Unleash Your Last Line of Defense, Dymium Ghost Files™

Skip the painful recovery process and outsmart the ransomware attackers.

Ransomware has evolved into an existential threat for businesses and critical infrastructure, evading traditional detection and prevention mechanisms. Security products have been designed to protect networks, applications, and devices, but they have proven less than effective at stopping ransomware from propagating into data stores. The tools and tactics of increasingly sophisticated cyber attack groups' ransom and extortion campaigns warrant new approaches to securing your most important asset, your data.

DYMIUM™

Los Gatos, CA | www.dymium.io

For more information, please contact: info@dymium.io

DYMIUM™

Befuddling the Threat Actors with Dymium Ghost Files™

- **Real-Time Detection**
- **Block Malicious Activity**
- **Robust Audit Trail**
- **Simple Integration**

Dymium Ghost Files protects files and file servers from data theft and modern ransomware and extortion campaigns by detecting and terminating activity at multiple stages of an attack. While others use a passive, recovery-oriented approach, Dymium constantly observes and meticulously records all file-related activity transacted on network-attached shares, uses multiple methods, including machine learning, to identify kill chain behavior early in a campaign, and terminates malicious activity.

Powered by Dymium Ghost Data Services™
A Layer for Real-Time & Secure Data Collaboration