Reservoir Labs

R-Scope®

Advanced Threat Detection

Do you know what is on your network?

R-Scope® puts your network under a microscope to empower security analysts with the tools needed to proactively detect and prioritize remediation efforts specific to advanced threats.

R-Scope is a network security appliance that provides real-time contextual visibility to shine a light into the dark spaces of your network infrastructure that traditional security solutions cannot illuminate. Our turnkey, enterprise-ready appliance seamlessly integrates into security operations, equipping teams of all sizes with a flexible tool to create new, or enhance existing workflows.

More specifically, R-Scope provides contextual network and security metadata, a powerful and flexible analytical engine, and real-time security event detection by dynamically analyzing network traffic in real time.

R-Scope does this by layering enterprise grade performance, security, and stability on top of the most advanced and open threat detection engine available — Zeek.

This approach empowers R-Scope users to identify vulnerable assets and automate simple rule-based alerts that provide critical insights on or before day zero.

R-Scope Features

R-Scope adds value above and below the Zeek engine. Our R-Scope Acceleration Layer includes patent pending technology to accelerate packet ingest into Zeek, while the R-Scope Manageability Layer wraps the whole system in a seamless command-line environment to streamline systems management and Zeek script development. All system management and Zeek Script development is accomplished through the command-line interface, enabling configuration and management by personnel at all skill levels.

R-Scope Core Features

- ✓ Comprehensive Customer Support
- ✓ Hardened Application & OS
- ✓ Disk Encryption Keyed to Device
- ✓ High Performance
- ✓ Intelligent Traffic Queuing
- ✓ System Diagnostics
- ✓ Secure Updates

Enterprise Integration

- ✓ Multi-User, Multi-Role User Management
- ✓ RADIUS Authentication
- ✓ SNMP Health Monitoring
- ✓ Out-of-Band Management
- ✓ Ansible Orchestration
- ✓ Fully scriptable

Network & File Extraction

- ✓ Selective Packet Capture (pcap)
- ✓ File Extraction

Threat Intelligence

- ✓ Direct Partner Integration
- ✓ Easy Custom Intel Integration

Data Export Mechanisms

- ✓ Export Logs, Files, and pcap
- ✓ Syslog, Kafka, SCP Transport
- ✓ Integrated Splunk Forwarder

Reservoir Professional Services

- ✓ Custom Analytics
- ✓ Custom Protocol Analyzers

Zeek Support

- ✓ All Stock and Custom Zeek Script Fully Supported
- ✓ Development Sandbox
- ✓ Zeek Script Development Workflow Support
- ✓ PCAP Replay
- ✓ Zeek Script Versioning
- ✓ Internal/External Git Repo Sync
- ✓ Log Management
- ✓ Release into Production

Log Integrations

splunk> APACHE METRON elastic

File and Capture Workflows

FireEye THREATQUOTIENT malwr ThreatTrack iSIGHTPARTNERS EnCase® Forensic

R-Scope Appliance Specifications

Model	R-Scope PACE
Operational Mode	Network Sensor
Throughput	10 Gbps
Traffic Interfaces	4 x 10 Gbps SFP+
Dimensions (H x W x D)	1U rack-mount (1.7" x 17.1" x 27.5")
Weight	39 lbs.
Power	120V/240 VAC, 50/60 Hz, 750 W Redundant PSUs
Support	On-site, email, and phone