Enigma Networks

Executive Briefing

Securing Clinical Trials in the Age of Insider Risk and Supply Chain Complexity

Enigma Networks © 2025. All rights reserved.

The Stakes Are Higher Than Ever

Executive Summary

Clinical trials are increasingly digital, decentralized, and interconnected – involving multiple research partners, CROs, cloud services, and specialized devices spread across the globe. This complexity accelerates scientific advancement but creates a cybersecurity nightmare.

A high-profile example of the risks facing clinical trials occurred in December 2020, when the European Medicines Agency (EMA) was breached by threat actors who accessed sensitive documents related to the BioNTech/Pfizer COVID-19 vaccine. The attackers infiltrated internal systems and exfiltrated regulatory data before public release, demonstrating that clinical trial environments are prime targets for cyber espionage.

Cybercriminals know clinical trials are goldmines. Intellectual property, patient data, and trial integrity represent billions in potential value. **Yet most clinical trial organizations still operate with a massive blind spot: the internal network.**

The Problem: Legacy Security Tools Fall Short in Research Environments

Perimeter defenses like firewalls, ZTNA, and EDR focus on who gets in. But the real risk moves inside: a compromised contractor, an exposed cloud service, or an unmanaged lab device communicating unexpectedly with external servers.

According to Verizon's 2023 Data Breach Investigations Report, 74% of all breaches include the human element – whether through error, credential misuse, or social engineering – yet traditional security tools consistently miss these attack vectors in complex research environments. This highlights why internal network visibility is critical even for trusted users and legitimate access.

Traditional security tools struggle to deliver:

- Visibility into unmanaged assets like specialized lab equipment, IoT sensors, or partner systems
- Detection of lateral movement across hybrid research networks before data staging
- Insider threat monitoring across CRO environments and third-party systems
- Low-friction deployment that won't disrupt ongoing trials or slow research
- Compliance-ready auditability for FDA 21 CFR Part 11, HIPAA, NIST, and international data localization requirements

The Solution: Enigma AI™ and ZTNX for Clinical Trials

Enigma AI is the first cybersecurity platform purpose-built for Zero Trust for Internal Networks (ZTNX) – enabling you to see, segment, and secure everything inside the research environment, without agents or manual effort.

Key Capabilities Designed for Clinical Trial Complexity:

1. Complete Research Network Visibility – Without Disrupting Science

Clinical trials span multiple organizations, research centers, CROs, and cloud-based platforms. Traditional tools require agents or predefined rules that simply aren't feasible across third-party systems, specialized lab equipment, or shared environments.

Enigma AI passively discovers and monitors every device and communication – including unmanaged lab systems, IoT sensors, and legacy equipment – without deploying agents or impacting research workflows.

2. Advanced Protection Against Insider Threats and Supply Chain Risk

Research shows that 68% of clinical trial security incidents originate from trusted insiders (research staff, contractors, CRO personnel) or supply chain compromise (access via IT providers, cloud services, or partner networks). These threats often go undetected for months by perimeter defenses.

Enigma AI continuously baselines normal behavior patterns and immediately flags anomalous internal activity – like unusual data staging, peer-to-peer transfers, or lateral movement between research zones – that other tools completely miss.

3. Compliance Excellence for FDA, HIPAA, and Global Data Requirements

Modern compliance frameworks require not just access controls and encryption, but continuous internal monitoring, network segmentation, and comprehensive audit trails. Regulators increasingly demand evidence of internal visibility and control.

Enigma AI provides continuous east-west traffic monitoring, automated segmentation policy recommendations, and comprehensive audit logging that demonstrates internal controls and data residency compliance across your entire research infrastructure.

4. Unified Monitoring Across Multi-Cloud and Hybrid Research Infrastructure

Decentralized trials, real-world evidence (RWE) studies, and remote data capture create complex multi-cloud, multi-region, multi-partner environments that traditional tools can't effectively monitor.

Enigma AI provides complete visibility across VPC-to-VPC, on-prem-to-cloud, and hybrid connections – showing exactly who's communicating with what across research, data, and clinical systems, even when third-party vendors or shadow IT are involved.

5. Zero-Maintenance Operations That Scale with Research Velocity

Legacy security tools demand constant tuning, rule creation, and data science expertise. Research environments prioritize speed, flexibility, and minimal operational overhead.

Enigma AI is agentless, AI-powered, and self-learning – no rules to write, no signature files to maintain, no agents to manage across your research ecosystem.

Why This Matters to Clinical Trial Organizations

Critical Requirement	Traditional Security Tools	Enigma AI
Discover unmanaged lab and partner devices	✗	✓
Monitor lateral movement across hybrid networks	⚠ (Partial coverage)	✓
Detect insider threats across CRO environments	⚠ (Limited visibility)	✓
Works seamlessly across third-party CRO systems	✗	✓
Deliver compliance-ready visibility and control	⚠ (Limited visibility)	✓
Deploy without disrupting research operations	✗	✓

The Business Impact

A single clinical trial breach can cost:

- $50-200M+ in R&D investment loss and trial delays
- 12-24 months of FDA approval timeline extension
- $100M+ in regulatory fines and legal settlements
- Complete loss of competitive advantage and IP

Why Act Now?

- Insider threats targeting clinical trials increased 40% in 2024 – with most going undetected by traditional tools
- Regulatory scrutiny is intensifying – FDA and international bodies are demanding evidence of internal network controls
- Attackers are using AI to navigate research networks faster than ever, making signature-based detection obsolete
- Clinical trial complexity is exploding – with decentralized trials, wearable devices, and multi-partner studies creating unprecedented attack surfaces

The Bottom Line

Clinical trial organizations can't afford to operate blind to internal network activity. Every day without internal visibility is a day attackers can move freely through your most valuable research assets.

Enigma AI closes the last major blind spot in clinical trial cybersecurity with a solution built specifically for the complexity, compliance requirements, and operational realities of modern research.

No blind spots. No assumptions. No disruption to science. Just complete visibility, intelligent control, and research-grade security.

Enigma Networks® is proud to lead the ZTNX movement. To learn more or see the platform in action, visit **getenigma.ai** or request a demo today.