Aerohive™ NETWORKS

whitepaper

Cloud Services Platform

Security and Availability Controls

Table of Contents

Offering Statement

The Aerohive Cloud Services Platform is a globally distributed, cloud-based infrastructure that is home to Aerohive developed Software-as-a-Service (SaaS) applications. HiveManager Online is the cloud-based management system that provides access to configuration and networking monitoring statistics for all managed Aerohive network devices

Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled Wi-Fi and routing solutions for medium and large enterprise headquarters, branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations.

Aerohive's approach enables scalable, secure and reliable network applications by taking advantage of the Cloud while also preserving an unmatched level of flexibility often associated with on-premise solutions. Customers can still decide what to run, when to upgrade and comply with customer's network operation policies.

Data Centers

Geographically Distributed

Aerohive employs data centers geographically distributed to optimize customer networks connectivity. Data centers are located in North America, Europe and Asia Pacific region.

Certifications

All Aerohive Cloud Services operations are hosted in SAS70 (superseded by SSAE 16) Type II data centers. Aerohive utilizes industry-leading 3rd party providers with public statements of SAS70 and SSAE-16 compliance. Aerohive reviews vendor's capabilities, scale, SLA's and cost-benefits associated with their offerings in order to determine the best operational platform.

International Compliance and Safe Harbor

Aerohive meets European privacy controls and Safe Harbor certification by adhering to data geographic policies. The European-based data center performs cross data replication within the EU region in order to meet EU privacy controls.

Physical Access

Physical access to datacenters is restricted to authorized staff, through a two-factor authentication including biometric authentication. Access is strictly controlled 24x7 by professional security staff, video surveillance and other electronic means.

Logical Access

Segmentation of logical vs. physical access is achieved through Policies enforced with the Technical Operations team. Third party cloud providers do not possess logical access to Aerohive systems. Selected Technical Operations staff requires extra credentials to access Production systems.

Facilities Robustness

- **Data centers are physically isolated and housed in non-descript facilities**

- **Automated systems and personnel monitor and maintain optimal temperature and humidity**
- **Redundant uninterruptible power supply (UPS) units for essential systems, and generators to provide backup power for the entire facility**
- **Automatic fire detection and suppression systems**
- **Multi-zoned systems, with double interlocks to prevent accidental water discharge**
- **All facilities meet or exceed requirements for local seismic building codes and lower risk flood areas**

Software Upgrades

Flexibility Advantage

For any minor or major software updates, Aerohive enables the customer to choose when they would like to migrate, and to self-manage the process. These updates at times may include features that increase the security posture of the solution. This type of flexibility – often found only with non-cloud systems – is unmatched in the cloud & networking industry and allow our customers to decide when to migrate based on their network policies and schedule convenience.

Security

Aerohive automatically applies critical security patches deemed necessary to maintain integrity of HiveManager Online (HMOL) and Cloud-based servers.

Change Control Policy

Aerohive employs a three-stage Change Control Process policy. Software is delivered, tested and exercised through a Beta program. Once a candidate final release is selected, it is put through a staging scenario, then tested and operated as if it were in production. After passing all the operational production tests, the release is moved into a production environment. Changes to production environment are performed on pre-scheduled, announced maintenance windows. Aerohive performs quarterly reviews on its Cloud Services Platform Access and Change Control policies.

Data Protection

Privacy

No actual data traffic from the managed Aerohive network devices (APs and routers) is forwarded or traverses the Aerohive Cloud Services Platform. Third parties employed for our Cloud delivery platform don't have logical access to our customer's data.

Data Sensitivity

HiveManager Online provides access to configuration management and networking monitoring statistics. Data stored does not include anything traditionally considered "personal information" such as name plus either social security, driver license, financial account numbers, passwords, medical or insurance information.

Data available in Cloud Services Platform

HiveManager Online (HMOL) defines users with different roles and permissions; SHA-2 encryption and 512-byte key is deployed for login passwords. HMOL provides access to configuration management and networking monitoring statistics for all managed Aerohive network devices. Information may include the following:

- **For each user, information as to when the client device authenticates to an AP, to which AP, and when it deauthenticates.**
- **For each user, user name from 802.1x or Captive Web Portal; however it does not receive the login credentials from the AP. It will also have the client device's MAC address, IP address, and OS detected.**
- **For each user, records of aggregate traffic, but not any detail as to individual destinations.**
- **If StudentManager or TeacherView applications are enabled, then HiveManager will have data as to what URLs are accessed by individual clients registered in those applications.**
- **If Guest Management capabilities are utilized, some information may be collected for a guest registering for PPSK access. For example, fields to enter visitor name, email address, company and sponsor, PPSK, start time, end time, and SSID assigned.**
- **If Management of Bonjour Services is enabled, the type of services re-advertised will be collected but not the actual service data.**

Monitoring & Incident Response

Aerohive Technical Operations performs quarterly reviews of Cloud Services Platform access and changes by Tech Ops personnel. There are Operations and Support personnel 24x7, with additional staff on call for incident escalation responses. If Aerohive were to detect any breach or other major security incident, its staff would immediately escalate, investigate and remediate as necessary. The Escalation notification list includes the VP of Operations.

Breach History and Notifications

As of Q3, 2012, Aerohive Networks has not experienced any data breaches on its Cloud Services Platform. Aerohive aims to notify its affected customers within 7 days of detecting any security breach to its Cloud Services Platform and provide as much information as available on the extent of any breach. Aerohive will meet any other notification requirements as required by United States federal and California laws.

Forensic Analysis Procedures

Aerohive has Operations and Support personnel 24x7, with additional staff on call responsible of performing forensic analysis if required. The Technical Operations staff has the ability to collect the relevant logs and records using proper chain-of-custody procedures.

Operations Structure

A cross-functional security team exists in the company, composed of members from Operations, QA, Engineering, Customer and Networking support. The security team follows compliance of assessment made on product requirements and operational practices. Operations and Networking Members of the security team hold certifications in Networking Access Security.

Availability

Uptime

HiveManager Online is guaranteed for 99.99% uptime, excluding scheduled maintenance windows.

Disaster Recovery (DR)

Aerohive's Disaster Recovery plan includes proactive monitoring of customer performance data. Hourly snapshots are taken to assess operational health programmatically. In addition, hourly backups are taken for all customer configurations; ensuring recovery from a theoretical disaster situation by restoring changes that happened up to 1 hour ago. In addition, daily backups are performed to preserve all collected data beyond configuration.

Business Continuity Plan (BCP)

Aerohive's Cloud Platform includes High Availability mechanisms operating with Active-to-Active redundancy for data requiring critical access and low latency responses. Active-to-Passive redundancy systems are also employed for selected components. HiveManager, as a Network Management platform is not in the data path of customer data nor its failover impacts the ability of customers accessing the network.

Backup & Storage Strategy

- **Cross-backups are performed utilizing storage in opposing data centers.**
- **In order to maintain privacy and European Safe Harbor compliance, data centers in different locations within the EU region perform cross backups.**
- **Hourly backups are taken for customer device configurations and daily (nightly) for all customer data.**
- **Backups are stored in both local and remote servers (on different data centers) in a compressed format and inaccessible to users.**
- **Backups are archived for 7 days in its local server and for 30 days in a remote server.**
- **The backup data does not include anything traditionally considered sensitive personal information.**
- **Authenticated administrative-level user is required to restore the data in corresponding user accounts.**

Data Recovery

Customer data backup can be recovered in all potential cases of: malfunction within an account, malfunction of a logical server, malfunction of a physical server, or malfunction of an entire datacenter. Since the configuration data is backed-up hourly, is possible to restore a customer configuration up to changes performed up to 1 hour ago.

System Monitoring

Complete monitoring is performed for our Cloud Service platform encompassing usage of a global System performance monitoring tool, measuring service level monitoring & notification, and cloud HTTP monitoring. Aerohive's Operations team has access to dashboards measuring production capacity, usage & trend monitoring. Performance snapshots are taken of our running systems and programmatically raised as Alarms when internal thresholds are met for learnt performance metrics.

Managing critical events after-hours

The Aerohive Technical Operations (TechOps) and Technical Support team have personnel operating 24x7, with additional staff on call as required for subsequent help.

Technology

Cloud Scaling

Aerohive's Cloud Service platform scales by taking advantage of cloud elasticity. New servers and backend infrastructure can be instantiated as needed based on current load, customer and partners growth and as consequence of monitoring operations for learnt patterns of system performance. Scaling becomes transparent to our customers.

Traffic Encrypted & Restricted

All administrative network traffic is encrypted. HiveManager uses CAPWAP over HTTPS for uploading & downloading relevant traffic (such as HiveOS image files, full configurations, captive web portal pages, and certificates) from HiveManager Online to & from devices.

Aerohive Technical Operations can perform traffic restriction by IP address at any time, if determined desirable. No unauthenticated users have administrative of monitoring access to HiveManager Online.

Logging

All logs in the system can be redirected to a central syslog server, if desired. In addition, our cloud approach with HiveManager Online permits collecting all relevant Events/Alarms/Logs in a centralized manner.

Vulnerability Scans, Penetration Tests and Antivirus

Aerohive's infrastructure – including our Cloud providers – manages proactively firewall and networking security policies for the services hosted. Typical security and access procedures are followed to limit access and permissions to these systems.

Segmented Environments for Development, UAT and Production

Separate environments are maintained for Development, User-Acceptance and Production. Aerohive's products go through a 3-stage process of Development, QA, Beta testing before getting staged in a production environment, tested again and finally deployed in Production. Our Cloud Service platform allows customers to participate in our Beta program, test-driving our latest functionality by trying HiveManager Online Betas without having to upgrade their entire network and disrupt operations.

Third Party Software Patches

Third party patches are applied into our systems following the same three-stage Change Control Policy as our product releases. Major version upgrades of 3rd party software are planned as part of a main development cycles implying a longer duration testing cycle and gained stability for intermediate software releases.

User Roles Policies

HiveManager Online provides administrative options to manage user roles and levels of permissions for users. A customer will have a superuser account with ability to create users with granular permissions within the realm of his/her account.

Customers having accounts managed by a Partner (an integrator or VAR) will be able to restrict/grant access to their parent Partner (i.e. for preventing partner staff from monitoring or configuring their system, or alternatively granting them access for partner maintenance). Partners can disable a customer account (i.e. for non-paying or terminated customers).

Account Provisioning

New accounts are provisioned when HiveManager Online is being evaluated or sold to a customer. The new user will be registered with enough Admin permissions to create other users within the account realm. Aerohive's Technical Operations (TechOps) and Technical support has potential logical access to the system for troubleshooting purposes.

Password Policies (Resets, Storage)

Only an administrator who has enough permission to administer other users within his/her account realm can perform password resets. All passwords are stored encrypted. Users can utilize the "Forgot Password" option in the login page to reset passwords. Alternatively, customers can contact their account representative who will perform a full verification with the company or partner registered for that account.

SSO, Session Timeouts

Aerohive supports SSO within the MyHive environment that includes the portals for HiveManager Online, Portal and Redirector. Administrative sessions are closed if idle for 15 minutes. Timeout expiry values are configurable. Reports of failed login attempts could potentially be requested.

About Aerohive

Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital and New Enterprise Associates, Inc. (NEA).

Aerohive™
NETWORKS

Corporate Headquarters
Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199
info@aerohive.com
www.aerohive.com

EMEA Headquarters
Aerohive Networks Europe LTD
Sequel House
The Hart
Surrey, UK GU9 7HW
+44 (0)1252 736590
Fax: +44 (0)1252711901

WP1104009