Nubeva Technical White Paper - 2022

# RANSOMWARE REVERSAL

An Active Approach to Neutralizing Ransomware Disruption

## The Leading Global Threat

Ransomware is an ever-growing threat to thousands of organizations and businesses worldwide. The US has been experiencing 4000+ attacks every day for several years, and the damages are growing exponentially.[1] In 2015, it is reported that ransomware attacks caused $325 million in damages, and that amount increased to $5 billion by 2017 and $20 billion in 2021.[2]

The threat shows no mercy, targeting businesses, organizations, and governments of all sizes. The median ransom in 2021 averaged $170K, and the rise of mega-ransoms hit an all-time high at $40million.[3]

## The Shocking Cost of Recovery

The big cost to companies and businesses comes during the recovery phase of ransomware attacks. As reported by Forbes, the current average cost to recover from a ransomware attack is $2 million, making the cost 10X the price of the ransom itself.[4] While it is encouraged never to pay the ransom, upwards of 70% of victims end up paying the criminals with the hopes of recovering.

**$2M**
**AVERAGE RECOVERY**

**THE CURRENT AVERAGE COST TO RECOVER FROM RANSOMWARE ATTACK IS 10X THE RANSOM DEMAND**

Table of Contents


**THE STATE OF RANSOMWARE** 1

- Bad to Worse-Why? 2
- A Gap in Current Solutions 2

**RANSOMWARE REVERSAL** 3

- Ransomware Encryption 3
- Nubeva Approach 4
- Operating Modes 5
- Product Overview 5
- Why Ransomware Reversal? 8

## Why Is Ransomware Going from Bad to Worse?

1. The attack surface has grown due to mass vulnerabilities and an increase in distributed work environments / remote workforce, etc.

2. Ransomware groups partner with delivery services via readily available software development kits (SDKs) to increase their chances of breaching defenses.

3. Cryptocurrency enables easy, untraceable payments.

4. Modern ransomware uses industry-standard unbreakable ciphers to encrypt files and backup systems, assuring that victims cannot recover their data unless they pay the ransom. To make matters worse, ransomware gangs do not always provide reliable decryption solutions even when victims pay the ransom.

5. Ransomware is fast and efficient. In one minute, a single instance of modern ransomware can encrypt 20GB, in 10 minutes 200GB, and in one hour 1.2 TB.

6. Success. The sheer success of attacks has established the ransomware business as a "growth industry." Most experts predict sharp growth in volume, sophistication, and costs of attacks in the coming years.

## Current Gaps in The Ransomware Response

Despite new technologies and best efforts, ransomware continues to get past anti-malware, anti-virus, and next-generation firewalls.

The encryption throughput utilized in an attack enables it to encrypt large amounts of data before EDR, NDR, and XDR systems can detect and respond if they respond at all before it is too late.

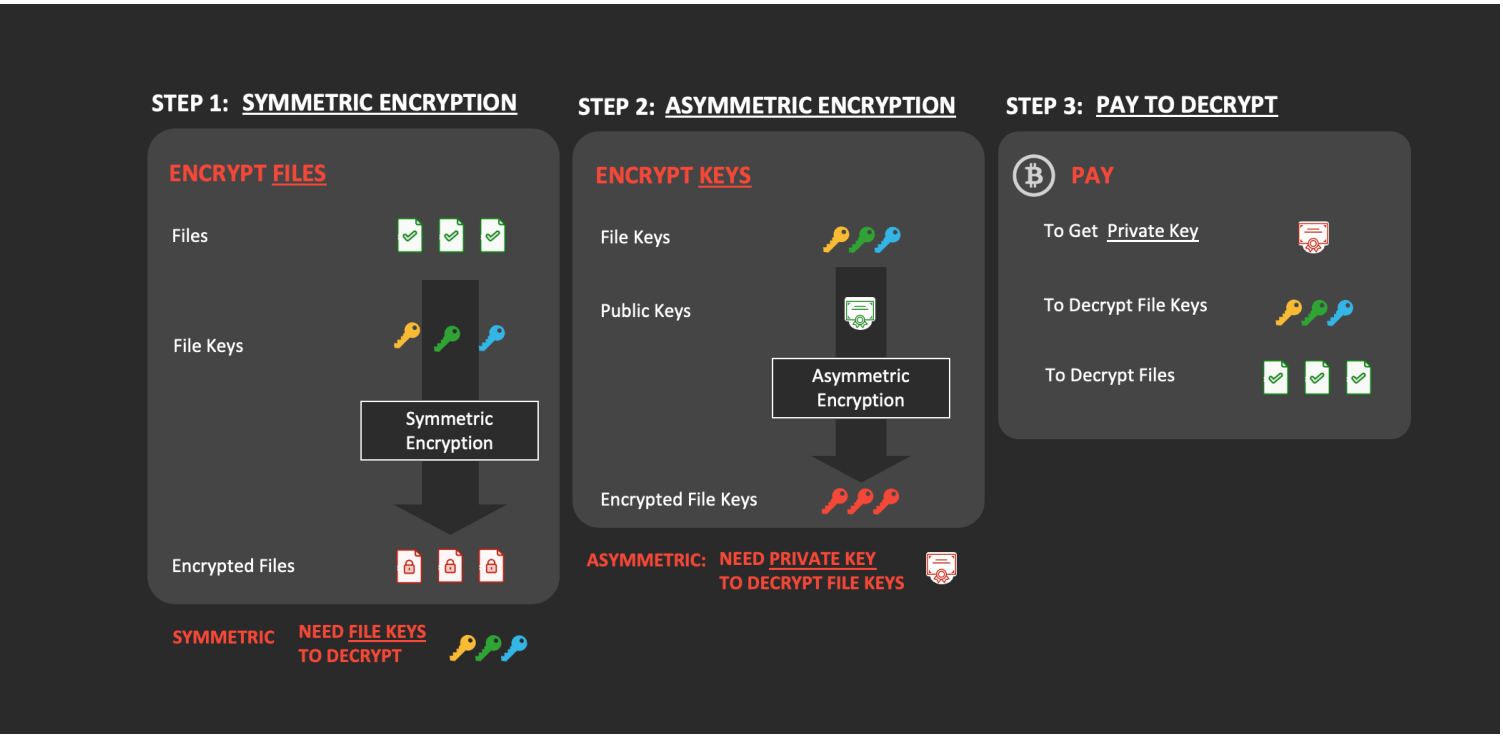
The storage industry offers backup as a means of recovery; however, the average recovery time is twenty-one days.[5] Businesses cannot afford such long downtimes, leading victims to consider the payment as the best option. And real-time backups of everything, "just in case," is costly and operationally unrealistic.

# RANSOMWARE REVERSAL

The missing option for response is giving victims of an attack the power to decrypt ransomed files and recover systems without paying a ransom, regardless of the availability of backups. Nubeva's Ransomware Reversal (NRR) delivers that option. 1) Instantly detects ransomware activity and can immediately alert your SOC/SIEM/SOAR to take quick/decisive action. 2) Restores encrypted data quickly and correctly without restoring from backups or paying the attackers.

## Ransomware Encryption Overview: Modern Ransomware Uses a 2-step Encryption Process

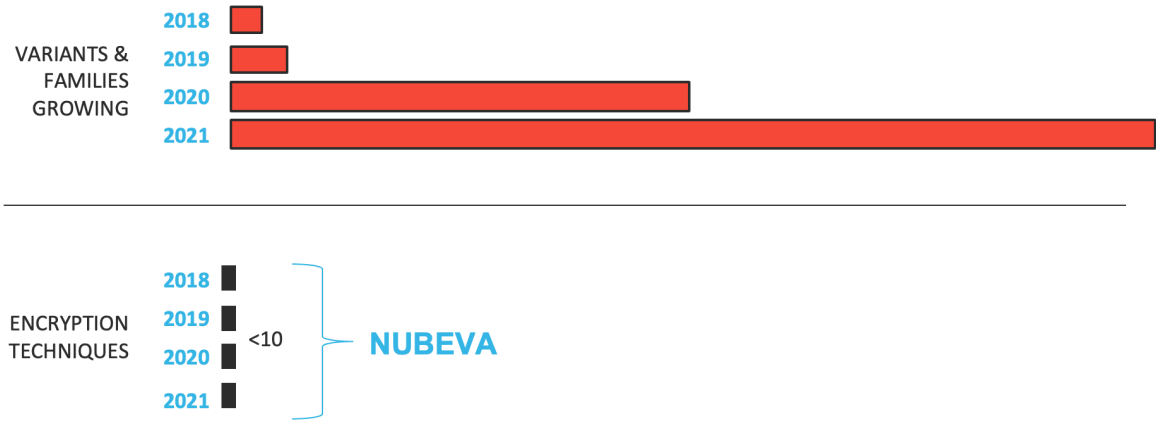
Symmetric encryption is used for data encryption due to its efficiency and throughput, enabling damage without fast detection. After the file's encryption process, they apply asymmetric (e.g., RSA) encryption to lock the keys using a public and private key. Once this step is completed, there is no way to get the files back without obtaining (buying) the private key to recover the file keys (symmetric keys) to unlock the files and data. It has been observed that all modern ransomware uses this approach.



As a result, the only way to decrypt ransomware without paying for the private keys is to get copies of the original files' encryption keys BEFORE they are encrypted with the asymmetric key. This is the basic strategy and approach of the NRR solution. Nubeva has perfected detecting ransomware encryption and intercepting the encryption keys used to encrypt the files. Then, with original file encryption keys available, decryption is not only possible but is straightforward and fast. Nubeva enables the reversal of successful ransomware attacks without paying the ransom for "ransom-less" decryption.

## Ransomless Decryption: A New Approach

Nubeva's solution takes a different approach to ransomware response. While there are tens of thousands of ransomware variants and techniques to evade defense and detection, there are only a handful of encryption methods. Nubeva's proprietary and patented key extraction technology (SKI-Session Key Intercept) automatically detects encryption processes running in applications and processes in real-time and then monitors those code segments to intercept copies of the ransom keys. This function works across shared and kernel services, as well as for static-linked and embedded encryption code in any ransomware. The focus on a very limited scope of functions assures a high percentage of key detection.




The implications of the Nubeva approach are twofold. The first is to decrypt the attack for fast and easy data recovery. The second, and potentially of equal importance and value, is the real-time signaling of ransomware events. More specifically, due to the nature of Nubeva's technology, it captures keys at the moment of ransom encryption. As a result, NRR can alert SOC/SIEM/SOAR of ransoming events in near-real-time to enable automated and rapid response to isolate and contain attacks.

## Operating Modes:

With NRR's ability to detect and intercept encryption, customers are given two choices for operating modes:

Mode 1: Known-Bad. The Nubeva solution filters encryption monitoring to only intercept keys from tested and validated ransomware hashes and family software cores. This model produces exceptionally high fidelity and low noise of signaling of indication of compromise but at the risk of missing new variants.

Mode 2: Universal. The Nubeva solution detects and intercepts all encryption but filters out known-good applications and processes (akin to whitelisting). This model delivers the highest levels of protection but at the cost of the potential to generate signals from some legitimate process representing encryption.

The two operating models enable security teams to employ the model that best fits their risk and operational needs. This can include using both methods across an organization for hybrid coverage—for example, universal for servers and known-bad for clients.

## Product Overview:

NRR is implemented as a small operating system service agent that runs on clients and servers, both of which are vectors for ransomware to encrypt files on local files and shared and mounted volumes. The SKI technology does not require changes to software, libraries, or systems operations and uses negligible memory and CPU. As a single binary, it can be deployed through GPO or any automation tools without restart or built into "golden" images for new systems.

NRR's universal method addresses nearly all ransomware attacks and does not introduce new operational overhead. Existing SOC/SIEM/SOAR solutions provide powerful means for organizations to manage and efficiently reduce operational noise caused by false positives.

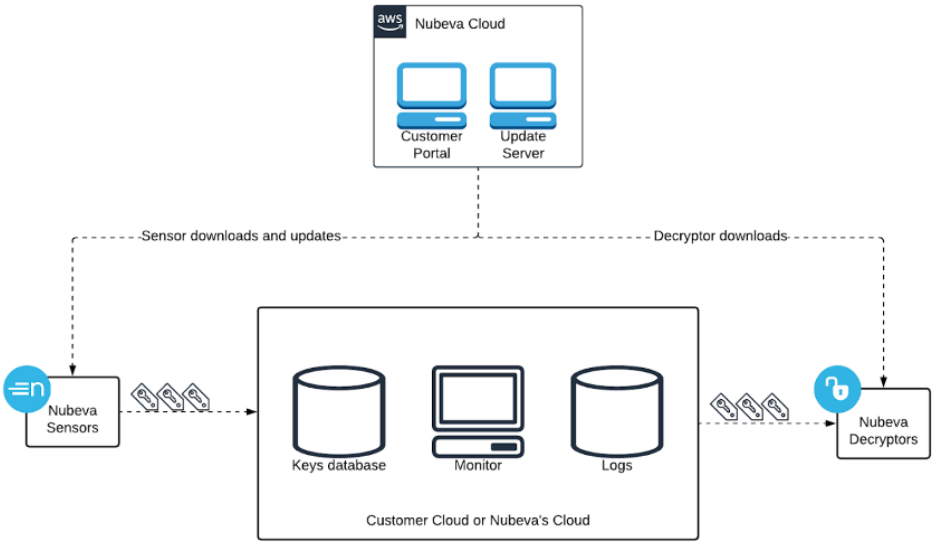
## What are the "Keys"?

Nubeva SKI technology intercepts encryption “keys” to enable decryption. “Keys” are a data record that includes: timestamp, source IP Address, Machine Name/ID, sourcing PID (process id), sourcing Application/Process (file name and path), and the cryptographic key materials itself (keys and nonces). Combined, these elements represent an NRR “Key” record that is saved in several protected and hidden local spaces and exported to a cloud database and provides essential data to enable incident responders in the decryption and recovery process.


```
{
  "hostid": {
    "S": "c46e2b45-b6eb-4f9f-b0aa-5bd5d239896d"
  },
  "uniqueid": {
    "S": "7814de2ac872a879f254a0dab54d74a3f42423b3f5081b8e667762fa1b7e3498"
  },
  "secret": {
    "S": "726f777365720000000000000a000000004f2b0500403d7f5b02000030cb2c05"
  },
  "projectid": {
    "S": "e8SoCT9IFkmLKxENHxY2THX1LjnRkYVzgN2QiDpBYXICXqmiTFIElBGgkdcGAdSX"
  },
  "metadata": {
    "S": "{\"Pid\":16848,\"Flags\":0,\"Handle\":0,\"Ticks\":0,\"ProcessName\":\"AcWebBrowser.exe\",\"ProcessVersion\":\"2.0.5.100\"}"
  },
  "index": {
    "S": "f0b62e05c8d16900"
  },
  "encmethod": {
    "S": "Salsa20"
  }
}
```


## Solution Architecture

Nubeva’s NRR solution is depicted below. The system has been architected using cloud models to enable global availability, resilience, and economic scaling. The entire architecture is stateless and enables enterprise and service providers to enhance or modify components to specific needs without jeopardizing functionality or supportability.



## Ransomware Reversal: Product Components

1) Sensors: a sensor is a fire-and-forget Windows executable that run on Windows clients and servers. Sensors constantly check the SaaS backend for new versions and automatically update themselves. When sensors detect encryption by a known or suspicious process, they can trigger an alert while extracting the encryption keys and metadata that associate the key with the file and storing this information in the cloud database and on the local disk.

2) Key Database: the database can be either AWS DynamoDB or Azure's Cosmos DB. Nubeva provides provisioning scripts to create the required tables in the respective database based on the users' preferences. The key database can run inside a user's own private cloud subscription, inside a MSSP's cloud, or in Nubeva's cloud.

3) Logging: AWS CloudWatch or Azure Monitor stores sensor heartbeats and key extraction events. Nubeva's SaaS backend runs dedicated Grafana containers with built-in dashboards that connect to the cloud log services chosen by the user. Users may also run monitoring containers in their networks. Customers have the option to run in private subscription, in their service providers, or in Nubeva's cloud, depending on the product version and source chosen. Cyber teams can easily configure these off-the-shelf cloud systems to redirect logs and alerts to private enterprise systems.

4) Nubeva's Cloud Backend: The customer portal provides IT and Security teams access to software and documentation and optionally runs a visualizer GUI to monitor the number of sensors in service and key events. Additionally, Nubeva maintains global, resilient sensor update servers that enable sensors to download updates automatically and silently without restarts.

5) Decryptors: Nubeva provides a growing library of automated decryptors. These utilities automatically read and match keys to encrypted files and decrypt them at the same speeds at which they were encrypted. Nubeva provides these decryptors, usage notes and documentation, and support services to aid Incident Response (IR) teams in speedy recoveries. In the event that Nubeva does not have decryptors available for a new variant, Nubeva's product includes a decryptor creation service to build and deliver working decryptors.

## Why Ransomware Reversal?

Nubeva NRR provides a new, essential layer of defense in the fight against ransomware. NRR delivers a safety net in the gap between cybersecurity and backup systems. While these remain vital to every organization, they are increasingly insufficient in the face of the rising threat of ransomware.

NRR is easy to implement. Sensors do not have a startup delay, all encryption keys are captured and safely stored, and Decryptors are fast and reliable. NRR can trigger an alert at the moment encryption beings. And in the event of a successful attack, NRR restores data as fast as it was encrypted. After the malware is removed, an organization can fully recover from a ransomware attack within hours rather than weeks or months, without paying the ransom and without restoring from backups.

## Complements Current Cybersecurity Defense Stacks:

Modern cyber security systems primarily attempt to block threats. When that fails, they aim to detect ransomware within 1 minute, understand the attack within 10 minutes, and entirely block it within an hour. During this time, a single instance of modern ransomware can encrypt 20GB, 200GB, and 1.2 TB, respectively. The damage is multiplied across infected systems. Faster versions of ransomware can encrypt much more data in the same amount of time. The time to recover 1TB of data can be days. The total downtime when backups are available is measured in weeks. Downtime and lost data have significant business implications.

The fact remains that many organizations cannot afford to purchase and implement, let alone correctly operate all of the cyber controls required for the highest levels of defense. This has created a significant window of opportunity for execution by ransomware actors. Nubeva provides an enhanced detection capability and fills gaps as a backstop for the most sophisticated cybersecurity programs or as a critical and immediate control for the less mature organizations.

## Complements Backup and Restore Systems:

Every organization should invest in backup and recovery solutions. However, increasingly, modern ransomware has built-in steps to disable or corrupt snapshots, drive mirrors, and other backups to create data gaps to exploit and maximize the ransom opportunity. Similarly, not every organization can afford to implement and operate real-time backup systems of all critical data.

In reality, the best-case scenario to restore from backups is typically 5-7 days. Nubeva provides an effective backstop to backup system corruptions and can reduce frequencies and volumes of backups driven by ransomware risk to help reduce costs.

## Business Value:

The net value of Nubeva reduces the damage of successful ransomware attacks. By triggering earlier detection and enabling fast and easy data recovery, Nubeva provides a new form of technical insurance and data assurance to this global threat by providing a path to faster and easier data recovery.

For organizations with mature cybersecurity systems, NRR becomes a new layer of defense. For less mature organizations NRR offers a critical solution to handle the likely eventuality of an attack.

Learn More and Request a Demo: www.nubeva.com/ransomware_reversal

Nubeva is at the forefront of modern network visibility. We are committed to solving problems for our customers, the industries they serve, and the connected world as a whole, so we can progress forward, together, with clarity and confidence. Our cutting-edge decryption technologies give customers unprecedented network visibility and protection from cyber threats.

Learn More: www.nubeva.com
333 W San Carlos St. Suite 600
San Jose, CA 95110
info@nubeva.com

REFERENCES:

(1) Ransomware Prevention and Response for CISOs — FBI. FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf.

(2) The George Washington University. “What Is Cyber Analytics?” GW Cybersecurity Online, The George Washington University, 19 Nov. 2021, https://onlinecybersecurity.seas.gwu.edu/news/what-is-cyber-analytics/#:~:text=In%202015%2C%20ransomware%20damages%20worldwide,percent%20each%20year%20through%202026.

(3) “Ransomware Recovery Cost Reaches Nearly $2 Million, More Than Doubling in a Year, Sophos Survey Shows.” Ransomware Recovery Cost Reaches Nearly $2 Million, More than Doubling in a Year, Sophos Survey Shows, Sophos, 27 Apr. 2021, https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.

(4) Sjouwerman, Stu. “Council Post: Seven Factors Analyzing Ransomware's Cost to Business.” Forbes, Forbes Magazine, 29 July 2021, https://www.forbes.com/sites/forbestechcouncil/2021/07/29/seven-factors-analyzing-ransomwares-cost-to-business/?sh=15a271ef2e98.

(5) “Downtime: The Real Cost of Ransomware.” Security Boulevard, Delphix, 29 Sept. 2021, https://securityboulevard.com/2021/09/downtime-the-real-cost-of-ransomware/.