CUSTOMER CASE STUDY | STATE & LOCAL GOVERNMENT

Eau Claire County Simplifies IT Operations and Strengthens Data Protection with BrickStor SP

A Wisconsin county replaced its traditional Windows file server with BrickStor SP, gaining full visibility, automated defense, and self-service file recovery.

At a Glance	CUSTOMER	SECTOR	DEPLOYMENT	WORKLOAD	CUSTOMER SINCE
	Eau Claire County, Wisconsin	County government serving 108,800+ residents	BrickStor SP virtual appliance	Department file shares	2019

Overview

Founded in 1856, Eau Claire County serves more than 108,800 residents across 13 towns, 3 cities, and 3 villages in west-central Wisconsin. Its Information Systems team supports every county department with a lean staff and growing demands for cybersecurity visibility and control.

AxCel Technology, whose team brings more than 75 years of combined experience helping businesses evaluate and select cybersecurity solutions, introduced the county to RackTop's BrickStor SP. In 2019, Eau Claire County deployed the platform as a single virtual appliance, replacing its Windows file server for all department drives.

The Challenge

The county's department drives lived on a standard Windows file server that offered almost no insight into what users were doing with their data. As ransomware shifted from attacking operating systems to encrypting data directly, and as compromised accounts and insiders made data theft a real concern, a basic Windows file share had become a liability.

> **"Our cybersecurity program is ratcheting up to the point where we need way more visibility and way more control over what's going on."**
>
> Network Analyst, Eau Claire County

Day-to-day operations carried a cost too. Every accidental deletion meant a senior administrator signing into the backup system to restore files. One department alone has a couple hundred employees across divisions that must not see each other's files, which demanded strict access boundaries.

The Solution

In 2019, Eau Claire County deployed BrickStor SP as a single virtual appliance, replacing the Windows file server for all department drives. Employees kept the same familiar SMB file shares, while the IT team gained native Active Defense at the storage layer. Every file action is logged, user behavior is measured against protective thresholds, and snapshots are exposed directly through Windows Previous Versions for fast recovery.

The Results

Visibility into every file action

BrickStor SP logs everything every user does and categorizes alerts so they are easy to read, even for someone who isn't a storage expert. Instead of digging through Windows event logs, the team pulls historical activity from built-in reports. Most events turn out to be an accidental delete or a large cleanup, and IT knows about each one right away.

Automated defense that stays out of the way

When a user's behavior crosses a threshold, BrickStor SP quarantines that user from the file share and sends an alert to the team mailbox. The county runs RackTop's default thresholds, which it calls the sweet spot. Lockouts occur at most once or twice a month, with IT often calling before users notice and restoring access instantly once cleared. Many employees now flag large deletions in advance, and planned year-end purges use temporary exceptions that expire automatically.

Self-service recovery that frees up senior staff

Because BrickStor SP snapshots appear in Windows Previous Versions, help desk technicians and tech-savvy employees restore files with a right-click. The help desk never needs access to the backup system, and the senior administrator is no longer pulled into routine restores. "It's just so fast and easy, and you can browse so quickly through all the previous versions to find where your file last was," says the county's network analyst. "That's a big time saver."

Strengthening defenses around county data

To date, the county has not faced a ransomware or data theft incident, a record it credits to a cybersecurity program that has matured significantly over the past seven years. BrickStor SP is part of that defense, with patented Active Defense designed to detect and stop both ransomware and data exfiltration, and to restore only the affected files with a 1-minute RPO and 3-minute RTO.

Support That Keeps Them Confident

For a Windows-focused team, RackTop support is a deciding factor. Engineers go above and beyond, digging into the details whenever something needs attention.

> **"I usually patch the server late at night. I submitted a ticket, and before I could even shut my computer down, they were reaching out and resolved the issue right away. I usually don't get that from anybody else.**
>
> Network Analyst, Eau Claire County

About RackTop

RackTop Systems helps county and municipal IT teams protect the shared files that keep local government running. Founded in 2010 by U.S. Intelligence Community veterans, RackTop combines file and object storage with built-in security. Its BrickStor SP platform detects and stops ransomware and data theft in real time, while snapshots help teams recover deleted or changed files.

To discuss protection and recovery for your county's department file shares, contact sales@racktopsystems.com or visit www.racktopsystems.com.