Intrusion

PREVENTION-FIRST SECURITY FOR HEALTHCARE

Protect Patient Care. Skip the Noise.

An overview of how INTRUSION's Shield platform delivers prevention-first defense and high-fidelity network visibility for hospitals, health systems, clinics, and payers.

THE OPERATIONAL CHALLENGE

Healthcare networks carry life-critical traffic across electronic health records, connected medical devices, and clinical systems, and a single intrusion can disrupt patient care, not just data. Many of these devices cannot run a security agent, and detect-and-respond tooling is left to sort real threats from noise after traffic is already inside. The root cause is structural: malicious traffic is permitted onto the network and evaluated after the fact. Prevention removes the question before it is ever asked.

46%

of security operations center alerts prove to be false positives, generating no security value.

73%

of security teams name false positives their top detection challenge, per the 2025 SANS survey.

3 in 4

U.S. healthcare organizations report patient care disruption from cyberattacks, per Proofpoint and Ponemon Institute, 2025.

THE INTRUSION SHIELD PLATFORM

Enforcement: threats stopped, not queued

Shield Stratus and Shield OnPremise block known-bad and unauthorized traffic bi-directionally and autonomously, before it reaches the network. Powered by the Global Threat Engine and its 8.5 billion IP and DNS combinations, a blocked threat never becomes an alert to triage.

Visibility: observe-only network insight

Shield Sentinel monitors enterprise traffic at up to 100 Gbps in observe-only mode, giving security operations teams clear visibility into traffic patterns across the environment without adding enforcement to a monitored segment.

VALUE TO HEALTHCARE ORGANIZATIONS

Care continuity protected

Malicious traffic stopped before it can disrupt clinical systems or patient care.

Coverage for unagentable devices

Network-level enforcement protects connected medical devices that cannot run an agent.

Analyst capacity reclaimed

Blocked threats never become alerts, so lean teams spend hours on genuine investigation.

Visibility across the network

Sentinel surfaces traffic patterns other tooling is not watching.

WHERE A CONVERSATION COULD START

The next step is a short discovery session to explore how Shield applies to your environment and what a scoped, baseline-validated evaluation might look like. To arrange one, contact Andrew Wildrix, VP of Business Development, at Andrew.Wildrix@intrusion.com.