



ILLUSIVE PLATFORM FEATURE BRIEF:

Ransomware Protection

Ransomware has evolved past “spray and pay” attacks aimed at any target that might take the bait and is now more frequently targeted at specific organizations like an advanced persistent threat. Fight back with the Illusive Platform, which stops the lateral movement enabling advanced Ransomware on endpoints before any files or fileshares can be encrypted. With Illusive’s high-fidelity lateral movement detection, organizations can immediately identify malicious encryption attempts and ultimately divert them towards deceptive files that seem real to attackers. Identify imminent attacks, stop advanced ransomware, and collect threat forensics, all in real time.

BENEFITS



Identify ransomware attackers’ lateral movements when targeting organizational assets



High-fidelity detection of genuine attacks that is not based on activity monitoring and doesn’t generate false positives



Goes beyond detection to enable a real-time response, preventing the systematic damage that occurs when assets are encrypted



Collect source-based forensics on in-progress ransomware attempts to prevent future attacks

Block the Lateral Movement Enabling Ransomware

With Illusive’s high-fidelity detection of unauthorized lateral movement, malicious-encryption attempts can be immediately identified, diverted, and delayed. Illusive can automatically stop advanced ransomware programs, trigger alerts, and gather source-based forensics, all in real time.

Fill Critical Ransomware Protection Gaps

With successful testing conducted against top ransomware families, the Illusive Platform is proven to help obstruct the most common advanced ransomware threats and fill gaps in commonly available ransomware solutions.

How Illusive Ransomware Protection Works

1

Tailored deceptive ransomware files and fileshares are deployed across networks, endpoints and servers

2

Ransomware is diverted toward deceptive files and fileshares and away from genuine assets

3

As soon as deceptive ransomware targets are engaged, organization is alerted in real time before malware can encrypt files

4

Ransomware activity is halted on affected endpoints before any damage is done