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 November 1, 2018 through October 31, 2019.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF GREATHORN, INC. MANAGEMENT 1

INDEPENDENT SERVICE AUDITOR'S REPORT 3

Scope 4

Service Organization's Responsibilities 4

Service Auditor's Responsibilities 4

Inherent Limitations 5

Opinion 5

GREATHORN, INC.'S DESCRIPTION OF ITS EMAIL SECURITY PLATFORM SYSTEM 6

Section A: GreatHorn, Inc.'s Description of the Boundaries of Its Email Security Platform System 7

Services Provided 7

Infrastructure 8

Software 8

People 9

Data 10

Processes and Procedures 10

Section B: Principle Service Commitments and System Requirements 11

Regulatory Commitments 11

Contractual Commitments 11

System Design 11

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 Platform System (system) throughout the period November 1, 2018, to October 31, 2019, 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 November 1, 2018, to October 31, 2019, 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 November 1, 2018, to October 31, 2019, 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

Kevin O'Brien
Chief Executive Officer
GreatHorn, Inc.
260 Charles St
Waltham, MA 02453

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 Platform System (system) were effective throughout the period November 1, 2018, to October 31, 2019, 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 Platform system were effective throughout the period November 1, 2018, to October 31, 2019, 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

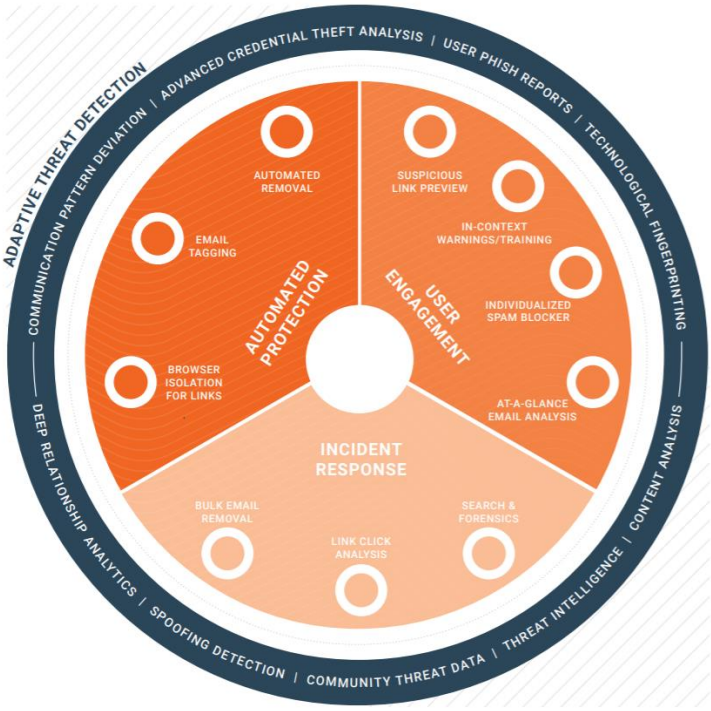
December 31, 2019

GREATHORN, INC.'S DESCRIPTION OF ITS EMAIL SECURITY PLATFORM SYSTEM

SECTION A:
GREATHORN, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS EMAIL SECURITY PLATFORM SYSTEM

Services Provided

GreatHorn, Inc. (GreatHorn) provides an email threat detection and response solution that provides protection before, during, and after an email attack. GreatHorn's cloud-native solution is built on a foundation of machine learning and automation to protect client organizations using Office365 and Google G Suite against advanced 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.



The following are the key features and benefits of GreatHorn's service solution:

- A single, unified model provides comprehensive internal and external email security before, during, and after an attack.
- The solution integrates with cloud email platforms to provide protection without changing mail routing or MX records.
- The detection technology offers content analytics to identify advanced threats more accurately than reactive methods.
- User engagement tools, banners, and alerts help end users make decisions, improve business process adherence, and reduce the risk of fraud.

- Integrated incident response capabilities streamline response processes, reducing threat exposure.
- Deep forensic capabilities ensure administrators can quickly understand an incident's full impact.

Infrastructure

GreatHorn's CloudOps teams maintains a network diagram, which illustrates the technical infrastructure in place to support service delivery. The diagram is reviewed and updated at least annually and must be approved by the Chief Technology Officer and the Vice President of Engineering.

The organization also maintains an inventory of all critical system components, including virtual technologies. The inventory records the device name, type, vendor, function, operating system, and location of each item.

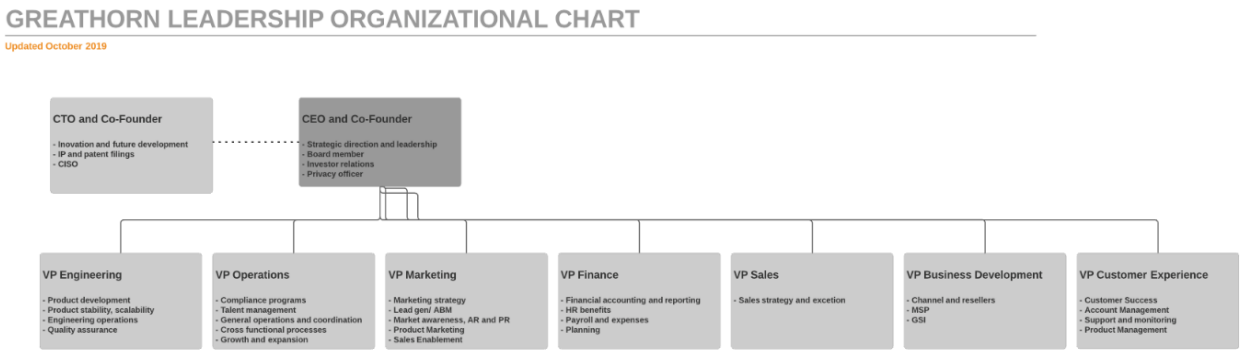
Software

GreatHorn maintains an inventory of the critical software components used to support its system design and functionality. The inventory records and tracks the name, version, vendor, and function of each of the following items: Amazon Web Services (AWS) console

- Azure console
- Datadog
- GHC
- GitLab
- GoLang
- Helm
- Jira
- Justworks
- Kubernetes
- Node
- Postgresql
- Python
- RabbitMQ
- Redis
- Salesforce
- SendGrid
- SharePoint
- Solr
- Threat Stack

People

GreatHorn operates with a hierarchical structure, illustrated in the chart below, that supports broad management oversight, separation of duties, and clear reporting lines. The structure is divided into seven primary operational areas—Engineering, Operations, Marketing, Finance, Sales, Business Development, and Customer Experience—led by dedicated Vice Presidents that report to the Chief Executive Officer. The Chief Technology Officer, who serves as the security officer, exercises operational independence and reports directly to the Chief Executive Officer.



The organization has also identified the following roles as critical to the operation of this structure and the achievement of service delivery and security objectives:

- Account Executive
- Business Development Representative
- Chief Executive Officer
- Chief Technology Officer
- Controller
- Customer Success Lead
- Customer Success Manager
- Demand Generation Manager
- Marketing Coordinator
- Principal Engineer
- Quality Assurance Engineer
- Quality Assurance Intern
- Sales Development Representative
- Sales Engineer
- Senior CloudOps Engineer & Team Lead
- Senior Content Marketing Manager
- Senior Customer Success Manager
- Senior Data Scientist
- Senior Quality Assurance Engineer
- Senior Quality Assurance Engineer Lead
- Senior Software Engineers
- Senior Software Engineer Lead
- Software Engineers
- Senior Solutions Engineer
- Strategic Account Executive
- Support Engineer
- Vice President of Business Development
- Vice President of Customer Experience
- Vice President of Engineering
- Vice President of Finance
- Vice President of Marketing
- Vice President of Operations
- Vice President of Sales

Data

GreatHorn collects, stores, processes, and transmits a variety of data types to provide its email security platform and application programming interfaces (APIs) customers use to integrate the GreatHorn solution with log aggregation and other tools. GreatHorn retrieves data for a customer from third-party services (e.g., Office365 and G-Suite) periodically, and adds it to a database provisioned for that customer. That data is then moved through a data processing pipeline, which analyzes data for anomalies and known attack indicators; applies customer-defined policies; and, finally, incorporates that data into the anonymized dataset called Fingerprint. Customer-defined policies can be configured to take any of a number of actions, such as emailing administrators, quarantining emails, or modifying an email or message. Processed data is added to a search engine that allows the customer fast access to data via the GreatHorn dashboard website and APIs.

The organization uses a variety of technical mechanisms, including encryption and secure transmission protocols, to protect customer data at every stage of processing and service delivery. All at-rest data is stored in encrypted, separate customer databases using 256-bit AES encryption supported by the AWS cloud hosting service. Communication channels between GreatHorn and its hosting providers and clients are encrypted with TLS using ECDHE key exchange, 256-bit AES, and SHA-386 to ensure the integrity and security of data transmissions.

Processes and Procedures

GreatHorn has established regular meetings, implemented security alerting and monitoring tools, and developed standard monitoring procedures to support its information security program and posture.

- CloudOps personnel meet daily to review Threat Stack alerts, assign action items, and generate Jira tickets for action prioritization.
- A security operations team meets monthly to review and discuss default configuration settings, changes, permissions and roles, log reviews, and other necessary security and infrastructure topics.
- Threat Stack is used for threat detection related to suspicious addresses, file integrity monitoring at the operation system level, and package vulnerability.
- The kube-bench tool is used to run daily Center for Internet Security (CIS) Kubernetes benchmark checks within the Kubernetes cluster. Results are reported and addressed according to established vulnerability management policies.
- Alerts from monitoring and detection tools are evaluated and escalated for additional action (e.g., activation of the incident response plan) as needed.

SECTION B:
PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

Due to the nature of the services it provides and the industries of some clients, GreatHorn is impacted by the following regulatory measures:

- GreatHorn is considered a data processor under the European Unions (EU) General Data Protection Regulation (GDPR).
- The organization is considered a service provider under the California Consumer Privacy Act (CCPA).
- GreatHorn signs business associate agreements to meet the requirements of its clients impacted by the Heath Insurance Portability and Accountability Act (HIPAA).

GreatHorn has designed its service system, contractual materials, and internal control programs to meet its service delivery and data security and privacy obligations under these regulatory measures.

Contractual Commitments

GreatHorn uses contractual materials, including terms of service, to define the type and scope of its service commitments to clients. Contractual materials may be tailored to individual client needs but generally include sections on the following topics:

Subject matter of processing
Duration of processing
Categories of data subjects
Nature and purpose of processing
Types of personal information
Client acceptable use policy
Support policy
Service level agreements (SLAs)

System Design

GreatHorn designs its email security platform 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.