THE AIR GAP IS A MYTH. HERE'S WHAT'S REALLY PROTECTING YOUR OT NETWORK.

Somewhere on a factory floor right now, a "decommissioned" controller is still running. It has been online for 847 days. It has never been scanned, never had an agent installed, and appears nowhere in any asset inventory. Last Tuesday, it made its first outbound connection—to an IP address associated with a known APT group.

No alert fired. No one noticed. Your firewall never saw it.

This is not a hypothetical. This is the Dark Segment—and it exists in every industrial network we've ever assessed, without exception.

THE PROBLEM: Why Your Security Stack Is Forbidden on the Factory Floor

OT security has an uncomfortable paradox at its core: the tools that provide the deepest visibility in IT environments are the ones most likely to cause a production shutdown in OT. Active scanners have crashed legacy PLCs. EDR agents have introduced latency into millisecond-sensitive control loops. The result is an unspoken rule across most industrial facilities—the security team doesn't touch the OT network.

And so the factory floor becomes a black box. Attackers have known this for years. The average dwell time in OT environments before detection isn't days. It isn't weeks. Industry data consistently puts it at 200+ days—enough time to map every process, every failsafe, every safety interlock.

The Air Gap Myth: Most organizations believe physical separation between their IT corporate network and OT production zone provides a security barrier. VStrike consistently finds this assumption is wrong. Dual-homed engineering laptops, rogue wireless access points, and misconfigured VLANs routinely bridge the gap—invisibly, silently, and with enormous blast radius.

THE SOLUTION: Passive Fabric Observability — Watch the Wire, Not the Device

VStrike solves this by changing the fundamental question. Instead of asking "What will a device tell us about itself?"—which requires agents, scans, and cooperation from the device—VStrike asks: "What does the wire prove this device is actually doing?"

Network traffic cannot be faked. A PLC communicating via Modbus to an HMI is generating packets that traverse your switch fabric regardless of whether any security tool is installed on it. VStrike ingests those packets passively—via NetFlow, IPFIX, SPAN ports, and sFlow—and builds a complete, real-time graph of every device and every relationship on your OT network.

→ Zero operational risk: No agents, no scans, zero chance of crashing a controller or introducing process latency.

→ Native OT protocol support: VStrike understands Modbus, EtherNet/IP, mapping the relationships between HMIs, Engineering Workstations, and PLCs as they actually exist, not as they appear in a stale CMDB.

→ Air gap validation: VStrike identifies every hidden bridge between IT and OT—dual-homed laptops, rogue access points, misconfigured VLANs—and calculates the blast radius of each one.

→ Complete dark segment illumination: If a device emits a single packet, VStrike sees it and places it on the map. No prior knowledge required.

THE INTELLIGENCE LAYER: DeepTempo — Behavioral Baselines Built for Industrial Logic

VStrike maps the Where. DeepTempo provides the How.

OT environments have a property that makes behavioral detection uniquely powerful: stability. **Unlike threshold-based anomaly tools that evaluate individual events in isolation, DeepTempo's foundation model embeds observed behavioral sequences in high-dimensional space — enabling compound detections that catch the slow, multi-step lateral movement patterns that define sophisticated OT attacks and that single-event rules will never see.**

A well-running process controller does the same thing, on the same schedule, to the same endpoints, for years. This predictability isn't a limitation—it's a weapon. Any deviation from that baseline isn't just suspicious. In OT, it's almost certainly significant.

DeepTempo's foundation model baselines every device on your OT network and maintains that baseline continuously. When deviation occurs—a dormant safety controller suddenly initiating

an outbound connection, a PLC receiving commands from an IP it has never seen, an Engineering Workstation querying assets outside its normal operational zone—DeepTempo flags it as a high-fidelity anomaly with minimal false positives. **In production OT deployments, DeepTempo has been shown to operate at well below 1% false positive rates — compared to 15% or higher from traditional anomaly and rules-based detections — because the model was built for industrial behavioral patterns, not adapted from IT environments where user behavior is inherently noisier.**

Why this matters in OT specifically: In IT environments, behavioral baselines are valuable but noisy—users change behavior constantly. In OT, a controller that has communicated the same way for 10 years deviating from that pattern is not noise. It is either an attack or a fault. Either way, you need to know immediately.

LIVE SCENARIO: The Abandoned Controller

Day 0: Production line decommissioned. Equipment physically removed. Network switch left powered on—no one turns off the breaker.

Days 1–846: Legacy HMI continues running on the subnet. Invisible to IT (no agent, no CMDB entry). Invisible to OT team (assumed offline). Unpatched for 2+ years.

Day 847: VStrike detects first anomalous outbound connection from dormant device. DeepTempo flags: 847-day baseline broken, destination IP matches known APT infrastructure. Alert fires in under 60 seconds.

T + 5 min: VStrike blast radius analysis: compromised HMI has legacy network path to active production PLCs on adjacent subnet. Crown jewel exposure confirmed.

T + 8 min: AI SOC enriches alert with VStrike attack path visualization. Full context delivered to analyst: device identity, location, blast radius, C2 destination, lateral movement risk.

T + 20 min: Device isolated, network path severed, incident contained. Production line unaffected. Forensics replay initiated.

Without VStrike: Device remains invisible. Attack progresses undetected. Discovery occurs weeks later—after lateral movement to production PLCs.

Industry average OT dwell time: 200+ days Time to contain with VStrike + DeepTempo: 20 minutes Risk of PLC disruption from monitoring: Zero

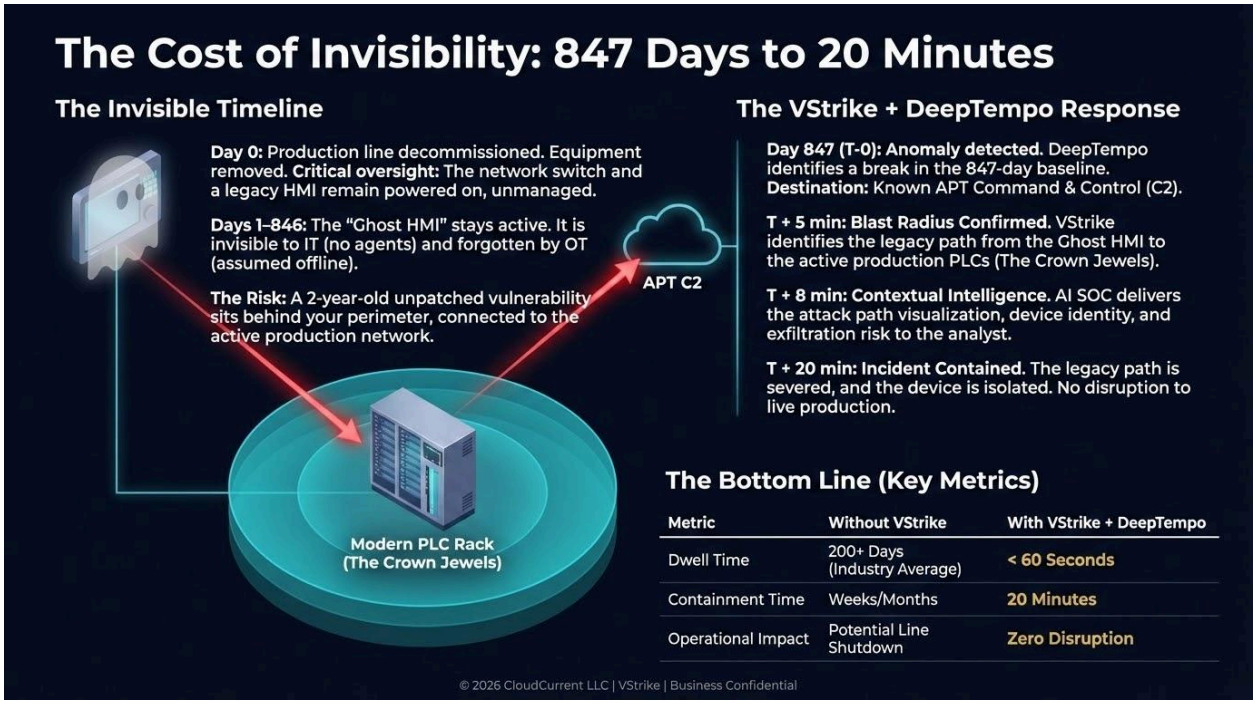

Figure 1: Cost of Invisibility

THE STRATEGIC OUTCOME: Operational Continuity and Cyber Resilience Are Not a Trade-Off

For years, industrial organizations have accepted a false choice: either accept the visibility gaps created by "forbidden" security tools, or risk the operational disruptions those tools introduce. VStrike and DeepTempo eliminate this trade-off entirely.

Passive monitoring means the security team can finally operate on the factory floor without IT/OT conflict. Protocol-aware mapping means the OT team finally has a shared language with security analysts. And behavioral baselines built for industrial stability mean that when something truly anomalous occurs—an attack, a fault, an insider threat—it surfaces immediately, with context, before it reaches your crown jewel assets.

"The Dark Segment is not a technology problem. It's an assumption problem. Organizations assume the air gap holds, that decommissioned means offline, that unmonitored means safe. VStrike replaces assumptions with evidence. If it's on the wire, it's on the map."

The organizations that will avoid the next Colonial Pipeline, the next Ukraine grid incident, the next water treatment compromise, are the ones that stopped trusting their asset inventory and started trusting their wire.

Request a live Proof of Value. See your Dark Segment in 30 days. info@cloudcurrent.biz
CloudCurrent · Protecting the Pulse of Our Infrastructure