*An Innovative Healthcare Customer Secures its Applications in AWS Cloud and Meets HIPAA Compliance Requirements With Avocado Security Platform.*

**Customer Challenge:** Enterprise and government systems and applications are rich targets for malicious attackers. By evading perimeter security, attackers can gain a foothold inside data centers or on public clouds. Once inside, attackers usually can move unimpeded laterally to other systems (this is 'east-west propagation') and steal valuable information.

One of Avocado's very innovative healthcare customers planned to migrate their applications into AWS cloud. During the migration, they created a pilot environment on AWS to test their healthcare applications for security and compliance. During pilot, they used sample data which was not subjected to HIPAA compliance. Almost every day, they were noticing intrusions and application attacks from unknown attackers. They had strong feeling that their applications are constantly being attacked however; they were unable to find out who these attackers were and where were they coming from.

**Solution - Avocado Security Platform:** The customer reached out to Avocado Systems and deployed Avocado Security Platform in the same pilot environment which segmented their applications securely. Avocado's micro-segmentation involves dynamically grouping and segregating applications to prevent or limit penetration and the propagation of threats laterally.

As soon as Avocado Security Platform was deployed, and applications were ring-fenced in microsegments, the applications were secure. Avocado solution captured every application attack from various GEO locations around the world. The following report shows detailed correlation of applications attacked. In this case, customer's MySQL servers were constantly being attacked by malicious attackers around the world and Avocado Security Platform managed to thwart every single attack, captured all details on attack forensics and sent it to SIEM solution like Splunk for further analysis.

**Excerpt from Application Attack Report**

| Application Name | Customer / Label 1 | Department / Label 2 | Server IP | Server Port | Client IP | Client Port | PID | Total Rejections |
|---|---|---|---|---|---|---|---|---|
| mysqld | | IT (36) | | 3306 | 123.249.27.70 | 3757 | 4140 | 366 |
| mysqld | | IT (36) | | 3306 | 61.143.157.115 | 1308 | 4140 | 366 |
| mysqld | | IT (36) | | 3306 | 119.1.109.96 | 2563 | 4140 | 366 |
| mysqld | | IT (36) | | 3306 | 123.249.27.70 | 4618 | 4140 | 366 |
| mysqld | | IT (36) | | 3306 | 59.38.35.243 | 17529 | 4140 | 366 |

Attacked Applications

Customer Info masked for privacy

Customer Server Info masked for privacy

Attackers IP Addresses

Persistent Threats trying to get in using different port numbers

Avocado's advanced micro-segmentation is un-breachable and impassable by members of other micro-segments and alien application entities, both within or outside the data center. These include Advanced Persistent Threats and Malware entities. The creation of micro-segments is fully automatic without external intervention and policy specifications. At the same time, Avocado allows a great amount of programmability for specific needs of multi-tenancy, business unit hierarchies, and further proprietary mapping.

Avocado Security Platform protects applications in data center or in the cloud from DDOS, Malware, APTs, Man-In-The Middle, Zero-day, Injections like SQL injections, session hijacking and spoofing attacks.

Avocado Security Platform is certified by Redhat for its container deployment.