Off the Network. Still connected.

How Phizzle's Connected Plant™ platform eliminates the IT burden of scientific instruments without sacrificing a single data point.

THE PROBLEM

Scientific Instruments Were Never Meant to Live on Your Network.

Today's pharmaceutical manufacturing environments are packed with hundreds of scientific instruments: chromatography systems, spectrometers, balances, bioreactors, and more. Most of these instruments are running decades-old operating systems, lack modern security protocols, and expose your enterprise network to significant risk the moment they're connected.

Every instrument on your network is a potential vulnerability. IT teams spend enormous time and resources trying to patch, isolate, monitor, and manage devices that were designed to measure, not to be managed.

THE HIDDEN COST NO ONE TALKS ABOUT

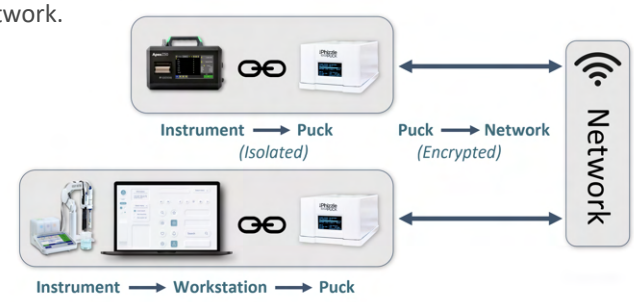
"For every instrument we connect to the network, IT estimates 40+ hours per year in management overhead: patching, monitoring, exception handling, and audit documentation. Multiply that by 200 instruments, and you have a full-time job just keeping the lights on."

THE PHIZZLE SOLUTION

Remove the Instrument. Keep the Data.

Phizzle's Connected Plant™ platform takes a fundamentally different approach: instead of trying to make legacy instruments behave like modern network citizens, we remove them from the network entirely, and replace that connection with something far more secure.

The Phizzle Edge Puck™, Phizzle's purpose-built edge device, sits between each instrument and your enterprise environment, acting as a secure, air-isolated gateway that collects, validates, and forwards data without ever exposing the instrument to your network.



ARCHITECTURE

Traditional Architecture	Connected Plant Architecture
• Instruments on enterprise network	• Instruments fully off the network
• OS patching required per device	• Zero OS management on instruments
• Network monitoring for each device	• Single secure Puck per instrument
• Antivirus/EDR on legacy OS	• No endpoint exposure at all
• Ad hoc file transfers & manual pulls	• Automated, validated data streams
• Audit trail gaps	• 21 CFR Part 11 compliant by design

HOW IT WORKS

The Phizzle Edge Puck™ - Secure by Removal

1. **Instrument connects only to the Puck**
   Via USB, RS-232, or Ethernet, locally and directly. No network hop, no IT dependency.
2. **The Puck validates, encrypts, and packages the data**
   Every data record is timestamped, checksummed, and audit-ready before it ever leaves the edge.
3. **Data flows securely to your enterprise systems**
   Into LIMS, MES, cloud data lakes (Azure, AWS, GCP), or your QMS, via your existing infrastructure.
4. **IT sleeps soundly**
   No instrument on the network means no instrument attack surface. Patching, monitoring, and vulnerability management disappear from the instrument layer entirely.

MODERNIZATION WITHOUT THE RISK

Your Architecture, Upgraded.

Most pharma IT modernization projects stall because legacy instruments can't be upgraded: they're running Windows XP, proprietary firmware, or vendor-locked software with no supported path forward. Ripping and replacing is cost-prohibitive. Leaving them in place is a security liability.

Connected Plant Threads the Needle

- Instruments stay exactly as they are: no firmware changes, no software updates, no re-qualification
- The Puck provides the modern connectivity layer, managed and updated centrally
- Data pipelines are standardized, documented, and audit-ready from day one
- New instruments can be onboarded in hours. Phizzle supports 250+ instrument types

PROVEN AT SCALE

Phizzle has been in continuous production at a Top 3 Pharma Manufacturer for over 4 years, managing instrument data across multi-vendor lab environments, with zero network exposure for connected instruments.

PLATFORM CAPABILITIES

Everything Your Data Ecosystem Needs

Connectivity
250+ instrument types across all major vendors. USB, RS-232, Ethernet, and file-based transfer protocols.

Compliance
21 CFR Part 11 and GAMP 5 compliant. Full audit trail, electronic signatures, and validated data integrity.

Security
Air-isolated connectivity, encrypted data in transit and at rest, no instrument-level network exposure.

Integration
Native connectors for LIMS (LabWare). Connectors for other cloud platforms such as Azure, AWS, GCP and more.

943 Howard Street, 2nd Floor, San Francisco, California 94103 - sales@phizzle.com - www.phizzle.com