BI Helper Information Security Guide

Version	Date (Y-M)	Author	Summary
1.0	2020-02	Ishan Rastogi	Initial release
2.0	2021-04	Ishan Rastogi	Added sections on security standards, PDF generation and email process
2.1	2021-08	Kiran Hosakote	Minor edits and updates
3.0	2022-08	Kiran Hosakote	Added SOC2 and HIPAA, code repo sections
3.1	2023-03	Ishan Rastogi	Guard Duty related updates
3.2	2023-10	Ishan Rastogi	Upgraded vulnerability section
3.3	2024-04	Kiran Hosakote	Added DMARC Compliance

SECURITY STANDARDS AND COMPLIANCE

Security Standards

BI Helper **https://portal.bihelper.tech** (“application”) is hosted in the AWS US East 1 Region. It is designed, built and deployed by **Vega Solutions** LLC (Vega) to the following security standards.

1. **CIS AWS Foundations Benchmark** which is defined by the Center for Internet Security as an objective, consensus-driven security guideline for AWS Cloud Providers.

2. **AWS Foundational Security Best Practices standard** which is defined by AWS as a set of controls that detect when deployed accounts and resources deviate from security best practices. This standard provides actionable and prescriptive guidance on maintaining and improving the organization's security position.

SOC 2 and HIPAA Compliance

SOC 2: On an ongoing basis, Vega runs a SOC 2 assessment from AWS Audit Manager on the BI Helper application and infrastructure. It also runs a monitoring tool on its code repositories for code vulnerability testing. The evidence collected from these activities along with other controls for data security and privacy is used to generate periodic SOC 2 assessment reports. Please email support@bihelper.tech for the latest assessment report.

HIPAA: As defined in 45 CFR 160.103, Vega Solutions LLC is a Business Associate, not a HIPAA covered entity. When a covered entity subscribes to a BI Helper license, Vega will execute a Business Associate Contract with them to enable BI Helper to access their data in compliance with HIPAA.

APPLICATION SECURITY

Application Roles

There are four roles defined in the application, which are used as follows:

- System - Used for audit logs and automated internal tasks.
- Anonymous - Used for actions performed anonymously, e.g., password reset.
- User - End-user signups, to provide access to setup and run PDF generation and distribution campaigns.
- Admin - Access to user management, logging controls, service health checks.

Login - JWT Tokens

On presentation of credentials, users are presented with JWT tokens and logins are done in a stateless manner.

- JWT tokens are signed and cannot be altered by an end-user.
- JWT tokens are signed using a Base64 encoded string.
- The securing keys have a length of 512 bits.

Cookie Theft Protection

BI Helper has a complete cookie theft protection mechanism. It stores your security information in a cookie as well as in the database, and each time a user logs in, the values are modified and checked to see if they have been altered. So anyone who steals your cookie will be able to use it only once, at the most.

CSRF Protection

CSRF protection is provided out-of-the-box.

SSL Enabled

The core application runs behind a proxy, with SSL access only. The SSL Certificates are renewed every 3 months.

INFRASTRUCTURE SECURITY

BI Helper **https://portal.bihelper.tech** runs entirely in the AWS cloud. It does not require users to install any agent or client within their IT networks in order to generate and distribute PDF reports.

Virtual Private Cloud

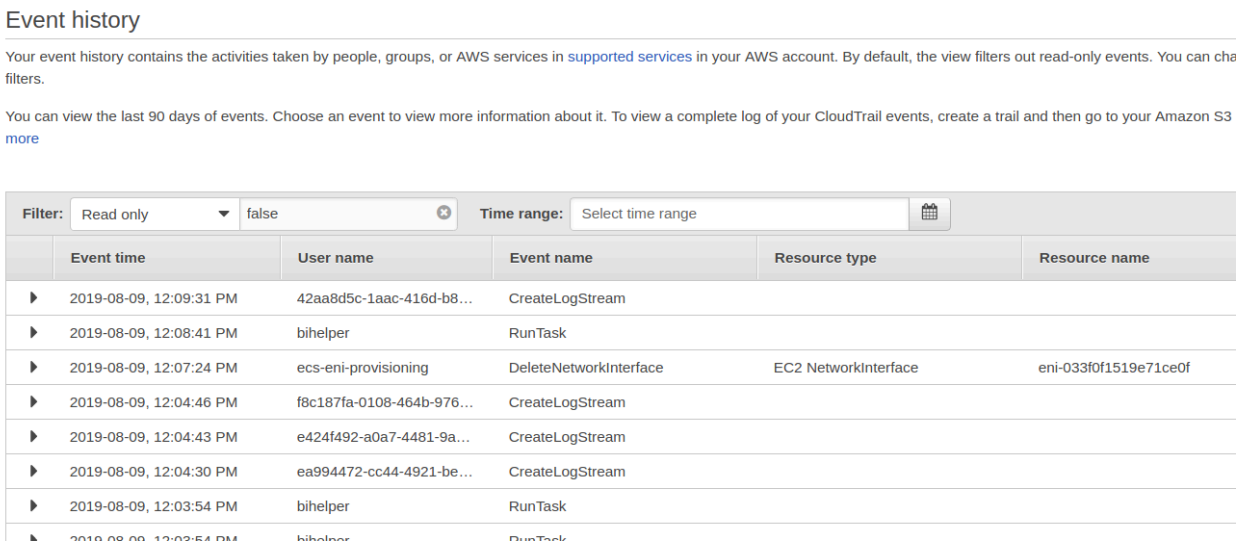
BI Helper is hosted in the AWS US East 1 Region in its own Virtual Private Cloud within the AWS cloud. All infrastructure resources reside in this AWS VPC, providing complete isolation of the network and resources from all other AWS users. In addition to the VPC, the databases and internal services reside in a private subnet.

The only site open to the public internet is BI Helper, where users log into the application. No other microservices are accessible to the public internet.

Note: For any clients with data sovereignty requirements, BI Helper can generate and store their PDFs in any AWS geo region.

Logging and Alerting

Infrastructure Events Snapshot: The logs for access to the infrastructure are stored, and can be used to establish any trail within the infrastructure.



Application Events Snapshot: The logs for access to https://portal.bihelper.tech are stored in the database and are available for complete audit of user access.

08/08/19 09:07:55	admin	AUTHENTICATION_SUCCESS
08/08/19 06:40:03	admin	AUTHENTICATION_SUCCESS
07/08/19 17:04:12	admin	AUTHENTICATION_SUCCESS
07/08/19 16:48:06	admin	AUTHENTICATION_SUCCESS
07/08/19 15:19:16	admin	AUTHENTICATION_SUCCESS

Infrastructure monitoring services:

In addition to the above we have the following AWS services running 24*7 to monitor infrastructure security:

- AWS Security Hub keeps a check on the best practices for security and notifies us of any deviations from them.
- AWS Guard Duty fires events in case of anomalies in infrastructure access or in case of unauthorized access attempts.
- AWS WAF blocks unauthorized and malicious web access.

Access to Infrastructure Resources

Applications within the BI Helper VPC are treated as users when they need to access BI Helper resources. Separate users **(IAM)** / roles are created for such services and each service is allowed access only to the required resources.

Data Retention and Encryption

BI Helper saves the generated PDF reports in client-specific AWS S3 buckets. Data retention periods are license driven:

- Standard license: No data is retained in BI Helper. All PDFs are deleted immediately after the emails are sent. This is user auditable.
- Premium license: PDFs are retained for 5 days in designated client folders on a dedicated SFTP server and are deleted thereafter. Folders have user access credentials and the PDFs are ONLY accessible to the named client users and BI Helper system administrators. The BI Helper SFTP server is not publicly accessible on the internet.
  Premium license users are required to share the IP addresses from where they run BI Helper. These are whitelisted and login credentials are created and shared with the users, enabling them to access their PDFs on the BI Helper SFTP server.
- Enterprise license: PDFs are retained in designated client folders on the SFTP server, as with the Premium license. Data retention (days) can be configured to user requirements.

The files stored in AWS S3 are AES 256 encrypted, and users may provide their own keys to encrypt their data.

The S3 buckets are always private and their data policy changes are strictly enforced.

Key Rotation Policies

AWS Systems Manager is used to access development and production servers. No SSH Keys are used for any development or for accessing production servers.

The OAuth2 token encryption keys (user authentication) are rotated once in six months.

Email Security

BI Helper uses AWS SES to send emails with the attached PDFs to end-users.

Standard and Premium License: By default, AWS SES uses *opportunistic TLS*. This means that AWS SES first attempts to make a secure connection to the receiving mail server. If it cannot establish a secure connection, it sends the message unencrypted.

Enterprise License: BI Helper provides the following email security options:

- TLS Enforcing (Optional): AWS SES only sends the message to the receiving email server if it can establish a secure connection. If AWS SES can't make a secure connection to the receiving email server, it drops the message.
- S/MIME / PGP Encryption of emails: You can use AWS SES to send messages that are encrypted using S/MIME or PGP. Messages that use these protocols are encrypted by the sender. Their contents can only be viewed by recipients who possess the public keys that are required to decrypt the messages.
- Custom Mail From Domain: Setup a custom MAIL FROM Domain for a Verified Email Address.

DMARC Compliance: In order to send DMARC (SPK, DKIM) compliant emails, BI Helper enables clients to set up branded “MAIL FROM” domains.

AWS Resources Compliance Report

The AWS Resources Compliance Report is generated using the rules defined by AWS Config. Please write to support@bihelper.tech for a detailed report.

CODE REPOS AND VULNERABILITIES

BI Helper's codebase is hosted in Bitbucket. The code repositories are integrated with Snyk. Snyk is a security platform which continuously monitors the codebase for vulnerabilities and reports daily on any new ones detected. Automated Pull Requests are raised and reviewers assigned in case of any detection.

In addition to their own feed, Snyk monitors the following vulnerability databases:

- Common Vulnerabilities and Exposures (CVE): Provides "...an identification number, description, and at least one public reference for publicly known cybersecurity vulnerabilities." Launched in 1999, CVE is a standardized resource for other tools and services to track and evaluate vulnerabilities.

- National Vulnerability Database (NVD): A U.S. government repository of standardized vulnerability management data, including impact metrics such as CVSS. It uses CVE as one of its inputs.

STAFF DEVICES

All BI Helper devices are scanned every day for the following attributes:

1. Antivirus
2. Disk Encryption
3. Updated Device OS
4. Screen lock

The above attributes are mandatory for all devices and any deviation is reported to the system administrators.

SECURE USER LOGIN - OAUTH2 AND MFA

BI Helper runs the PDF generation and emailing processes in the cloud. This requires BI Helper to access IT resources of the users, such as login credentials and report publication URLs.

To access these resources via APIs, BI Helper uses the OAuth2 protocol. By default, BI Helper works with Microsoft OAuth2 to fetch reports in Power BI Service.

BI Helper can be extended to add any OAuth2 provider to access the underlying reports from other BI tools.

OAuth2 tokens are encrypted using **AES 256 encryption and** stored in the application database using AWS Secrets Manager. They are only decrypted at the time of user login, and are not human readable when stored.

BI Helper integrates with any **Multi-Factor Authentication (MFA)** setup in your organization, providing the additional benefits of:

1. Greater user control in BI Helper.
2. Ensuring that no user other than the service account used by BI Helper can access your resources.
3. Enabling your sysadmin to easily revoke access of BI Helper to your reports.

PDF GENERATION AND EMAILING

When a BI Helper job is run, new servers are spawned for PDF generation. These servers are transient in nature. During process execution, the PDFs are encrypted and saved in S3. Once the PDF generation process is complete and emails are sent to the respective users, the servers and the storage associated with them are destroyed.

Job execution logs for this process are stored in AWS Cloudwatch and are accessible after the process ends. The logs contain metadata about job execution and no confidential information is written into them.

Job execution logs are retained for three months and are only used to assist users with support requests.

- **End of document** -