Avocado Systems™

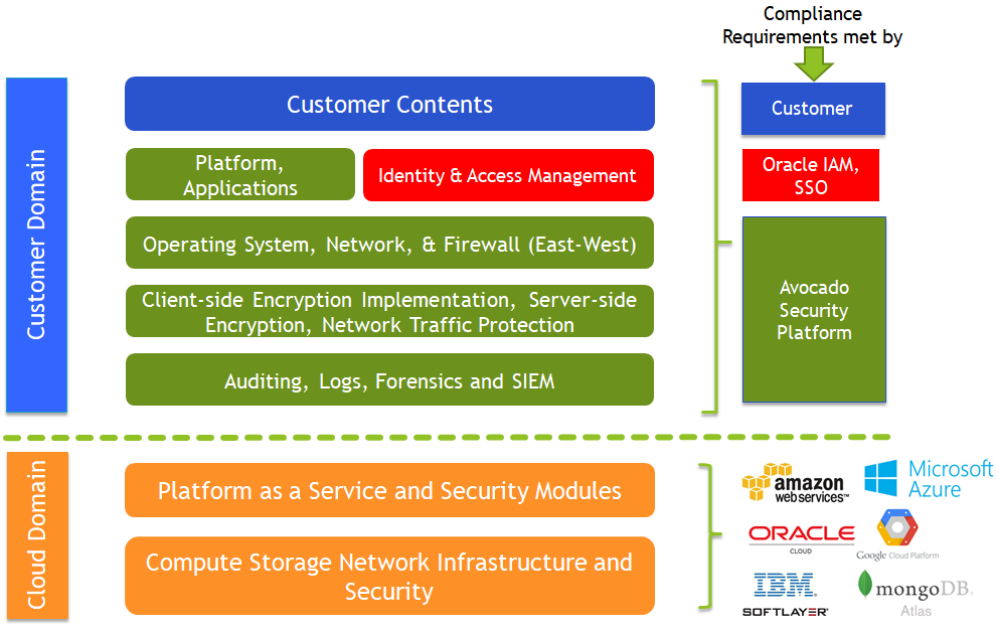
HIPAA Compliance | Any App | Any Platform | Any Cloud

Healthcare technology leaders are faced with the daunting challenge of rapidly supporting new clinical initiatives, securely storing patient data, and integrating disparate systems all while managing an aging infrastructure, tight budgets, and a constantly evolving regulatory landscape. To address some of these challenges, customers are migrating their applications and data to Clouds solutions which makes perfect sense. However, making a cloud based solution as healthcare IT infrastructure raises questions about data security and HIPAA compliance.

Avocado Security Platform delivers real-time application protection with integrated security and HIPAA compliance. It eliminates needs for expensive add-on services, streamlining processes, while simplifying complexities for IT security team. Avocados Security Platform locks in security while scaling with your business. Imagine that. Spoof-Proof, Always-On Application Security and HIPAA compliance, no more expensive add-on services, reduced IT headaches, while lowering annual costs.

HIPAA Compliance Framework for the Clouds

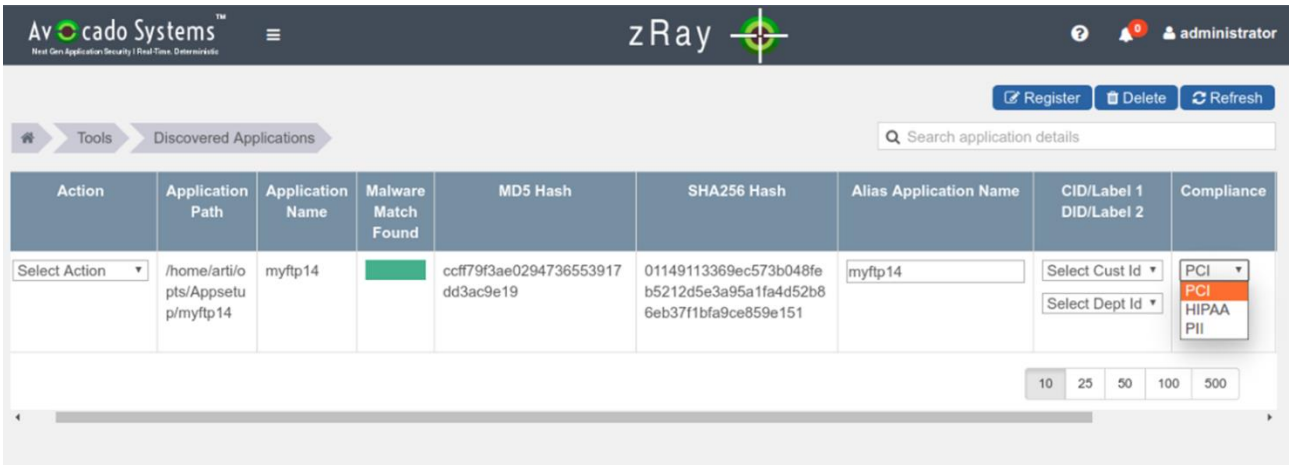
The AWS, Microsoft Azure, IBM Softlayer and Oracle Clouds (SaaS,PaaS, IaaS) (SaaS,PaaS, IaaS) offer a complete security framework that controls not only North-South server traffic, **but also West server communications.** Other Cloud vendors will tell you Application and Database security are up to you. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site datacenter.



Working with Avocado Systems, the Cloud vendors provide security and HIPAA compliance for both **Cloud domain** and **Customer domain**.

Avocado Security Platform provides applications segmentation, client and server side encryption along with full auditing, log and forensics to ensure HIPAA compliance is met.

As applications are provisioned and deployed in the Clouds, they are added with Avocado plug-in protection. Once the plug-in is enabled, applications can simply be automatically discovered, registered and included in a desired application segment.



Avocado Security Platform delivers application self-protection and HIPAA compliance, with built-in security driving a laser focus on east-west traffic, transforming Data Center and Cloud security, unleashing a simplified, and less costly solution. Following are some of key benefits:

Feature	Benefits
Secured Applications and Data	• Secures applications running within physical, virtual or container platforms • Across any data center, private, public, or hybrid clouds
Stops Lateral Threat Spreads (APTs, Malware, Zero Day attacks)	• Applications are segmented down to individual processes on workloads • All unauthorized connection attempts are auto-blocked • Kills attempts for cross-site scripting (XSS), SQL injection (SQLi), cross-site request forgery (CSRF), command injection, Data exfiltration, Session hacking
Zero False-Positives	• Threats are identified deterministically at the lowest attack surface and using mathematical algorithms • Resulting in zero false-positives
Meets Compliance Requirements	• PCI, HIPAA, and other compliance requirements are easier to meet via application segmentation • Includes comprehensive log and forensic collection
Detects & Eliminates Pre-existing APTs or Malware in Real-time	• Catches an APT's first attempt to communicate with an ADPL-protected application • Kills APT's processes instantly in real-time • Automatically creates a ticket with ServiceNow™ ITSM solution
Real-Time Visualization of attacks and compliance status	• Real-time communications between workloads, within and across applications display via interactive graphical maps • Logs are sent to any SIEM solution such as Splunk or IBM Q-Radar

Avocado Systems™

HIPAA Compliance | Any App | Any Platform | Any Cloud

The technical requirements to implement HIPAA security on a cloud-hosted environment are lengthy; for example, the Responsibility Matrix for a specific Cloud Platform is more than 50 pages long. However, following are high level overview of HIPAA requirements:

High Level overview of the HIPAA Requirements	Met by
Access Controls	
Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.	Cloud Vendor IAM/SSO
Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	Cloud Vendor
Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Cloud Vendor
Encryption and Decryption: Implement a mechanism to encrypt and decrypt ePHI.	Cloud Vendor (Data at rest), Avocado (Data in flight)
Audit Controls	
Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	Avocado (Software based)
Integrity	
Mechanism to Authenticate ePHI: Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	Avocado
Authentication	
Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Cloud Vendor IAM/SSO Avocado (Session Spoofing)
Transmission Security	
Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	Avocado
Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Avocado for data in flight

HIPAA Compliance for Any App on Any Platform, in Any Cloud

Real-Time, Deterministic Detection

- Threat detection at the lowest possible attack surface i.e. application socket descriptor
- No human intervention
- One-touch segmentation at the smallest attack surfaces
- No payload encryption required

Effortless Deployment

- DevOps friendly, integrated with Chef, Puppet, OpenShift and CloudFoundry
- No policies to configure
- No code changes
- No re-compiliation or re-linking
- Auto-discovery & security configuration
- Removes shadow IT challenges

Real-Time Threat Visualization

- Application session level security event visualization
- Collects detailed forensic & log information for compliance and auditing
- Integrated with SIEM (Splunk) and ITSM (ServiceNow)

Deterministic Application Security