

# Why Modern DevSecOps Needs Decrypted Visibility



**NUBEVA**



During the past several decades, IT and standards bodies worked to develop strong, reliable encryption. With the adoption of TLS 1.3, we benefit from many security and performance improvements. Encrypted connections are now more secure and faster than ever. But you can't secure what you can't see. Network security and DevOps teams need total visibility into decrypted packet payloads for optimal security.

In the following pages, we look at the ins and outs of decrypting encrypted traffic in the public and private cloud. And, we provide some how-to advice designed to help your IT team embrace decryption without exposing data to more risk.

## Contents

Network Encryption Adoption is on the Rise, and That's Good.....	3
Encryption Everywhere Matters.....	6
Why SecOps Needs Decrypted Visibility .....	8
A New Out-Of-Band Solution to Get Total Visibility of Your Encrypted Traffic.....	14
A Word about Compliance and Your Protected Data .....	18
Ready to Get Started?.....	19

# Network Encryption Adoption is on the Rise, and That's Good.

“...encryption thwarts interception of your information and ensures the integrity of information that you send and receive.”

It's 2020 and more than [90% of web traffic to Google](#) is encrypted. And Google's goal is to reach 100% encrypted traffic across all Google products and services. Encryption makes sense because it is designed to keep us safe.

“HTTPS web connections protect against eavesdroppers, man-in-the-middle attacks, and hijackers who attempt to spoof a trusted website. In other words, encryption thwarts interception of your information and ensures the integrity of information that you send and receive. Because older hardware and software often don't support modern encryption technologies, users of these devices may be more vulnerable to security threats.”<sup>1</sup>

[In a survey conducted by Enterprise Management Associates](#), 31% of respondents said their organization's use of encryption rose between 26% to 50% in a 18-month period from 2017 to 2019.<sup>2</sup>

In addition to Google, Apple, Microsoft, most other large web server and browser vendors have implemented the new encryption standards in an effort to ensure critical data is protected and safe. These new standards have all contributed to accelerate TLS 1.3 adoption.

What's more, the new TLS 1.3 standards have pressed enterprises to accelerate adoption of the new protocol. According to the Enterprise Management Associates study, TLS 1.3 adoption is driven primarily by the need for data security and privacy (73% and 67% respectively).<sup>3</sup>



## SO WHY TLS 1.3? THE SIMPLE ANSWER: “IT’S SUPERIOR.”

TLS 1.3 removes the vulnerable and dated elements of TLS 1.2, which was first defined in 2009 and refined in 2011. The newly adopted protocol enforces perfect forward secrecy (PFS). PFS makes the encryption stronger and makes its duration shorter and requires that each session has new encryption (0-RTT notwithstanding since it is rarely enabled by default and support for 0-RTT is, at the time of this writing, limited). In this way TLS 1.3 makes:

- Encryption keys stronger
- Encryption keys ephemeral — they last for only a few seconds before a new key is required
- Encryption only apply to the packets in the session in which the keys were created

This means that even in the unlikely event that a packet and its key are intercepted and cracked, that key cannot be used to decrypt and read other traffic.

This is a fundamental and important shift from the old-school RSA key exchange that previous decryption solutions required.

With RSA key exchanges, the same key was used for a longer period of time to encrypt and decrypt many sessions, requests, traffic and communications between a server and many clients. With new PFS, not only does each client-server pair have its own unique key (keys are not shared) but each key only lasts for a single session (or even more quickly with configuration).



“TLS 1.3 leaves out insecure and outdated elements obtainable in TLS 1.2, such as AES-CBC, SHA-1, DES, RC4, MD5, 3-DES, EXPORT-strength ciphers (responsible for FREAK and LogJam) and arbitrary Diffie-Hellman groups (CVE-2016-0701),” writes Rohan Pinto, CTO/Founder of 1Kosmos BlockID. “Also, TLS 1.3 supports PFS by default. The cryptographic method includes an additional layer of privacy to an encrypted period, making certain that the two endpoints are the only ones capable of decrypting the traffic.”<sup>4</sup>


PFS mandates strong encryption like Elliptic Curve Diffie-Hellman Ephemeral (ECDHE), which creates a unique, one-time use, symmetric, session key that is just for a single session. Because of how ECDHE works, the unique session key is known by the server and the client but cannot be derived from any of the shared information in the initial TLS Handshake.

Compromising an encryption key does not expose other communications between that server and client since the keys are only good for a single session.

“

**TLS 1.3 supports PFS by default. The cryptographic method includes an additional layer of privacy to an encrypted period, making certain that the two endpoints are the only ones capable of decrypting the traffic.<sup>4</sup>**

*Rohan Pinto, CTO/Founder of 1Kosmos BlockID*



It is equally important to encrypt east-west traffic – for example, the traffic running from server to server within a data center. This traffic is dynamic, distributed and decentralized: Modern application architectures require encryption for safety as they communicate amongst themselves. And, with modern compute environments, IT must address new network architectures presented by public clouds, Kubernetes and containers.

## A Few Definitions

### **Dynamic**

Scaling up and down. Short lived compute workloads might be compromised and then cease to exist. How do you verify threats, trace lateral movement and identify weak points?

### **Decentralized**

Collections of connected workloads, some of which are yours, some of which belong to others. You don't control the encryption coming in from other systems that you rely upon like libraries, API calls, etc.

### **Distributed**

Live in many places: many geographies, many types of workloads that require ad hoc and on demand networks to connect them as needed.



In cloud subscriptions like **AWS, Azure and Google**, the networks are more ephemeral and elastic. Workloads pop into and out of existence, making tracing and root cause even more important. As a result, there is no well-defined perimeter. Everything is “middle” in the cloud.

**Kubernetes** is designed to run distributed systems in a cluster of machines. These distributed systems make networking a central and necessary component of Kubernetes deployment. Understanding the Kubernetes networking model enables network architects to correctly run, monitor and troubleshoot your applications running on Kubernetes. In an internal Kubernetes networking environment, there are no fixed IP addresses, but inspection still matters.

**Containers** are small and agile, and teams update them all the time. They require a dynamic architecture around continuous deployment, management and networking infrastructure.

Scale in a container based software world leads to new requirements. Where in the past enterprise solutions ran in a handful of virtual machines, in a container world the number of micro service instances can grow dramatically. This architecture is highly distributed and includes many connection points.

The 2019 Cyber Security Breaches survey found that spyware or malware attacks were identified by

**27%**

of businesses over the past year.<sup>5</sup>

Source: *Encryption: 2020's Double-edged Sword*, TechRadar, Dec. 2019



When you decrypt, you're getting access to packet data to inspect the details of that traffic – web-based email, traffic to unknown sites, communication with business partners, and online storage and file sharing. Decrypting and inspecting this traffic helps protect network assets from malware, data loss prevention, and conformance to data sharing policies. Having visibility into decrypted traffic is vital to ensure insight into any potential threat.

## Decryption

is the process of decoding traffic to render it for consumption; however, between the sender and receiver, all data are transmitted in a cyphered traffic stream.

## Encryption

gives us reasonable security when performing financial transactions and conducting business with trusted agents. We're ensured that communications can't be deciphered by a third party, and the data is only shared with appropriate parties.

Encrypted traffic also presents threats to your data security. Encryption prevents you from seeing into what traffic is egressing your network. In fact, in a survey of CIOs conducted by Vanson Bourne, 90% of respondents said their organization had experienced – or expect to experience – a network attack using SSL or TLS encryption during the course of this year. In addition, the 2019 Cyber Security Breaches survey found that spyware or malware attacks were identified by 27% of businesses over the past year.<sup>5</sup>





While encryption helps to secure data, it is also used to hide botnets, command and control traffic, malware, and viruses traversing the network. When you can't see encrypted traffic, you're exposed to potential threats.

Clearly, we should all be concerned about how this lack of visibility created by new encryption protocols impacts security. 87% of CIOs believe their security defenses are less effective [when] they cannot inspect encrypted network traffic for attacks. A new solution is therefore required if organizations are to take advantage of the benefits of encryption, yet ensure they are not subject to this new type of threat.<sup>6</sup>



# 87%

of CIOs believe their security defenses are less effective [when] they cannot inspect encrypted network traffic for attacks.

*Source: Encryption: 2020's Double-edged Sword, TechRadar, Dec. 2019*



# The Pros and Cons

	Encrypted Traffic	Decrypted Traffic
Uses TLS 1.3 protocols to enhance security and allow users to trust that sensitive transactions and communications are more secure	☒	
Requires all-encompassing security and data protection policies	☒	
Enables bad actors to hide their malicious activity in traffic	☒	
Provides a false sense of security	☒	
Helps to prevent hidden threats, malware, attacks and data leakage		☒
Increases accuracy of security and analytics tools		☒
Makes obvious privilege escalation and authentication attempts to applications and workloads		☒
Reveals SQL injection attacks		☒
Reveals lateral movement		☒
Reveals command and control communication		☒
Makes API calls readable		☒
Reveals inbound malicious threats		☒
Enables application performance troubleshooting		☒
Helps to distinguish between expected traffic and payload from anomalous and dangerous ones		☒



Obviously encryption is important for security, but decrypted visibility is imperative to maintain security and prevent bad actors from using encryption to hide their activities.

Clearly, not encrypting is not an option, even when network traffic has successfully passed a traditional perimeter. Full payload inspection and monitoring of network traffic is critical for security, but encryption hinders it.

Fortunately, you can analyze full packets and payload of encrypted network traffic that uses SSL/TLS protocols. The trick is knowing how to decrypt the encrypted traffic in a safe, efficient and effective way.

**Clearly, not encrypting is not an option, even when network traffic has successfully passed a traditional perimeter.**



## Problems with In-Line Decryption

- It's slow and resource intensive
- Relies on firmware/hardware to decrypt
- Introduces latency
- Architecturally impractical to "hairpin" all traffic through a central chokepoint
- Eliminates the advantages of a distributed, dynamic and decentralized cloud architecture
- Eats workload resources and adds operational costs
- Increases risk and exposure by downgrading encryption
- Financially irresponsible to add a device in every "middle"

## IN-LINE DECRYPTION IS NOT A LONG-TERM SOLUTION.

In-line decryption, like in a firewall or in-line security device, is slow and resource intensive. While TLS 1.3 ensures a greater level of security, it flags non-terminating decryption attempts as a man-in-the-middle (MITM) attack, terminating the session before malicious or legitimate traffic can be distinguished.

Using TLS 1.3 standards, certificates are encrypted, which means the proxy in the middle must establish a full TLS session before it can see the certificate details and then determine a site category. At this point it can no longer drop out of the session and hand it back to the client. So, users must either proxy and decrypt everything (reducing performance) or find an alternative method to derive the site category without establishing the full session.

*"...the decryption process is painfully slow and compute intensive. Drawbacks such as a degradation of the user experience, poor performance, and unexpected blocking of legitimate traffic are not uncommon. As a result, some organizations forgo decryption altogether, allowing unscanned traffic into their networks and putting their entire cyber infrastructure at risk."*<sup>7</sup>

In addition to firewall and proxy solutions being slow and incapable of decrypting TLS 1.3, it's important to recognize that there is no middle in the cloud, so it's impossible to terminate, inspect, re-encrypt and send data on to its destination in cloud environments. What's more, adoption rates of Kubernetes continues to soar. Kubernetes pod to pod, container to container traffic is invisible. Connections and workloads are not only ephemeral, they're in constant motion as the orchestrator continually optimized workload resources, connections and internal networks. Kubernetes makes pinning down a workload and its connections next to impossible. Where do you drop a device?

# A New Out-Of-Band Solution to Get Total Visibility of Your Encrypted Traffic

Because of out-of-band's many advantages, a new innovation that makes out-of-band decryption work has been created – and it works with the latest TLS 1.3 protocols and ciphers.

## HOW NUBEVA TLS DECRYPTION WORKS.

Nubeva TLS Decrypt is the only out-of-band decryption solution that works on TLS 1.3 as well as with all earlier encryption standards, protocols and ciphers. This solution is not a proxy. It is out of band and therefore it will never terminate an existing TLS connection or downgrade encryption in an intercept-terminate-inspect-re-encrypt-send-on cycle.

### **What does this mean for you and your traffic inspection requirements?**

- It means your connections are safer
- It means your data integrity is preserved
- It means your chain of custody is faultless
- It means clear text is not sent over the wire

The tools you use today for inspection, detection, DLP, APT, threat hunting and troubleshooting require packet data to get to the bottom of the matter and ensure correct validation in one pass. Nubeva TLS Decrypt feeds your tools with the clear text at the tool itself – keeping the workload secure.

Modern decryption for PFS and TLS 1.3 require two things: a) the mirrored packet traffic, and b) the symmetric encryption key. Nubeva works with any tool and any packet source, whether in the public cloud, in a private cloud or in your data center.

This solution works with existing taps and spans as well as cloud taps like Amazon VPC traffic mirrors, Microsoft Vtaps, Google packet mirroring – virtually any commercial taps from tech leaders like Garland and packet brokers like Gigamon, Ixia, and others.



**Nubeva can also handle your packet mirroring duties — capturing and mirroring packet traffic from inside Kubernetes clusters, including:**

- Container to container traffic inside the same Kubernetes pod
- Container to container traffic between Kubernetes pods
- Inter and intra container traffic from any workload into Kubernetes
- Inter and intra container traffic from stand-alone containers or Docker managed containers
- VM to VM traffic

Nubeva TLS Decrypt discovers the symmetric encryption keys from working memory during the TLS Handshake from or to any workload. The solution can use either Kubernetes Daemon Sets to accomplish this or a read-only sensor. It's not an agent, and there is no kernel modification.

This out-of-band solution then uses AI-based rules and signatures to identify and continually learn where in memory the symmetric keys will appear. There is never a need to alter SSL configurations or change libraries or application settings. Nubeva discovers the keys at line rate on its own with no outside help. As fast as the keys can be generated, they are available. And because TLS Decrypt is host based, it can run in any cloud or data center environment.

Nubeva is designed to provide security tools, DevSecOps users and security processes with both the originally encrypted and fully decrypted packet streams. With this information in hand, important encrypted stream metadata is preserved for analysis and fingerprinting, while the decrypted streams are made available to your tools for inspection.



Once obtained, the mirrored packet traffic is sent to your tool(s) or load balanced destinations. The software based decryptor runs as a container right on the tool destination of your choice or in stand-alone mode. You can use it to build your own software based decryption appliance that runs in your secure decryption zone or dedicated compliance security VPC/VNET.

This gives you the ultimate flexibility in complying with regulatory standards like PCI, HIPAA, GDPR, FIPS and others. The Nubeva decryptor also reads in files like pcaps from storage, buffers incoming encrypted streams, securely retrieves and matches the correct symmetric encryption key for the packet, and provides both the originally encrypted packet with all header data intact in addition to the newly decrypted packet, also complete with all header data.

Because you always control the mirroring, you get to choose what data to send to the decryptor and what data to ignore. With this control, you get on-demand decryption, for example, in the case of an alert or event trigger. Because the decryptor can be deployed directly on the inspection and detection tools, no clear text data – including regulated data – traverses the network.

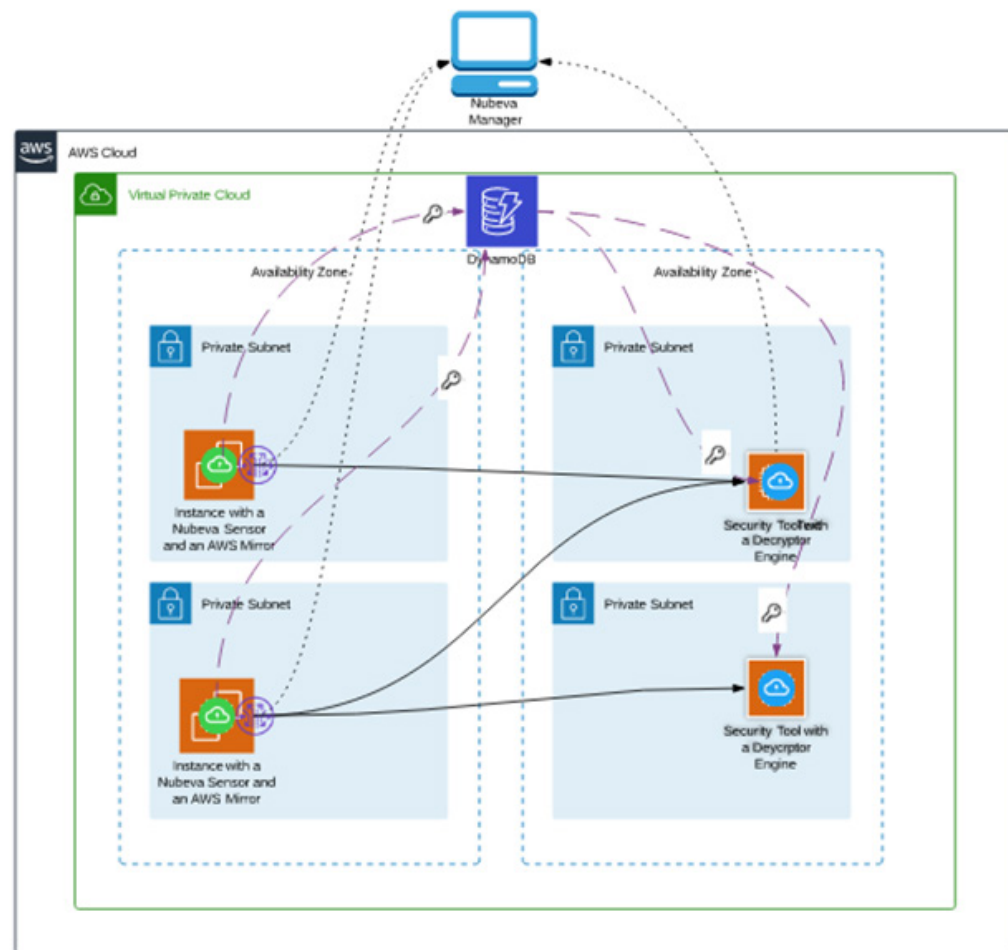
Nubeva provides policy-based mirroring and decryption controls as well as strong access controls, allowing both DevOps and SecOps teams to have full visibility without jeopardizing compliance and regulatory control.

**Because you always control the mirroring, you get to choose what data to send to the decryptor and what data to ignore.**

## Decryption Made Easy with Nubeva TLS Decrypt

- Both symmetric key discovery and retrieval are protected with TLS 1.3
- There is no need to daisy-chain tools or worry about clear text packet traffic making its way around multiple EW networks
- No need to upload RSA keys, adjust certificates, alter workloads or application libraries, or tell the Nubeva Key Discovery Daemon Set / Sensor where to look

Nubeva provides policy-based mirroring and decryption controls as well as strong access controls, allowing both DevOps and SecOps teams to have full visibility without jeopardizing compliance and regulatory control.







As the diagram on the previous page depicts, Nubeva uses Symmetric Key Intercept decryption. It is the only TLS decryption solution to offer it in a fully cloud-native and infinitely scalable way. Nubeva TLS Decrypt decouples symmetric key discovery from the final act of decryption with a unique store-and-forward key-plane architecture. The Nubeva Kubernetes Daemon Set, or read-only Key Discovery sensor, securely sends the symmetric key to the symmetric key depot. There it can be preserved as long as needed or flushed as rapidly as desired. The Nubeva decryptor receives mirrored and tapped packets, then retrieves the correct symmetric key from the key store. Multiple decryptors receiving the same mirrored packets can each retrieve the same symmetric key corresponding to that packet. This architecture allows unlimited parallel, balanced processing across multiple tools.

[Click here](#) for more details about how Nubeva TLS Decrypt works with open source tools like Wireshark, Moloch, Suricata, Ntop and Zeek.

# A Word about Compliance and Your Protected Data

Because Nubeva is focused solely on decryption, your compliance, regulatory and other access control policies remain untouched and intact. Nubeva outputs decrypted packet traffic to tools at the tool destination. The settings and controls placed on your tools to guarantee and enforce access requirements never need to be changed.

If you're a security project owner or a super administrator, or somewhere in between, then you're a potential user of Nubeva TLS Decrypt.

- Security professionals and SOC managers responsible for ensuring their cybersecurity tools have access to full, decrypted network packet traffic will appreciate the ease of deploying Nubeva TLS Decrypt for a specific instance.
- Super administrators charged with inspecting and securing traffic will immediately benefit from running Nubeva TLS Decrypt in a widely deployed or on-demand monitor and inspect mode.

**Because Nubeva is focused solely on decryption, your compliance, regulatory and other access control policies remain untouched and intact.**



# Ready to Get Started?

Create a free proof-of-concept environment for AWS with our Cloud Tools. Or, schedule time to speak with Nubeva's decryption engineers and get your questions answered in real-time so you can start decrypting encrypted traffic with ease.

Visit [nubeva.com](https://nubeva.com) or call **844.538.4638**.

## Source Material

<sup>1</sup>Google Transparency Report <https://transparencyreport.google.com/https/overview>

<sup>2</sup>TLS 1.3: A Good News, Bad News Scenario, Dark Reading, <https://www.darkreading.com/endpoint/tls-13-a-good-news-bad-news-scenario/a/d-id/1334180>

<sup>3</sup>TLS 1.3 Adoption in the Enterprise: Growing Encryption Use Extends to New Standard, Enterprise Management Associates, Paula Musich, Research Director, <https://www.slideshare.net/EnterpriseManagementAssociates/tls-13-adoption-in-the-enterprise-growing-encryption-use-extends-to-new-standard>

<sup>4</sup>TLS 1.3 is Coming: Here's What You Need to Know to be Prepared, Forbes, Dec. 10, 2019, <https://www.forbes.com/sites/forbestechcouncil/2019/12/10/tls-1-3-is-coming-heres-what-you-need-to-know-to-be-prepared-for-it/#22af031458af>

<sup>5/6/7</sup>Encryption: 2020's Double-edged Sword, TechRadar, Dec. 2019, <https://www.techradar.com/news/encryption-2020s-double-edged-sword>

## ABOUT NUBEVA TECHNOLOGIES LTD.

Nubeva Technologies Ltd. develops Software-as-a-Service (“SaaS”) solutions that enable enterprises to obtain visibility of encrypted cloud traffic. Nubeva’s Symmetric Key Intercept architecture provides universal TLS decryption and works in any cloud platform. The service unlocks cloud traffic for best-of-breed security. The scalability and ease-of-use of Nubeva enable any organization to adopt aggressive encryption in the cloud needed for network monitoring and security tools. Visit [nubeva.com](https://nubeva.com) for more information.



[nubeva.com](https://nubeva.com)

©2020 Nubeva, Inc. All rights reserved.