ProtocolPatroller

ICS cybersecurity monitoring and anomaly detection solution

As increasingly sophisticated cyberattacks on Industrial Control Systems (ICS) in general, and supervisory control and data acquisition (SCADA) systems in particular, are becoming an industry norm, North American utilities are experiencing thousands of attacks each month.

Perspecta Labs' ProtocolPatroller part of its Secure**Smart**™ critical infrastructure solution line, is providing utilities continuous cyber monitoring and anomaly detection and protection. The award winning Secure**Smart** ProtocolPatroller delivers extensive protocol-specific security capabilities for smart grid and other ICS and SCADA applications.

Detect and stop cyberattacks in real time

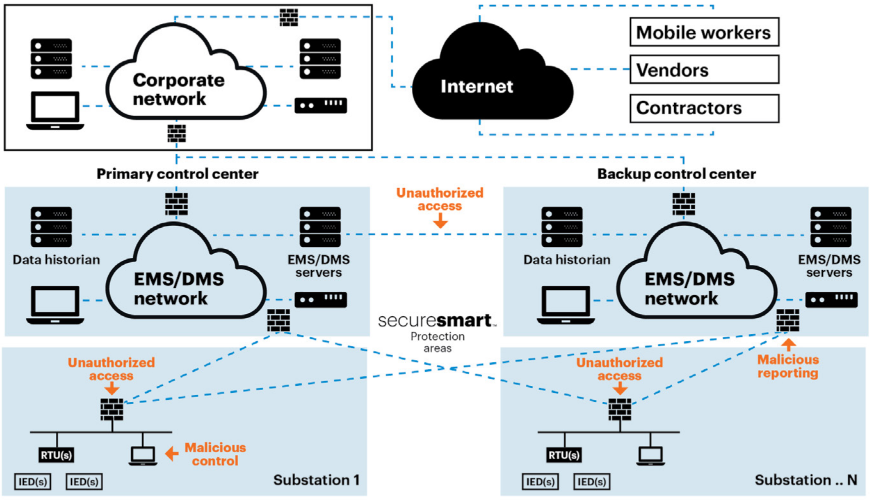
ProtocolPatroller provides cybersecurity protection across a wide range of threats and SCADA protocols, including:

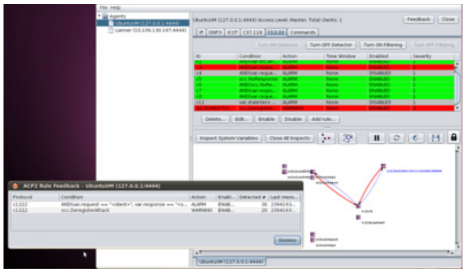
- SCADA Distributed Network Protocol (DNP3)
- Substation Automation 61850-Generic Object Oriented Substation Events (GOOSE)
- Schweitzer Engineering Laboratories (SEL) Fast Message protocol at the SCADA application layer
- Inter-Control Center Communications Protocol (ICCP)
- Landis + Gyr 8065
- Synchrophasor Protocol C37.118
- Advanced Metering Infrastructure (AMI) Data Transport Protocol C12.22
- Telnet at the IP layer, Hypertext Transfer Protocol (HTTP), Address Resolution Protocol (ARP)

More broadly, ProtocolPatroller employs a modular architecture that can be readily extended to support additional ICS protocols. For each such protocol, ProtocolPatroller employs a collection of protocol-specific stateful model checkers that have been verified with formal methods to detect communication anomalies. Using these robust checkers, ProtocolPatroller detects ongoing attacks, including zero-day attacks, and alerts operators through a user-friendly dashboard. When used in the in-line protection mode, ProtocolPatroller can perform predetermined actions to help stop the ongoing attacks.

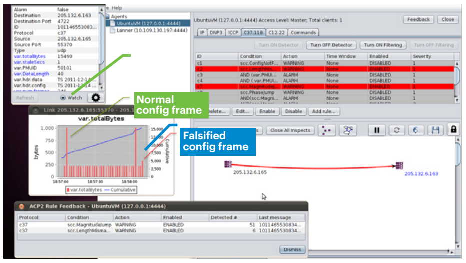
ProtocolPatroller software can be co-hosted as well as reside in a customer's existing IT hardware or software platforms. Co-hosting can occur at gateways (e.g., in data centers or control centers), customers and servers (e.g., ICCP nodes, smart meter data collection engines), Intelligent Electronic Devices (IED), or even in a service cloud. Hosting is available as a dedicated platform.

SecureSmart protection against vulnerabilities

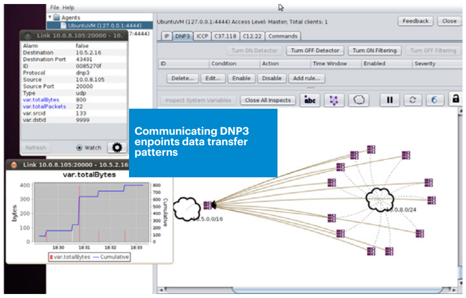




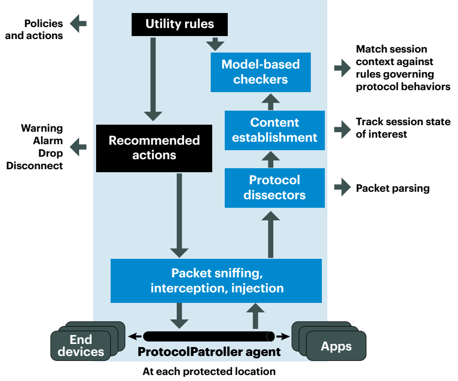
AMI traffic anomaly alerts



False configuration frame alerts



Visibility intro DPN3 endpoints data transfer patterns



ProtocolPatroller software agent

Two modes of deployment

ProtocolPatroller deployment is available in two modes:

- Monitor mode: passively analyzes, detects, and alerts on behavior anomalies using a predefined set of protocol-specific rules and environment parameters
- In-line protection mode: actively intervene according to prescribed actions to mitigate malicious behavior and terminate sessions

How ProtocolPatroller does it

To detect misbehavior and map communication flows, ProtocolPatroller real-time protocol and communication session analyzer performs deep packet inspection and identifies anomalies based on tracking communication sessions between each endpoint pair using state models and predefined rules. ProtocolPatroller graphically maps communication flows between each endpoint pair not only at the network (IP) layer, but at application protocol layers to discern different communication flows between devices. For instance, ProtocolPatroller flow mapping enables comparison of IP connectivity maps against DNP3 master-outstation flows based on DNP3 IDs. Drilldown capabilities provide detailed information for each session.

Flow maps graphically highlight session links with anomalies and unrecognized devices detected in the environment. The monitoring and filtering of potential vulnerabilities are available through the built-in and user-defined rules in ProtocolPatroller offerings. Moreover, the dashboard provides operators with great flexibility in terms of choosing which protocol they would like to monitor and protect, which set of communication sessions and endpoints they would like to pay attention to and which rules they would like to apply. ProtocolPatroller provides the ability to display only sub-nets for large networks.

Comparing ProtocolPatroller to other tools

Almost all cybersecurity tools employed in ICS and power system applications take the form of a gateway, with traditional capabilities including firewall, VPN, port scanning features or custom IDS for enterprise applications. ProtocolPatroller goes beyond these traditional IDS and perimeter protection approaches to protect when intrusions have infiltrated into your networks. ProtocolPatroller is an industry leading protocol-specific capability based on stateful model-checkers to patrol SCADA protocol communication contexts and behaviors, while applying deep-packet inspection to track event sequences and perform cross session comparisons. ProtocolPatroller has been installed and is currently operating in selected utility operating centers for monitoring ICCP, C12.22 and DNP3 traffic.

Operational benefits

- Validate EMS/RTU polling flows
- Visualize polling hierarchy and master-outstation relationships
- Find polling errors
- Identify intermittent or unresponsive ICS devices
- Identify unexpected devices on the network, validate device lists and network subnets
- Examine connectivity at different layers of the stack (i.e. Layer 2, IP/TCP, DNP3 connectivity)
- Supports serial over IP protocols
- Tracks both SCADA and engineering/management and flows

ProtocolPatroller rules and behavior analytics

- Detection of devices outside of authorized subnets
- Device white listing
- Request/response matching
- Detection of abnormal or illegal protocol traffic
- Detection of back-end scanning
- Validation of end-point configuration
- Energy protocol specific rules can be dynamically added to address additional utility security concerns

Protection against known vulnerabilities

- Rogue nodes
- Unauthorized use of address space
- Injection of forged or injected packets
- Compromised field nodes
- Field-based back-end network attacks
- Misconfigured/altered devices (Datalink ID, data object mapping)