R-Scope®

Reservoir Labs

| Solution Brief

Advanced Threat Detection

R-Scope® is a powerful network security sensor for threat hunting and threat detection. R-Scope gives SOC analysts the right analytics and context to assess the network threat landscape and identify the most critical threats, faster. Incident Responders benefit from R-Scope's rich historical metadata, file object extraction, and selective packet capture, ensuring rapid and thorough remediation.

Machine Learning and Artificial Intelligence solutions provide the horsepower to produce invaluable insights into your firm's vulnerabilities and exposure to sophisticated threats. R-Scope enables you to take full advantage by providing comprehensive multi-domain security data for analysis. R-Scope metadata adds quality context and deep visibility, with over 60 log types and hundreds of unique data points.

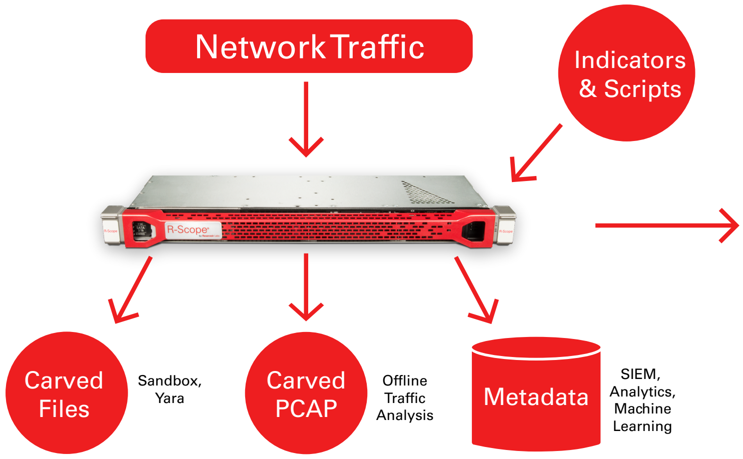
R-Scope is built on open-source Zeek software (formerly Bro), a powerful network analysis framework. Over 20 years in the market, Zeek supports a vibrant open-source community. R-Scope maintains the power of Zeek while enhancing its scalability and stability with patented technology for rapid Enterprise deployment.

At its core, Reservoir Labs is a research and development firm offering professional services in cybersecurity, high performance computing, algorithms, and analytics. While Reservoir's novel research informs the development of R-Scope, Reservoir's engineers are available to develop a range of custom solutions for your unique organization as specific as custom protocol analyzers and as broad as bespoke packet path engineering.

Features

- Comprehensive Network Visibility
- Selective Packet Capture
- On-System Analytics
- File Carving
- Robust Scripting Language
- Native Development Environment
- Multiple Deployment Options
- Professional Services & Support

R-Scope® in Action



Custom Dashboards

Incident Response & Hunting

Full network visibility, all the time. R-Scope is used by some of the most respected hunt teams because it provides the effective metadata that Incident Response teams need for threat hunting. Optional selective packet capture enables responders to go deep when needed without the cost and complexity of full packet capture.

Lateral Movement Visibility

R-Scope enables users to easily monitor lateral traffic across the entire enterprise, stopping bad actors before they can infiltrate hosts inside your network.

Fuel Analytic Pipeline

Get meaningful results. Security analytics are only as good as the data they consume. R-Scope hits the sweet spot with comprehensive metadata and contextual analytics that Machine Learning and Artificial Intelligence solutions require.

Operationalize Threat Intelligence

Reduce response time with customizable, on-box analytics. Automate alerts based on your environment and needs, and deploy any threat detection analytics shared within the broader Zeek community.

Real-Time Behavioral Analytics

Identify the threat before a compromise. Get the most out of your Indicators Of Compromise (IOC) by seamlessly matching known bad IPs, domains, file hashes, and other indicators, with current network activity.

File Carving

Integrate R-Scope's fully customizable, real-time file carving functionality with any third party malware analytics solution. You define which files, and under what conditions those files are extracted from your network. Leverage built-in automation to enable fire and forget file analysis.

Reservoir Labs

(212) 780-0527
info@reservoir.com

632 Broadway, Suite 803
New York, New York 10012

www.reservoir.com/r-scope