nubeva

Ransomware Response & Reversal

info@nubeva.com
844.538.4638

REVERSE RANSOMWARE
GET BACK TO BUSINESS

Universal Solution to Detect & Decrypt Ransomware Without Paying Ransom or Restoring from Backups

STOPPING RANSOMWARE: THE CHALLENGE

Ransomware continues to dominate as the most visible cybersecurity risk playing out across our nation's networks. Rapidly evolving vulnerabilities, like SolarWinds, Log4j, and large-scale successful attacks, like Colonial Pipeline, have shed new light on the far-reaching destruction these attacks can cause. Yet, despite best-in-class security systems, ransomware continues to get through network security systems and goes unnoticed by end-point detection and response (EDR) systems to await detonation. Once ransomware detonates and encrypts files, corrupted systems require fast recovery. Options today are limited, slow, and potentially expensive.

✗ RECOVER BY BACKUPS

- Average recovery time 21+ days and expertise required.
- Viable backups? Criminals corrupt backups.
- Full time/real time backups are expensive.

✗ PAY RANSOM TO DECRYPT

- No guarantee data recovery even if payment is made.
- Likelihood of being targeted again after payment is made.
- Possible extortion for additional payments after initial payment.

✓ RECOVER ENCRYPTED DATA NO PAYMENT OR BACKUPS NEEDED

Nubeva has partnered with Guardian Eagle to provide clients the ability to recover stolen data—without the need to use backups or provide payment for ransomware decryption keys. Utilizing Nubeva's Ransomware Response and Reversal (R3) technology, encryption keys used during a live ransomware attack are stolen, copied, and securely stored allowing the organization to reverse the attack and get back to normal operations almost instantly.

COPY ENCRYPTION KEYS → **SAFELY STORE ENCRYPTION KEYS** → **DECRYPT THE DATA QUICKLY & EASILY**

GUARDIAN EAGLE

Since 2003 Guardian Eagle has become an industry leader providing data security solutions and managed services. Ransomware represents a significant and growing risk to business and government enterprises. While layered defenses that attempt to block ransomware are important, they are increasing being circumvented allowing hackers to encrypt and ransom your data files.

Data backups remain an integral part of the defense strategy, but are insufficient to ensure data integrity and guarantee data recovery can occur.

Nubeva's breakthrough R3 technology backed by Guardian Eagle managed services represents the next evolution in data protection for your organization.

Guardian Eagle
111 2nd Ave NE
Suite 360
St. Petersburg, FL 33701

sales@theguardianeagle.com
(727) 252-6214

Nubeva R3 Offers Protection Against Most Known Ransomware.

SOLUTION OVERVIEW

Nubeva's Ransomware Reversal technology instantly detects ransomware encryption and the silent sensor intercepts copies of the encryption keys used to lock up files. Simultaneously, alerts can be fired to any SOC/SIEM/SOAR of an immediate indicator of compromise. When the organization is ready for recovery, initiate attack reversal, unlock the files, and get back to normal operations almost instantaneously. The solution is simple, flexible, scalable and easy to operate with affordable pricing.

Technical Value Promise:
Detect & decrypt successful ransomware attacks, quickly and easily.

Business Value Promise:
Reduce or eliminate potential downtime costs and consequences.

Global Value Promise:
Eliminate the crypto-ransomware threat as we know it today.

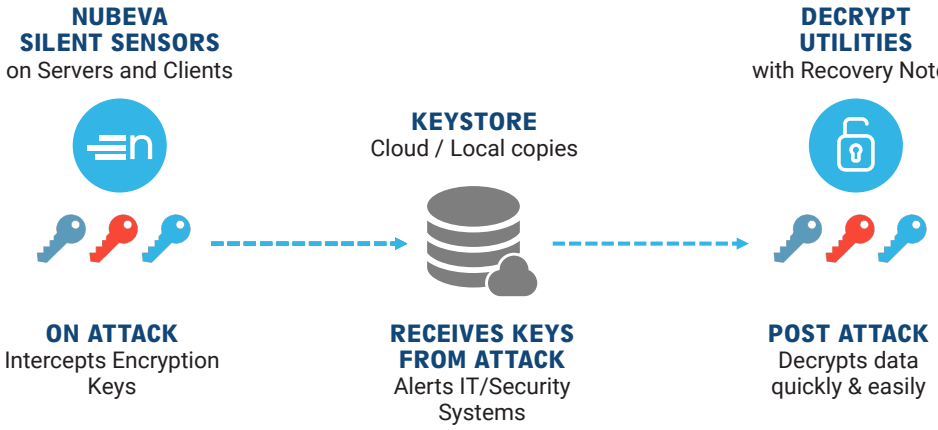
HOW WE REVERSE THE IRREVERSIBLE

Nubeva has perfected the ability to learn and extract the symmetric file encryption keys used by ransomware. Delivered as a small and efficient read-only system service on a client or server, the software can reliably detect ransomware encryption events and intercept copies of keys. With file keys available, restoration is not only possible but is fast and straightforward. The capability is an adaptation of Nubeva's patented SKI (Session Key Intercept) technology, initially developed for intercepting TLS/SSL session keys to enable next-generation network traffic decryption and inspection. SKI is a patented and proven technology licensed by numerous cybersecurity and application monitoring companies around the world.

HOW IT WORKS?

1. Install Nubeva's silent sensors*
2. The sensors instantly detect encryption key activity during a ransomware attack.
3. Sensors signal instant alerts and copy/store keys in multiple protected locations.
4. When users are ready for data recovery, Nubeva support provides decryptors and assistance to decrypt and restore the data using the intercepted keys.

** When no ransomware events are active, Nubeva's silent sensors use negligible memory and CPU. The silent sensors auto-update, without restarts, to ensure the latest coverage of ransomware families.*



nubeva
Steve Perkins
info@nubeva.com
844.538.4638

LEARN MORE: WWW.NUBEVA.COM