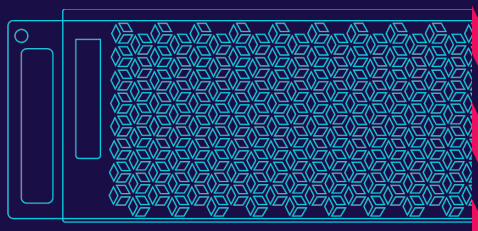
CASE STUDY: FLORIDA KEYS ELECTRIC COOPERATIVE ASSOCIATION

How Florida Keys Electric Cooperative Safeguards Data Archives From Ransomware

Electric Utility Provider Selected RackTop's BrickStor SP For Real-Time Visibility and Cyber Resilience

Key Risk Factors

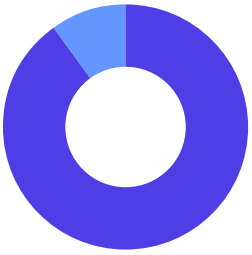
- Accelerating Ransomware Threats
- Complex Auditing and Reporting Compliance Requirements



Situation

Tamie Fox, Director of IT for the Florida Keys Electric Cooperative, a member-owned, not-for-profit electric utility serving approximately 33,000 customers across the upper and middle Florida Keys, can still remember the first time her company fell victim to a targeted ransomware attack. It happened back in 2015, several years before ransomware emerged as the primary variant of a global cyber pandemic that continues to spread across sectors today. Within a matter of hours, the non-profit electric utility's data archives were suddenly on the brink of irremediable damage.

"It hit us out of nowhere," said Fox. "We were lucky to have still been writing data to magnetic tape at the time, which allowed us to pull it back without paying the ransom. But the thought of not being able to recover from something like that was always scary."



10% of all industrial-related ransomware attacks targeted electric utilities over the previous two years.

NEXTGOV.COM

RACKTOP

Fast forward to May 2021, when Colonial Pipeline Company was hit by the largest ransomware attack on a critical infrastructure provider in U.S. history. Fox witnessed the fallout from that incident, which temporarily cut off fuel supply to a majority of the East Coast, and couldn't help but envision the prospects of a similar attack on FKEC. With threat actors more skilled and motivated than ever before, the threat landscape was rapidly evolving. The volume and velocity of ransomware attacks was on the rise amidst accelerations in cloud migration and digital adoption. And electric utilities, in particular, had been targeted in 10% of all industrial-related ransomware attacks over the previous two years.

> **"With BrickStor SP, I'm more confident in my data than ever before. I know it's there. I know it's protecting my archives. And I know that if I have a ransomware problem, I can go in and recover very easily."**
>
> — Tamie Fox, Director of IT, Florida Keys Electric Cooperative

Earlier that year, a hacker infiltrated the network of a Florida-based water treatment facility in an attempt to contaminate the City of Oldsmar's (Fla.) public water supply. The plant was located just a few hours north of FKEC's headquarters – representing a clear microcosm of the real and imminent threat that cybercrime posed on their business. It hit close to home.

"That attack made people realize this was happening in our backyard," said Fox. "I had been telling my management team all along that it wasn't a question of if it would happen to us, but rather a question of when. We were going to be hit at some point in time. We had to make sure we could respond."

After already making significant investments in its software infrastructure, FKEC needed a scalable data management solution that could "turn the lights on" with real-time visibility and access controls to proactively prevent, detect, and mitigate ransomware attacks.

As fate would have it, the RackTop Systems team was ready to help.

Strategy

Following a series of consultations with RackTop representatives, Fox enrolled FKEC in the RackTop Jumpstart Training and Enablement Program, which offered a free 90-day subscription to deploy its virtual BrickStor SP solution for data-centric Zero Trust capabilities. At the conclusion of the program, FKEC would then have the option to extend the partnership by purchasing an annual licensing agreement.

In this case, however, RackTop didn't need 90 days to deliver unrivaled ransomware protection. The value was evident from the beginning of the program.

"Within three weeks of deployment, I was already sold and signing contracts," Fox said. "I was on the phone with them saying, 'I need this right now.' From its deployability and price to its ease of use, I was very impressed with the BrickStor SP product."

The flexibility of BrickStor SP enabled FKEC to layer it on top of existing hyperconverged

hardware infrastructure, which helped avoid hefty replacement costs. By leveraging the product's Transparent Data Movement (TDM) functionality, FKEC was able to extend 8 Terabytes of data storage to a secure cloud file server. RackTop's team of expert technicians was available for 24/7 onboarding support – ensuring a seamless deployment process from start to finish.

"When I decided to go live with BrickStor SP, I didn't think to tell the RackTop team because most companies don't really care," said Fox. "If they already sold you the product, they don't care to know if you implemented it or how you're using it. But with RackTop, the entire support staff wanted to know I went live and be available around the clock so that any issues were resolved. You just don't get that kind of customer service nowadays."

Results

Upon deployment, BrickStor SP immediately created a unified layer of defense to safeguard FKEC's sensitive data archives from threat actors. Notable benefits included active defense against ransomware and insider threats, air gap data protections, tool consolidation, enhanced data security, advanced cyberstorage capacity forecasting, user behavior auditing and analysis, snapshots and file indexing. Furthermore, it was all delivered at an affordable rate to maximize ROI.

BrickStor SP also enabled FKEC to streamline storage compliance for both on demand auditing and predetermined interval reporting.

> **"I was very impressed with the BrickStor SP product... I can stop an attack right there in the interface."**

Considering all access records were generated from RackTop's immutable database, the company could determine in confidence that its compliance reports were entirely accurate to meet federal and state regulations.

When considering the business value of a Cyberstorage solution like BrickStor SP, Fox said "Compared to other products I've paid for, I was in disbelief when I saw the price, "RackTop is very up front and honest with you about pricing, which I appreciated because, again, not every company is like that. They'll show you a great product, tell you why you need it, and then hit you with a bill that makes you wonder 'How in the world will I ever put this in front of management?' RackTop didn't do that."

With real-time, actionable insights into network user behaviors, FKEC gained the critical foresight to identify potential ransomware threats by knowing:

- **What sensitive files were accessed**
- **Who accessed them**
- **When they were accessed**
- **Where they were accessed from**
- **Why they were accessed**

"The user interface, while simplistic in design, makes it easy to use because you're not digging through a ton of layers to try and find something," said Fox. "I can not only see what my users are doing, but also what someone posing as a user is doing as well. I can stop an attack right there in the interface. I don't need to switch between 12 different tools.

"While we're a small cooperative, that doesn't mean we're not a ransomware target. We'll need to be able to respond. I feel more confident that we can with RackTop's product."