mindbody

Cybersecurity Whitepaper

Summary

Keeping your data secure, confidential, and readily accessible are our greatest priorities. Mindbody's industry-leading cybersecurity program is based on the concept of Defense in Depth: securing our organization and your data at every layer.

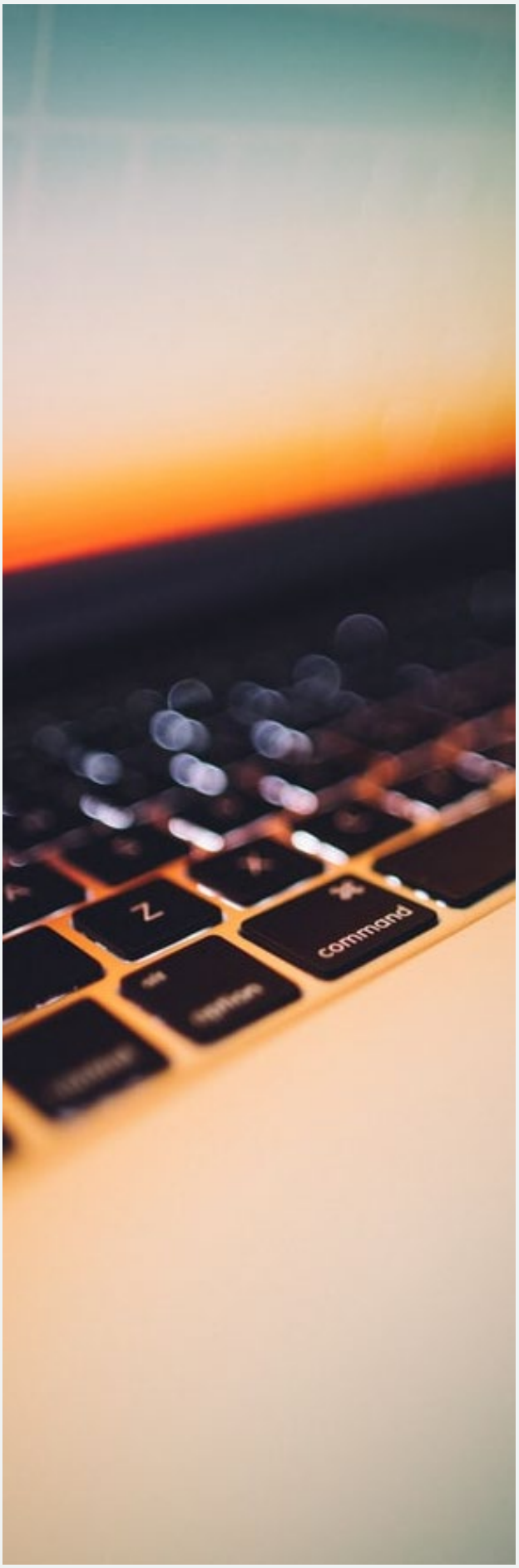
Our cybersecurity program aligns with CIS CSC 20 and NIST Cybersecurity frameworks, and Mindbody is HITRUST CSF and PCI DSS Level 1 service provider certified. While no system can guard against every potential threat, Mindbody's defensive line is advanced and monitored 24/7, 365 days a year by skilled, highly trained professionals.

Privacy Policy:
https://www.mindbodyonline.com/privacy-policy

Security Policy:
https://www.mindbodyonline.com/security-policy

Mindbody's Cybersecurity Team, led by our Chief Information Security Officer (CISO), is responsible for the implementation and management of our cybersecurity program. The CISO is supported by the members of Mindbody's Cybersecurity Team, who focus on Security Architecture, Product Security, Security Engineering and Operations, Detection and Response, and Cybersecurity Risk.

The focus of Mindbody's Cybersecurity program is to protect the confidentiality, integrity, and availability of our customer's data. To this end, our team of dedicated cybersecurity practitioners, working in partnership with peers across the company, take specific steps to identify and mitigate risks, implement best practices, and continuously develop ways to improve.



Migration to Amazon Web Services (AWS) and Devops (IAC)

As of Q3 2021, driven by the need for faster to market product improvements, dynamic scalability, and innovation acceleration, Mindbody has migrated it's IT workloads and systems to the AWS cloud. AWS is PCI Level 1, HITRUST CSF, ISO 27K, and SOC1/2/3 compliant and certified. AWS Cloud Services provide advanced cybersecurity tooling by providing a standardized approach to cybersecurity using built-in Identity and Access Control, Infrastructure Security, and Data Protection, which enable the Mindbody Cybersecurity Team to operate faster and more effectively.

Along with our migration to the AWS cloud, Mindbody has pivoted to embrace DevOps through re-architecting our core services to Infrastructure as Code (IaC). IaC provides greater visibility and testing of the security configuration of an environment. Immutable infrastructure combined with version-controlled automated deployment processes ensures that security is applied universally, eliminating configuration drift and one-offs.

Software Security By Design

Mindbody's Software Security team has built a robust and secure software development lifecycle (SDLC) that involves several key components:

Refinement
Mindbody's Software Security team works hand-in-hand with development teams and product owners on defining and refining security requirements prior to development.

Development
The Software Security team provides services, tooling, and consulting to teams developing products requiring high security.

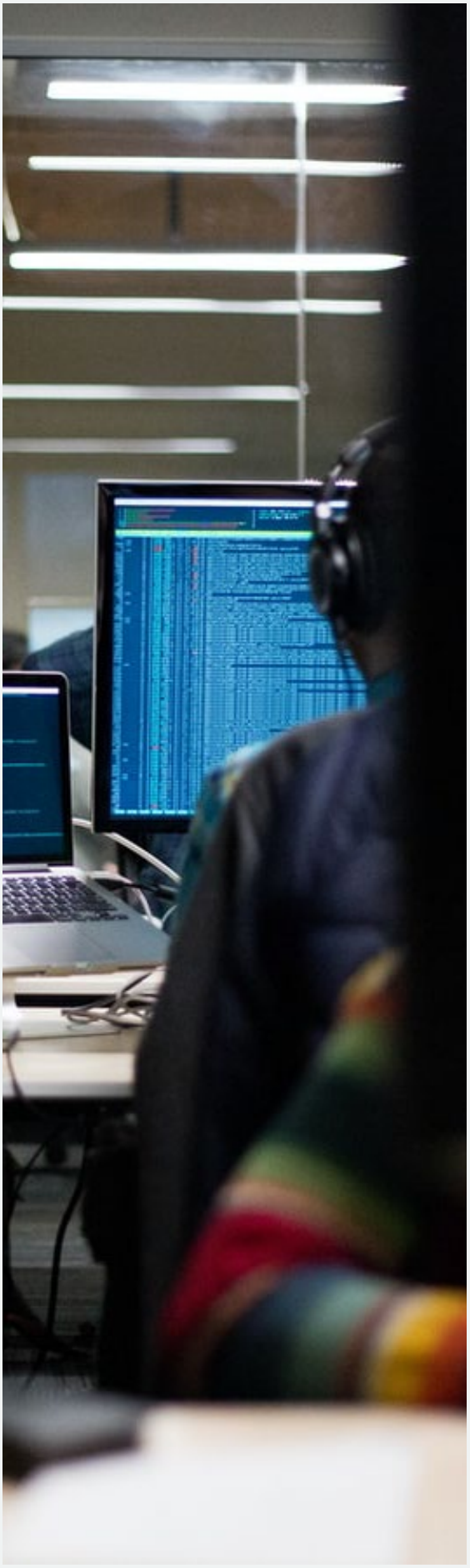
Testing
The Software Security QA team collaborates with development teams to incorporate security tests into their standard QA processes.

Release
Software Security provides oversight, conducts code reviews, and manages automated secure code scanning within Mindbody's release pipelines.

Post release
The Mindbody Software Security Red Team conducts ongoing penetration tests to help insure against exploitable vulnerabilities within our software.

Responsible Disclosure

While we strive to catch all vulnerabilities within each phase of the SDLC, we realize that sometimes mistakes can happen. With this in mind, we have created a public bug reporting program to facilitate responsible disclosure of potential security vulnerabilities. All identified vulnerabilities are validated for accuracy, triaged, and tracked to resolution.



Data Encryption

In transit

All data transmitted between Mindbody clients and the Mindbody service us strong encryption protocols. Mindbody supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.2 or greater protocols.

At rest

Credit card and personal health information (PHI) that is written into the SOAP notes field is application level encrypted using FIPS 140-2 compliant encryption standards. All encryption keys are stored in a secure and segregated KMS with restricted access.

Mindbody has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials. Our customer data is hosted in AWS shared infrastructure, logically separated and is encrypted at rest using AES256.

Tokenization

Mindbody is actively deploying a tokenization service to store sensitive data such as credit card numbers. Tokenization is the process of turning a meaningful piece of data, such as an account number, into a random string of characters called a token that has no meaningful value if breached. Tokens serve as a reference to the original data but cannot be used to decipher the original values. Unlike encryption, tokenization does not use a mathematical process to transform sensitive information into a token. There is no key or algorithm that can be used to derive the original data for a token. Instead, tokenization uses a database, called a token vault, which stores the relationship between the sensitive value and the token. The real data in the vault is then secured. This dramatically reduces the risk of exposure or breach of data even compared to strong encryption.

Perimeter Protections

Access to Mindbody's production environment from open, public networks is restricted, with only a small number of production services accessible from the internet. Only network protocols essential for the delivery of Mindbody's service to its customers are open at our perimeter. Cloud-based web application firewalls are deployed across Mindbody services to protect against application layer web-based attacks. Mindbody utilizes third-party Content Distribution Network (CDN) services for redundancy and performance of services. Distributed Denial of Service (DDoS) and Bot protections are provided through third-party services.

Endpoint Security

All virtual servers, workstations, and containers are protected using advanced endpoint detection and response solutions. Windows servers and all workstations are hardened prior to deployment following the Center for Internet Security (CIS) benchmarks.

Mindbody workstations encrypt data at rest, have strong passwords, and lock when idle. Workstations run up-to-date monitoring software to report potential malware, unauthorized software, or other compromises.

User Security

All Mindbody team members are required to participate in ongoing Cybersecurity Awareness and Privacy training quarterly and annually. End-user communications are protected from phishing and business email compromise using industry-leading email protection solutions.

Multi-factor authentication (MFA) is required for all Mindbody team members accessing business systems and services, such as email and third-party cloud solutions.

Access Control

To minimize the risk of data exposure, Mindbody adheres to the principles of least privilege and role-based permissions when provisioning access. Team members are only authorized to access data that they reasonably must handle to fulfill their current job responsibilities. All production access is regularly reviewed and is an integral part of compliance with SOC1, PCI, and HITRUST.

To further reduce the risk of unauthorized access to data Mindbody employs a dedicated and separate identity authority as well as MFA for privileged access to systems with highly classified data, including our production environment where customer data resides.

System Monitoring, Logging, and Alerting

Mindbody monitors environments using coordinated, centralized logging and alerting. This allows both real-time analytics and retention for a comprehensive view of Mindbody's state of security across all corporate and production systems and services. Activities such as administrative access, privileged commands, and system calls on servers hosting sensitive data are logged, analyzed, and retained following PCI and HITRUST requirements.

Systems and services are monitored using a Security Incident Event Management (SIEM) system that gathers logs and creates alert triggers based on correlated events. In addition to an internally managed SIEM, Mindbody utilizes third-party Endpoint Detection and Response services for additional monitoring and analysis.

Vulnerability Management

Mindbody systems and services are frequently reviewed for potentially harmful vulnerabilities.

We use industry-recognized, third-party cybersecurity services, enterprise-class cybersecurity solutions, and custom in-house tools to regularly scan and analyze our systems and services to ensure that all vulnerabilities are identified and swiftly mitigated.

We employ qualified cybersecurity tools to provide regular dynamic scanning of our applications and systems and continuous static analysis of our codebase.

All found vulnerabilities are triaged, prioritized, and remediated promptly.

Business Continuity and Disaster Recovery

High Availability & Resiliency by Design
Mindbody takes advantage of the AWS cloud by distributing our platform across multiple availability zones (AZ) in each region we operate. Each AZ is a fully isolated partition consisting of at least one physical datacenter.

Fault Isolation and Failure Recovery
Systems are deployed across multiple availability zones or datacenters. Whenever possible, changes are made to only one zone at a time.

Data Backup and Recovery Testing
Customer data is backed up regularly using Amazon S3 Storage Services and replicated across multiple AZ's. Mindbody tests the integrity of backup data by performing automated data restoration processes.

Cybersecurity Incident Response

Mindbody has established policies, standards, and procedures for responding to potential cybersecurity incidents. The Mindbody Cybersecurity Incident Response team manages all cybersecurity incidents. Incident response procedures are tested, simulated, and updated annually at a minimum.

Vendor Management

To run efficiently, Mindbody relies on sub-service organizations. Where those sub-service organizations may impact the Cybersecurity of Mindbody's production environment, we take appropriate steps to ensure our Cybersecurity posture is maintained by establishing agreements that require service organizations to adhere to commitments we have made to users. Mindbody monitors the effective operation of the organization's safeguards by conducting reviews of all service organization's controls before use.

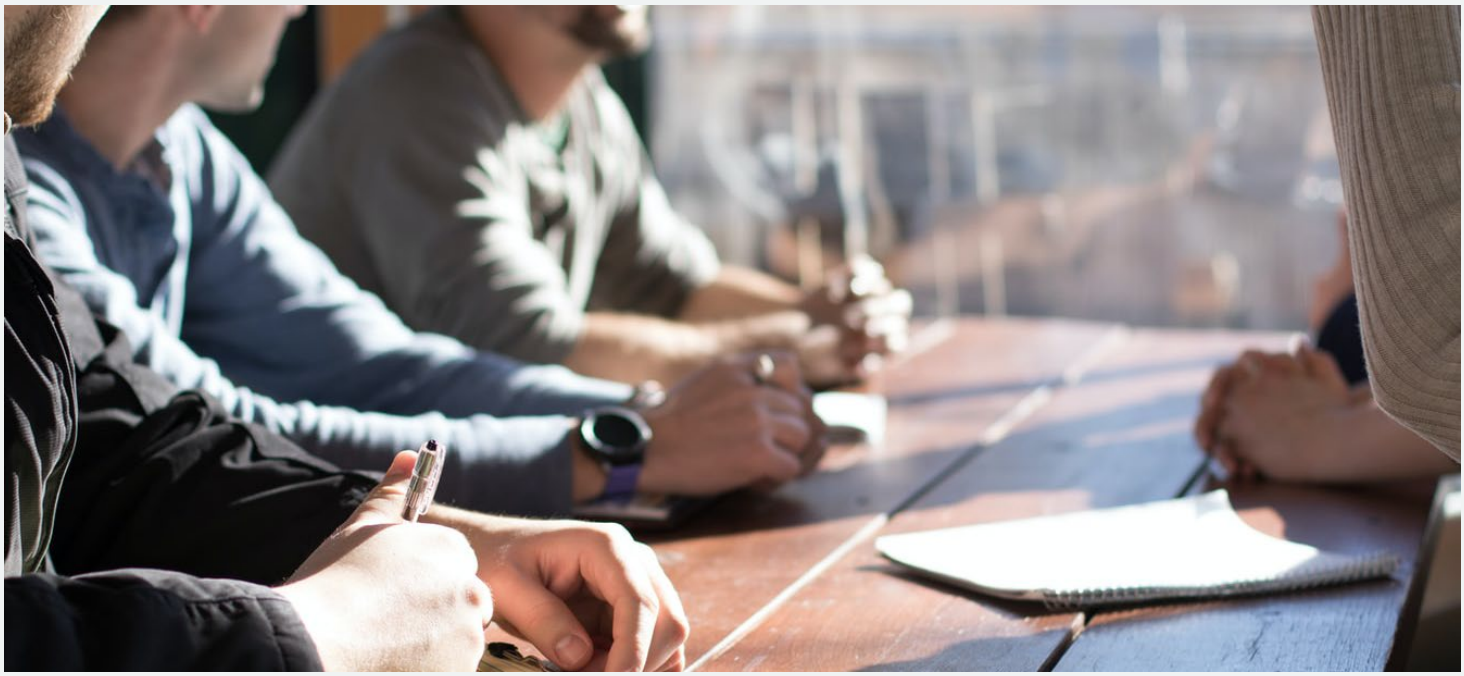
Our Cybersecurity Risk team manages a comprehensive third-party risk management program where each new vendor/third-party is evaluated for its cybersecurity risk and privacy program.

Security Compliance Audits and Assessments

Mindbody is continuously monitoring, auditing, and improving the design and operating effectiveness of our cybersecurity controls. These activities are regularly performed by both third-party credentialed assessors and Mindbody's internal Cybersecurity Risk and compliance teams. Assessment and audit results are shared with senior management, and all findings are promptly tracked to resolution.

Penetration Testing

In addition to our compliance audits and assessments, Mindbody engages both internal red teams and independent external entities to conduct application-level and infrastructure-level penetration tests at least annually. The results of these tests are shared with senior management and are triaged, prioritized, and remediated promptly.



Conclusion

Our commitment to wellness and the success of our customers is at the core of everything we do at Mindbody. As part of that, we work tirelessly to stay ahead of threat actors, always seeking to advance our cybersecurity capabilities. This document provides a view of Mindbody's industry-leading cybersecurity program. Please contact your account executive if you have any questions or concerns.

Jason Loomis
Chief Information Security Officer