

# Cybersecurity Readiness Podcast Series

Episode 95: Defending Digital Trust – Battling the Deepfake Surge with AI-Powered Detection

Host: Dr. Dave Chatterjee, Duke University

Guest: Sandy Kronenberg, Founder and CEO, Netarx

Podcast Portal: <https://www.cybersecurityreadinesspodcast.com/>

## Summary Pitch

In this episode, Dr. Dave Chatterjee sits down with Sandy Kronenberg, Founder and CEO of Netarx, the first AI-driven platform designed to detect and prevent synthetic impersonation across video, voice, and email. With deepfake fraud incidents skyrocketing by 3,000 percent and costing organizations an average of \$500,000 per attack, Kronenberg and Chatterjee unpack how AI can now help defeat AI—turning defense innovation into a frontline imperative.

Together they explore the evolution of deepfake technology, the psychology of digital deception, and how organizations can safeguard their people and data from real-time manipulation. Through the Commitment–Preparedness–Discipline (CPD) framework, Dr. Chatterjee underscores how leadership discipline, continuous monitoring, and technology integration are central to building a high-performance cybersecurity culture in an era of generative AI threats.

## Discussion Highlights

- **The Deepfake Explosion:** Why AI-generated deception has become the fastest-growing digital threat to trust and authenticity.
- **From Cloud to Counterfeit:** How Kronenberg’s entrepreneurial journey—from early cloud computing to AI-powered identity validation—shaped the creation of Netarx.
- **AI vs AI Defense:** How Netarx uses multimodal signal ingestion and voting ensembles across 50+ digital features to validate identity in real time.
- **Layer 8 Security:** Moving beyond the 50-year-old OSI model to protect the human layer—where trust is exploited most.
- **Visual Threat Indicators:** The innovation of “FLIRT” (visual threat alerts) that provide users immediate, on-screen confidence in communication authenticity.
- **Training Meets Technology:** Why security awareness programs must be enhanced—not replaced—by disinformation defense tools.

- **Cross-Channel Verification:** Using blockchain and decentralized identity to secure email, video, and text interactions under one integrated platform.
- **Practical Adoption Path:** Why organizations should start with protecting high-risk users—C-suite, finance, and HR—before scaling enterprise-wide.

### Actionable Recommendations

- **Recognize the Human Layer:** Treat cognitive and behavioral manipulation as part of the cybersecurity attack surface.
- **Adopt AI-Assisted Detection:** Implement multimodal, cross-channel solutions that integrate seamlessly with video, email, and messaging platforms.
- **Embed Disinformation Security:** Extend security programs beyond phishing to cover synthetic voice, video, and document validation.
- **Empower a Chief Trust Officer:** Establish dedicated trust operations to govern authenticity, reputation, and brand integrity.
- **Apply CPD Principles:**
  - **Commitment** — Executive-level endorsement of disinformation defense and authenticity verification.
  - **Preparedness** — Develop simulation drills involving AI-driven deception scenarios.
  - **Discipline** — Maintain continuous tool calibration and user training as deepfake technology evolves.
- **Start Small, Scale Smart:** Prioritize protection for financial and HR workflows before expanding to enterprise communications.

### Time Stamps

- 00:49 — Dave introduces the topic and deepfake threat surge.
- 02:37 — Sandy shares his professional journey and early exposure to cyber fraud.
- 07:28 — Discussion on the human layer and OSI model limitations.
- 09:55 — Integrating deepfake detection within enterprise security architecture.
- 13:01 — How AI models ingest 50+ signals for real-time identity validation.
- 17:48 — Zoom and video call trust issues in remote business settings.
- 19:40 — Why siloed tools fail—importance of cross-channel correlation.
- 23:30 — Continuous learning loops: retraining AI models against new deepfake generators.

- 26:59 — The rise of Trust Officers and Trust Operations in corporate governance.
- 32:15 — HR, finance, and brand use cases for disinformation security.
- 35:18 — Balancing training and AI automation.
- 37:16 — Expanding defense to email and multimodal verification.
- 41:18 — Closing takeaways on readiness and adoption strategy.

### Memorable Quotes

“You can’t trust everything on your screen—AI has made deception instantaneous.” — Sandy Kronenberg

“Deepfake detection must become a Layer 8 priority: securing the human element.” — Dr. Dave Chatterjee

“It’s not about more tools; it’s about the right integrated ones that can see across voice, video, and email.” — Sandy Kronenberg

“Commitment, Preparedness, and Discipline remain the anchors of resilience—especially when reality itself can be faked.” — Dr. Dave Chatterjee