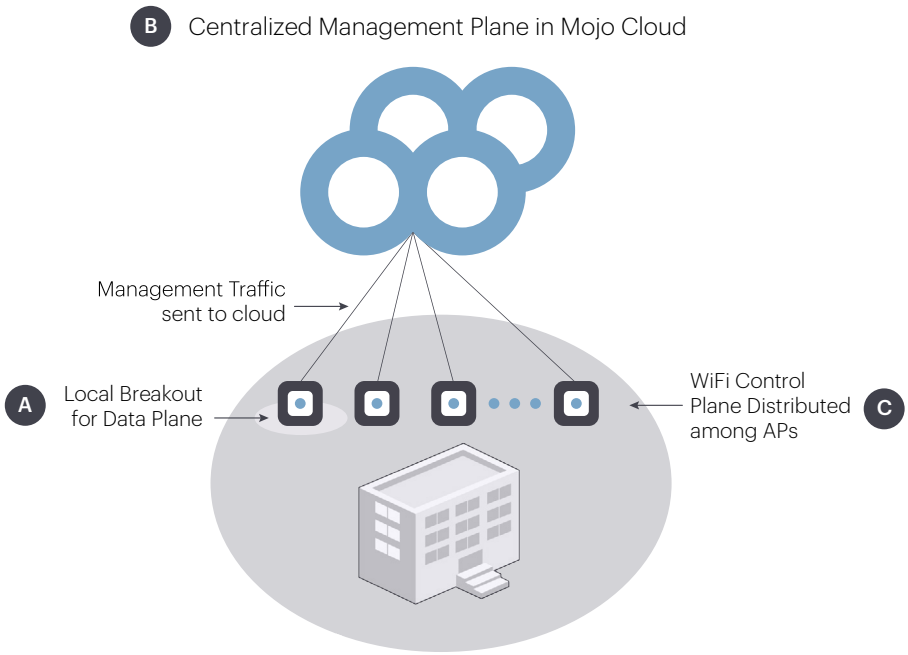
Security of the Cloud

Whitepaper

Mojo Cloud WiFi Architecture

Across enterprises and public sectors alike, migrating in-house data processing to the cloud has become an accepted strategy among IT departments. This often raises eyebrows within the security department because data security controls that were traditionally managed in-house now move into the hands of third parties. Cloud managed WiFi is no exception to this dogma. Hence, Mojo has taken proactive steps to build a robust security program for the cloud that strengthens its WiFi access and security solution. The Mojo cloud security program comprises multiple pillars as described throughout this paper.



Local data plane and cloud management plane

In the Mojo cloud architecture, the wireless data plane **(A)** is kept local to the enterprise network, while the management plane lives in the cloud **(B)**. Wireless data transacted through Mojo access points (APs) does not flow to the Mojo cloud; rather it is routed locally on the enterprise network based on the enterprise's routing controls. This also facilitates local enforcement of data security controls such as content filtering and forensic logging. The authentication and authorization functions of the data plane are also kept local to the enterprise network.

The management console used to configure and monitor the wireless network is provided from the Mojo cloud. This console also provides security monitoring of the WiFi environment at the enterprise to detect and contain any undesirable activity in that air space.

The control plane operates locally in the enterprise network among APs **(C).** This plane implements inter-AP messaging for handoffs, load balancing, RF optimization etc and does not require constant input from the management plane past its initial configuration.

Data collected by cloud management plane

The cloud management plane collects and stores MAC and IP addresses of devices on the enterprise network that are seen by APs deployed within the network. It also collects metadata about devices such as their layer 2 wireless activity (probing, associations), OS, hostname, application usage, locations to the level of proximity to APs, and 802.1x login identities that are transmitted over the air in order to connect to the WiFi network.

It's important to note that employee passwords used for 802.1x authentication are not collected or stored in the cloud, as they are validated by local enterprise RADIUS servers. 802.1x user passwords are also not readable by the APs since they are only passed between the client and the authentication servers.

For Guest WiFi, the cloud management plane also collects and stores identities of guest users used during WiFi authentication to facilitate security audits of guest visitors. Enterprises can, if they wish, implement a Guest WiFi network with anonymous login as well.

AP-to-Cloud Communication

There are three security measures in place to ensure proper protection for AP-to-Cloud communication.

Mutual authentication: This occurs anytime an AP initiates a connection with the cloud. This is always an inside-out request, and both the AP and cloud authenticate to one another in the process. This verifies the identity of both parties.

Per message authentication: This uses an HMAC SHA-1 authentication code for every message sent from an AP to the cloud. This ensures the integrity of the communication by confirming the message is sent by the correct entity and is not changed in transit.

AES encryption: This is used throughout AP-to-cloud communication. This ensures the messages remain confidential and cannot be intercepted.

Cloud environment in AWS data center

The Mojo cloud is deployed as a virtual private cloud (VPC) in the Amazon Web Services (AWS) data center. In the VPC architecture, the Mojo cloud environment is logically isolated from environments of other entities that co-exist within the AWS data center. The physical and environmental security for the VPC is provided by AWS **(1).**

Multiple subnets are provisioned inside the Mojo VPC that host Mojo application servers. Each subnet has a network ACL (Access Control List) that only allows certain protocols in and out of the subnet **(2).** The application server virtual machines are deployed as EC2 (Elastic Compute Cloud) instances and are connected to these subnets. Each EC2 instance that Mojo deploys has a host-based firewall that is configured to only allow protocols required for corresponding applications in and out of the server **(3).** The Mojo applications that run on these EC2 virtual machines themselves are port hardened to ensure that unwarranted services and ports are not accessible on them **(4).**

The Mojo cloud is deployed in AWS data centers located around the globe, and the footprint is rapidly growing as Mojo acquires more global customers.

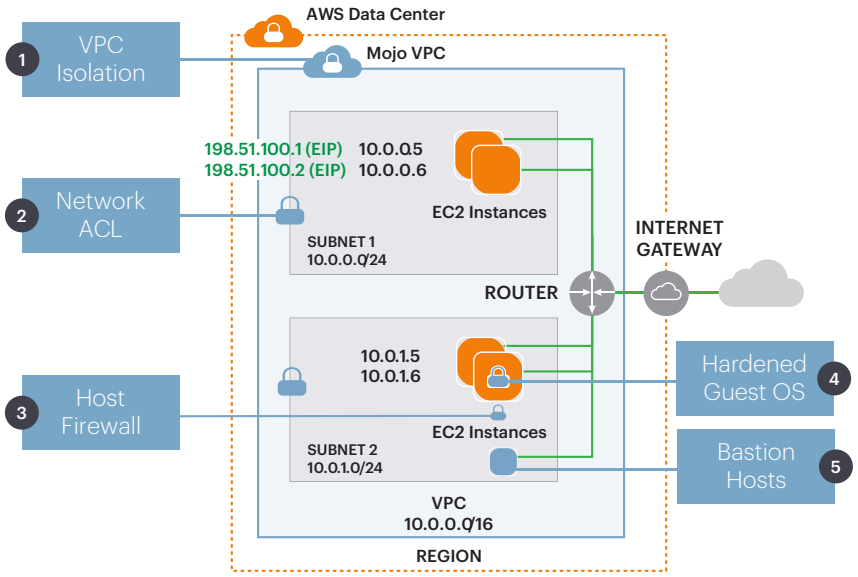
Vulnerability scanning

Mojo regularly performs three types of vulnerability scans on its cloud-hosted applications as follows.

Port scans: As compute instances are launched in different parts of the data center, it is essential to validate that open ports are restricted to only those that are essential for accessing the application functionality. This reduces the attack surface considerably. Mojo performs regular port scans on its cloud environment.

WAS (Web Application Security) scans: WAS scans focus on finding vulnerabilities at the web application level. Since the cloud application is accessible over HTTPS (port 443) and thus the Internet at large, the objective of a WAS scan is to ensure that there are no exploitable vulnerabilities if an unauthorized user attempts to access the application. Another important objective is to prevent an authorized (authenticated) user from breaching application security controls, such as injection attacks, privilege levels, multi-tenancy, and so on. Mojo deploys 24x7 automated WAS scanning using WhiteHat Security services and complements it with twice a year manual (deep) scans by WhiteHat Security experts.

Mojo VPC in Amazon Data Center



Software components scans: These scans are performed to audit software modules within the application for any missing security patches, stale versions, and misconfigurations. Mojo performs software component scans on all its cloud applications at least once a quarter using the Nessus Enterprise tool.

Data encryption

Mojo encrypts data in transit using AES. This includes management GUI (HTTPS) communication between the Mojo AP and the cloud and all interactions between different Mojo servers and applications in the cloud (HTTPS).

AES encryption is also applied to data at rest. Database backups of Mojo applications in the cloud are stored in AWS S3 and Glacier that are also AES encrypted. The live database of Mojo Wireless Manager (MWM), the flagship application that provides the wireless management console, resides in AWS EBS (Elastic Block Storage) and is also AES encrypted.

Access control

Mojo personnel need to access cloud applications for the purposes of provisioning, maintenance and resolving trouble tickets. Mojo implements access control mechanisms that limit Mojo personnel access of customer accounts to a basic minimum. Privilege escalation for any task that requires higher level of access is subject to the customer's permission and available for a temporary period of time. Employees who might work with such privileges must pass background screening first.

Maintenance access to EC2 server must go through the bastion hosts. Login to the bastion hosts requires SSH and is allowed only from specific IP addresses. Bastion hosts implement strong access control and auditing functions to prevent unauthorized maintenance access **(5).**

Compliance certifications

Mojo pursues security compliance certifications that include third party scrutiny (audit) and validation of the Mojo cloud security controls geared towards confidentiality, integrity, and availability (the CIA triad).

Mojo Networks has achieved **ISO 27001:2013** certification for its Information Security Management System (ISMS). The scope of Mojo's ISO certification covers all its operations.

Mojo Networks has obtained its own **SSAE 16 SOC 2** validation for its production cloud. Of course, the AWS data centers where Mojo applications are hosted are already SSAE 16 SOC 2 certified. However, data center SSAE certification by itself isn't adequate to guarantee comprehensive cloud security for the customers. This is because there are a number of cloud operations that are handled by application providers such as Mojo that are beyond the scope of SSAE certification of the data center itself. Mojo's SSAE control framework covers such operations.

About Mojo Networks, Inc.

Mojo Networks is redefining the modern WiFi platform. Imagine the scalability to set up millions of access points with a few clicks, all from your smartphone. Envision an Internet experience that engages users with your business to drive results. Stay secure on the same WiFi cloud powering major brands and the highest levels of government. And enjoy the cost savings of a cloud-first solution without the pricey markup of proprietary hardware. Welcome to the era of prolific connectivity. Founded in 2003, Mojo Networks (formerly known as AirTight Networks), serves customers in the Fortune 500, Global 2000 and large carriers around the world. Request a free demo of Mojo Cloud Managed WiFi Platform at **www.mojonetworks.com.**

The Global Leader in Secure Wi-Fi Solutions
Mojo Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1.877.424.7844 T 650.961.1111 F 650.961.1169 **www.mojonetworks.com** **info@mojonetworks.com**

mojo Networks