Cloud Services Platform
Security and Availability Controls Overview
Table of Contents

Offering Statement .............................................................................................................................................. 3
Data Centers ..................................................................................................................................................... 3
Software Upgrades .......................................................................................................................................... 4
Data Protection .................................................................................................................................................. 5
Availability ....................................................................................................................................................... 6
Technology ....................................................................................................................................................... 7
Offering Statement

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

Aerohive Networks reduces the cost and complexity of today’s networks with cloud-enabled Wi-Fi, switching, routing, and application 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, unified switching, 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 their network operation policies.

Data Centers

Geographically Distributed
Aerohive employs geographically distributed data centers to optimize customer network connectivity. Data centers are located in North America, Europe, and Asia Pacific regions.

Certifications
All Aerohive Cloud-based technical support 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 capabilities, scale, SLAs 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 geographic data 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 data centers is restricted to authorized staff and 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 Aerohive 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 local seismic building codes and are located in lower risk flood areas

CloudTrust Certified
Aerohive is CloudTrust Certified Enterprise-Ready.
Skyhigh Networks performs objective and thorough evaluations of the enterprise-readiness of cloud service based on a detailed set of criteria developed in conjunction with the Cloud Security Alliance (CSA). Services designated as Skyhigh Enterprise-Ready are the services receiving the highest CloudTrust™ Ratings, which fully satisfy the most stringent requirements for data protection, identity verification, service security, business practices, and legal protection.

Software Upgrades

Flexibility Advantage
Aerohive recommends that customers upgrade to the latest supported version of HiveManager Online in order to benefit from new performance and security features and the latest enhanced product experience. At all times, customers control and decide when to upgrade their Aerohive hardware devices (access points, switches, routers and HiveOS Virtual Appliances). Customers can
Cloud Services Platform: Security and Availability Controls

initiate their HiveManager Online upgrade either by themselves, or they can request Aerohive to upgrade on their behalf (by phone or by opening a ticket).

Occasionally, Aerohive may notify customers that Aerohive will upgrade the Cloud Services Platform to a newer version in order to address potential security issues and/or major bug fixes. Aerohive Applications, including ID Manager and Client Management, may also be upgraded periodically to provide new features and functionality to existing customers. Notifications are sent out prior to the upgrade and do not affect any Aerohive hardware devices or policy configuration.

Details about Aerohive’s upgrade policy can be found at:

http://www.aerohive.com/330000/docs/Cloud_Services_Platform_Upgrade_Policy.pdf

Security

Aerohive automatically applies critical security patches deemed necessary to maintain integrity of HiveManager Online (HMOL), cloud-based servers, and applications in the Cloud Services Platform.

Change Control Policy

Aerohive typically employs a three-stage Change Control Process for software releases and upgrades. Software is delivered, tested, and exercised through a Beta program. Once a candidate for final release is selected, it is put through a staging scenario, then tested and operated as if it were in production. After passing operational production tests, the release is moved into a production environment during pre-scheduled, announced maintenance windows.

Data Protection

Privacy

No actual data traffic from managed Aerohive network devices (e.g., Aerohive APs, switches, and routers) traverses the Aerohive Cloud Services Platform. Third parties employed for our Cloud delivery platform don’t have logical access to Aerohive customer data.

Data Sensitivity

Cloud Services Platform applications provide access to configuration, management, and network monitoring statistics. Stored data does not include anything traditionally considered "personal information," such as a name plus an associated social security, driver’s license or financial account number, or personal medical or insurance information.

Data available in Cloud Services Platform

HiveManager Online (HMOL) defines users with different roles and permissions: Login passwords are hashed with SHA-2 using 512-byte keys and the results are stored within each VHM. When administrators attempt to login, their submitted passwords are hashed and the results are compared to the stored hash values. 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 de-authenticates.
- For each user, user name from 802.1X, Private Pre-Shared Key, or Captive Web Portal; however it does not receive the login credentials from the AP. It will also detect the client device’s MAC address, IP address, and OS.
- 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.

• If Client Management is in use, Aerohive can detect installed applications, certificate data, and security policy configuration for each enrolled device as well as manage and revoke applications.

Monitoring & Incident Response

Aerohive has technical support personnel available 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 Client Services and representatives from technical support, cloud operations and product engineering.

Breach Notifications

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.

Information about security vulnerabilities or breaches are posted on the Aerohive corporate web site and can be found by following the links to how to contact us, and from there to the product security pages.  http://www.aerohive.com/support/security-center

Forensic Analysis Procedures

Aerohive has technical support personnel 24x7, with additional staff on call responsible for performing forensic security analysis if required. The technical support staff has the ability to collect relevant logs and records using proper best practice diagnostic procedures.

Availability

Uptime

HiveManager Online is guaranteed for 99.99% uptime, excluding scheduled maintenance windows. Aerohive’s Cloud Service Level Agreement (SLA) is available at:  http://www.aerohive.com/pdfs/Aerohive-Cloud-Services-Platform-SLA.pdf

Disaster Recovery (DR)

Aerohive’s Disaster Recovery Plan includes proactive platform 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.
Cloud Services Platform: Security and Availability Controls

Availability Monitoring
Aerohive employs a distributed availability monitoring system on our cloud infrastructure which includes transactional user login simulation monitoring from multiple regions. If the end user is unable to login to our Cloud Services Platform, an email alert and text message will be auto-generated and sent to the Aerohive Cloud Operations Team. Aerohive also provides proactive notifications to our customers via the Aerohive support portal.

It is important to note that HiveManager as a network management platform, is not in the data path of customer data nor does its failover impact the ability of end users or devices to access 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 on both local and remote servers (at different data centers) in a compressed format and inaccessible to users.
- Backups are archived for 7 days on a local server and for 30 days on a remote server.
- An authenticated administrative-level user is required to restore the data in corresponding user accounts.

Data Recovery
Backed-up customer data can be recovered in 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, it is possible to restore a customer configuration data which existed up to 1 hour prior to the failure. Applications such as ID Manager and Client Management are backed up daily and configuration data can be restored from the prior daily backup.

System Monitoring
Complete monitoring is performed for the Cloud Services Platform encompassing usage of a global system performance monitoring tool, measuring service level monitoring & notification, and cloud HTTP monitoring. Aerohive’s Cloud Operations Team has access to dashboards measuring production capacity, usage, and trend monitoring. Performance snapshots are taken of running systems and are programmatically raised as alarms when internal thresholds are met for learned performance metrics.

The Aerohive Technical Support Team has 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 the inherent elasticity of the cloud. New servers and back-end infrastructure can be instantiated as needed based on load, customer, and partner growth and as a consequence of monitoring operations for learned patterns of system performance.
Traffic Encrypted & Restricted
All administrative network traffic is encrypted. HiveManager uses CAPWAP over HTTPS and SSH 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 or monitoring access to HiveManager Online or other Aerohive applications.

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

Vulnerability Scans, Penetration Tests and Antivirus
Aerohive’s infrastructure proactively manages firewall and networking security policies for the services hosted. Aerohive utilizes best current industry practices regarding security and access procedures, to limit access and permissions to these systems. External security experts are under contract to perform regular vulnerability scans and penetration tests.

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, and Beta testing before getting staged in a production environment, tested again, and finally deployed in production. The Cloud Services Platform allows customers to participate in the Aerohive Beta program, test-driving the latest functionality by trying HiveManager Online and application Betas without having to upgrade their entire network and disrupt operations.

Third Party Software Patches
Third-party patches are applied into Aerohive systems following the same three-stage Change Control Policy as Aerohive product releases. Major version upgrades of third-party software are planned as part of 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 an Aerohive partner (an integrator or managed service provider) 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 Cloud Services Platform applications are being evaluated by or sold to a customer. The new user will be registered with Admin permissions and can create other users within the account realm. Aerohive’s Technical Operations (TechOps) and Technical Support Teams have potential logical access to the system for troubleshooting purposes.
Cloud Services Platform: Security and Availability Controls

Password Policies (Resets, Storage)
Only an administrator who has sufficient permission to administer other users within his/her account realm can perform password resets. No passwords are stored in clear text. 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, before making any changes.

SSO, Session Timeouts
Aerohive supports SSO within the MyHive environment that includes the portals for HiveManager Online, ID Manager, Client Management, Redirector, and Social Login. Administrative sessions are automatically closed if idle for 15 minutes. Timeout expiry values are configurable. Reports of failed login attempts could potentially be requested.
About Aerohive

Aerohive (NYSE: HIVE) unleashes the power of enterprise mobility. Aerohive’s technology enables organizations of all sizes to use mobility to increase productivity, engage customers, and grow their business. Deployed in over 14,000 enterprises worldwide, Aerohive’s proprietary mobility platform takes advantage of the cloud and a distributed architecture to deliver unified, intelligent, simplified and cost-effective networks. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif.

For more information, please visit www.aerohive.com, call us at 408-510-6100, follow us on Twitter @Aerohive, subscribe to our blog, join our community, or become a fan on our Facebook page.

“Aerohive,” “HiveManager” and “HiveOS” are registered trademarks of Aerohive Networks, Inc. All product and company names used herein are trademarks or registered trademarks of their respective owners. All rights reserved.