AWS Security Controls and Procedures

Classification: Confidential

Table of Contents

Introduction

As part of Phorest's commitment to providing a secure and reliable service to our clients, we have implemented a robust set of security controls utilizing builtin AWS security services alongside internal processes and procedures.

This document is designed to provide an overview of security controls implemented by Phorest within their dedicated production AWS environment providing transparency and demonstrating that the security of our cloud environment is a top priority.

Resources and areas covered in this document include but are not limited to the protection of EC2 Instances, S3 Buckets, Relational Database Services (RDS), Elastic Containers (ECS), Phorest AWS User Accounts and Monitoring.

Any AWS security controls, services or internal procedures documented within are currently in operation, this document does not include any controls, services or procedures that are currently in a development or testing phase unless explicitly stated.

The intended audience for this document includes Phorest clients, auditors and other stakeholders who have a vested interest in our AWS security practices.

This document is shared on a need to know basis, further sharing of this document is prohibited unless explicitly authorized by Phorest.

Identity and Access Management

Provisioning of Access

When provisioning access to AWS or its resources, Phorest follows an internal procedure to determine if an employee requires access to said resources based on their job function, role or day to day requirements.

In the event access is approved, user accounts are provisioned using the principle of least privilege, employees are granted access to data or resources based specifically on their job function or role.

Periodic reviews are conducted around access to AWS resources to ensure that there is no drift from our least privilege mindset.

User Account Security

User accounts are required to have complex passwords and two factor authentication enabled by default, account credentials are rotated at a set interval.

Roles and Policies

Clearly defined user roles and IAM policies are utilized to ensure consistent and appropriate access is provisioned, this includes but is not limited to policies accounting for the following:

- **Administrative Roles:**

  An IAM policy specifically for administrators of the AWS account, allows access to perform standard administrative tasks within the account.

- **Development Roles:**

  An IAM policy for developers allowing for programmatic access to the AWS environment to carry out development work and testing.

- **Infrastructure Roles:**

An IAM policy for internal infrastructure engineers to carry out day-to-day work both manually and in an automated fashion, accounting for programmatic access.

- **Service Account Roles:**

  IAM policies allow the required service accounts associated with monitoring, alerting or automated deployment mechanisms.

- **Read Only Account Roles:**

  IAM policies allow for the programmatic or direct read only access to resources.

A combination of roles and policies coupled with scheduled periodic revisions allow for easy maintenance and ongoing monitoring of a clearly defined permissions structure.

Multi-Factor Authentication

All user accounts granted access to the Phorest AWS environment are required to have 2FA enabled, this requirement is in place regardless of account type or access level.

Credential Management

Access keys for both user accounts and service accounts are regularly rotated, this process is arbitrary and automated.

AWS Secrets Manager is also utilized to securely store and manage additional keys deemed sensitive.

Access Analyzer

The AWS Access Analyzer service is used to monitor access that has been granted to resources outside of the Phorest zone of trust, this includes but is not limited to resources and data held in S3, EBS, RDS and other such services.

By implementing the highlighted AWS IAM security features our aim is to maintain tight access control around all of our resources and services, we couple these controls with automation, internal processes and regular manual reviews to ensure we are managing this access in an efficient and secure manner.

Network Security

Phorest have implemented a number of key security features to protect AWS resources and services, each of these services are regularly monitored, reviewed and assessed to ensure they are meeting requirements.

Virtual Private Cloud (VPC)

Phorest utilizes VPC's inside AWS to create networks that are isolated from the internet, inbound and outbound traffic across the VPC's is tightly controlled to ensure traffic is only allowed between trusted sources.

Security Groups

Security groups are in place to control inbound and outbound traffic to Phorest AWS resources, the groups in place control traffic based on protocols, ports and IP's deemed necessary by engineers.

These security groups contain rules that are only essential requirements for the running of services, a determined effort is made to ensure these groups do not contain ambiguous or unnecessary rules.

Network Access Control Lists (ACLs)

AWS ACLs are utilized to tightly control and filter traffic between subnets within Phorest VPCs, alongside security groups these stateless ACLs are in place to restrict traffic based on source, destination and protocols deemed necessary by Phorest engineers.

The ACLs in place are regularly revised based on requirements and changes to the AWS environment, a concentrated effort is made to control these ACLs to ensure strict control over inbound and outbound traffic.

Bastion Hosts

A small number of bastion hosts are utilized to act as a secure gateway to a set of Phorest AWS resources.

These bastion hosts are secured and hardened EC2 instances in private subnets that utilize the AWS SSM service. Their primary use is for service connectivity.

VPN Connection

Where applicable a VPN connection is used to access some internal Phorest business applications, provisioning of VPN access is based on necessity and granted only if a staff member requires it for their specific job role or day to day work.

AWS WAF

AWS Web Application Firewall is used across the Phorest environment to protect and monitor internet facing applications from web based exploits.

Phorest WAF rules are configured to monitor and prevent common web exploits such as but not limited to:

- Cross-Site Scripting
- SQL Injection
- LFI/RFI
- Command Injection

Alongside custom built rulesets Phorest also deploy a number of AWS managed rulesets including rules to address:

- Bot Control
- Automated vulnerability scanning tools
- DDoS

Block and allow rates are monitored closely to ensure implemented rules are performing as required.

AWS Guardduty

The AWS Guardduty service is used across the Phorest environment to monitor AWS resources for unauthorized or unusual activity.

Phorest utilize the Guard Duty threat detection service to monitor logs for every resource in the environment, this includes but is not limited to:

- Unusual user account activity
- S3 bucket policies

- Cloudtrail event logs
- RDS logs
- Malware Protection
- DNS logs

The Guardduty service is combined with internal alerting that notifies internal Phorest engineers of any findings.

Phorest engineers investigate any and all Guardduty alerts regardless of severity or classification to ensure any potential security threats are identified and addressed with priority.

Data Encryption

Phorest employ builtin AWS data encryption services at all points applicable to protect the confidentiality and integrity of data in transit and at rest

Encryption Compliance

Phorest ensures that all resources and services are deployed incorporating the recommended and best practice encryption configuration.

Adhering to security and privacy compliance and regulatory requirements such as GDPR, HIPAA and PCI DSS are vital to safeguarding Phorest's client data and privacy, as such there is a concentrated effort to ensure all systems and services meet regulatory requirements.

AWS Key Management Service (KMS)

Phorest uses the AWS KMS service to manage encryption keys for AWS resources, the KMS service provides a highly secure and scalable solution enabling for the easy management of sensitive encryption keys, access to this resource is monitored and closely managed.

Encryption in Transit

Phorest utilize and employ protocols such as SSL/TLS and HTTPS to encrypt and protect data in transit wherever possible.

Logging and Monitoring

Phorest have implemented a variety of logging and monitoring features to ensure we can respond to any potential security incidents in an efficient and timely manner.

AWS CloudTrail

The CloudTrail service is used across the Phorest AWS environment to monitor and log all API calls made within the account.

The CloudTrail service is used to ensure we have a complete and clear audit trail of all activity and actions taking place inside the Phorest AWS account, using this service helps our internal engineers detect unusual activity and security issues should they arise.

AWS CloudWatch

The AWS CloudWatch service is used by Phorest engineering teams to monitor the health and performance of AWS resources.

Custom alarms allow key teams and engineers to be alerted as and when resource alarms are triggered, which in turn allows engineers to respond to alerts quickly and efficiently to assess if alarms are triggered by potential security issues.

AWS SNS

Phorest implements the AWS SNS service to send notifications to internal engineering teams when key events are triggered, this allows the appropriate internal Phorest engineers to be notified extremely quickly allowing them to take immediate action to any alerts received.

AWS Config

The AWS Config service is used by Phorest engineers to track changes across AWS resources, monitor the compliance of security policies and provide a detailed inventory of AWS resources.

This service allows engineers to easily identify and remediate security or compliance issues with resources and policies.

Data Backup and Restoration

Phorest's backup policy within AWS follows a comprehensive approach to ensure the protection and recoverability of all critical data.

Backups are performed regularly across critical services including but not limited to S3, EBS Volumes, RDS (databases) and additional file systems where possible to mitigate the risk of data loss and unintended downtime due to technical or security incidents.

Databases related to Phorest cloud systems and applications are automatically incrementally backed up once per day outside of region specific business hours, these incremental backups are securely retained for 30 days allowing for quick quick restoration and retrieval of data if necessary.

A combination of full backups and snapshots are utilized, this approach allows for the protection of full data sets using full backups and incremental snapshots to capture changes in between full backups.

In order to meet regulatory requirements and obligations Phorest retains some backups for a longer defined period of time, these retention periods are determined based on a number of factors such as data sensitivity, regional compliance obligations and operational needs.

Regular internal review of backup policies and procedures is conducted in order to align and evolve with changing business requirements and data protection best practices, this includes the evaluation of new backup features and options supplied by AWS to help enhance and continuously improve upon current policies and procedures.

Conclusion

In conclusion, this document provides a high level overview of the various AWS security features and measures Phorest implement to secure our AWS environment.

We understand the importance of security and have taken a multi-layered approach to ensure that Phorest customer data, applications and infrastructure are safeguarded from potential security threats.

Our AWS security measures include the use of AWS Identity and Access Management (IAM) to manage access control to our AWS resources, network security services such as VPC's, Security Groups and ACLs, data encryption mechanisms like AWS KMS and S3 encryption alongside logging and monitoring services such as CloudTrail and Cloudwatch and a comprehensive approach to backup and recovery.

Phorest continuously monitors, reviews and improves upon security measures in order to stay up to date with the latest security threats and vulnerabilities, our commitment to security ensures that our customers data is safe, secure and we maintain their trust.

We believe that our AWS security measures provide a solid foundation for a secure AWS environment and are confident that we can quickly identify and respond to security incidents.

Phorest will continuously remain committed to maintaining the highest level of security and endeavor to keep enhancing our security posture for the benefit of our employees and customers.