Dragon Data Aggregator
Tame the Data Beast

24
Dr
Dragon

The Challenge:

Security teams don't need more data—they need better intelligence. Traditional security platforms flood teams with raw logs, forcing them to sift through bloated, chaotic, and resource-intensive data just to find what matters. Data overload drives up costs, slows response times, and requires expert personnel just to manage the noise.

In physical security, the challenge is even more pronounced. Most facilities rely on fewer, but more critical, data sources, yet many platforms treat every source the same—displaying endless logs instead of filtering, processing, and detecting threats in real time. The result? Security teams are stuck manually monitoring dashboards and screens instead of focusing on real-world threats.

The solution isn't more hardware, software, or raw data—it's smarter detections that surface only the most relevant insights. Security teams need a system that automates threat detection, reduces noise, and enables real action – all without adding unnecessary complexity.

What is PDR?

Think of PDR as a coordinated security team—each member watching a different entrance. Truman connects your physical and digital security systems, helping them work together to detect threats, share insights, and respond quickly and effectively.

The Solution:

Dragon, the data-taming engine behind **Truman PDR (Physical Detection & Response)**, designed to cut through the noise and deliver only what matters. Unlike traditional data aggregation tools that flood teams with raw information, Dragon refines data streams, prioritizes detections, and automates alerts so security professionals only receive notifications when a true security event occurs.

Unlike cybersecurity, where hundreds of sources generate constant alerts, physical security operates differently—detections should be fewer, but when an alert fires, it's meaningful. Dragon's advanced filtering and intelligent processing ensure security teams aren't glued to their screens, sifting through endless feeds. Instead, they receive targeted, high-value notifications that drive immediate action. Whether deployed on-premises or in the cloud, Dragon's flexible architecture integrates seamlessly into any security stack—without unnecessary baggage.

Key Dragon Benefits

- **See What Matters:** Dragon filters the noise, surfacing only critical detections.
- **Smart Alerts, Less Fatigue:** Triggers only when necessary, avoiding constant distractions.
- **Sharper Insights, Faster Action:** Focus on real threats with clean, actionable data.
- **Scalable & Cost-Effective:** Base Truman includes ten sources, unlimited detections, and flexible expansion.

- **Lower Costs, Higher Efficiency:** Reduce storage, processing, and personnel overhead.
- **Optimized for Facility Security:** Tailored for corporate facilities, critical infrastructure, and beyond.
- **Deploy Anywhere:** Runs on-premises, in the cloud, or hybrid with minimal setup.
- **Simple & Powerful:** Lightweight, easy to manage, and built for efficiency.

Key Features:

Why Dragon:

Security teams don't need more data—they need smarter intelligence. Most facilities rely on fewer, but key critical sources, yet traditional tools flood them with noise, driving up costs and burying real threats in endless logs.

Dragon, the data-taming engine behind Truman PDR, refines data, prioritizes detections, and automates alerts so teams only act when it matters. It filters out the clutter, optimizes performance, and seamlessly integrates into any security environment—on-premises, in the cloud, or hybrid without unnecessary overhead. **Less noise, smarter security.**

Learn more: securepassage.com/dragon

Flexible Deployment & Minimal Footprint

- **Run Locally or in the Cloud:** Choose the best fit for your security strategy and infrastructure needs.
- **Rapid Prototyping & Testing:** Develop locally to reduce cloud costs and accelerate implementation.
- **Lightweight & Portable:** Single-binary deployment, with the ability to run in resource-constrained environments like on a Raspberry Pi.
- **Minimal Infrastructure Overhead:** Reduce hardware, software, and maintenance costs without sacrificing performance.

Intelligent Data Processing

- **Advanced Filtering & Refinement:** Cleans, prioritizes, and structures security data for meaningful insights while eliminating noise.
- **Detection-Driven Intelligence:** Triggers alerts only when a real security event occurs, ensuring teams focus on action, not overload.
- **Seamless Facility Integration:** Optimized for key critical sources per facility, with scalable expansion options.

User-Friendly Management

- **Easy Configuration:** Form-based, guided source configuration for quick and hassle-free setup.
- **Near Real-Time Monitoring:** Instantly view pipeline health, performance, and bottlenecks.
- **Tracing Metrics:** Quickly identify, analyze, and troubleshoot security data issues.

About Secure Passage:

At Secure Passage, security isn't just about technology—it's about protecting life and your ability to live it—at work, at home, and at play—in safety, without disruption. True security isn't about overwhelming you with data; it's about surfacing only what matters, when it matters. Our human-centered approach ensures security works seamlessly in the background, so you can focus on living, not watching. Whether safeguarding businesses, communities, or critical infrastructure, Secure Passage delivers AI assisted, intelligence-driven solutions that keep you informed, not overloaded—because real security should feel effortless.