NUBEVA TLS DECRYPT

A New Way to See TLS Encrypted Traffic for Your Public and Private Cloud

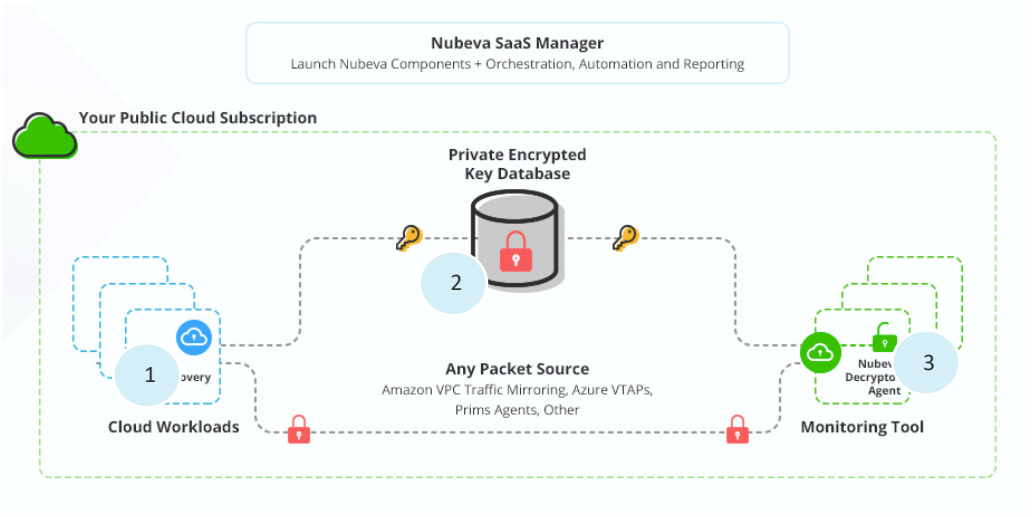
NUBEVA

Universal TLS Decryption Solution

Strong, end-to-end encryption is a top recommendation for securing applications across public, private and hybrid cloud infrastructures. In fact, Over 70% of network traffic is encrypted and that percentage is growing. With stricter encryption standards such as TLS 1.3, Elliptic Curve Diffie Hillman (EDDH), Perfect Forward Secrecy (PFS) and pinned certificates, traditional decryption methods are failing and out-of-band solutions no longer work in public, private and hybrid clouds.

Until now. Nubeva's TLS Decrypt solution enables out-of-band, decrypted visibility in the cloud. With patent-pending symmetric key intercept approach, Nubeva eliminates the "either/or" conundrum of security or visibility.

Nubeva TLS Decrypt: The Industries Only Solution for Total TLS Visibility



Nubeva TLS Decrypt is an out-of-band solution to enable security and devops tools to inspect and monitor their data. Nubeva offers a born-in-the-cloud architecture that solves for next-generation encryption like TLS 1.3, ECDHE, PFS and pinned certificates. Our software works with any packet source, in any cloud including AWS, Azure and Google as well as private cloud. No code, library or architecture changes are required which empowers organizations to aggressively adopt next-generation encryption standards for security without compromising critical visibility regardless of cloud strategy or monitoring tools.

How TLS Decrypt Works: Symmetric Key Intercept

1

Key Discovery

Nubeva TLS Key Discovery probe is a lightweight, read-only, container agent that runs on any cloud workload including VMs, containers and Kubernetes clusters. It detects and extracts symmetric keys after the TLS handshake with nearly zero impact on CPU and memory. This method uses AI and machine learning based rules to identify symmetric keys from either side of the TLS handshake (client or server) without changes to application configurations or workload restarts.

2

Key Storage

Detected keys are securely sent to a customer owned, key database in the customer's own cloud subscription. The symmetric keys are encrypted and stored. The encrypted key database retains the keys for security and monitoring tools and enables them to perform parallel, decentralized and scalable decryption when and where needed; whether for full time monitoring, on-demand or on point-servers. Keys may be purged or stored for as long or as little as the customer wants.

3

Secure SSL/TLS Decryption

Decryption of replicated traffic happens on the tool workload using the containerized Nubeva Decryptor agent. Traffic may come from any packet replication source or stored pcap. This decryptor synchronizes and buffers incoming encrypted packet traffic and pairs it with the correct symmetric key, retrieved from the database. Decryption is high-speed and happens right on the tool of choice so decrypted traffic is never passed across the network. Both the originally encrypted and decrypted traffic are sent to the tool so that encrypted traffic headers can be inspected as well as the decrypted payload. The decryptor supports the the newest ciphers including AES-GCM and ChaCha20 (AEAD).

Decryption Use Cases

- **Threat Hunting:** Encrypted packet traffic can hide security threats such as malware, phishing attempts, data exfiltration and internal data leaks. With a majority of traffic being encrypted, the data may be secure but security teams lose the visibility to monitor indicators of compromises, threats and active attacks. Decryption allows deep packet and payload inspection for threat hunters and their tools.

- **Incident Response:** Should an incident occur, the ability to access broad and pervasive (and preferably historical) decrypted traffic will enable incident responders to perform deep forensic analysis.

- **Compliance:** Certain industries like banking, finance, healthcare and others face compliance standards for deep packet inspection, which is not possible without a decryption solution. This results in organizations delaying cloud adoption or suffering the consequences.

- **Application and Network DevOps:** It is not just security teams that benefit from decryption visibility in the cloud. Decrypted traffic enables rapid troubleshooting, debugging, and support of applications or services in order to get a quick, complete and timely view of what is going wrong.

NUBEVA

Higher Security Than Previous Decryption Methods

Nubeva's Symmetric Key Intercept architecture was built for use in the cloud with modern encryption standards. The security of your data was at the forefront of development of our patent pending solution. There are four core components to the security of our software:

Keys

- Symmetric keys are only relevant to a single session.
- With the introduction of perfect forward secrecy there are no longer master "keys to the kingdom". Any stored keys can be regularly purged.

Database

- The symmetric keyDB is created and owned within the client's cloud and governed by the client's IAM rules. Nubeva has no access.
- Keys are encrypted in transit and in the secure DB at rest.

Agents

- Lightweight agents are read-only and cannot modify the host.
- There is no inbound contact with the agent and can only talk to to host to pull key signatures.

Architecture

- Keys and the packets run in parallel, never together and never leave your environment,.
- The manager only contacts these agents through an outbound rest call.

Why Nubeva:

Nubeva has the Industry's ONLY Solution for Total Visibility of Modern TLS.

1. **Universal TLS Decryption Coverage :** Handles all TLS encryption ciphers including TLS 1.3 and TLS 1.2 with PFS and ECDH and supports both TLS client and TLS server side connections.
2. **100% Passive, Out of Band, Overlay Solution:** Nubeva requires no app or library changes, has no network or architecture restrictions and has no certificates or PKI requirements.
3. **High Security:** Data and keys never leave your environment and the secure database is hosted in your subscription with your IAM rules. Data is never transmitted over the network in clear text form.
4. **Cloud Native:** Our solution is modular, auto-scales and auto-updates. We support restocking and regular workload refreshes without impact.
5. **Open and Flexible:** Universal solution that works with any packet source, any tool, any use case with any cloud – public, private and hybrid.
6. **Disruptive Pricing** : Nubeva is offered at <1/5th the cost of traditional decryption solutions and it is easy to get started and use, thereby unlocking modern decrypted visibility for everyone, anywhere.

Get Started for Free

www.nubeva.com/decryption

Cloud Visibility. Unlocked.

Nubeva TLS Decrypt the only solution for universal TLS visibility in the cloud.