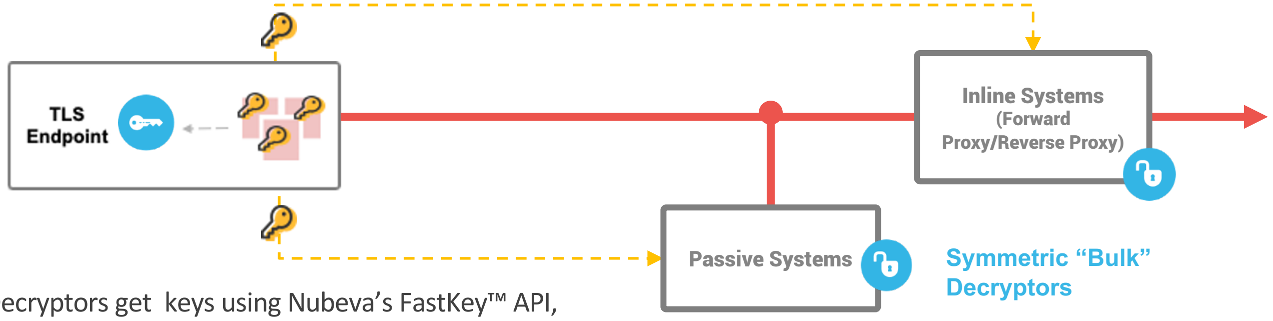
=nubeva

Nubeva Product Overview - SKI Decrypt

SKI Decryptor

Nubeva SKI Decryptors are a turnkey container solutions that receive encrypted mirrored traffic and output decrypted traffic on a standard network interface. SKI Decryptors decrypt TLS records with TLS session secrets extracted by Nubeva SKI Sensors to enable deep packet inspection software. SKI Decryptor are high-speed, lightweight and support TLS 1.3, TLS 1.2 PFS, and legacy TLS protocols.


TLS Endpoint
Inline Systems (Forward Proxy/Reverse Proxy)
Passive Systems
Symmetric "Bulk" Decryptors

SKI Decryptors get keys using Nubeva's FastKey™ API, as well as AWS DynamoDB and MongoDB data retrieval APIs.

Use Cases

SKI Decryptors can be integrated with any deep packet inspection software, both inline and passive, that does not have decryption capabilities, or cannot decrypt TLS 1.3. SKI Decryptors also enable inspection systems to offload decryption to improve performance and throughput.

Decryption can be done in real-time e.g. (IDS/IPS) or after the traffic was sent (forensics). Users have full control over what and when to decrypt. Decryption capacity can be increased by scaling up and out using standard load balancing methods.

Passive Systems: IDS, NDR, APA, APM, DOIM

Reverse Proxy: Next-Gen Firewalls, IPS, ALB/NLB

Forward Proxy: Secure Web Gateways, Next-Gen Firewalls, IPS, DLP, CASB

Product Specifications

- SKI Decryptors are available as Linux containers
- Decryption of TLS 1.3, TLS 1.2 with PFS, Legacy TLS.
- Session renewal and key update support
- VXLAN traffic inputs
- Configurable encrypted and decrypted output
- REST API and file-based configuration
- Session Key Protocols: Nubeva FastKey™, DynamoDB, MongoDB.
- 2Gbps decryption throughput, scales out with multiple containers.

Core Benefits:

- Universal solution expands decryption of any TLS, any environment and any location
- Integrates with any OpenSource and commercial traffic monitoring tools over a standard interface
- Easy to implement and operate, can be launched and configured by any orchestration system

SKI Decryptors are a component in the Nubeva Session Key Intercept solution architecture for the decryption of modern and legacy TLS, enabling deep packet inspection for inline and passive applications. SKI Decryptors use session secrets detected by SKI Sensors. 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.