CONATIX
CYBERSECURITY ANALYTICS
cysana

Publication Date: August 24, 2026

CYSANA TECHNICAL BRIEF

STOPPING THE CLOCK

The research behind CYSANA's pre-execution detection and independent anti-encryption defense – and why removing the race matters more than winning it.

DETECT WHAT'S THERE.
PREVENT WHAT'S COMING.

A CONATIX PRODUCT
WWW.CONATIX.COM

STOPPING THE CLOCK

The research behind CYSANA's pre-execution detection and independent anti-encryption defense — and why removing the race matters more than winning it.

IN THIS BRIEF

CYSANA
POWERED BY CONATIX

Two Intervention Points. One Security Decision.

CYSANA changes the point of intervention. Instead of waiting for a suspicious file to reveal itself through execution or behavior, CYSANA is designed to evaluate software at the point of download — before it opens, installs, or becomes active. A separate anti-encryption capability provides another intervention point against cryptographic ransomware.

Pre-Execution

Analyze software before it is allowed to become active.

AI-Based Analysis

Use deep-learning image classification to identify malicious characteristics.

Anti-Encryption

Provide an independent layer intended to stop ransomware before user files are encrypted.

DESIGNED FOR SECURITY TEAMS AND SERVICE PROVIDERS

CYSANA was developed for managed security service providers (MSSPs), managed service providers (MSPs), and Enterprise Security Teams. Its value proposition is straightforward:

- Identify and neutralize threats earlier
- Provide an independent layer of ransomware protection

CYSANA reduces the need for security teams to:

- Detect
- Contain
- Remediate

ransomware after encryption has already begun.

By combining pre-execution malware detection with proactive control over unauthorized encryption activity, CYSANA helps stop threats before they can damage critical data.

Source basis: University of Luxembourg SnT

Detect Earlier: Before the File Runs

Many endpoint security techniques learn about a file from signatures, reputation, sandboxing, or behavior observed during execution. CYSANA adds a different decision point: analyze newly downloaded software before it opens, installs, or engages in activity on the endpoint.

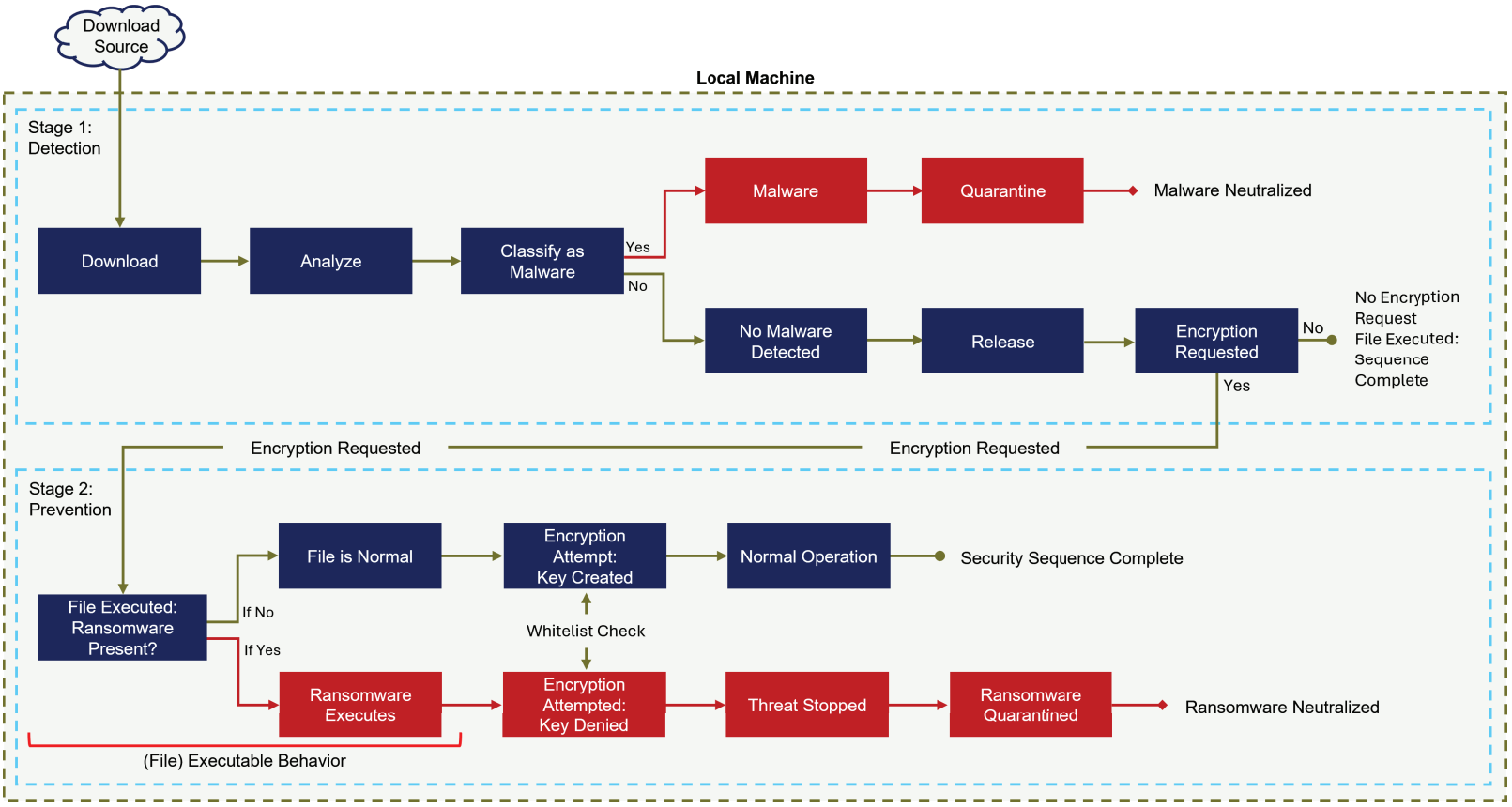
THE SIMPLE IDEA

A file should not have to execute before security decides whether it is safe to run.

The diagram illustrates CYSANA's two independent and complementary layers of protection. In **Stage 1**, each downloaded file is analyzed and classified before execution. Files identified as malware are immediately quarantined and neutralized, while files not classified as malicious are released for execution.

Stage 2 provides an independent layer of proactive anti-encryption protection. If an executing file does not request encryption services, the security sequence ends. When encryption is requested, CYSANA applies a whitelist-based access-control policy. Authorized applications are permitted to create encryption keys and continue normal operation. If previously undetected malware executes and ransomware fires, its unauthorized encryption request is denied, preventing key creation before user files can be encrypted. The threat is then stopped, quarantined, and neutralized.

From Download to Verdict



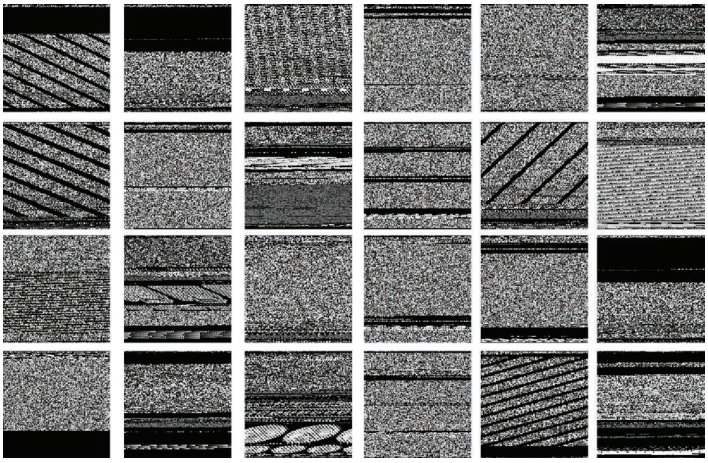
cysana
POWERED BY CONATIX

Image-Based Deep Learning

CYSANA converts the binary contents of executable files into grayscale images. Individual byte values become pixel intensities, revealing structural patterns associated with executable code, data, resources, packing, compression, and obfuscation. Benign and malicious applications can produce visibly different combinations of textures, boundaries, repetitions, and high-entropy regions. A deep-learning image classifier analyzes these complex spatial patterns and determines whether a newly downloaded file more closely resembles learned benign or malicious software. Because the analysis is performed on the file itself, CYSANA can produce a verdict before the application opens, installs, or executes.

*For an MSP or MSSP, the message is easy to carry downstream: **CYSANA** is designed to make a security decision before an unknown file gets its first opportunity to act.*

MALICIOUS



The **MALICIOUS** figure contains executable samples classified as malware.

Compared with the benign examples, these samples appear to contain more frequent combinations of:

- Dense noise-like regions
- Abrupt transitions between textures
- Repeated diagonal patterns
- Large, highly uniform sections
- Unusual section boundaries
- Repeated structures across different samples
- Compressed, packed, obfuscated, or embedded content

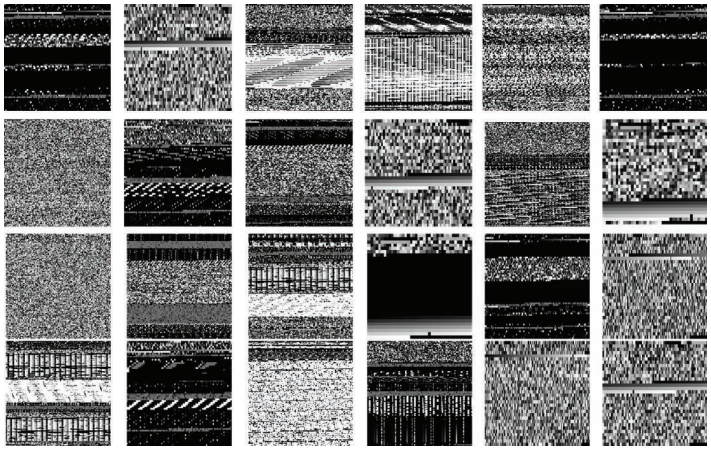
Malware authors frequently pack or obfuscate executable code to conceal malicious instructions and frustrate conventional analysis. Packed or encrypted payloads may produce high-entropy regions that appear visually dense or noisy. A small loader may appear as one structured region, while the concealed payload appears as a different and more irregular region.

BENIGN

The **BENIGN** figure contains software samples classified as legitimate or non-malicious.

The images show a broad mixture of:

- Structured horizontal bands
- Repeating code and data patterns
- Distinct boundaries between file sections
- Areas of dense and sparse information
- Regularly organized blocks
- Mixed regions of high and low visual complexity



These patterns can reflect the conventional organization of legitimate executable files. A normal application may contain clearly separated headers, executable code, libraries, user-interface resources, images, configuration information, digital signatures, and unused or padded space.

The important point is not that benign files all look alike. They clearly do not. Rather, their internal structures tend to fall within patterns the model has learned from legitimate software.

cysana
POWERED BY CONATIX

Ransomware: Stopping the Clock

Ransomware creates a timing problem. Once encryption activity begins, detection and response are competing against the speed of the attack. **CYSANA** approaches that problem by creating intervention points before user data is encrypted.

REACTIVE APPROACH	EXECUTION	ENCRYPTION ACTIVITY	DETECTION	RESPONSE
CYSANA	DOWNLOAD	PRE-EXECUTION ANALYSIS	QUARANTINE	NO EXECUTION

DON'T WIN THE RACE. REMOVE THE RACE.

If a malicious file can be identified and quarantined before it executes, the attack never gets the head start that reactive detection must overcome.

Independent Anti-Encryption Protection

CYSANA also incorporates anti-encryption research developed at the University of Luxembourg. The underlying approach targets ransomware that relies on cryptographically secure random-number generation to create the strong encryption keys required to lock user data. By enforcing whitelist-based access control over those critical operating-system resources, CYSANA permits authorized applications to create encryption keys while denying requests from unauthorized processes. This independent anti-ransomware layer prevents applicable ransomware from obtaining the encryption keys required to damage user files.

Research Results

97.1%
726 of 747 samples stopped

RESEARCH RESULTS — NOCRY ANTI-RANSOMWARE

University research reported that the NoCry anti-ransomware approach stopped 726 of 747 active cryptographic ransomware samples before any user file was encrypted. The research also documents limitations: samples that did not call the targeted CSPRNG APIs, or where interception failed, were not stopped by that mechanism.

Important: *this figure reflects one independently run University research test set under controlled conditions — not a guarantee of detection performance in any specific customer environment.*

CYSANA
POWERED BY CONATIX

Two Independent Layers. One CYSANA Solution.

The value of **CYSANA** is not simply that it performs two security functions. The two intervention points address different stages of the threat and are designed to provide independent opportunities to stop an attack.

LAYER 1 Detect the Threat	LAYER 2 Stop the Encryption
• Analyze newly downloaded software before activity begins • Apply deep-learning image classification • Identify malicious characteristics • Quarantine the file before execution	• Operate as a separate anti-ransomware control • Target cryptographic resources used by applicable ransomware • Deny unauthorized access to cryptographic key-generation resources • Protect user files from being encrypted

Why This Matters to MSPs and MSSPs

A differentiated security story that is easy for technical sellers to explain.

An additional pre-execution decision point for newly downloaded software.

- A separate anti-encryption control for applicable cryptographic ransomware.
- Research-backed technology developed through collaboration with the University of Luxembourg's SnT.
- A security capability designed from launch with cybersecurity service providers and CISO teams in mind.

CYSANA can be positioned as an additional protection layer in a broader security architecture. Specific interoperability, deployment, management, licensing, and integration details should be validated against the current CYSANA product documentation before customer deployment.

Research-Backed Protection. Built to Intervene Earlier.

Deep learning + anti-encryption research in one security platform

CYSANA was developed by Conatix in collaboration with the University of Luxembourg's Interdisciplinary Centre for Security, Reliability and Trust (SnT). Its neural-network models were trained and tested on the MeluXina supercomputer, and the anti-ransomware technology incorporated into CYSANA is patented by the University of Luxembourg in 15 countries.

The CYSANA Difference

- Evaluate software at the point of download, before it becomes active.
- Use deep-learning image classification to identify malicious characteristics.
- Add independent anti-encryption protection against applicable ransomware behavior.
- Give security teams more than one opportunity to stop an attack.

How Ransomware Really Encrypts Your Data.

- Malware that reaches your computer may be looking for valuable data.
- Some malware activates as ransomware, encrypting that data to deny you access.
- The most damaging cryptographic ransomware uses strong, properly implemented encryption.
- Once the data is encrypted, recovery may be impossible without backups or a working decryptor—and paying the ransom does not guarantee recovery.
- Strong encryption depends on unpredictable keys and other cryptographic material.
- Generating that material reliably requires cryptographically secure random numbers.
- Operating systems such as Windows provide a limited set of trusted cryptographic services for generating them.
- Many ransomware operations depend on those onboard services to produce the encryption material needed to lock data securely.

Sources:

Content adapted from NIST SP 800-90A, CISA public guidance, and Microsoft cryptographic API documentation

REFERENCES

University of Luxembourg, SnT. "Stopping ransomware in its tracks: new enterprise app integrates AI & university research," April 2024.

University of Luxembourg research (NoCry). Evaluation of cryptographic ransomware interception; 726 of 747 samples stopped before user-file encryption in the reported test set.

Dyrmishi, S., Ghamizi, S., Simonetto, T., Le Traon, Y., Cordy, M. "On The Empirical Effectiveness of Unrealistic Adversarial Hardening Against Realistic Adversarial Attacks." University of Luxembourg / SnT. Background research on adversarial robustness in malware classification.

National Institute of Standards and Technology (NIST). SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators – cryptographically secure random-number generation standards referenced in Section 2.

C**ybersecurity and Infrastructure Security Agency (CISA).** Public guidance on ransomware prevention and cryptographic best practices.

Microsoft. Windows Cryptographic API (CAPI/CNG) documentation – operating-system cryptographic services referenced in Section 3.

CYSANA is developed by Conatix. Product claims, deployment requirements, and integration details should be validated against current CYSANA product documentation.

CONATIX
CYBERSECURITY ANALYTICS
cysana

A CONATIX PRODUCT
WWW.CONATIX.COM

STOPPING THE CLOCK.

See how **CYSANA** adds earlier threat detection and independent ransomware protection to your security architecture.

SCHEDULE A TECHNICAL BRIEFING

conatix.com/cysana | team@conatix.com

CYSANA

DETECT WHAT'S THERE. PREVENT WHAT'S COMING.