LET'S TALK interactive

White Paper

Web: **letstalkinteractive.com** Email: **hello@letstalkcounseling.com** Phone: **844-880-8255**

Table of content

About Let's Talk Interactive

Founded in 2001, Let's Talk Interactive is a leader in creating custom, cutting-edge telemedicine solutions for healthcare providers and organizations. The firm's software pairs seamlessly with a host of hardware solutions and peripheral options and can be further enhanced with custom development and provider network solutions to create long term value and lasting relationships with clients.

Let's Talk Interactive recognizes that innovation in telemedicine expands beyond a "one size fits all" solution and continues to invest in intellectual property, including a proprietary software solution, to enable clients to successfully execute a 21st-century approach to healthcare.

Let's Talk Interactive offers four main solutions to users

1

Web design and custom software development

Our developers are experts in encryption and security with years of experience in the development of HIPAA-compliant websites, provider/patient portals, custom software and cloud applications, content management, e-commerce and web apps, along with API integration into a host of EMR/EHR platforms and devices.

2

Provider networks

We have an extensive network of healthcare and behavioral care providers, offering coverage and servicing all 50 states, including Puerto Rico. Our networks are developed nationwide, servicing Employee Assistance Programs, assisted living facilities, urgent care clinics and hospitals.

3

Software solutions

We offer a breadth of HIPAA compliant software solutions to fit a range of use cases, from a solo provider solution to sophisticated virtual and walk-in clinic software. Our software has the capability to service use cases ranging from behavioral healthcare, law firms, mortgage lenders, to providers with a need for live bio-analytics and remote patient care.

4

Hardware and software

We've made it simple to integrate and deploy HIPAA compliant video conference software, live bio-analytics, and our telemedicine office suite with a host of equipment and peripheral options. Bio-analytics are pushed live through the virtual clinic interface to any provider, on any device, anywhere in the world.

Importance of security and telehealth

Mainstream adoption of telemedicine is exploding. According to a recent Arizton research report, the U.S. market is expected to grow at a CAGR of about 30% between 2020-2025. With the rapid adoption of telehealth comes the increased need for a secure and reliable cloud-based connection between patient and provider that also provides a high-quality, HIPAA compliant experience.

It is critical for healthcare providers to partner with a telehealth provider who can enable them to keep patient privacy and their infrastructure secure by safely and properly deploying the technology.

Purpose of the paper

The purpose of this paper is to provide information on the security features and functions that Let's Talk Interactive has put into place across all of its secure software and hardware platforms.

These security measures provide the high quality and HIPAA compliant experience that providers and patients expect and that are necessary for patient safety and privacy.

Security

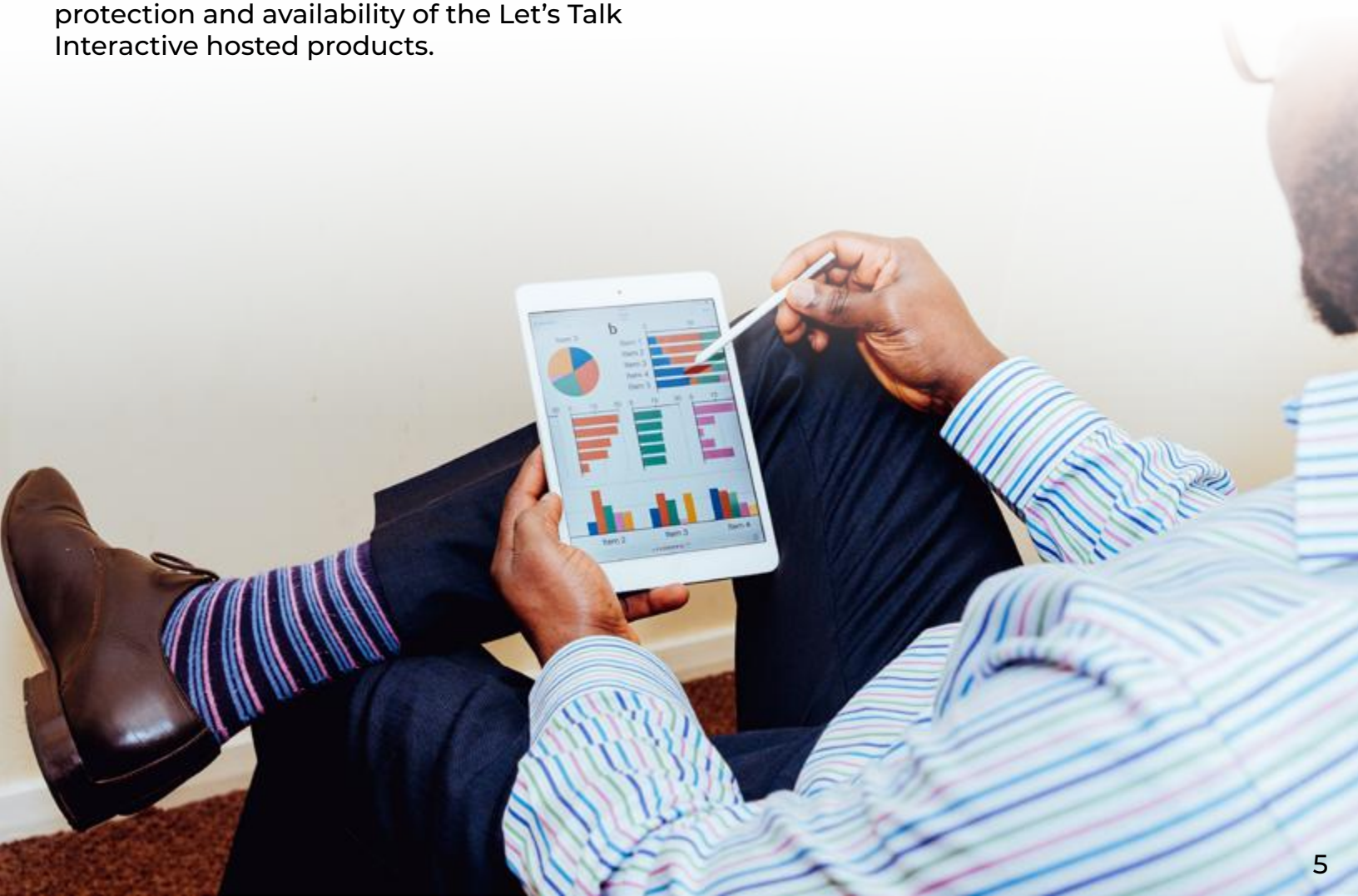
At Let's Talk Interactive, we understand the importance of data privacy, security and availability.

Our products are built around industry-leading best practices for data privacy and Information security. Our products are hosted on AWS, the market leader in public cloud. The Let's Talk Interactive production instance runs on the North Virginia AWS region.

The AWS Security Platform provides several industry leading security capabilities and services to increase the privacy and security of their cloud. This includes network firewalls, encryption in transit with TLS across all services, DDoS mitigation capabilities, data encryption, monitoring/logging, identity management/access controls and third-party penetration testing. These capabilities help to ensure the privacy, protection and availability of the Let's Talk Interactive hosted products.

AWS Infrastructure provides a secure computing environment to host the Let's Talk Interactive products and associated customer data. Physical and environmental controls protect data and services from unauthorized intrusions and interruptions, while technology and policy-based security measures defend against unauthorized disclosure and manipulation.

Security related processes and procedures include 24 x 7 monitoring of the Infrastructure and applications, a formalized backup and recovery system, security management procedures and a disaster recovery program. All of these measures are designed to ensure the confidentiality, integrity, and availability of customer applications and data.



Data and physical security measures

Physical and digital security measures are used to ensure your data is protected while in transit and at rest.

Data Security Measures

- Encryption In Transit
- 256-bit SSL encryption
- 256-bit keys
- Supports TLS 1.2 and 1.3
- Encryption At Rest
- Amazon EBS encryption with keys securely stored in KMS
- Audit logs for user activities
- Secure passwords
- Password Hashing
- Password complexity requirements
- MFA enforced
- Role-based access controls
- Secure HTTPS login utilizing industry-standard PKI
- Encrypted session ID cookies to uniquely identify each user
- FIPS 140-2 certified libraries
- SRTP media encryption
- Third-party penetration testing
- Internal and external vulnerability scanning.
- Intrusion Detection
- Web Application Firewall
- IP Restrictions

Physical Security Measures

- AWS has designed its systems to tolerate system or hardware failures with minimal customer impact
- AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches
- Two-Factor authentication
- AWS authorized staff must pass two-factor authentication a minimum of two times to access DC
- All visitors and contractors are required to present identification/sign-in and are continually escorted by authorized staff
- AWS - SOC 1/SOC 2/SOC 3/ISO/PCI/ HIPAA/ compliance
- High-definition CCTV of all interior and exterior strategic locations and access points
- Data Centers use generators to provide backup power in event of failure

Video security

Security is important in order to protect the login process from eavesdroppers and hackers. Let's Talk Interactive uses industry-standard public key infrastructure, whereby each component is issued a digital certificate by a trusted third-party certifying authority. This allows endpoints to verify the identity of LTI and helps prevent malicious users from eavesdropping on communication. With TLS security enabled, the LTI video service establishes an encrypted HTTPS channel with each endpoint that attempts to access the system.

Before transmitting any login information, the LTI endpoint or web browser validates the video certificate and verifies it was issued by a trusted third-party certifying authority. Once the certificate is verified, login and password information is transmitted securely to LTI over the same encrypted HTTPS channel.

Identity authentication

The use of continuous identity authentication is critical. The most common is multi-factor authentication (MFA, also known as two-factor authentication, or 2FA), which allows you to present two credentials when logging into an account. MFA use can reduce the possibility of an unauthorized user posing as an authorized individual to gain access to sensitive resources and applications.

On AWS we use separate users for each person and each application or service that interacts with the cloud.

Application and programmatic services users

Application and services use only programmatic keys to access the system and each one has a separate policy to allow access only to the necessary cloud service.

Users who interact with the cloud also have the same "least privilege" principle to allow them access. Administrators have a read-only role with an "assume-role" policy that allows them to assume the "admin" role. This admin role can ONLY be assumed if the user has MFA on his account. an MFA key will be asked every time the user wants to assume this role.

To simplify the process, we use https://github.com/99designs/aws-vault . it stores the profiles to assume and the keys of AWS in a secure way with keychains or encrypted files.

Video security (continued)

Password policy and rotation

Password rotation is set at 180 days. but no automatic password rotation will happen. Users have to manually change it. Passwords must be strong, minimum 8 character passwords as per HIPAA regulation.

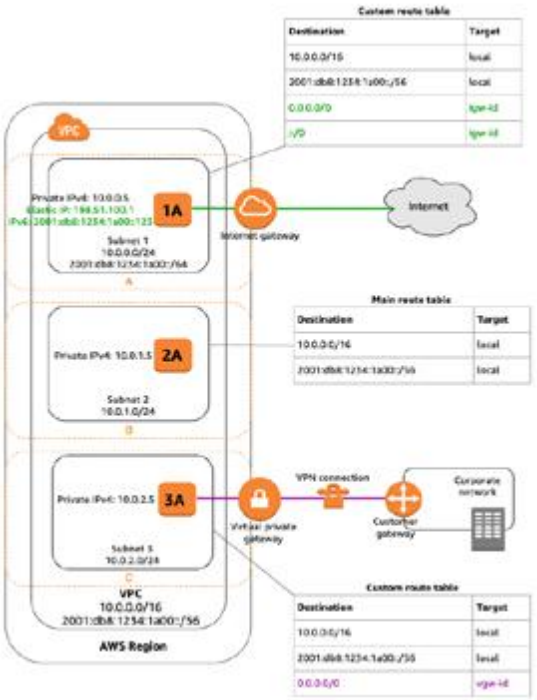
MFA

Multi-factor authentication is enforced to every non-programmatic user to access even read-only API endpoints and web console.

Networking

Several different subnets exist for the infrastructure in one separate VPC. Please refer to terraform to see the different created subnets and security groups.

This graph shows a simplified schema of it. →



Public Subnet should be differentiated from private ones. Only allow internet access directly on the public subnet on specific port/protocols. Maintain Network ACLs and security groups for other subnets.

User Login and Database Security

Key security features

- SRTP media encryption
- FIPS 140-2 certified libraries
- Secure HTTPS login utilizing industry-standard PKI
- TLS using strong encryption ciphers for signaling
- Password hashing in database
- Encrypted token technology for session security
- No login information retained on the client

Cloud HIPAA compliance

The Health Insurance Portability and Accountability Act (HIPAA) provides standards to protect the confidentiality, integrity, and availability of protected health information (PHI). This includes electronic protected health information (ePHI). HIPAA provides guidance on levels of protection for ePHI while still allowing healthcare providers to have access to the necessary information to perform their roles. The Let's Talk Interactive video service offering is designed with HIPAA compliance in mind, allowing healthcare providers and other covered entities to use our services for video communication.

Zoom telehealth integration

The Zoom telehealth integration enables an existing Zoom account to provide HIPAA compliant services with a customized workflow. A suite of services is available including a patient-facing calendar, secure document sharing, and the ability to take payments.

Client application

The following pre-meeting security capabilities are available to the meeting host:

- Secure log-in using standard username and password or SAML single sign-on through custom API integration
- Start a secured meeting with a passcode
- Schedule a secured meeting with a passcode

In order to provide control over meeting access information, the host can selectively invite participants via email, IM, SMS or from a specific email domain.

LTI retains event details pertaining to a session for billing and reporting purposes. The event details are stored at the LTI secured database and are available to the customer account administrator for review on the customer portal page once they have securely logged-on.

LTI can encrypt all real-time media content at the application layer using Advanced Encryption Standard (AES).

Chat encryption allows for a secured communication where only the intended recipient can read the secured message.

End-to-end encryption, when enabled, ensures that communication between all meeting participants in a given meeting is encrypted using cryptographic keys known only to the devices of those participants. This ensures that no third party - including LTI - has access to the meeting's private keys. End-to-end encryption is available as a technical preview to all customers.

Zoom telehealth integration (continued)

Meeting security - Role-based user security

The following in-meeting security capabilities are available to the meeting host:

- Waiting Room
- Enable wait for the host to join
- Expel a participant or all participants
- End a meeting
- Lock a meeting
- Chat with a participant or all participants
- Mute/unmute a participant or all participants
- Screen share watermarks
- Audio signatures
- Enable/disable a participant or all participants to record
- Temporary pause screen-sharing when a new window is opened

The following in-meeting security capabilities are available to the meeting participants:

- Mute/unmute audio
- Turn on/off video
- Blur snapshot on iOS task switcher

Encryption at rest

Every disk (EBS) is encrypted, with the exception of the ECS instances that do not store any PHI on it, they have an attached EFS filesystem to store persistent data.

Encryption is managed by AWS with KMS to store the master keys

Encryption at transit

For the frontend, all access is redirected from HTTP (80 TCP) to HTTPS.

Every site has to have an SSL Certificate, nginx supports TLSv1.1 and TLSv1.2. With the new releases to come on nginx it should support only TLS v1.2 and TLS v1.3. this can be reviewed on /xxxxxxxxxxxx.conf on the server.

Monitoring and threat detection

In case of Zero-Days vulnerabilities a series of monitoring services are deployed to detect and block suspicious actions on the network and also over Web applications.

IDS, WAF, IP banning

Falco IDS: Falco2 is an open source project for intrusion and abnormality detection for Cloud Native platforms. It runs as a service on the ECS Cluster with a policy to expand an instance per EC2 server that is on the cluster.

Falco send logs to Cloudwatch where rules are set to send an alarm in case of an abnormality.

WAF

Sites with cloudflare enabled have a WAF with core OWASP rules and custom one to protect request and responses.

Fail2Ban

Fail2Ban acts on the nginx logs to ban IPs directly at a network level when an IP reaches a score of threat. If the IP is testing HTTP VERBS or some abnormal paths the IP is automatically banned and alerts are sent.

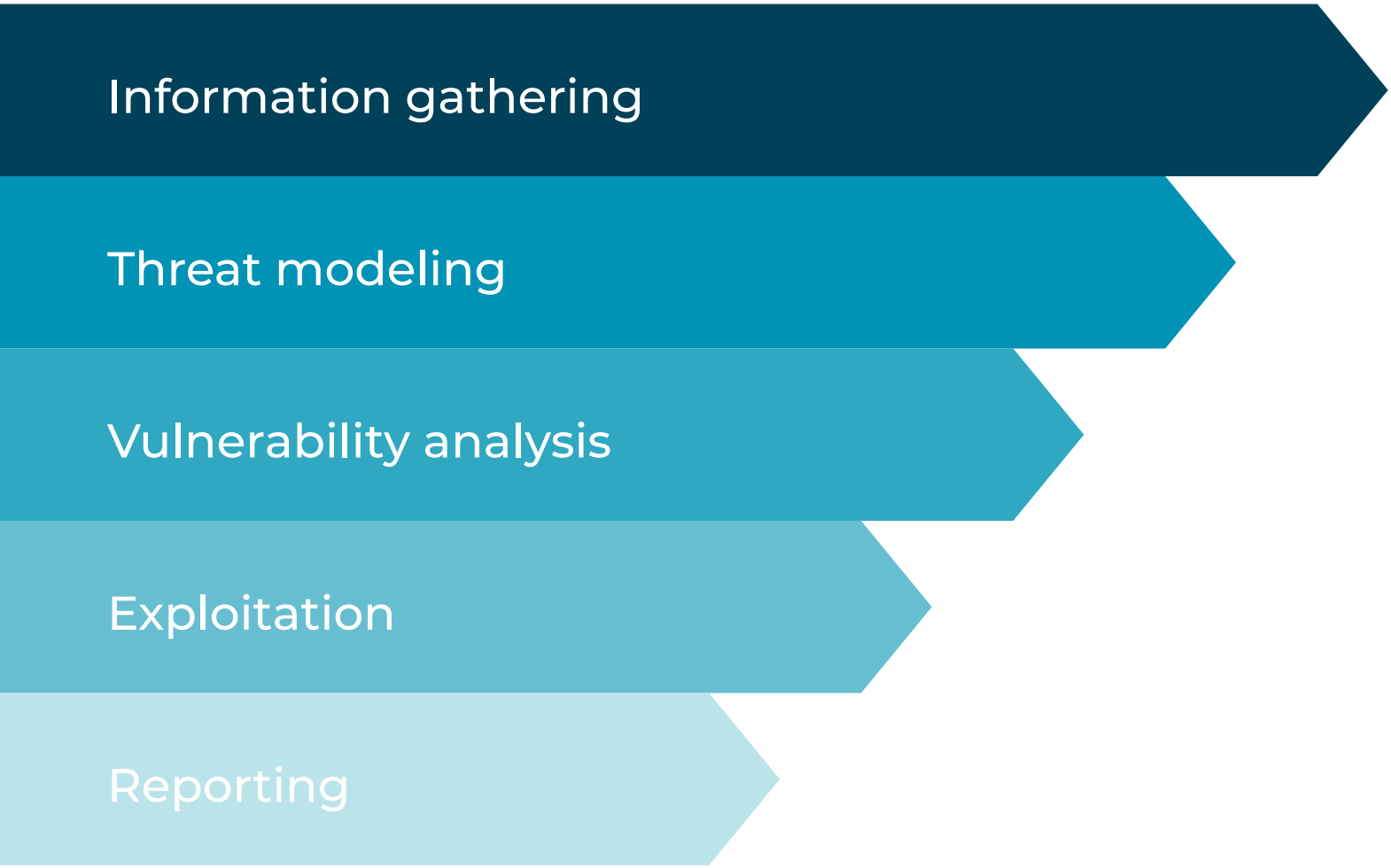
Security testing

Penetration Testing and Vulnerability Scanning

Penetration testing and vulnerability scanning is part of the larger information security strategy at Let's Talk Interactive and includes third-party vulnerability monitoring.

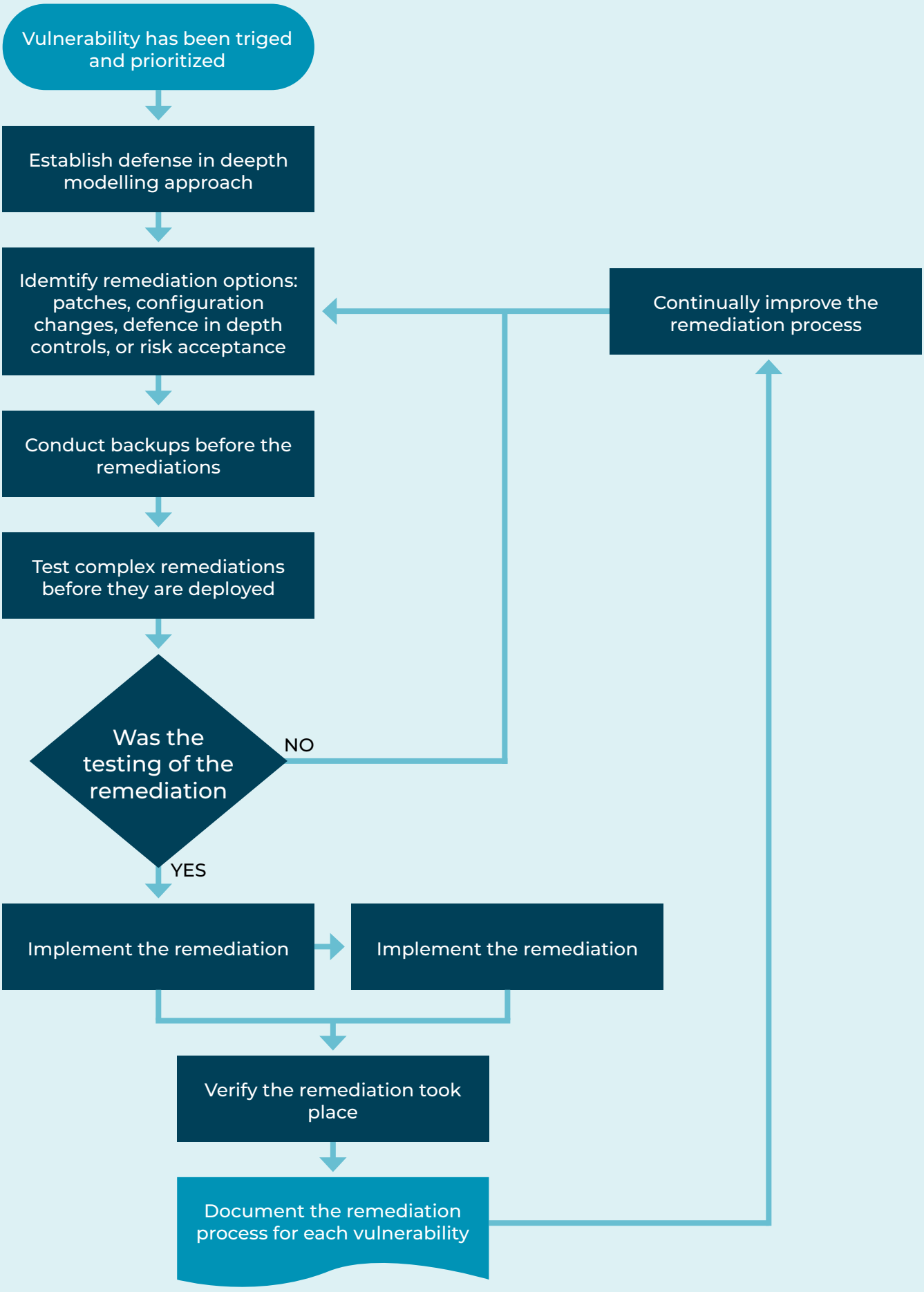
Let's Talk Interactive has a contract with a third-party Managed Security Service Provider to perform ongoing security testing. The security testing combines the results from industry-leading scanning tools with manual testing to enumerate and validate vulnerabilities, configuration errors, and business logic flaws.

The penetration testing methodology assesses the target(s) using a multi-layered approach: Information Gathering, Threat Modeling, Vulnerability Analysis, Exploitation and Reporting.



In addition, Static Application Security Testing (SAST) is performed against all source code. SAST is white-box testing, where source code is analyzed from the inside out, while components are at rest to identify vulnerabilities, bugs, and best practice violations. This enables us to catch vulnerabilities, bugs and best practice violations earlier in the development process.

Vulnerability management process



Disaster recovery

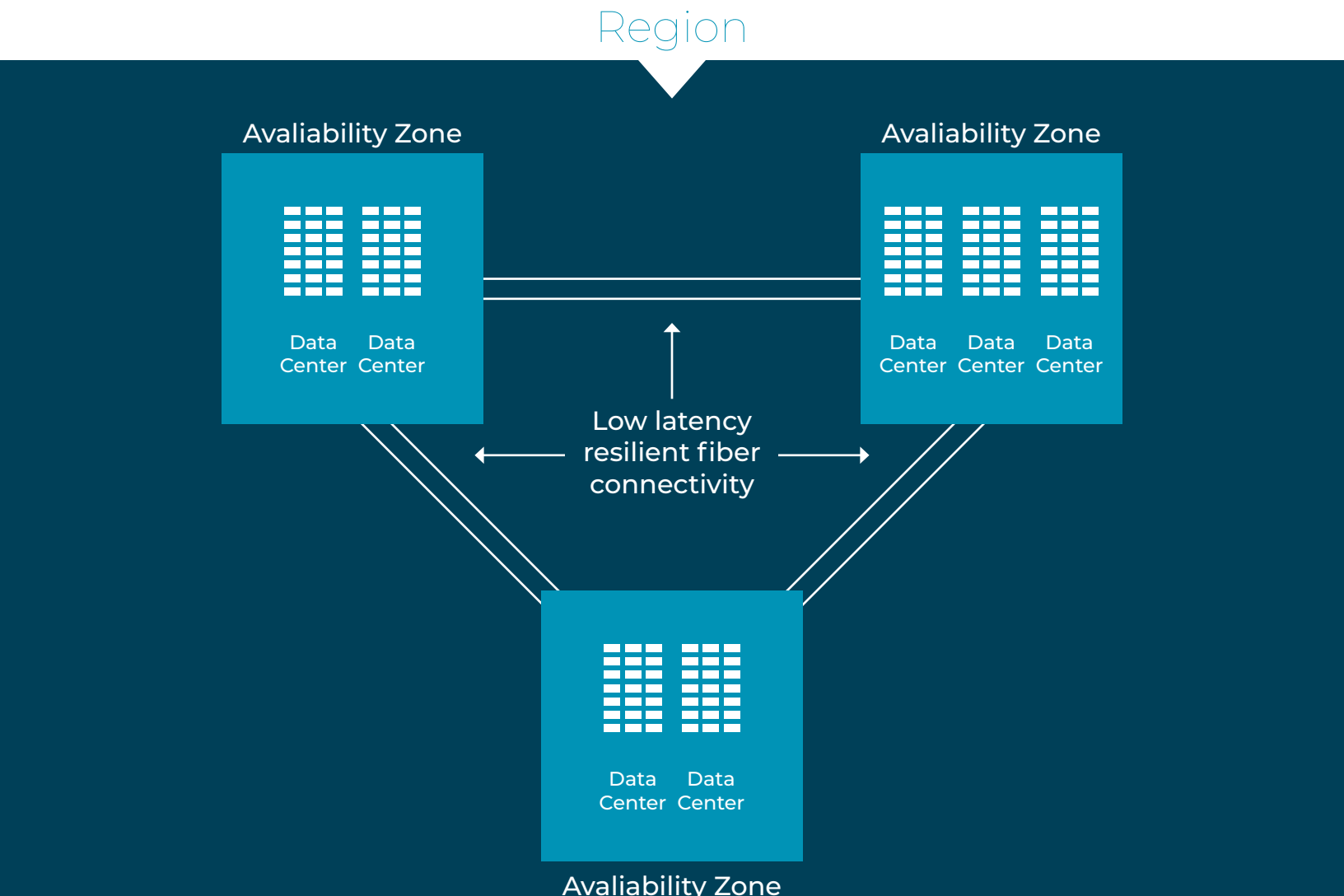
Let's Talk Interactive leverages AWS to host our products. We leverage AWS Availability Zones which allows for fast and automated recovery by replicating servers, applications and data in the US East (Ohio) Region across 3 availability zones/physical data centers to provide customers a highly available solution.

An Availability Zone is a high-availability offering that protects servers, applications and data from datacenter failures. Each Availability Zone is a separate datacenter with independent power source, networking, cooling, etc. This is to ensure maximum resilience and high availability across an AWS region. The physical separation of Availability Zones within a region protects servers, applications and data from datacenter failures. With Availability Zones, AWS offers industry best 99.99% uptime SLA.

In the event that an entire AWS region (multiple data centers) goes down, backups are replicated to a secondary region to allow for recovery to a secondary region (US West (Oregon) Region). Backup jobs run twice a day for database snapshots and once a day full database backups.

Recovery Time Objective (RTO): **3 hours**

Recovery Point Objective (RPO): **24 hours**



CRITSIT process

Critical Situation Management

Process Basics

Every disk (EBS) is encrypted, with the exception of the ECS instances that do not store any PHI on it, they have an attached EFS filesystem to store persistent data.

Encryption is managed by AWS with KMS to store the master keys

When a critical situation erupts, Support staff will either independently or by request open a conference bridge and open a case/ ticket so they can begin to document details and collect participants onto the call via all available communications methods including phone calls, email, chat, or even physically going and getting people.

In most common cases, an IT Executive/Manager will serve as the Situation Manager, however anyone can be the situation manager and in certain cases of subject matter expertise non-managers should take over as the Situation Manager.

Post Incident Actions

The Scribe will produce the full activity log within 24 hours of the closure of the incident to the Situation Manager and all participants.

Participants are expected to review and submit additions or changes to the Situation Manager within 24 hours of receiving the activity log.

Within 36 hours of the closure of the incident the SM will provide the activity log with a summary cover letter to management for dissemination to the business (constituents).

If a Root Cause Analysis (RCA) is required, the Situation Manager will determine who shall author it and when it is due not to be greater than 10 business days.

It is the responsibility of the SM to collect the RCA by the due date and disseminate it to the business (constituents).

RSA Process

Root Cause Analysis

Process Basics

An RCA must not only state the cause and resolution of the incident but more importantly must stipulate post-incident ACTION ITEMS that are meant to mitigate future occurrences of the problem. An RCA without action items is merely an informal report of the incident. Most action items will occur in twos because there are usually an action item to implement a change and then a companion item to monitor for that element so that it doesn't surprise us in the future.

Key elements that must be in every RCA are the following:

- RCA Number or Name
- Site where the incident took place
- How the incident originated, usually a problem ticket (e.g. case/ticket #)
- RCA author(s)
- Incident and RCA participants
- Date and times of the incident
- Who was impacted by the incident
- The problem description
- Incident duration
- Chronology of events
- Root cause explanation
- Any secondary issues that fell out of the primary issue(s)
- Conclusion and recommendations

The guidelines for determining whether or not an RCA should be done include the following considerations:

- Management requests one (Manager and above) or a customer requests one
- The outage lasted 4 hours or more
- The number of customer calls exceeded 10

Continued Compliance

To ensure that future changes to the infrastructure keep all the necessary compliance requirements, AWS Config is used with a set of rules that keep track of security issues at every change on the infrastructure.

The rules on AES config are configured from AWS security advisor. Some alarms are set when:

- There are changes on the policy for S3 buckets to detect intrusions.
- There are routing tables changes.
- IAM policies change with some users.

AWS Security HUB

AWS Security HUB creates a set of rules applied on AWS config to check configurations per

region. Most of the rules apply for a HIPAA compliant solution.

Privacy details

Let's Talk Interactive is required to comply with health care privacy laws and regulations and we go to great lengths to ensure that personal information is secure. We are committed to conducting our business in accordance with the following principles to ensure the confidentiality of personal information is protected and maintained.

Notice of privacy practices

Let's Talk Interactive does not disclose personal information to third parties, except where required by law. This includes selling, renting, trading, sharing, or giving information via any medium.

Non-Identifiable Data: When you interact with LetsTalkInteractive.com through the Site, we receive and store certain personally non-identifiable information. This information is collected passively using various technologies and cannot presently be used to specifically identify you. LetsTalkInteractive.com may store such information itself or such information may be included in databases owned and maintained by LetsTalkInteractive.com affiliates, agents or service providers. This Site may use such information and pool it with other information to track, for example, the total number of visitors to our Site, the number of visitors to each page of our Site, and the domain names of our visitors' Internet service providers. It is important to note that no Personal Data is available or used in this process.

The company collects non-identifiable data during account creation and use of the site. This information may be used as follows:

- For verification of the user's legal right to use the software,
- To identify accounts when support is requested by the account holder,
- To inform users of product changes,
- For support and marketing,
- To enforce licensing terms,
- For inclusion in aggregate usage data for the purpose of studying and improving the product, and
- To enable features of LetsTalkInteractive.com

Privacy details (continued)

Let's Talk Interactive does not use personally identifiable information for any use other than stated above. We will protect personal information by reasonable security safeguards against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. We may change this statement from time to time with notice.

Aggregated personal data

In an ongoing effort to better understand and serve our Users and Providers, LetsTalkInteractive.com often conducts research on its customer demographics, interests, and behavior based on the Personal Data and other information provided to us. This research may be compiled and analyzed on an aggregate basis, and LetsTalkInteractive.com may share this aggregate data with its affiliates, agents and business partners. This aggregate information does not identify you personally. LetsTalkInteractive.com may also disclose aggregated user statistics in order to describe our services to current and prospective business partners, and to other third parties for other lawful purposes.

Information provided to providers

We do not collect any information that a User provides directly to any Provider and not through our Site, including but not limited to during a session with such Provider. The Provider, along with any applicable professional guidelines, determines the recording, storage and use of any information that is collected in a session, and is solely responsible for maintaining the privacy of such information. If a user has questions about the privacy of the information they share with a Provider, they should discuss directly with the Wellness Professional.

For more information on our privacy policy, visit letstalkinteractive.com/privacy-policy