GreatHorn

GreatHorn, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, and Confidentiality categories for the period of January 1, 2021 through December 31, 2021.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF GREATHORN, INC. MANAGEMENT

ASSERTION OF GREATHORN, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within GreatHorn, Inc.'s email security software-as-a-service system (system) throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that GreatHorn, Inc.'s service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that GreatHorn, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). GreatHorn, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that GreatHorn, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Kevin O'Brien
CEO & Co-Founder
GreatHorn, Inc.
1075 Main Street, Suite 210
Waltham, MA 02451

Scope

We have examined GreatHorn, Inc.'s accompanying assertion titled "Assertion of GreatHorn, Inc. Management" (assertion) that the controls within GreatHorn, Inc.'s email security software-as-a-service system (system) were effective throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that GreatHorn, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

GreatHorn, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that GreatHorn, Inc.'s service commitments and system requirements were achieved. GreatHorn, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, GreatHorn, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve GreatHorn, Inc.'s service commitments and system requirements based on the applicable trust services criteria

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve GreatHorn, Inc.'s service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within GreatHorn, Inc.'s email security software-as-a-service system were effective throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that GreatHorn, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

January 26, 2022

GREATHORN, INC.'S DESCRIPTION OF ITS EMAIL SECURITY SOFTWARE-AS-A-SERVICE SYSTEM

SECTION A:
GREATHORN, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS EMAIL SECURITY SOFTWARE-AS-A-SERVICE SYSTEM

Services Provided

GreatHorn, Inc. (GreatHorn) provides an email threat detection and response software-as-a-service (SaaS) solution that provides protection before, during, and after an email attack. The platform integrates with Office 365 or Google Workspace to help organizations identify and stop sophisticated types of email threats, such as targeted phishing attacks and social engineering attempts aiming to compromise data, credentials, and financial resources. The solution combines threat detection, continuous monitoring, end-user education, and integrated remediation capabilities to support adaptive threat detection.

Administrators access the product dashboard, which provides metrics regarding malicious and potentially malicious activity in the user's email environment. Metrics include the number of malicious links detected, spoofed email addresses, emails quarantined, phishing emails reported by end users, and automatic actions taken. Administrator users work with GreatHorn staff to develop policies to take specified actions on emails when matching specified criteria. The product comes with standard, non-configurable policies such as detection for domain look-alikes, authorization risks, name spoofs, malicious attachments, and malicious links. The product also contains customizable policies to meet client needs, and administrators can create custom policies from scratch. Each policy has a set of potential actions, which include deleting an email entirely, removing attachments, or enrolling a user in end-user training. Additionally, policies can be configured to send email alerts to an administrator and/or the end user.

End users interact with the product through an Outlook or Gmail plugin. The plugin provides real time analysis of each email, including how well the end user knows the sender, how well colleagues know the sender, and whether the email is actually from the sender. The plugin allows end users to mark an email as spam, report a phish, and block senders.

Services Walkthrough

Perspective clients find the organization via searches, advertisements, or whitepapers and request a product demonstration or contact a Sales Development Representative (SDR). SDRs then establish an interview with the customer to understand the customer's needs. After agreeing to the terms of service and completing a non-disclosure agreement (NDA), a product demonstration or proof of concept (PoC) installation is established, which takes one to three weeks. The PoC can be deployed into the client's test or production infrastructure, and during this time, the Sales Engineer works directly with the client to provide training on secure use of the product and develop policies that meet the client's needs. At the conclusion of the PoC, GreatHorn provides the client with a report to convey the results of running the product. The client then decides whether to proceed to a full contract.

Upon signing a contract, clients are handed off to a Customer Success Manager (CSM). The CSM provides extended education on the product, closely reviews the customer's common threat scenarios, and further refines email security policies. Customers are also introduced to the knowledgebase hosted in Zendesk. The CSM works with the client for the life of the contract and tracks client relationship data in Salesforce. If needed, Sales Engineers can escalate customer requests by creating tickets in Jira.

For deployment, a Sales Engineer and CSM work with the client to ensure that correct permissions are enabled in Office 365 and Google Workspace. GreatHorn engineers configure client specific databases and provide at least one administrator-level account for the client. Further, OAuth is integrated with the Cloud Email Security Platform to provide authentication for users. The Cloud Email Security Platform stores usernames and associated permissions, but the platform does not store passwords.

Once Cloud Email Security Platform is implemented, customer mailboxes are scanned, and emails are ingested on a configured schedule (typically between every two seconds to two minutes). The full text of the body of the email is analyzed and compared against risk policies but is never written to a database. After the text analysis, the header, subject line, and URL links are analyzed, and metadata and relationship data are stored in Amazon Web Services (AWS) Relational Database Service (RDS) databases. Attachments are downloaded and scanned for malware using a licensed version of Sophos. URLs are analyzed and verified.

Infrastructure

GreatHorn maintains network diagrams to depict its network infrastructure and secure connections. The diagrams are updated annually or upon significant changes, and the Chief Technology Officer (CTO) & Chief Information Security Officer (CISO) and CloudOps Engineer are responsible for maintaining network diagrams.

In addition, the organization maintains a system inventory that includes cloud-hosted systems and employee laptops.

Software

The organization maintains a software inventory to track critical software licensing information. GreatHorn uses the following critical software:

- Aurora MySQL
- AWS
- Azure
- Elasticsearch
- Glasgow Haskell Compiler (GHC)
- GitLab
- GoLang
- Grafana
- Helm
- Jenkins
- Jira
- JustWorks
- Kubernetes
- Node
- PostgreSQL
- Python
- RabbitMQ
- Reddia
- Salesforce
- SendGrid
- SharePoint
- Spinnaker
- SpotIO
- Threat Stack

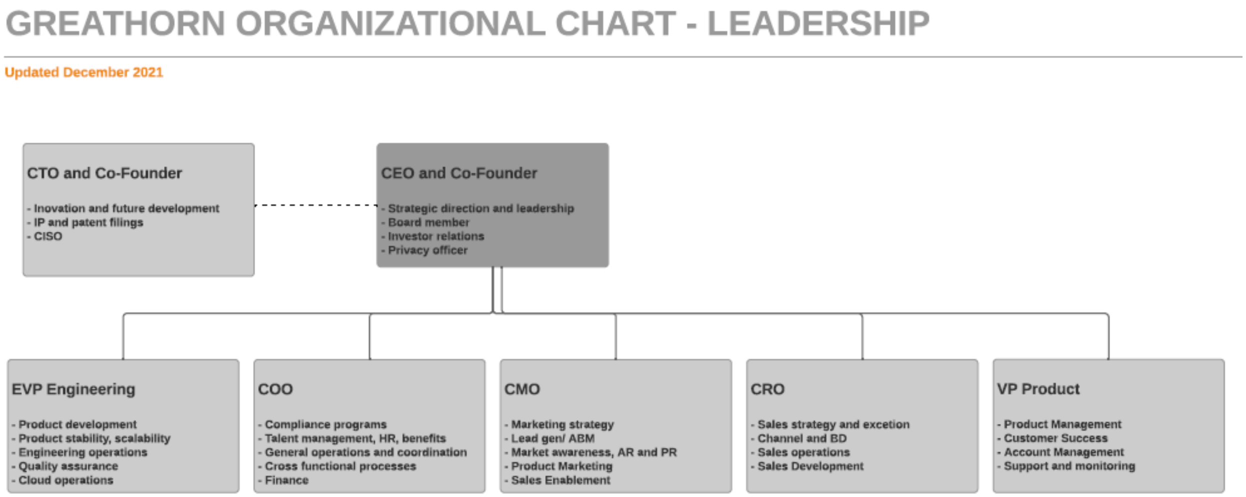
People

GreatHorn is overseen by a Board of Directors that is composed of the co-founders and business partners. The board meets quarterly to discuss operations, metrics, and/or governance issues.

Further, the organization maintains a traditional hierarchical structure composed of the following departments:

- Sales
- Engineering
- Finance
- Operations
- Marketing
- Customer Success and Product Management

The following organizational chart is maintained to depict the organization's internal structure and reporting lines:



GREATHORN ORGANIZATIONAL CHART - LEADERSHIP

Updated December 2021

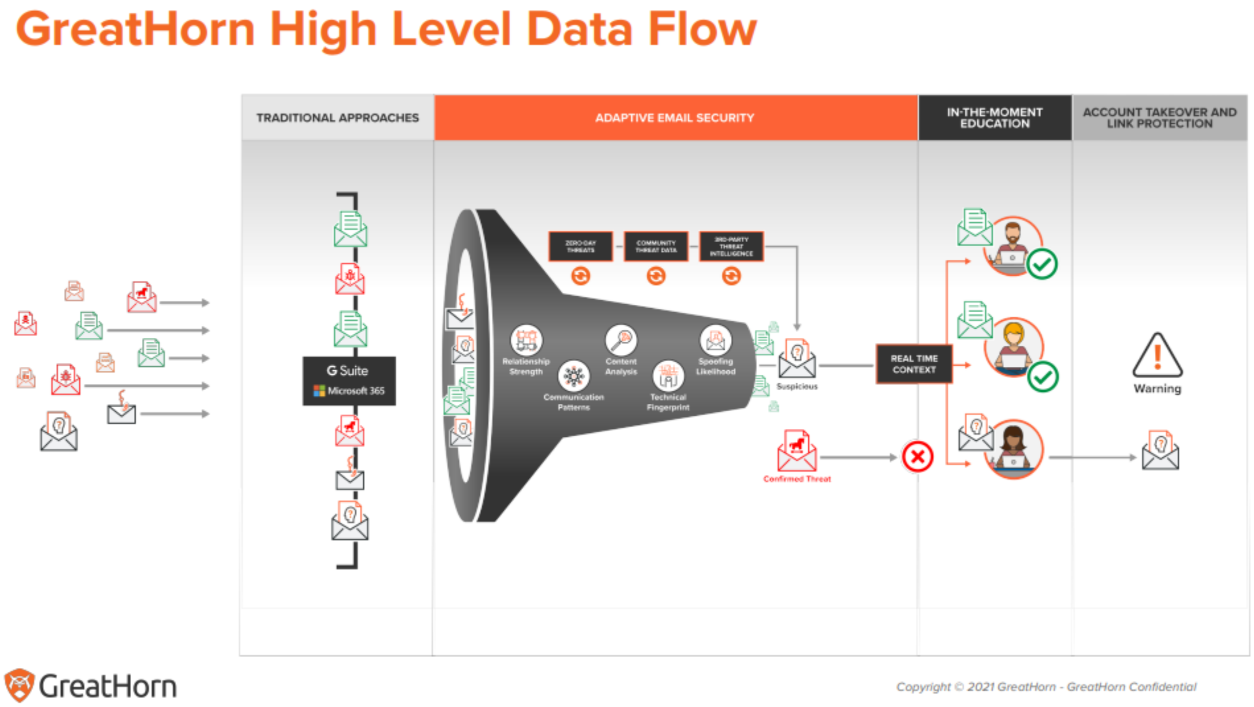
Data

The organization stores, transmits, and processes the following types of information that are relevant to its service offerings:

- Email event data
- Relationship data
- Directory listings
- Audit logs
- De-identified anonymized data

Data is protected with strong encryption protocols. Transport Layer Security (TLS) 1.2 and 1.3 are used to protect data in transit. Data is also appropriately retained. Retention requirements are defined for event data, relationship data, directory listings, and configuration information. Data is retained for active customers and purged during the offboarding process, and offboarding procedures are automated using a script, which includes customer data removal. De-identified and anonymized data is retained indefinitely. In addition, the organization uses QuickBooks Online to process payments for a small number of customers who pay for monthly services.

The following data flow diagram is maintained to depict how data securely moves throughout GreatHorn systems, and the diagram is updated by the CTO & CISO and CloudOps Engineer annually or upon significant changes:



GreatHorn High Level Data Flow

Copyright © 2021 GreatHorn - GreatHorn Confidential

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

SECTION B:
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

As a data processor, GreatHorn is subject to General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) requirements. The organization also complies with the EU-US Privacy Shield Framework. Further, the organization executes business associate agreements (BAAs) when necessary for customers required to comply with Health Insurance Portability and Accountability Act (HIPAA) regulations.

Contractual Commitments

The organization communicates its service commitments to customers via contractual materials. Customer agreements include the following service information:

- Annual payment terms
- Contract length of three years
- Cancellation terms
- Terms and conditions
- Support policy

In addition, appropriate service-level language is included in contracts with vendors.

System Design

GreatHorn designs its email security SaaS system to meet its regulatory and contractual commitments. These commitments are based on the services that GreatHorn provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that GreatHorn has established for its services. GreatHorn establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in GreatHorn's system policies and procedures, system design documentation, and contracts with clients.