PACKETVIPER™

Product Brief

Operational Technology Remote (OTR) Solution

Easily Secure Remote OT/ICS and SCADA Environments

Effective and Easy-to-use Remote OT/ICS Security

Securing remote Operational Technology (OT) and Industrial Control System (ICS) assets requires more than visibility of unpatched devices or mere detection of anomalies. Effective cybersecurity depends on providing front line operators the required information to act quickly when potential threats are in motion. PacketViper OTR removes the complexity from securing critical operations and provides operators with an easy-to-use, industrial-grade defense and protection tool. Our unique approach ensures that sensitive and complex devices are not disrupted.

Rapidly Monitor, Detect, and Prevent Threats in Critical Operational Networks

Operational technology (OT) and Information Technology (IT) systems have converged to optimize production, drive innovation, and increase efficiency. However, that convergence increases the attack surface by connecting network segments that had previously been air-gapped and exposing them to broader networks and the Internet. Detecting complex and evolving cyber threats requires advanced tools, knowledge, and training. The PacketViper OTR Solution utilizes easy to understand interactive dashboards that allow operators to monitor status in real time, without the need for advanced cyber security knowledge or experience.

Enterprise-wide Visibility, Management, and Control

Whether your organization is a small two-site location or large, multi-node distributed environment, detecting and then stopping an attack is difficult without the correct tools. PacketViper OTR provides control system visibility, security device management, threat mitigation and containment in a single solution. The OTR solution eliminates blind spots and network risk in either flat or segmented environments. Dashboards provide granular and easy to understand, real-time views of devices. Operators can rapidly identify threats, weakness, and risks from potentially vulnerable devices within critical networks.

Next-gen OT/ICS and SCADA Security

We understand security, and the many differences between IT and OT/ICS/SCADA networks. We also know that effective cybersecurity requires a layered approach in any environment. Our mission is to provide effective, easy-to-deploy, and affordable solutions that defend and maintain the availability of ICS and OT networks, including how they interface and connect with IT infrastructure. Finally, you have a security solution for your critical infrastructure that protects your OT Network and its many components, including HMIs, PLCs, RTUs, SCADA assets, Historians, and more.

PacketViper OTR Solution

PacketViper OTR is a system of security software and hardware components that enables critical infrastructure and industrial organizations to secure and protect OT/ICS and SCADA assets, networks, and environments at local and remote locations.

- Provides granular real-time visibility, monitoring and management of network communications between local and remote locations.
- Utilizes interactive security components including contextual filters, decoys, sensors, and sirens that detect unauthorized devices or network communication.
- Employs easy to understand interactive dashboards that display network traffic context to quickly identify threats and anomalies without the need for extensive security expertise.
- Includes a Centralized Management system to configure and manage remote locations, monitor network communication, and identify anomalies.
- Contains an Enterprise Management interface to configure, manage and protect remote locations
- Equips supervisors and operators with real-time alerting and reporting, with the option to enable automated defense of the network.

PacketViper OTR enables organizations to protect OT/ICS and SCADA networks from threats originating from external sources or from within the network. OTR provides better security, visibility, and network control without the risk of interfering with normal industrial control communications or processes. OTR gives operators a simple method of identifying anomalies without any prior network or security knowledge.

Purpose Built Hardware

PacketViper OTR remote location appliances consists of a family of fanless metal case devices designed for critical infrastructure applications in harsh and space constrained environments. These models all provide the highest levels of threat detection, prevention, and response to protect industrial control systems and critical infrastructure facilities from remote on-site online attacks. High availability (HA) and Bypass-enabled configurations are available, as well as a variety of other deployment options including custom NEMA-Rated outdoor enclosures.

PacketViper OTR Solution Architecture

The PacketViper OTR solution architecture includes a Boundary Security Unit (BSU), Control and Management unit (CMU), and Remote Security Unit(s) (RSU) for remote locations. These units are connected using network cables to the existing network infrastructure.

The Boundary Security Device (BSU) is the device that protects the outer network boundary of the OT/ICS environment from external threats. The BSU is typically a single device placed on the exterior boundary between the ICS environment and the IT environment or Internet. The OTR BSU deploys an array of tools that proactively detect and prevent threats North to South, and South to North.

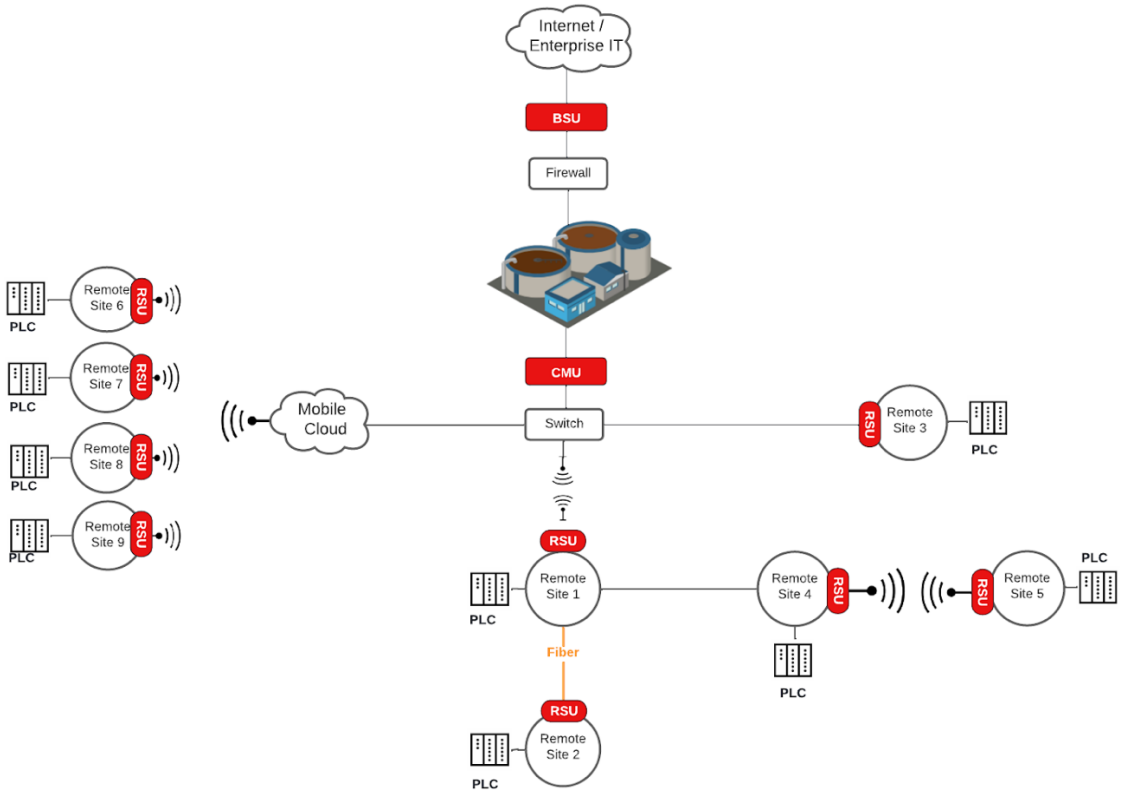
The Control and Management Unit (CMU) is typically a single device installed at the primary facility of the control environment, normally near network equipment and other control system servers. In large, complex, or regionalized environments, multiple CMU units may be required. This device monitors internal east, west, north, south network communications, propagates policies and manages connected RSUs.

The Remote Security Unit (RSU) is typically one from a family of small ruggedized industrial devices which can be DIN rail mounted or enclosed in a custom NEMA container. The RSUs primary purpose is to identify anomalies within the remote site, and if configured to, contain unauthorized connections or devices, notify incident response teams, and the CMU. The RSU provides visibility and control of network connections and devices within remote locations.

The BSU, CMU, and RSU can be configured as a bridged connection which transparently monitors network communications, or as a mirror which receives a copy of the network communications from a smart switch.

Once implemented, the OTR solution monitors the network communications from the BSU, CMU, and RSU(s) devices, and aligns them to the customers established security policies. These policies can be configured with an array of cybersecurity actions, including logging, filtering, alerting, messaging, throttling, and blocking.

At the client's option, RSU(s) can be configured to contain threats and anomalies within a remote location when they are discovered. This is achieved when the RSU detects a threat, then automatically creates a rule to prevent the unauthorized device or communication, while simultaneously sending an alert, and notifying the CMU. The CMU then notifies the remaining RSU(s) and propagates the filter rule, protecting the remaining locations on the network by containing the threat at the impacted remote site.



Meaningful Cybersecurity Outcomes and Benefits

PacketViper OTR enables essential two-way communications with connected remote assets while delivering critical security, visibility, and compliance benefits.

- Prevents external threats from taking control of remote OT assets
- Limits loss of revenues from unplanned downtime
- Detects and reduces dwell-time of internal threats
- Stops internal threats from establishing outbound connections
- Confines local threats to the impacted location
- Enhances cybersecurity without unplanned downtime
- Provides Real-time protection against active threats
- Enables 2-way communication supports active monitoring
- Supports compliance with multiple standards
- Establishes a compensating control for vanishing air gaps
- Facilitates active vendor monitoring and risk management
- Delivers threat detection and response without complex and costly orchestrations
- Ensures protection of public health and safety
- Mitigates attack-related outages and damages

Critical Infrastructure Sectors Supported

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, OTR and Deception360 product families deliver 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.