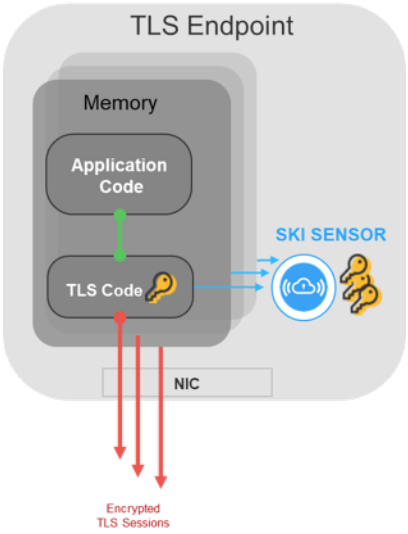
SKI Sensors: Learn, Extract and Forward Session Keys With Security, Reliability and Speed

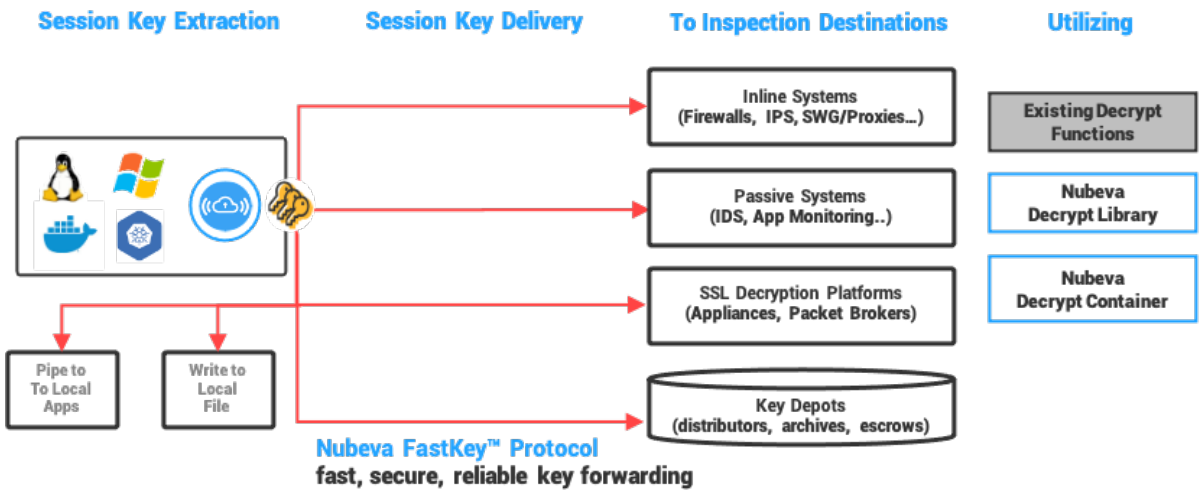
Nubeva SKI Sensors are endpoint software that learn and extract TLS session encryption keys from client and server memory and securely and quickly forwards them to decryption and inspection systems. SKI Sensors are the base element of the SKI (session key intercept) solution for TLS decryption to enable better, faster, and easier inspection of TLS traffic for cybersecurity and application assurance applications.



SKI sensors detect TLS code in-process memory using advanced and proprietary key extraction signatures that decode session secrets appear and exports them to local or remote decryption function or archives. SKI Sensors operate as low resource, automatic and non-disruptive system services requiring no changes to architectures, code, libraries, or interaction with PKI and certificates.

SKI Sensors work across today's myriad of TLS implementations and a growing list of host platforms. Seamlessly extract keys for any session from the client or server-side of a connection, intra- and inter-machine, in cloud, hybrid, and data centers and for "metal", virtual machines, and container environments. Key interception is independent of TLS protocols, ciphers, and certificates, including pinned and client certificates.

Sensors extract keys efficiently and reliably then forward keys to customer-defined destination with total security. Keys can be utilized on existing and embedded decrypt functions or with Nubeva's Decryptor container or High-Speed Decrypt C Library for full visibility into traffic. Nubeva SKI sensors complete the cycle learning, extraction, and delivery process in under 200usec, to enable real-time local and inline applications as well as passive and historical use-cases.



Product Specifications

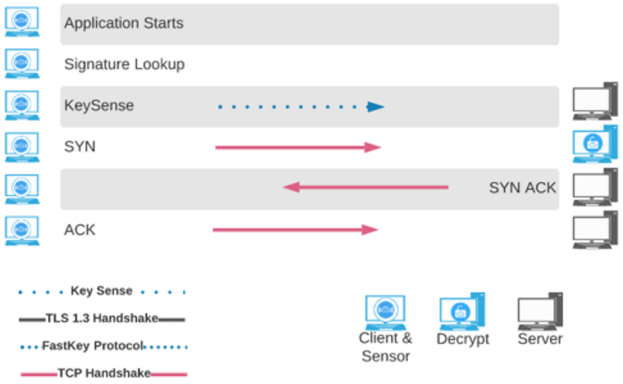
TLS 1.3, TLS 1.2 with PFS, Legacy TLS/SSL	
Key capture, export, and delivery of session secrets 200µs after the secrets are created before handshakes complete, and 500µs before the first encrypted application date is received using FasKey™ protocol.	
Not limited by pinned certificates, client certificates, or third-party services	
Support for session resumption.	
Exclusive Keysense™ technology signals receiving systems if keys are not available for alternate traffic handling.	
Operational simplicity	
Written in GoLang, sensors are available as containers and DaemonsSet as well as native OS system services on the following platforms (with growing support):	• Linux: Ubuntu, RHEL, CentOS and AWS AMI, container and native Linux Daemonsets. • Windows Server 2012, Server 2012 R2, Server 2016, Server 2019, and Windows 10. • Kubernetes using Docker or CRI-O. • OpenShift 4.x using Docker or CRI-O.
A vast and growing set of extraction signatures including support for:	• OpenSSL: all versions from 0.9.7 to 1.1.1i • OpenSSL FIPS: all versions from 1.0 to 2.0.16 • NSS Libraries: all versions from v3.15 • WolfSSL: Version v4.3.0 • Windows Applications using Windows Schannel.dll: See list in the schannel section of the documentation. • Windows applications: Dropbox, MS Edge, Google Chrome • Signature update notifications are made available hours after new libraries and applications are released.

Product Applications

- Enhances outbound inspection on Secure Web Gateways, Web Proxies, SD-Wans, Firewalls, IPS, and DLP systems.
- Enhances inline inbound and East-West traffic inspection in Firewalls, IPS, APT's, and TLS Visibility systems.
- Enables passive inspection of PFS traffic (TLS 1.3 and 1.2) on IDS's, NDR's, Application Monitoring systems, etc.
- Simplifies localized decryption on clients or servers for firewall, intrusion detection and prevention, application monitoring.
- Reduces the complexity and improves decryption capabilities of 5G and Service Mesh - Inspect container-container and inter-node/cluster traffic for 5G packet cores, services meshes, and Kubernetes.
- Not bound by pinned certificates, enabling zero trust security policies to be applied in any workflow or supply chain.

Key Sense

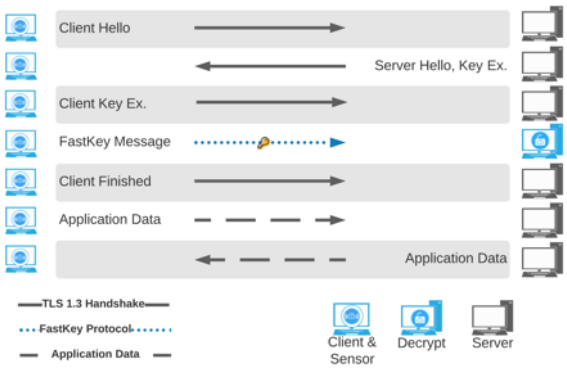
In the rare event that an application uses a library that does not have a signature, the sensor can send an indication to the decryption system, telling the system not to expect a key for the current application. This indication is sent as soon as a TCP handshake is detected: a SYN message on the client or a SYNACK message if the sensor is running on the connection's server side. KeySense operates before TLS handshakes begin, giving decryption time to select the inspection mechanism to use.



FastKey™ Delivery Protocol

Nubeva has developed a new FastKey protocol to deliver keys to decryption systems using TLS encrypted tunnels.

FastKey delivery protocol combines DTLS for speed with REST for backup. FastKey DTLS uses a binary representation of TLS 1.2 and TLS 1.3 session secrets. Combined with signature-based session secret detection, FastKey assures quick release of session secrets, ensuring that secrets are transferred securely and are readily available to the highest throughput decryption applications.



Core Benefits

- SKI offers an alternative to the legacy methods of man-in-the-middle, proxy termination, and passive decryption offering superior capability, price/performance, and simplicity of deployment.
- No involvement in handshakes, server key pairs, certificates, CA's, PKI.
- SKI sensors are not limited by pinned certificates enabling visibility and inspection not possible before.
- Automated updating of signature libraries assures day-one coverage of new applications and libraries.
- High throughput and efficiency provide visibility without compromising application performance.
- Key availability reduces, if not eliminates, MITM overhead in security devices and virtual functions, boosting efficiencies and reducing operational costs.

SKI (Session Key Intercept) – Product Suite:

SKI Sensors are a key component in the Nubeva Session Key Intercept solution architecture for the decryption of modern TLS, enabling deep packet inspection for inline and passive applications. SKI Sensors quickly forward them to inspection systems running SKI Decryptors or SKI Decryption Libraries for decryption after detecting session secrets. SKI offers an alternative to the legacy methods of man-in-the-middle, proxy termination, and passive decryption offering superior capability, price/performance, and simplicity