PACKETVIPER™

Cyber Defense of Distributed OT Endpoints to Preserve Uptime and Protect Public Health and Safety

The Challenge: Ensuring the Safe, Secure and Reliable Operations of Essential Services in our Physical World

Organizations with distributed operational technology (OT) endpoints need a cost-effective, low-maintenance way to ensure the secure, reliable and continuous operations of process control systems. Previously air-gapped OT endpoints are increasingly being connected to corporate information technology (IT) networks. This creates new attack vectors that can lead to greater exposure to cyber-threats. Successful attacks on connected OT networks can have catastrophic results, up to and including threats to public health and safety.

IT/OT convergence offers many advantages to operator teams while at the same time creating new risks of attacks from external threats. Attacks originating from higher-risk external networks threaten the loss of control of connected devices that regulate critical processes. Successful attacks may also result in system breakdown, damage to equipment and revenue loss in addition to public health risks.

Safe and secure two-way communications with connected OT assets are essential. Important analysis related applications on the corporate network must get real-time updates from the operational network and operators need to perform real-time equipment monitoring.

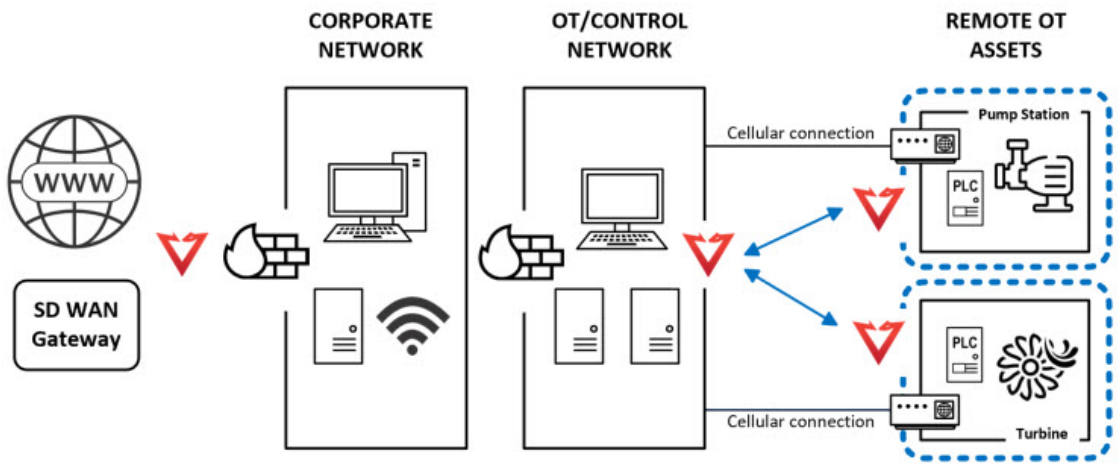
PacketViper'sOT360 Active Protection Across Distributed OT Endpoints

PacketViper's OT360 provides the ability to obfuscate critical, remote OT network assets that require connectivity to operate effectively. This can include, but are not limited to, pumps, wellheads, turbines, motors and more. The solution prevents external threats from identifying connected assets during reconnaissance and from using them to get on the network. It also contains and stops internal threats on the network from proliferating, spreading or establishing external communications.

Operators appreciate active cyber defense for connected and remote OT assets with agentless threat detection, prevention and response. Active 2-way boundary defense can replace firewalls, unidirectional gateways and data diodes in certain industrial network environments.

Real-Time Cybersecurity. No Unplanned Downtime.

When deployed across network boundaries and within network segments and remote locations (image below), the solution secures IT/OT integration and protects operations. Operators also have 2-way communication capabilities and real-time access to data.



- Protected 2-way data flow
- Automated attack prevention
- Threat containment
- Equipment obfuscation
- Centralized management

Cost-Effective Next Gen OT/IT Cybersecurity

The static nature, limitations and maintenance requirements of traditional solutions such as boundary firewalls, data diodes and unidirectional gateways are not enough to withstand the dynamic nature of today's cyber threats. For a very affordable price per asset, OT360 makes critical assets almost impossible to discern during reconnaissance. And in the event threat get onto the network, OT360 can detect them earlier, reducing dwell time while actively preventing command and control communications from being established and stopping exfiltration.

Properly functioning OT networks frequently push the limits of legacy devices as manufacturers announce impending end of support timelines, and as technologies approach their end of useful life. PacketViper OT360 allows operators and security teams to secure aging assets and protect operations without a costly 'rip and replace'.

Meaningful Cybersecurity Outcomes and Benefits

OT360 enables important two-way communications with connected assets while delivering meaningful security, visibility and compliance benefits.

- Ensure protection of public health and safety
- Prevent attack-related power outages and damages
- Prevent external threats from taking control of OT assets
- Prevent loss of revenues from unplanned downtime
- Detect and reduce dwell-time of internal threats
- Prevent internal threats from outbound connections
- Enhanced cybersecurity without unplanned downtime
- Real-time protection against active threats
- 2-way communication supports active monitoring
- Support compliance with multiple standards
- Compensating control for vanishing air gaps
- Active vendor monitoring and risk management
- Threat detection and response without complex and costly orchestrations

Purpose Built Hardware

All OT360 appliances feature a fanless, metal case designed for harsh, space constrained, critical infrastructure applications. These models all provide the highest levels of threat detection, prevention and response to protect industrial control systems and critical infrastructure facilities from remote online attacks.

High availability (HA) configurations are available, as well as a variety of other deployment options.

Critical Infrastructure Sectors Supported

Water & Wastewater | **Energy & Utilities** | **Manufacturing** | **Government & Defense** | **Telecommunications** | **Pharmaceuticals** | **Transportation & Logistics**

About PacketViper

PacketViper provides transformative and trusted cybersecurity solutions for organizations seeking to modernize the cybersecurity of converging OT and IT networks and defend distributed OT endpoints. PacketViper's OT360 is an agentless detection, prevention, and response technology that automates attack prevention from both external and internal threats. PacketViper customers cover multiple public and private sector industries.

For more visit packetviper.com