Behavioral Health Link

2023

Security Summary for BHL Platform

The purpose of this document is to provide a comprehensive overview of the security measures and processes implemented by Behavioral Health Link (BHL) regarding updates, patching, remote access, and security regarding the Software as a Service product 'The BHL Platform'. This document serves as a response to a Request for Proposal (RFP) from a potential client or partner, who is seeking assurance that their confidential information will be protected by a secure and reliable system. By providing a detailed explanation of our security measures and procedures, we can demonstrate our commitment to maintaining a high level of security for our clients and differentiate ourselves from competitors who may not prioritize security to the same extent.

Table of Contents

Brandon Rennolds

IT Security Manager

404-666-5793

brennolds@ihrcorp.com

behavioralhealthlink.com

Behavioral Health Link

System Overview

The BHL Platform is a cutting-edge Software as a Service (SaaS) application that operates on Microsoft Azure and boasts a SOC 2 Type II certification, attesting to the system's robust security and reliability measures. The application leverages Azure App Services, Azure SQL Server, Azure Storage, and multiple microservices to provide a comprehensive suite of tools and solutions for managing behavioral health services.

The BHL Platform is meticulously maintained by a Continuous Integration/Continuous Deployment (CI/CD) process via Azure DevOps. Application changes are subject to rigorous testing and deployed to multiple test environments, undergoing a meticulous quality assurance process, before being finally released to the production environment. This approach ensures that the platform is kept up-to-date, thoroughly vetted, and always at peak performance.

1201 Peachtree St NE Building 400, Suite #1215. Atlanta, GA 30361
behavioralhealthlink.com
404-420-3202

Behavioral Health Link

Security Measures

System Updates and Patching

All services within our infrastructure are hosted on Microsoft Azure, which negates the need for operating system virtualization. As a result, Azure directly manages and updates all services, as outlined in the referential documentation provided (here). In addition, our team diligently monitors and updates code-level packages to ensure timely identification and mitigation of any detected vulnerabilities.

To detect vulnerabilities, we use Microsoft Defender for Cloud, which conducts weekly vulnerability scans based on the FedRAMP 'High' controls. Additionally, an endpoint vulnerability management system scans code vulnerabilities, ensuring that the machines developers work on, and the code they deploy, remain up-to-date and free of severe vulnerabilities. This comprehensive approach to vulnerability management enables us to maintain a secure environment and prevent potential security breaches.

Remote Access

The BHL Platform, being a SaaS application, imposes no network restrictions on access to the public client interface. For internal developers and administrators, a robust SSL VPN has been implemented to provide secure remote access. The VPN appliance is automatically updated with the latest firmware releases as they become available, ensuring optimal protection. Direct access to the Azure infrastructure mandates the use of VPN access.

VPN login credentials are federated through Microsoft Azure Active Directory and reinforced by multifactor authentication. We maintain audit logs that are regularly monitored to identify and investigate any unusual or suspicious activities.

At the database level, access is controlled via role-based access control (RBAC) mechanisms to prevent unauthorized access and ensure that individuals have only the necessary privileges. Microsoft Azure manages the database logins, and multifactor authentication is employed to further secure direct database access.

Behavioral Health Link

Infrastructure Security

Firewall

The BHL Platform employs a robust security infrastructure, utilizing an Azure-hosted web application firewall (WAF) that is seamlessly integrated with Azure Front Door, adhering to a zero-trust framework. The WAF is equipped with a comprehensive set of predefined protection policies that defend the application against a wide range of cyber threats, including distributed denial of service (DDoS) attacks, SQL injections, directory traversal attacks, cross-site scripting, and more.

In addition to serving as a content delivery network (CDN) and load balancer, Azure Front Door offers supplementary route protection mechanisms to mitigate risks associated with denial-of-service attacks, further bolstering the platform's security posture.

Monitoring and Logging

The BHL platform leverages Azure Sentinel as a Security Information and Event Management (SIEM) system for comprehensive logging of Azure activity, detection of suspicious behavior, and tracking and auditing of all actions within the cloud platform. This seamless integration extends to Azure App Service, Azure SQL, and all backend infrastructure components of the BHL Platform.

Azure Sentinel boasts an extensive array of playbooks and automations designed to alert BHL's security team in the event of active incidents or unusual activity. Moreover, external applications, such as the SSL VPN appliance, are also integrated into this system, ensuring comprehensive coverage and continuous monitoring across the entire BHL environment.

IDS

BHL employs Microsoft Defender for Cloud as an Intrusion Detection System (IDS) and for vulnerability management within the Azure infrastructure. Defender for Cloud offers comprehensive continuous monitoring for any entity accessing Azure services. Automated vulnerability scans are conducted weekly and addressed in accordance with BHL's vulnerability management policy.

Furthermore, Defender for Cloud delivers automatic alerts for issues such as atypical logins, SQL injection attempts, and service misconfigurations, effectively covering a vast range of potential attack vectors. For regulatory compliance, Defender incorporates numerous predefined controls that align with standards such as SOC 2 and FedRAMP. BHL takes advantage of these compliance offerings to ensure that services are configured to consistently meet and maintain compliance with all applicable regulations.

Hardware / Software Refreshes

At BHL, the majority of developers rely on Azure Virtual Desktop for their daily operations. This eliminates the need for a hardware refresh cycle and allows for immediate resource upgrades as needed. BHL ensures that all software utilized, including industry-standard tools such as Visual Studio, VS Code, and SQL Server Management Studio, remains up-to-date and supported. This also extends to code packages, which are consistently updated to minimize BHL's exposure to vulnerabilities.

Given that all services are deployed from a serverless perspective, there is no hardware refresh requirement for any public-facing components. Additionally, no software needs to be redeployed to the primary application apart from code updates.

Behavioral Health Link

Reporting

BHL is prepared to provide the following report monthly for clear concise communication ensuring potential clients and partners are kept informed.

- Availability of critical systems
- Vulnerability Scans and remediations taken
- Intrusion Detection Reports
- Security enhancements made in the environment
- Security incidents that occurred within the month, along with affected resources and remediations taken

1201 Peachtree St NE Building 400, Suite #1215. Atlanta, GA 30361
behavioralhealthlink.com
404-420-3202