



## Application Security, Segmentation and Compliance

### Any App, Any Platform, Any Cloud

In 2015, the Office of Personnel Management that holds all personal data on US government employees including those with Top Secret Security Clearances was breached, enabling the thief to walk off with 21.5 Million highly sensitive records; in 2017, Equifax, who holds the most private financial data on Americans lost 148 Million records; in 2018, Marriott lost FIVE HUNDRED MILLION of their customer's confidential data records! What these breaches all have in common is they were all protected by the best PERIMETER data protection money could buy, but once a threat broke in, they roamed undetected inside the data center for YEARS, plundering at their leisure.

Avocado Systems employs innovative, deterministic, Pico-Segmentation technology to stop lateral movement of threats to secure applications in cloud and data center environments. It prevents lateral movement of threats that have penetrated perimeter defenses. Pico-Segmentation represents the next advance in Intra-domain cyber-security in that it further defines potential attack surfaces in terms of characteristics such as ports used, protocols allowed, time of day, traffic volume and packet sizes to distinguish legitimate traffic from unauthorized connections and attacks.

Avocado's Security Platform (ASP) utilizes a "policy-free" approach and validated "zero-false positive" results to reduce security resource allocation over traditional approaches to cloud and data center security thus saving money and time.

Avocado Systems' patented Security Platform (ASP), is uniquely designed (12 US Patents) to deliver unsurpassed application protection, policy-less pico segmentation as well as compliance to applications across Data Centers and Cloud environments.

The Avocado Security Platform (ASP) protects applications deterministically in real-time:

- With process level dynamic application segmentation that stops lateral movement of threats and keeps applications secure and compliant.
- ASP adds plugins to applications, with no existing security infrastructure changes, no policies to configure and no recompilation or even re-linking.
- ASP provides security functions (Firewall, IDS, IPC etc.) into its plugins that sit next to the applications, it abolishes the need for more expensive add-ons and east-west (server-server traffic) security appliances, eliminating traffic bottleneck.
- ASP protects the lowest possible application attack surfaces during run time, producing zero false positives.

The Avocado Security Platform is fully optimized to keep customer's cloud migration path smooth, while helping them to meet compliance requirements for PCI, PII, HIPAA and others; so, they can continue to focus on their business goals. See [www.avocadosys.com](http://www.avocadosys.com) for more information.