^C CryptoStopper

Ransomware Protection from the Inside Out

How CryptoStopper™ works

Workstation — Share File Server
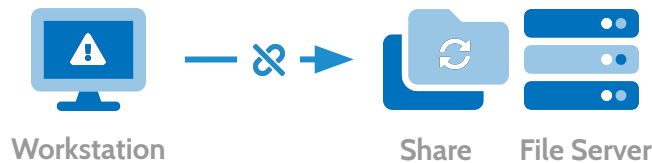
1.
Ransomware monitoring on network (all endpoints)

2.
Ransomware (encryption) detected

3.
Endpoint isolated automatically

4.
Administrator is notified via Email

Deception Technology
CryptoStopper™ seeds the network with files, creating a trap to detect ransomware. These bait files quickly detect the attack and trigger proactive steps to shut down the attack.

Signature-less detection
Traditional antivirus relies on a signature to detect a threat, which limits the response to known attacks. CryptoStopper™ uses the encryption process itself to detect and stop the attack.

Stopped in milliseconds
The unique detection and response algorithms of CryptoStopper™ have proven to stop a ransomware attack in milliseconds, preventing business downtime and recovery from the attack.

Last line of defense
Designed to keep you *left of boom*, CryptoStopper™ works in your existing stack and adds a last line of defense layer of security against an unavoidable threat.

For more information visit **www.getcryptostopper.com**