

PEER-TO-PEER DISAGGREGATOR™ TECHNOLOGY

Peer-To-Peer Disaggregator™ (P2PD) is the culmination of a unique set of technologies developed by SafeMedia Corporation that effectively end illegal broad scale P2P file sharing. By preventing user upload and download to contaminated P2P networks (networks which contain illegal digital files), P2PD drains them of content and reduces their appeal and use effectively eliminating them as sources of illegally obtained digital files.

P2PD accurately, scalably, and robustly drops all contaminated P2P network traffic while allowing the unimpeded passage of all uncontaminated P2P network traffic, all done at network speed and without invading user privacy.

Achieving these results required a new paradigm in system architecture encapsulating the total functionality of many advanced technologies on a chip, and deploying multi/hyper processing architecture created specifically for network operations, resulting in far higher, scalable processing capacity than the bandwidth it services.

P2PD embodies the following breakthrough technologies:

- **Adaptive fingerprinting and DNA markers:** The P2PD library of all P2P clients and protocols is the world's largest and most current library of fingerprints and DNA markers and is updated every 3 hours. P2PD looks for fingerprints and DNA markers in outgoing and incoming packets and, depending upon identity strength, employs three levels of analysis. In the few cases where fingerprints alone are insufficient, P2PD actually combines DNA marker evidence from multiple packets using stored evidence history.
- **Adaptive network patterns:** Not all protocols can be easily identified with a single set of packets. As such, P2PD is set to monitor packet flows and adapt its filtering technique based on what it has already seen and what it sees now. This extensible system utilizes a technique called experience libraries. P2PD looks for patterns of certain identifiable characteristics of network events and determines if the packets are legal or illegal. Illegal packets are dropped and legal packets continue on their way.
- **Intelligent libraries:** SafeMedia's experience libraries are knowledge-based and created from the actual operations of the clients and include specific fingerprints/DNA markers in addition to the adaptive network patterns.
- **Remote update and self-healing:** All maintenance and defense actions—updates, integrity checks, sanity validations, system housekeeping, and self-defense—are remotely performed through SafeMedia's (Akamaized) servers with no delay in network operation.

P2PD technologies provide the foundation to implement the following advanced features:

- **No Invasion of User Privacy:** P2PD detection does not invade user privacy, never captures or records user IDs, does not decrypt any traffic, and allows the execution of all current security techniques (Tunneling, SSH etc.). P2PD never opens packets to determine file legality or illegality. That determination is based solely upon what type of transmission it is-never its content.
- **Accuracy:** P2PD is fully effective at forensically discriminating between legal and illegal P2P traffic with no false positives (i.e., identifying another protocol as the targeted protocol) whether encrypted or not.
- **Speed:** P2PD operates at network speed with little or no latency.

(See P2PD Technology Portability and Product Line for additional information.)