setups," says Casey Davis, senior software developer at SkyHelm. "And when we implement these solutions, we make sure they are configured properly with best practices that are tuned for distribution co-ops."

Once TITAN is up and running, all the log data and alerts from the security devices at the client's facilities are routed to SkyHelm's SOC. SkyHelm has also developed a client dashboard that enables cooperative IT directors like Vance to see at a glance any issues that require their attention.

More Security, Less Burden

This was the administrative relief Vance was looking for. "The managed service provider agreement with SkyHelm has enabled us to have that high-end NOC [network operations center]/SOC experience without having to implement it ourselves," he says. "My job has turned into project management rather than having to deal with day-to-day minutiae, like hunting down a rogue alert and trying to figure out what is going on. SkyHelm evaluates it, and they let me know if they see an issue. Or If I notice something, I can reach out to them, and usually 10 to 20 minutes later, I have an answer. This has allowed me to focus on a lot of the bigger-picture sort of things that I need to be able to do."

Currently, HCEC has FortiGate firewalls and FortiSwitch Ethernet switches installed at its corporate headquarters in Crockett. Plans are to deploy FortiGate firewalls in the substations as well, replacing legacy systems from a large networking vendor. "One reason that I was so interested in the Fortinet suite was that we could get [updated equivalents to] a lot of the products that we were already using, packaged up as one," Vance says. "In doing so, we have eliminated several other vendors from our network."

Leveraging the Security Fabric To Create Comprehensive Service Offerings

SkyHelm has been incorporating Fortinet solutions into its offerings since 2014. "We evaluated Fortinet against many other vendors out there," says Dreyer. "They have the right technology for the right price. The FortiGate and FortiSwitch solutions are a great fit for our customers, and we have built onto that over time with other solutions, like FortiSIEM, and we will soon add FortiEDR [endpoint detection and response]. There are also other Fortinet products that we sell and deliver, such as FortiNAC [network access control] and FortiAuthenticator [user authentication], which I expect we will integrate into TITAN in the near future."

> *"We evaluated Fortinet against many other vendors out there. They have the right technology for the right price."*
>
> – *Jeremy Dreyer, Co-founder and CTO, SkyHelm Technology*

For HCEC, replacing aging networking and security products with an integrated FortiGate and FortiSwitch solution has transformed security, reliability, and efficiency for both the IT and the OT networks. The FortiSwitch integrates directly into the FortiGate NGFW through FortiLink, enabling direct control configuration and management and offering the same level of inspection as the ports on the FortiGate. HCEC's post-implementation RC3 assessments are still in progress, but SkyHelm expects to see improvements in line with their other electric co-op clients.

Still, according to Davis, product performance tells only half the story. "Our big reason for choosing Fortinet is the power of the Security Fabric," he says. "We can make other products integrate, but having ones that integrate out of the box is huge. If we pair a FortiGate firewall with FortiSIEM, the technology that Fortinet has incorporated in both of those products allows us to see exactly what is happening on the SCADA systems. So, it simplifies security management for the SCADA systems as well as everything else that the FortiGate firewalls are monitoring."

Davis sees the benefits of the Security Fabric carry over to the MSP's operational side as well. "It takes less time to manage the security hardware for all of our clients, and it is easier to get a big picture view of what is going on, to see and respond to threats more easily," he says. "We have also worked with Fortinet to co-develop some best practices for electric co-ops. Fortinet has really made an investment there."

A Trailblazer for Rural Co-ops

For now, only major electricity providers in the United States, such as investor-owned or municipal utilities, are required to file proof of compliance with NERC CIP standards. For the smaller distribution electric cooperatives, compliance is currently voluntary. But as threats proliferate to every corner of the globe, even the smallest providers will likely soon have to follow those same best practices. Thanks to Vance's diligence, HCEC is getting ahead of what many believe will be the prevailing norm within the next decade.

He is not stopping there. "I am considering moving all of my wireless infrastructure to FortiAP wireless access points, because of the same [FortiLink] integration and automation that they provide. Fortinet's product line, software, and support—combined with SkyHelm's skills, knowledge, expertise, and services—provide us with a great security benefit ensuring critical electric infrastructure is protected, monitored, and maintained in an efficient and cost-effective manner."

February 13, 2021 6:04 AM

123456-0-0-EN

cs-FA-rural-electricity-coop-fortifies-its-it-and-ot-networks-2102021