Introducing CYSANA: The Integrated Malware Detection & Ransomware Prevention Solution

Detecting the Hardest to Find Malware & Defeating the Most Dangerous Ransomware

CYSANA [CYberSecurity ANAlytics]

Invasive ransomware is delivered via hard-to-find malware embedded in executable software applications. CYSANA detects, and then uniquely prevents the very core capabilities of encryption and exfiltration, disabling would-be breaches before they start and eliminating dwell time.

Malware Detection

CYSANA uses multiple filters for malware detection combining conventional (fingerprint matching, digital certificate checks) and data-driven (AI-based neural network and NLP) approaches. Combined with a novel, unique method of preventing malware from becoming strong cryptographic ransomware.

Ransomware Prevention

Once encrypted, undetected malware becomes ransomware, causing irreversible damage. The unique CYSANA patented anti-encryption module prevents malware from becoming ransomware by blocking malware (whether CYSANA previously detected it or not) from using the encryption keys on to lock up data and hold it for ransom.

Deep Learning AI + Patented Anti-Encryption

CYSANA uses multiple filters for malware detection combining conventional (fingerprint matching, digital certificate checks) and data-driven (AI-based neural network and NLP) approaches. Combined with a novel, unique method of preventing malware from becoming strong cryptographic ransomware.

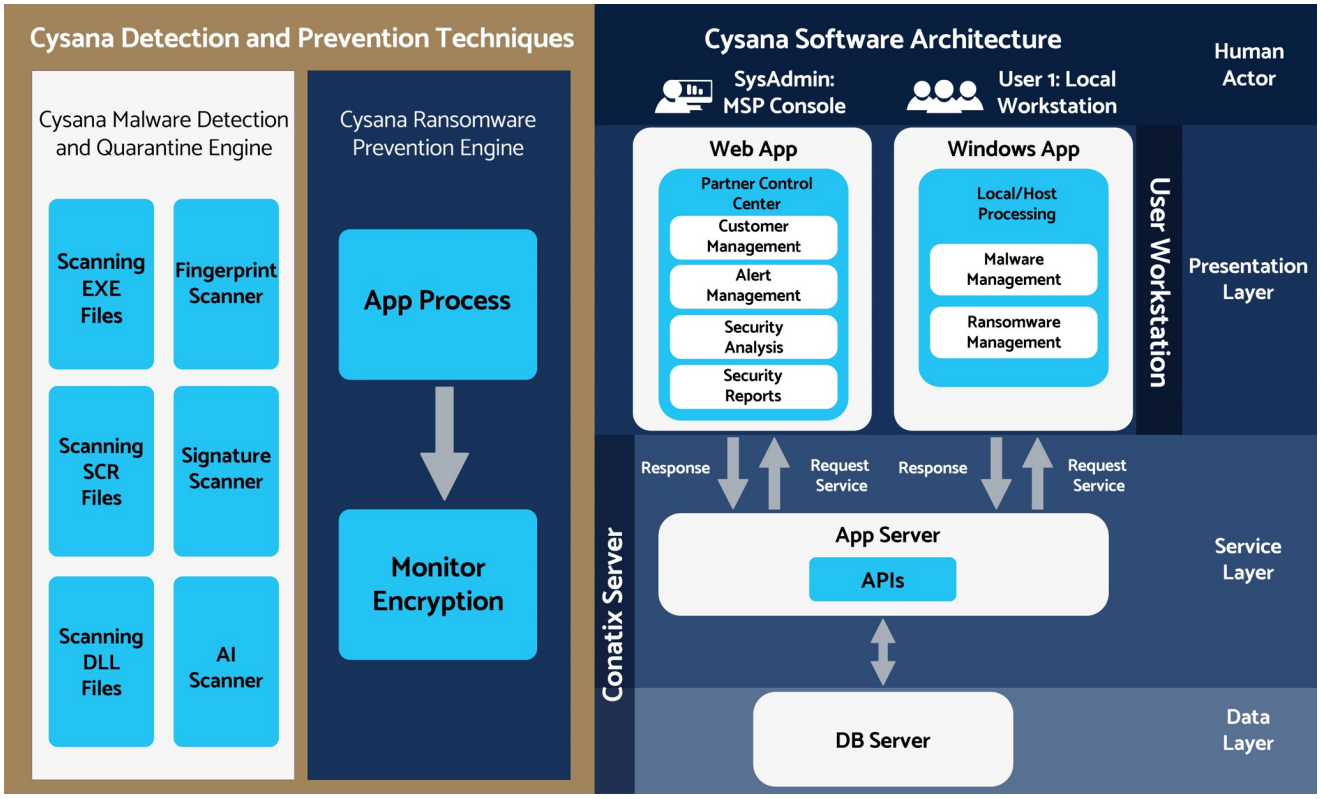
CYSANA detects malware embedded in software executable files AND blocks any type of malware from encrypting data and becoming ransomware

CYSANA: The Integrated Malware Detection & Ransomware Prevention

Solution Overview

ANALYTIC VIEW

ARCHITECTURAL VIEW



Robust

Multiple AI and conventional filters to detects malware that other tools miss

Lightweight

No legacy code so as not to conflict with other apps or slow down endpoints/network

Low computational cost

low maintenance, fast deployment

Integratable

Easily connected with Managed Detection & Response (MDR), and/or Remote Management & Monitoring (RMM) systems

Multitenant

cloud-based MDR

Deep

Decompiles software down to the atomic level to find even novel, unknown malware

Broad

Works across the broadest range of software file types

Fast

Detects AND quarantines malicious files in milliseconds, as executable files download

Early

Analyses files BEFORE they can install, activate or attack

Easy

Quick install, runs in background, simple UI

Demo and **free trial** available contact inquiry@conatix.com to learn more