WANAWARE SECURITY

Your customers can't secure what they can't see — and accurate inventory is the foundation everything else depends on.

Security conversations with technology advisors often stall at the product level: firewalls, EDR, SIEM. What most customers are missing is the layer underneath — a complete, continuously updated picture of every asset in their environment, and the context to understand what a vulnerability actually means for their business. WanAware Security starts with that complete asset inventory and evaluates every finding against the live Relationship Graph — so customers know the actual blast radius of a risk, not just its severity score. For advisors in regulated verticals, the automated compliance evidence across 20+ frameworks is frequently the capability that closes the deal.

Bring this up when your customer...

- Has a compliance audit coming up or recently failed one
- Can't confidently answer 'what devices are on our network right now?'
- Has unmanaged devices, shadow IT, or IoT/OT equipment with no security coverage
- Gets a lot of vulnerability alerts but has no way to prioritize which ones actually matter
- Is in a regulated vertical (healthcare, finance, energy) with specific framework requirements

10B+
IP addresses assesseddaily — IPv4 & IPv6

1,000+
Ports assessed per asset vs. ~80 for most tools

20+
Compliance frameworks automated

Context
Every CVE evaluated against actual blast radius

What You Can Show the Customer

WanAware Security builds on the AIM asset inventory — so every security assessment starts with a complete, current picture of the estate. This includes unmanaged devices, shadow IT, cloud resources spun up without IT involvement, and legacy OT equipment that will never host an agent. When a vulnerability is found, WanAware evaluates it against the live Relationship Graph to calculate blast radius and prioritize by actual business

How the Conversation Goes

The situation:

- Customer failed a compliance audit. Auditor found devices on the network that IT couldn't account for.
- Critical CVE published. Customer's security team can't determine which systems are affected without days of manual cross-referencing.
- Customer has a clinical environment with dozens of connected medical devices that have never been formally inventoried.

The Five-Step Security Workflow

Identify	Assess	Contextualize	Prioritize	Respond
Every asset found, classified, and added to live inventory automatically	Continuous vulnerability assessment across all ports, IPv4 and IPv6 daily	Findings evaluated against compensating controls and the Relationship Graph	Risk ranked by actual blast radius — not just CVSS score	Isolation workflows triggered automatically; compliance evidence assembled

Behavioral Shift Detection

WanAware's KDE continuously detects anomalies in network traffic that signal potential compromise before signature-based tools fire. AI evaluates context to suppress false positives and surface what actually warrants investigation.

Compliance Automation

WanAware automates evidence collection across 20+ frameworks including HIPAA, PCI-DSS, SOC 2, NERC CIP, and SOX. Compliance posture is tracked continuously — not assembled in a sprint before an audit. For customers facing regulatory pressure, this capability alone is often the deciding factor.