NUBEVA TLS DECRYPT

A New Way to See Modern SSL/TLS
Encrypted Traffic Out-of-Band.

NUBEVA

Universal SSL/TLS Decryption Solution

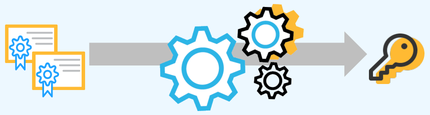
Strong, end-to-end encryption is a top recommendation for securing applications across the network. In fact, more than 70% of network traffic is encrypted and that percentage is growing. With stricter encryption standards such as TLS 1.3, Elliptic-curve Diffie-Hellman (ECDH), Perfect Forward Secrecy (PFS) and pinned certificates, traditional out-of-band decryption solutions no longer work. And, with no "middle" in the modern cloud architectures, in-line solutions add costs and complications, making them unsustainable.

Nubeva's TLS Decrypt solution re-enables passive, decrypted visibility for modern TLS. With our patent-pending Symmetric Key Intercept approach, Nubeva eliminates the "either/or" conundrum between network security or network visibility.

What is Changing in Modern Decryption?

Legacy Decryption

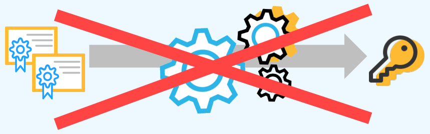
can (re)generate out-of-band



Before PFS and ECDH, a legacy out-of-band decryption system, could regenerate keys using the certificates in the packets, and ultimately get the keys and decrypt each session.

DH/PFS/TLS1.3

Can **NOT** (re)generate out-of-band

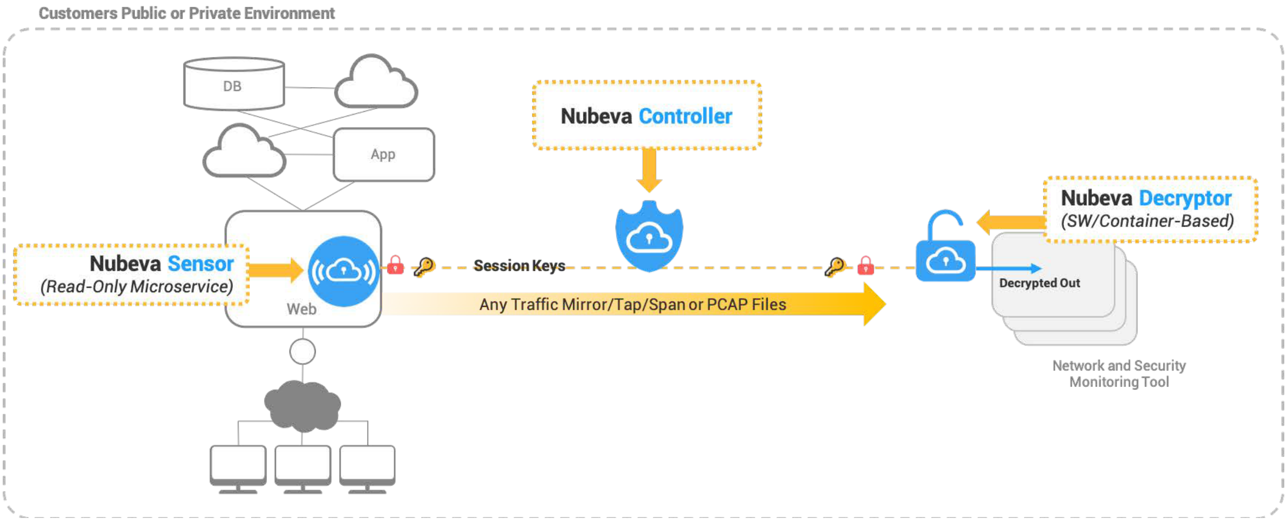


With modern TLS, client talks to server and completes a handshake to create a symmetric session key. In modern TLS users no longer regenerate keys to decrypt.

Nubeva's TLS Decrypt allows you to re-discover and extract the symmetric keys with security, and scale without any changes to the code or the libraries on either side.

Nubeva TLS Decrypt: The Only Solution for Total SSL/TLS Visibility

Nubeva TLS Decrypt re-enables the ability to inspect and monitor decrypted network data out-of-band, solving for modern TLS 1.3, ECDHE, PFS and pinned certificates. Our solution was built from modern computing and is open, scalable and affordable.



Nubeva Sensor - Real Time Symmetric Key Discovery

Deploy the lightweight, read-only, Nubeva Sensor on any cloud workload including VMs, containers and Kubernetes clusters. It detects and extracts symmetric keys on either the client or server-side after the TLS handshake. Our Container technology has nearly zero impact on CPU and memory and requires application configurations changes or workload restarts.

Nubeva Decryptor - Decrypt Stream and Files on Any Tool

Decryption of replicated traffic happens on your tool workload of choice. The Decryptor synchronizes the incoming encrypted packet traffic from any traffic mirror, tap, span or PCAP files, pairs it with the correct symmetric key, sent from the Nubeva Sensor, to decrypt the traffic and maintain end-to-end encryption.

Nubeva Controller - Symmetric Key Store for Buffering, Scaling and Retention

The Nubeva Controller enables decryption at scale. The store and forward capability, allows users to decrypt on multiple tools in parallel. The session-specific keys can be stored for a minute or in perpetuity in a customer-secure database as defined by user.

Decryption Use Cases

Our customers trust Nubeva to bring visibility back to core tools and teams and as such, reduce time to resolution, improve security and enhance existing tools and processes.

- Threat detection and threat hunting
- Security response
- N/S, E/W command & control traffic visibility
- DevOps support and troubleshooting
- Historical PCAP indexing
- Container to container monitoring
- Enhance network packet brokers
- Compliance requirements

Why Nubeva TLS Decrypt:

Universal Coverage : Only universal out-of-band solution on the market. Handles all TLS encryption ciphers including TLS 1.3 and TLS 1.2 with PFS and ECDH and most legacy ciphers.

Open and Flexible: Flexible deployment enabling N/S - E/W visibility. Works with any packet source, any tool and anywhere whether public, private cloud and on-prem.

Security: Nubeva TLS is inherently more secure than other solutions. Combined with the innate security of TLS 1.3, Nubeva's split plane architecture and optionality for private deployment allows organizations to maintain secure end-to-end encryption while providing teams and tools the visibility needed for monitoring.

Scalability: As a software, viable for a single individual to scaling to 100,000s of sensors, billions of keys and can decrypt petabytes of data to enable systemic cloud wide-monitoring.

$

Disruptive Pricing : Nubeva is offered at <1/5th the cost of traditional decryption solutions and with simple implementation to unlocking modern decrypted visibility for everyone, anywhere.

Get Started for Free

www.nubeva.com/product

Cloud Visibility. Unlocked.

Nubeva TLS Decrypt the only solution for modern TLS universal visibility.