Solution Brief

Closing the Infrastructure Device Blind Spot with Clear NDR®

Your network infrastructure devices – switches, routers, firewalls, and operational equipment – represent a critical blind spot in your security posture. These devices cannot run endpoint agents, leaving them invisible to traditional security platforms.

Meanwhile, sophisticated threat actors are actively exploiting this gap, compromising thousands of infrastructure devices using known vulnerabilities. Clear NDR® from Stamus Networks provides comprehensive visibility into infrastructure device behavior, detecting compromise attempts and malicious activity that endpoint security cannot see.

The Challenge: Infrastructure Cannot Run Agents

Modern security architectures rely heavily on endpoint agents to provide visibility into host behavior, detect threats, and respond to incidents. However, this approach creates a fundamental blind spot:

- **Network infrastructure devices** (switches, routers, firewalls) cannot run endpoint agents due to proprietary operating systems and vendor restrictions
- **Operational technology and IoT devices** lack the resources or compatibility to support agent software
- **Security appliances** themselves become vulnerable targets that your security platform cannot monitor
- **Legacy systems and specialized equipment** often predate modern security agent architectures

When these devices are compromised, your endpoint security platform has no visibility whatsoever. So, the attack is completely invisible to your existing defenses.

The Risk: Active Exploitation of Infrastructure

This blind spot is not theoretical. It is being actively exploited. CISA's Known Exploited Vulnerabilities catalog documents hundreds of critical flaws in network infrastructure from leading vendors:

Vendor / Platform	Recent Critical Vulnerabilities
Cisco ASA	CVE-2025-20333: Remote code execution affecting thousands of firewalls
Palo Alto PAN-OS	CVE-2024-3393: Command injection allowing complete device takeover
Ivanti	CVE-2025-22457: Actively exploited in the wild by suspected China-nexus actor UNC5221 starting in mid-March 2025
DrayTek Vigor	CVE-2024-12987: Mass exploitation of routers for botnet operations
Fortinet	Multiple CVEs: FortiGate and FortiOS vulnerabilities under active attack

In recent months alone, sophisticated threat actors have compromised thousands of routers and firewalls using these vulnerabilities. Once compromised, these devices provide attackers with persistent access, traffic manipulation capabilities, and a platform for lateral movement – all while remaining completely invisible to endpoint-based security solutions.

The Solution: Clear NDR for Network Visibility

Clear NDR solves the infrastructure blind spot by analyzing network traffic to provide comprehensive visibility into device behavior, regardless of whether agents can be installed:

Agentless Infrastructure Monitoring

Clear NDR passively monitors network communications to detect anomalous behavior from infrastructure devices. By analyzing traffic patterns, protocol usage, and communication relationships, Clear NDR identifies compromise indicators without requiring any software installation on the devices themselves.

Behavioral Analytics for Infrastructure

Clear NDR establishes behavioral baselines for your infrastructure devices and alerts on deviations that indicate compromise:

- Unusual administrative access patterns suggesting credential abuse or unauthorized access
- Unexpected outbound connections indicating command and control communication
- Protocol anomalies that suggest exploitation attempts or post-compromise activity
- Traffic redirection or manipulation characteristic of man-in-the-middle attacks
- Data exfiltration patterns through compromised infrastructure

Exploitation Detection

Clear NDR's threat intelligence identifies active exploitation attempts targeting infrastructure vulnerabilities, including the specific CVEs affecting Cisco, Palo Alto, Ivanti, Fortinet, and other vendors. This enables rapid detection and response before attackers establish persistent access.

Key Benefits

- Complete visibility across all network infrastructure, regardless of agent support
- Early detection of infrastructure compromise before attackers achieve their objectives
- Reduced risk from known vulnerabilities in network devices and security appliances
- Comprehensive threat context combining infrastructure and endpoint telemetry
- Simplified deployment without the complexity of agent management on infrastructure devices

Closing the Gap

The infrastructure blind spot represents one of the most significant gaps in modern security architectures. As threat actors increasingly target network devices that cannot be protected by endpoint agents, organizations need visibility that extends beyond traditional agent-based approaches.

Clear NDR provides that visibility, enabling security teams to detect and respond to infrastructure compromise with the same confidence they have in endpoint security—closing the blind spot that attackers are actively exploiting today.

Take the Next Step

The infrastructure blind spot is no longer a theoretical risk - it is a live threat that sophisticated attackers are actively exploiting. Your network devices are critical assets, but they cannot be secured with endpoint agents.

It’s time to **close the gap**.

See how **Clear NDR** delivers agentless, comprehensive visibility into infrastructure device behavior, providing the early detection and threat context you need.

Request a **personalized demonstration today** to gain confidence that your entire network, from the endpoint to the core infrastructure, is protected against today's most evasive threats. Or dive in immediately with a **30-day no-obligation evaluation** to experience the clarity your security team has been missing.

Contact Stamus Networks for a consultation and live demonstration to determine if Clear NDR is a good fit for your organization: contact@stamus-networks.com

ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That’s why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world’s most targeted organizations, our flagship offering – Clear NDR® – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

STAMVS® NETWORKS

229 rue Saint-Honoré
75001 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

✉ contact@stamus-networks.com
www.stamus-networks.com