Security Overview

Hive Technology, Inc.

September 2018

Table of Contents

Introduction

Thousands of businesses and organizations rely on Hive as a unified platform for their teams' collaboration, enabling them to communicate on, plan, execute and manage projects seamlessly. More than just a valuable hub for team collaboration, Hive is built to keep your organization's data secure. This whitepaper applies to all Hive products (Professional and Enterprise).

Application security

Hive user interfaces

Hive can be utilized and accessed through a number of interfaces, platforms, and devices; each has security settings that protect user data without compromising ease of use.

Web
The web user interface is accessible through any modern web browser. It allows users to upload, download, view, and share their files. The web interface also allows users to open existing local versions of files through their computer's default application.

Mobile
The Hive mobile application is available for Android and iOS devices. The mobile application allows users to communicate and collaborate with their team on the go.

Encryption

Data in transit
To protect data in transit between Hive user interfaces and Hive servers, Secure Sockets Layer (SSL)/Transport Layer Security (TLS) is used for all data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. On the web user interfaces we flag all authentication cookies as secure and enable HTTP Strict Transport Security (HSTS).

Data at rest
Hive data added by users are encrypted at rest using 256-bit Advanced Encryption Standard (AES). User data are stored across multiple availability zones using third-party systems.

Key management
Hive's key management infrastructure is designed with operational, technical, and procedural security controls with very limited direct access to keys. Encryption key storage, generation, and exchange is fully decentralized.

Access to production systems is restricted to unique SSH key pairs for each system. An internal system manages secure public key exchange processes, and private keys are stored securely. Hive's internal security team automates the distribution of sensitive keys to systems.

Protecting authentication data
Hive uses hashing to protect user login credentials. Each password is salted with randomly generated unique per-user salts. We encrypt the hashes with a key stored separately from our database, which keeps passwords secure in the event of a database compromise.

Malware scanning
Hive utilizes an automated scanning system designed to stop malware from being spread through our systems. The malware scanning system follows industry-standards and is regularly kept up to date through automated updates.

Network security

Hive's security team diligently and systematically maintains the security of our back-end network. The network security and monitoring techniques utilized at Hive are designed to provide multiple varied layers of defense. We employ firewalls, network vulnerability scanning, network security monitoring, and intrusion detection systems to make certain that only eligible and non-malicious traffic reaches our infrastructure.

Our internal private network is segmented according to use and risk level. Only authorized IPs and MFA-enabled access are capable of connecting to production systems. IP addresses with access are associated with the corporate network and are reviewed on a quarterly basis to ensure only secure access to our production environment. Access to maintain and modify the IP address list is restricted to a small subset of authorized individuals. Traffic from the internet to our production network is secured by multiple layers of firewalls and proxies.

Internet-bound traffic from the production network is carefully controlled through dedicated proxy services. Past that, the proxy services are protected by restrictive firewall rules.

Hive instruments industry-leading tooling to monitor laptops and desktops with Mac operating systems and production systems for malicious events. Security logs from the tooling are collected in a central location for incident response following industry standard retention policy.

We identify and mitigate risks through recurring network security testing and auditing by both our internal security team and 3rd party security specialist teams.

Vulnerability management

Hive's security team does automated and manual application security testing. We also work with 3rd party specialists on a regular basis to prevent, identify, and patch potential security vulnerabilities. The feedback from internal and 3rd party testing activities is assessed, prioritized, and assigned as immediately actionable items to be completed by our internal security team. As part of our information security management process, findings and recommendations and actionable next steps outputted from all of these assessment activities are reported to Hive management.

Change management

A formal Change Management Policy defined by the Hive engineering team ensures that application and infrastructure changes are authorized before implementation in production environments. Changes to source code are initiated by developers that would like to make enhancements or patches to the Hive applications and services. Changes are made and stored in a version control system (VCS) and are required to go through both manual source code review as well as automated and manual Quality Assurance (QA) testing to verify that security requirements are met. Successful completion of code review and QA processes lead to implementation of the change in staging environments and eventually production environments after a final review. Our software development lifecycle (SDLC) requires strict adherence to secure coding style and guidelines, as well as screening of code changes for potential security issues via our QA and manual review processes. Changes released into production are logged and retained. Alerts are sent to Hive Engineering Team management automatically.

Any changes to infrastructure and system configuration are restricted to authorized personnel only. The Hive Security Team is responsible for maintaining system configuration and infrastructure security; this includes ensuring that server, firewall, and other systems configurations are kept up to date with industry standards. These configurations and standards are kept up to date regularly.

Security scanning and penetration testing

Our engineering and security teams perform automated and manual security testing on Hive systems on a regularly recurring basis with a goal of identifying and patching security vulnerabilities. In addition to internal testing, Hive works with 3rd party specialists to perform regularly recurring penetration testing on production environments to keep our applications secure. Past internal and 3rd party testing, we leverage automatic analysis systems to scan for security vulnerabilities on proprietary systems and open source systems we leverage.

Information Security

The Hive team has established an information security management framework which describes the purpose, principles and policies for how we maintain trust. This framework is used to assess risks, maintain confidentiality, privacy, availability, and integrity of Hive production systems. We regularly review, improve, and update security policies to keep in line with industry standards. We also regularly provide internal security training, perform application & network-layer security testing, monitor compliance with security policies and conduct risk assessments.

Policies

We have established and maintained a set of security policies which cover Information Security, Data Privacy, Physical Security, Incident Response, Business Continuity, Logical Access, Physical Production Access, and Change Management. The policies for each section are reviewed and updated at least annually. The policies are enforced by the Hive Security Team. All employees and contractors are required to participate in security training when joining the company as well as in ongoing security awareness training.

Information Security

Policies related to user and Hive information with a key focus on authentication requirements, data security, systems security, user data privacy, restrictions on employee use of resources, and handling of potential issues in said areas.

Data Privacy

Requirements for how we handle and protect user data at Hive to ensure we adhere to our Privacy Policy agreement.

Physical Security

Requirements for how we maintain safe and secure environments for employees and property at Hive. See “Physical Security” section below for more detail.

Incident Response

Requirements for responding to, triaging, and taking action on potential security incidents. This includes how we conduct assessments, communication and investigation.

Business Continuity

Requirements, policies, and procedures for maintaining (and restoring if need be) business critical functions in the event of a disruption. Includes planning, documentation, incident response, and execution.

Logical Access
Requirements and policies for maintaining security for access to Hive systems and user data with a focus on access control.

Physical Production Access
Procedures and policies for restricting access to physical production systems. Includes management review of personnel as well as de-authorization of terminated personnel.

Change Management
Requirements and policies for source code review, QA testing, and managing changes that potentially impact security by developers. Cover potential changes to source code, system configuration, and releases to production environments.

Employee policy
All Hive employees are required to complete background checks, sign a security policy agreement, and non-disclosure agreement when hired. All new employees undergo mandatory security training as well as ongoing security education both as policies are updated and annually.

Employee access to Hive production environments is maintained through a central directory. Authentication for access is managed through a combination of password-protected unique SSH keys, multi-factor authentication and strong password requirements. Remote access requires use of VPN and multi-factor authentication. Access to production networks is strictly limited based on policies defined by the Hive Security Team. Additionally, our internal policies require employees accessing production environments to follow best practices for storage of SSH private keys.

Physical Security

Infrastructure
Physical access to organization facilities where production systems are hosted is restricted to personnel authorized by the Hive Security Team only when necessary for the personnel to perform their job function. All employee access to physical production environments requires explicit approval by management and the Hive Security Team.

Hive maintains records of access requests, approvals, and justifications for access. Upon approval, a member of the Hive Security Team will contact the subservice organization to request access for the approved individual. Upon approval by the subservice, the subservice will record the employee's information in their own system and grant approval for the employee's personnel badge. Once access is granted to the approved employee, the data center is responsible for ensuring access restricted to only approved physical systems.

Corporate offices

Physical security
The Hive office's physical security team is responsible for enforcing physical security policy and overseeing the security of Hive offices.

Corporate facility access policy
Physical access to corporate facilities is restricted to authorized Hive personnel and pre-registered visitors who are accompanied by authorized Hive personnel.

On-premises Capabilities

Hive Enterprise provides implementation and support for customers with requirements for hosting Hive production services on-premises. Our on-premises capabilities include hosting of containerized versions of Hive production systems to allow for maximum security should the customer or organization require it. On-premises implementations are specific to each customer but follow the standards outlined in this whitepaper where applicable.

Privacy

Organizations trust Hive with their most important work and data every day. It's our responsibility to protect this information and ensure it is kept private.

Privacy policy
Our privacy policy is available at hive.com/privacy-policy. The Hive Privacy Policy provides details on following items:

- What data we collect and why
- With whom we may share information
- How we protect data
- How long we retain data
- Where we keep and transmit your data
- What happens in the event the policy changes

Transparency
Hive is committed to transparency in handling law enforcement requests for user data. We scrutinize all data requests to ensure they comply with the law. We are committed to giving users notice, as permitted by law, when their accounts are identified in a law enforcement request.