VStrike and the Discovery of the Dark Segment

Purpose

This is one of the most powerful **“Aha!” moments** a customer experiences during a Proof of Value. Inside CloudCurrent, we call it **“The Truth from the Wire.”**

While other products depend on asset inventories (which drift almost immediately) or active scanners (which devices can hide from), VStrike relies on the one thing a device cannot spoof, mask, or manipulate: “**its conversation on the wire.”**

The moment VStrike reveals a device the customer didn’t know existed, the entire room shifts. That’s the Dark Segment coming into view.

What Is the Dark Segment?

The **Dark Segment** is the portion of the network where devices are physically connected and actively communicating, yet completely **unseen** by the customer’s management stack.

Why devices fall into the Dark Segment:

- No endpoint agent installed (CrowdStrike, etc.)
- Not included in vulnerability scans (Tenable, etc.)
- Misconfigured or orphaned IP ranges
- Incorrect VLANs, ports, or segmentation
- Industrial or IoT devices that were never onboarded

The VStrike Advantage:

If a device emits **one packet**, it generates a traffic log (NetFlow, Syslog, IPFIX).
VStrike ingests that log and **renders the device in 4D**, placing it instantly into the operational picture.

If it talks, VStrike sees it.
“The Dark Segment becomes illuminated.”

Why Other Capabilities Miss the Dark Segment

Most legacy tools suffer from a **Dependency Flaw** , they can only see what they are explicitly told to look for.

Feature	Legacy Tools	VStrike (CloudCurrent Standard)
Discovery Method	Active polling or agent-based	Passive traffic-log analysis
Requirement	Device must respond or run software	Device only needs to communicate
Blind Spot	Shadow IT, unmanaged IoT, hidden OT controllers	None, if it talks, it appears
Integrity	Can be fooled by firewalls or stealth settings	Unalterable, traffic logs don't lie

"Legacy tools trust what a device reports. VStrike trusts what the wire proves."

The Internal SE Talk Track

When VStrike lights up a device the analyst didn't know existed, anchor the moment:

**"See this node in the Dark Segment? Your inventory shows this segment as empty, but VStrike is pulling real-time traffic logs from your Arista switch proving a device is active here. It's communicating via Modbus to your PLC.

Your other tools missed it because they're looking for agents.
VStrike is looking at the behavioral truth of your network."**

This is when the customer realizes their tools weren't wrong — **they were blind.**

Addressing the 'Why' (Analyst Objections)

When the analyst inevitably asks:

"Why didn't my $1M firewall see this?"

Your answer is simple: **Architectural Validation.**

The Misconfiguration Reveal:

> “Your SPAN port or VLAN tagging wasn’t configured for this sub-segment. VStrike sees it because we’re ingesting the core switch logs, exposing a physical blind spot in your firewall.”

The Overpromise Reveal:

> “Your endpoint tool guarantees 100% coverage, but only for managed OSs. This is a headless Linux bridge. VStrike doesn’t care about the OS; we care about the data flow.”

“***VStrike doesn’t replace their tools, it reveals their assumptions.”***

The Dark Segment Checklist for CloudCurrent SEs

During every deployment, look for these three Dark Segment device types to demonstrate immediate value:

- **The Rogue Gateway**
  A device bridging to an external network that doesn’t appear in the official topology.
- **The Abandoned Controller**
  “Decommissioned” industrial hardware that is still powered on and talking.
- **The Misplaced Asset**
  A legitimate device plugged into the wrong port/VLAN, now invisible to its management server.

These three alone can justify the entire POV.

The Mic-Drop Moment

> ***“In a VStrike environment, you don’t manage an inventory, you witness the reality of your network. If it’s on the wire, it’s on the map. No exceptions.”***