FEND®

Physically Block Cyberattacks

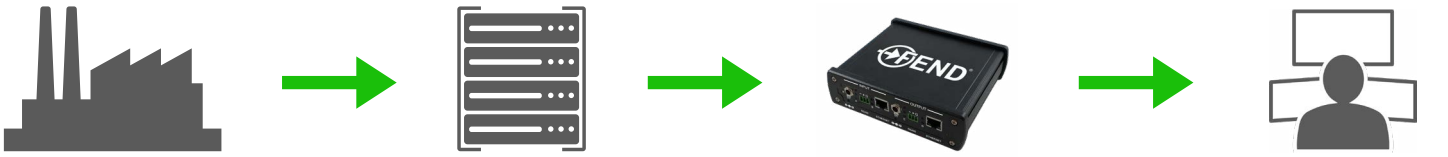
Protecting Higher Education Facilities While Increasing Operational Efficiency

Higher education institutions are increasingly at risk of cyber threats, from foreign state actors looking to steal valuable research and intellectual property to criminals attempting to gain user data for new phishing attacks. However, one of the most vulnerable assets to cyberattacks on campus can be the utilities that enable day to day operations. Boiler plants supplying steam and hot water can be taken offline. Building automation systems can be held for ransom. Backup generators at the university hospital can be disabled when they're needed most. The benefits of real-time utility system monitoring – efficiency, resilience, increased uptime – are driving physical plant operators to bring this equipment online, and now there's a way to do so safely by physically blocking cyberattacks.

Safely Monitoring Campus Energy Systems

Over its 200-year history, a state university had grown to include over 500 buildings with 200 miles of underground heating, cooling, water, and sewer lines spread across 3,000 acres. Most of these buildings are many decades old, with the current campus heat plant dating back to the 1950s. Operators of this critical resource, capable of heating some 10,000,000 square feet of classroom, research, and dormitory space, went without real-time monitoring until recently. Systems were mostly "air gapped" or isolated from outside networks. Critical performance data was extracted via physical media. Attempts to use firewalls provided an imperfect defense, and their maintenance cost thousands of dollars per device per year.

Operational data now flows in a physically-enforced one-way fashion without firewalls or manual processes.



The facilities management team turned to Fend to get performance data from their boilers and other key assets in a physically-enforced, one-way fashion. Fend's data diodes send information out in only one direction using a physics-based approach that blocks all incoming transmissions. Engineering teams can analyze the data remotely and even make use of AI-based tools while maintaining the security of an air gap and eliminating the threat of a network breach. The team set up recurring, one-way FTP transmissions of key performance log files across Fend's data diodes, delivering information in real-time rather than weeks between manual downloads. Fend's devices pay for themselves through savings on labor and firewall maintenance. Now, the facility management team has the data they need and the university community gets the operational resilience they deserve.

Did You Know?

In September 2023, the National Institute of Standards and Technology (NIST) updated their Guide to Operational Technology (OT) Security (NIST SP 800-82r3). The guide recommends the use of one-way data diodes to protect critical assets and mitigate the risk of cyberattack. Learn more at https://csrc.nist.gov/pubs/sp/800/82/r3/final.

Fend's Data Diodes – Made in the USA

Learn more about how you can protect your critical systems at www.fend.tech.

For More Information
info@fend.tech • 571-970-1382

www.fend.tech
4600 Fairfax Dr, Suite 410, Arlington, Virginia 22203