

Illuminating the Dark Network

Edge-to-Core Visibility for Critical
Infrastructure and OT Environments



You cannot secure what you do not know is connected.

The Threat

Undocumented operational technology (OT), physical-security devices, and shadow IoT represent an invisible attack surface.

The Reality

Traditional IT network scanners often fail to identify these specialized assets—or worse, disrupt fragile industrial control loops during discovery.

The Mandate

Find network-connected assets that are missing from traditional inventories to identify security weaknesses before they become active incidents.

The Void



See Every Device. Understand Every Risk.

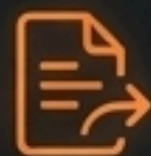
Introducing IPMeter™, an on-premises cybersecurity assessment and telemetry-collection platform engineered specifically for operational technology, IoT, connected devices, and physical-security networks.



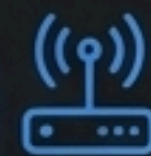
**Controlled
Assessment**



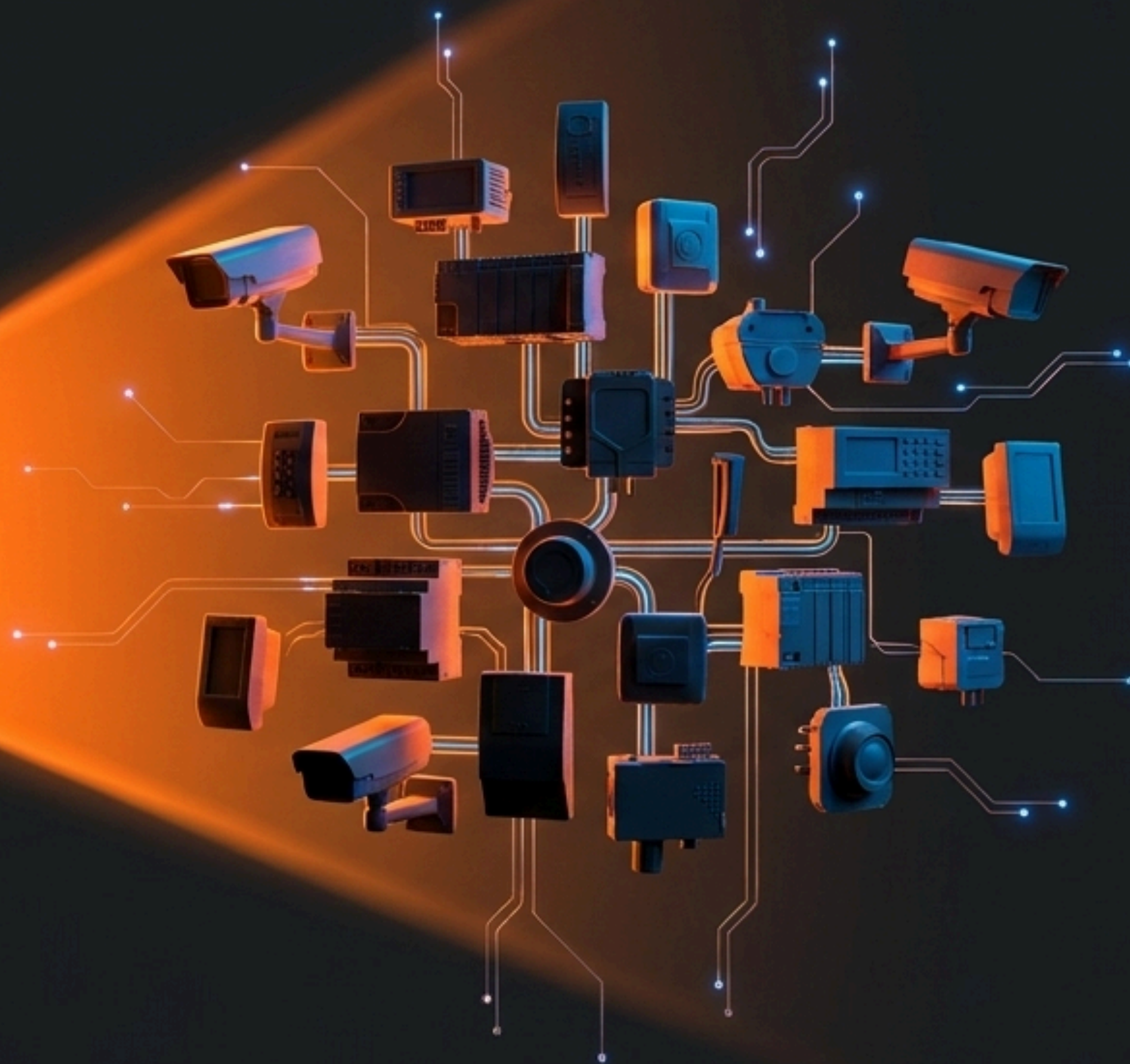
**Asset
Context**



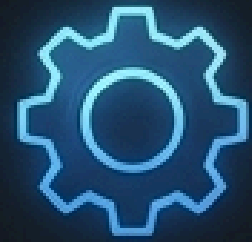
**Actionable
Reporting**



**Syslog and
SNMP Services**



Total Visibility Across the Modern Attack Surface



Operational Technology (OT)

Industrial and building systems [EPMS, BMS, PLCs] connected to the network.



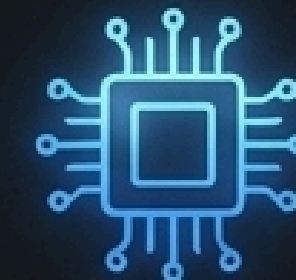
Physical Security

Cameras, access-control devices, controllers, intercoms, and security appliances.



IT Infrastructure

Servers, workstations, printers, switches, and standard endpoints.



IoT Devices

Specialized connected devices that exponentially expand organizational attack surfaces.



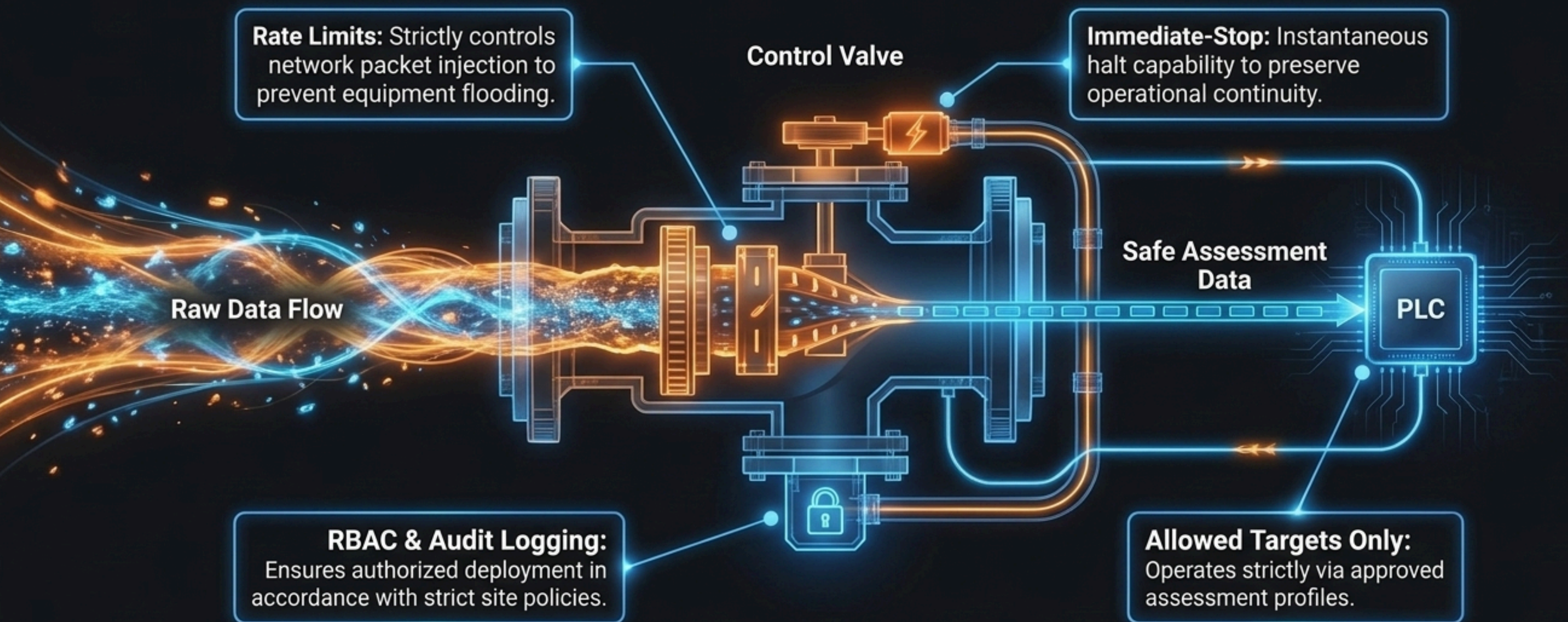
Takeaway: Discover the network before an attacker does.

Continuous Posture Improvement

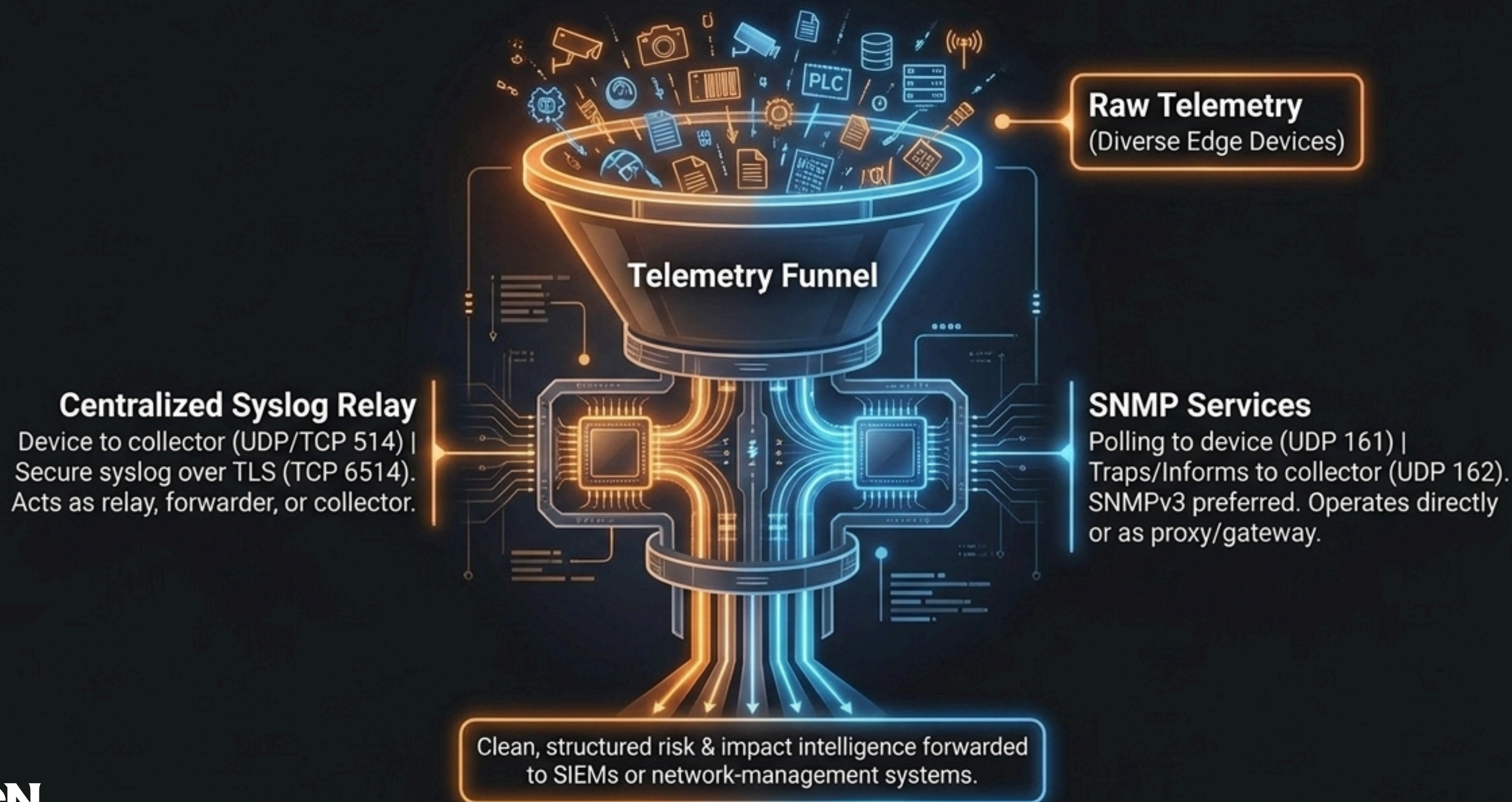


Safe Assessment for Fragile Control Loops

Traditional scanning breaks industrial tech. IPMeter gives OT and physical-security teams a controlled way to assess risk without turning the collector into part of the control loop.



Turning Network Chaos into Prioritized Intelligence



Three Appliances. One IPMeter Platform.

Choose the physical edge that fits the specific deployment environment and budget—ranging from everyday commercial networks to the harshest extended-temperature critical infrastructure sites. All platforms include a **2-Year Warranty** and **7-Day Lead Time**.



Vault



Helix



Karbon

Selecting the Right Hardware Edge

	Vault (Entry Level)	Helix: IPM-521-ST-32-1T (Industrial)	Karbon: IPM-521-XT-32-1T (Rugged)
Target Environment	Small business & commercial	Enterprise, Gov & Industrial	Critical infrastructure & harsh environments
Operating Temperature	15°C to 30°C	0°C to 50°C	-40°C to 70°C
Hardware Platform	OS agnostic / Intel Celeron (1.6 GHz)	Gov-approved platform / Intel Core Ultra 7 165H	Gov-approved platform / Intel Core Ultra 7 165H
Memory & Storage	8GB Cache / 120GB	32 GB DDR5-5600 / 1 TB industrial NVMe	32 GB wide-temp DDR5 / 1 TB industrial NVMe
Power Input	12 VDC	12 to 24 VDC	12 to 48 VDC (Automotive-capable)

Deploying Safely Within Critical Infrastructure

Designed for distributed use patterns across 16 CISA critical-infrastructure sectors.

Level 3.5
IDMZ (Industrial DMZ)

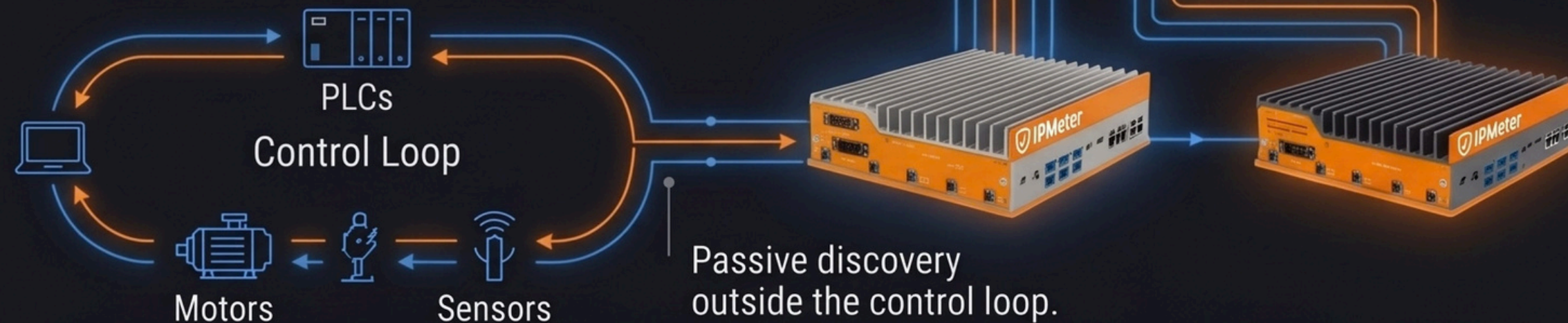
Syslog/SNMP
Receivers

Secure Data
Aggregation

Level 3
Site Operations

Telemetry moves upward without
bridging zones, bypassing firewalls,
or participating in the safety loop.

Level 1/2
Operational
Networks



Local-First Operation. Global-Scale Integration.

Edge-to-Core Architecture Map

The Core



Integration with IMRON UnityIS®
(Centralized Reporting, Real-Time Alerts),
SolarWinds, on-premise trouble-ticketing,
and major SIEM/NMS platforms

Approved syslog, SNMP, API, or middleware interfaces
transmitting evidence

The Edge



IPMeter Appliances operating independently or as peer
nodes in a federated deployment.

Note: Does NOT require a separate cloud management tier.

Reference-Aligned for **Industrial Cybersecurity**



NIST SP 800-82 Rev. 3

Aligned with the authoritative standard for securing operational technology and industrial control systems.



CISA Performance Goals

Directly supports CISA Cross-Sector Cybersecurity Performance Goals for critical infrastructure deployment.



ISA/IEC 62443

Engineered on the foundational concepts of the world's leading standard for industrial automation and control systems (IACS) security.

Visibility Before Vulnerability Becomes an Incident

The Outcome

Turn chaotic network data into actionable remediation insight.

The Advantage

Reduce attack surface.
Prioritize remediation based on operational impact.
Support audits with irrefutable local evidence.

The Reality

You cannot secure what you do not know is connected. Illuminate your network with IPMeter.

For pricing, deployment planning, and datasheets, access the IMRON dealer portal.