As a family-run business, Kelley Bros has been servicing the Syracuse, NY, community for 5 generations. From selling coal to operating as a general hardware store, Kelley Bros' current iteration supplies contractors with quality doors, frames, and access control solutions across 14 states. Their primary customers today include architects, hospitals, educational institutions, hotels, multifamily, residential, and high-rise apartment buildings.

"The coal towers are still there. The scale that they used to use to weigh the coal wagons is still underneath the parking lot," Kelley Bros IT Manager, Matt Ellsworth, said.

In his role as IT Manager, Matt was tasked—as many IT Managers are—with finding a robust and affordable cybersecurity stack that helps protect their 260 employees from a potential attack. When Matt joined the Kelley Bros team 7 years ago, the company was using OpenDNS to block base-level, large categories. After about a year, it was time to replace their firewalls, and they explored a Next Gen firewall solution that offered content filtering.

**A COSTLY ACQUISITION LEADS TO DNSFILTER**

In 2015, Cisco acquired OpenDNS leaving many customers like Matt in sticker shock:

"They decided to raise the price by a factor of a hundred-fold or something like that. It went from being, like, a couple of hundred dollars a year to $5,000 or $6,000 a year," he said.

He continued, "So for us, we were like, 'Hey, wait a minute, that's too big of a jump here' whenever something was wrong, and they got something miscategorized, it took them forever to get them corrected. And so I was like, 'well, I'm not gonna pay you for something you're bad at.'"

Matt began looking for other DNS security solutions and stumbled upon DNSFilter, where he found comfort in an accommodating pricing model.

"The pricing was transparent," he said. "There wasn't any running around trying to get a quote and trying to get a deal to find out how much a price was. It was just available. It was very simple to purchase. These other large name-brand solutions, you can't even find out what the list price is, much less your actual prices."

"WELL, I'M NOT GONNA PAY YOU FOR SOMETHING YOU'RE BAD AT."

**MATT ELLSWORTH**
Kelley Bros IT Manager
DNS Filter's Roaming Clients are installed for Kelley Bros' remote employees and on all computers at their 25 office locations. Roaming Clients are known to protect off-site company devices from malicious domains, but they also can provide IT managers like Matt with better reporting insights. Because the policy can be assigned by the user, DNS Filter query logs can show which person made a specific query.

DNS Filter also helps block various threats like phishing, malware, and ransomware on Kelley Bros' guest networks at all of their locations.

Matt highlighted one of DNS Filter's convenient capabilities as the most important to him:

"I wanted something that would allow me to block entire TLDs, and so, fortunately, DNS Filter allows me to do that," he said. "Let's say I wanted to block everything that's .xyz...then I just go in there, and I hit add rule, block .xyz and then no matter what some clever person comes up with as an .xyz domain, it will be blocked. So that was a big functionality that a lot of other DNS services were lacking."

Matt then went on to explain that when it comes to Kelley Bros' electronic access control systems, they are based on an outbound-only model and secure by design. Each device communicates to the controller (on-prem or in cloud) and then creates a tunnel to only talk to. "They just have access to the internet and not anything else," he said.

DNS-FRST MENTALITY

It has been said repeatedly that DNS is often the most important and overlooked part of the internet. DNS is typically considered the "first line of defense" in a cybersecurity stack, but because it is invisible to the user, it can be forgotten.

Matt explained the importance of paying attention to DNS security protection, specifically what DNS Filter brings to the cybersecurity space:

"There's the threat report function. Sometimes, I'll look up a domain to see whether or not DNS Filter thinks it's malicious. If it were reused in a phishing campaign against us, I'd report those as ways to help attempt to protect the community," he said.

Matt continued, "If they [DNS Filter] detect it's malicious, then they can block it, and it'll be blocked for many other people. That's just a good thing for the internet, right? The less bad stuff that goes on the internet, the better the internet is."