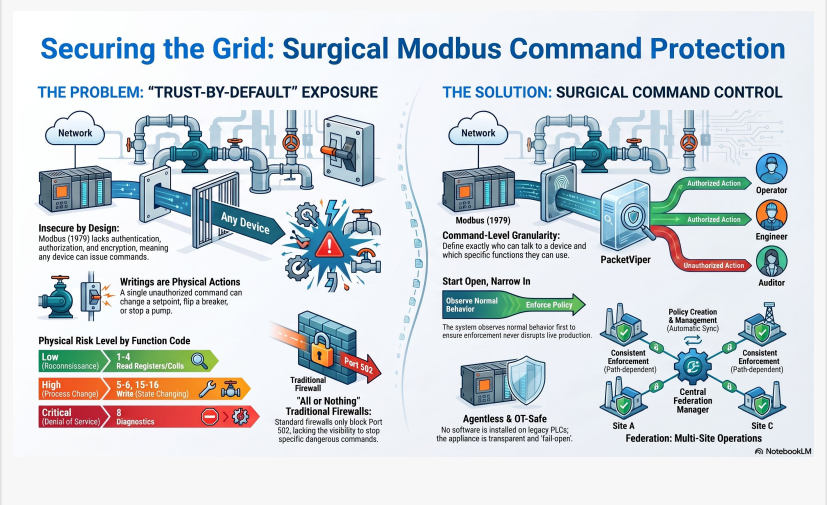
PacketViper Delivers Command-Level Modbus Protection for Critical Infrastructure Through Automated Moving Target Defense

Agentless, single-appliance protection inspects and enforces industrial control commands inline, closing a security gap in the most widely deployed OT protocol



PITTSBURGH, PA, UNITED STATES, July 7, 2026 /EINPresswire.com/ -- As attacks on critical infrastructure escalate, PacketViper is protecting the operational technology behind water, power, manufacturing, and transportation with command-level Modbus protection that inspects and enforces industrial control commands inline, with no agents on field devices and no disruption to operations. It runs on the same single appliance that delivers PacketViper's Automated Moving Target Defense, giving operators control over exactly what each connected device is allowed to do.

> Critical infrastructure runs on protocols never designed to be exposed to the modern threat landscape. You cannot simply patch or replace the systems that keep water flowing and the lights on."
>
> *Francesco Trama*

Modbus is the most widely deployed industrial protocol in the world. It runs the pumps, valves, breakers, drives, and controllers behind water systems, the power grid, manufacturing, oil and gas, and transportation. It was designed in 1979 for trusted, isolated serial links, and it has no authentication, no authorization, and no encryption. In practice, any device that can reach a Modbus endpoint can command it: change a setpoint, open or close a breaker, or force a controller offline. As attacks on critical infrastructure escalate, including a new generation of autonomous, AI-driven attacks, that trust-by-default exposure has become a national security concern.

Traditional firewalls cannot address it. They can only allow or block the connection wholesale,

with no understanding of the command inside it. PacketViper Modbus Command Protection changes that. It understands industrial commands at the level that matters and enforces a policy for each device that defines who may communicate with it and what they are permitted to do. An unauthorized command is stopped inline, on the specific device, without taking that device offline or disrupting legitimate control traffic.

Consistent with PacketViper's approach to operational technology, the capability starts by observing rather than blocking. Firewalls start closed and are opened, which risks interrupting a live process the moment they are deployed. PacketViper starts open and narrows in, learning normal behavior first, then applying surgical enforcement with confidence. It is agentless and transparent to the control network, so nothing is installed on legacy equipment that cannot be patched or disturbed.

"Critical infrastructure runs on protocols that were never designed to be exposed to the modern threat landscape, and you cannot simply patch or replace the systems that keep water flowing and the lights on," said Francesco Trama, CEO and Founder of PacketViper. "Our answer is to understand the command and enforce it inline, on the device, without disrupting the process. A blocked command is not the end of the story. It is the beginning of an investigation, a misconfiguration, an unknown integration, or a genuine threat, and we put that in front of the right people. This is preemptive defense for the systems the country depends on."

The capability is built for scale. A single policy authored at PacketViper's Federation Manager is applied identically across every appliance that sees a device, so protection is consistent across a national or metropolitan footprint with no gap and no bypass path. It is the model PacketViper is deploying for large-scale transportation authorities, alongside its command-level protection for signal and messaging systems.

Modbus Command Protection is one capability of a single-appliance platform that also delivers Automated Moving Target Defense, network sensors, and centralized federation. What competitors require several products to accomplish, PacketViper delivers on one agentless appliance, purpose-built for the constraints of operational technology.

The capability also supports control requirements in the major critical-infrastructure security frameworks, including IEC 62443, NIST SP 800-82, the NIST Cybersecurity Framework, and NERC CIP. Because every action and violation is recorded, the audit trail is a byproduct of normal operation rather than a separate reporting exercise.

About PacketViper
PacketViper's Automated Moving Target Defense protects operational technology and critical infrastructure with preemptive, agentless, inline enforcement on a single appliance. PacketViper is U.S.-owned and U.S.-staffed with no foreign ownership, control, or influence, and is available on the GSA Schedule and Army CHESS ITES-SW2. To learn more, visit www.packetviper.com.

Tim Jencka
PacketViper
+1 4122126348
email us here