

Dispel Launches Community Power & Water Program at APPA Cybersecurity & Technology Summit

Water and electric utilities face nation-state-grade threats with local-government-sized budgets. Dispel's new Community Power & Water Program closes that gap



SAN ANTONIO, TX, UNITED STATES,

September 14, 2026 /EINPresswire.com/ -- Dispel, the leader in Secure Remote Access (SRA) for Operational Technology (OT), today announced the opening of the Dispel Community Power & Water Program at the American Public Power Association's Cybersecurity & Technology Summit in San Antonio. The program brings the same [secure remote access capability](#) large utilities rely on to small water and electric utilities. Deployable by utility staff without an infrastructure overhaul, the system gives small utilities the ability to ringfence their environments from cyber attackers in a single work shift. Approved applicants receive special pricing designed to fit even the smallest utility's budget.

For a two- or three-person utility team, remote access is essential for day-to-day operations. It means being able to troubleshoot a lift station before ratepayers are impacted, or monitor a treatment plant without staffing a night shift. The difference between a remote fix and an in-person response is often the difference between a brief service dip and unplanned downtime for a community that depends on that water or power. The challenge is that while almost all utilities have set up remote access (or "trade access") to their equipment, very few have invested in solutions that meet any U.S. cybersecurity baseline.

Growing Cyber Risk to Municipally Owned Utilities

The risk the Dispel Community Power & Water Program addresses is not hypothetical. In late July 2026, more than [30 Minnesota municipal water utilities](#) reported cyberattacks within roughly 48 hours. Investigators found no sophisticated malware: attackers located internet-exposed programmable logic controllers (PLCs), logged in using default or missing credentials, and altered controller configurations and IP addresses directly, in some cases locking operators out of their own equipment. The activity closely follows the pattern described in a federal advisory, CISA AA26-097A, warning that threat actors have been targeting internet-exposed PLCs across U.S.

critical infrastructure; the Minnesota incidents themselves have not been formally attributed. CISA's guidance has been consistent: removing internet-facing exposure is now the top-listed control for reducing this risk. Subsequent reporting has identified similar activity affecting water systems beyond Minnesota, though exact figures remain provisional as the response develops.

Of the 148,000 water and wastewater systems in the United States, most are maintained by one or two shifts of operators whose expertise lies in water, not cybersecurity. The same reality faces many of the roughly 900 electric cooperatives in the United States. Millions of Americans get their water and power from utilities that lack dedicated cybersecurity staff or systems designed to meet cybersecurity standards. Most enterprise OT security tools, by contrast, are built for firms with dedicated security teams, months-long deployment windows, and budgets to match.

"Every community deserves the same protection, whether they are served by a utility with a fifty-person security team or three people wearing five hats each," said Ben Burke, President of Dispel. "The water coming out of a tap and the power keeping the lights on do not care how big the utility behind them is, and attackers do not discriminate by budget either. The Community Power & Water Program exists because the communities that can least afford a cyberattack are too often the ones most exposed to one, and we built it so that gap does not have to exist anymore."

Security That Fits the Team You Actually Have

Strip away the assumptions built into enterprise OT security tools, and a small utility's quick start shrinks to three things:

- Ringfence first, triage second: rather than waiting through a years-long assessment and redesign process while assets sit exposed, put a barrier around the network first. Ringfencing shuts down every connection route into and out of the environment and replaces it with a single, controlled, continuously monitored pathway, without touching the network's internal components. It is a one-shift task with Dispel, so utilities stay protected while the longer redesign work proceeds safely behind it.
- One standard access layer: instead of a different login and connection method for every vendor, contractor, and internal employee, everyone connects through the same pathway. That consistency reduces training complexity, administrative overhead, and the risk of human error that comes with juggling a patchwork of one-off VPN logins.
- One pane of glass: complex tools do not get effectively administered by teams already wearing multiple hats. The Dispel dashboard for the Community Power & Water Program provides self-service vendor onboarding, built-in compliance reporting, and access requests routed to equipment owners rather than dedicated security teams, helping small utilities avoid task

saturation while managing access into their environments.

The EPA and WaterISAC point to the same short list every utility can act on this year: remove control devices from direct internet exposure, replace shared credentials with individual accounts and MFA, and turn vendor access on only for the work at hand, then off. None of it requires new headcount; it requires an access model built around those defaults, instead of bolted onto a patchwork of legacy VPNs.

Applying to the Program

The moment for water and electric utilities to shift from reactive security to proactive risk reduction is now. The Dispel Community Power & Water Program gives small, budget-strapped teams a direct path to that shift, designed for utilities operating with real threats and budgets that were never sized for enterprise security. Approved applications receive special pricing designed to meet even the smallest utility budgets.

Utilities attending the APPA Cybersecurity & Technology Summit can meet the Dispel team on-site to ask questions about the program, or apply directly online at go.dispel.com/dispel-community-power-water-program.

About Dispel

Dispel delivers security that makes industrial operations run faster. The Dispel Zero Trust Engine securely connects people and operational data across complex OT environments, unifying secure remote access, industrial data streaming, Dispel Intelligence, Dispel Identity, Dispel Compliance, and OTFusion into one platform. Founded in 2015, Dispel pioneered network-level Moving Target Defense (MTD) and holds 60 patents, protecting over \$500 billion in manufactured goods annually and securing remote access for more than 60 million utility users worldwide. Built for Efficiency. Secure by Design. Audit Ready. Learn more at dispel.com.

Mark Lennon

Dispel

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/941527281>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire,

Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.