



Remedio Network Device Sensor

Closing the Network Layer Gap in Security & Compliance



The Problem

Network infrastructure is a persistent blind spot in security programs — often misconfigured yet critical to both risk & compliance.

Zero Trust demands every device and connection be continuously verified & secured, leaving no room for hidden weaknesses.



The Solution

Remedio's Network Device sensor brings the network layer into full view, offering automated detection of **misconfigurations** and **policy violations** across Cisco routers and switches (IOS, IOS-XE), aligned with security standards such as CIS, NIST, MITRE etc.

The sensor surfaces high-impact security and compliance issues that may otherwise go undetected, spanning SSH, SNMP, HTTPS, telnet, logging and authentication.



Key Metrics Monitored

- Missing ACLs on VTY-lines & SNMP interfaces
- Outdated web interfaces
- Insecure SSH, SNMP versions
- Overly permissive ACLs
- Default or weak passwords for device management
- Telnet usage



Built for Action

Findings are actionable, pre-prioritized, and fully integrated into the Remedio platform — with results visible in the UI and available for export to existing SIEM & reporting pipelines (via API or forwarding).



....

This unified management framework gives security leaders a complete picture of misconfiguration risk across infrastructure, endpoints, and applications — all in one place.



Always-On Enablement

Remedio's network device coverage, allows operators to:

- Ensure consistent, **secure configuration** across all network devices
- Continuously **assure compliance** according to defined standards
- **Streamline remediation** through SIEM, SOAR, and partner systems
- Improve **audit readiness** with detailed tracking and reporting
- Support **Zero Trust**, preventing unauthorized access and lateral movement



Safe, Straightforward Deployment

+++

The sensor is agentless, efficient, and easy-to-operate. It uses non-intrusive, read-only SSH access, and requires no system changes to the inspected devices. The sensor scans all devices in the network environment on a continuous 24/7 cycle, using minimal resources.



An Expanding Purview

This entry into the network device space represents a fundamental expansion of the Remedio product.

In addition to Cisco routers and switches, we will

- Extend support SDNs, cloud network infrastructure, and firewalls
- Expand in-system click-to-remediate capabilities
- Cover additional device types and vendors
- Analyze an ever-expanding number of metrics.

In this way we will continue to evolve in tandem with your business needs — ensuring your infrastructure remains both **secure and compliant**.

To learn more, please visit www.remedio.io or contact your Remedio representative.