AVOCADO SYSTEMS

Securing Legacy Application Traffic with FIPS Validated Transport Layer Security

On-demand Encryption for Legacy Workload Communications

Avocado Security Platform

Native runtime protection for workloads, apps, and APIs
Applies zero-trust down to the process level, allows only approved operations, even on trusted systems.

High security efficacy with near zero false positives
Local machine learning enables policies to be enforced directly on the protected systems.

High performance
Light weight plugin architecture requires minimal resources.

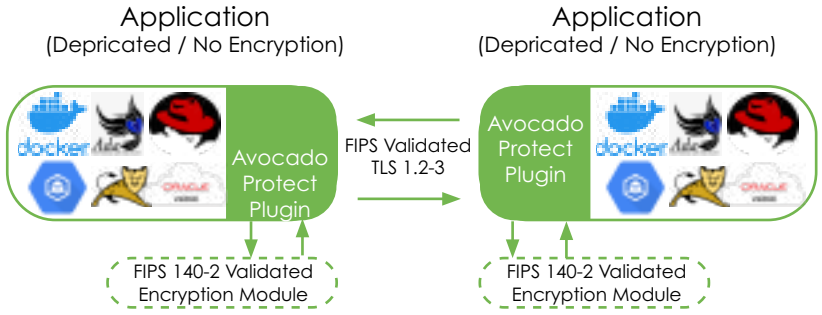
Automated application threat modeling
Discovery, dependency mapping, and threat exposure details in minutes.

Operational efficiency
Real-time threat detection and mitigation with virtually zero false positives eliminates alert fatigue and improves SOC efficiency.

The overwhelming growth of data theft coupled with the sophistication of modern cyber criminals have left security practitioners scrambling to update security on legacy applications. Modern application environments are distributed, scaled-out, and often extend across clouds. Networks can no longer be trusted, and all data exchanges must have adequate levels of encryption to ensure data is safe from data stealing threats lurking within the network.

Post the SolarWinds related breaches, organizations are applying a more stringent application of NIST Zero Trust security recommendations. In particular, they are now mandating that data in motion be encrypted and adequately secured, even on internal networks. The colossal challenge, however, is applying this governance to legacy applications that do not support or have deprecated transport layer security (TLS) crypto libraries.

Avocado Systems provides a solution which enables Zero Trust compliance for legacy servers and applications without needing to change a single line of application code or recompile. Avocado provides on-demand FIPS validated encryption from source to destination for modern or legacy apps that were not designed to support data-in-flight encryption.



- Address compliance requirements without recoding or significant investment
- Single solution platforms such as bare metal, virtualized, or container
- Addresses Zero Trust compliance across apps and workloads
- Secures current and/or legacy apps