REPORT ON LOGICMONITOR, INC.'S SOFTWARE AS A SERVICE SYSTEM RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY THROUGHOUT THE PERIOD APRIL 1, 2018 TO MARCH 31, 2019

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

COALFIRE CONTROLS

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: LogicMonitor, Inc. ("LogicMonitor")

Scope

We have examined LogicMonitor's accompanying assertion titled "Assertion of LogicMonitor, Inc. Management" (assertion) that the controls within LogicMonitor's Software as a Service System (system) were effective throughout the period April 1, 2018 to March 31, 2019, to provide reasonable assurance that LogicMonitor'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

LogicMonitor is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that LogicMonitor's service commitments and system requirements were achieved. LogicMonitor has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, LogicMonitor is responsible for selecting, and identifying in its assertion, the applicable trust service 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 LogicMonitor'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 LogicMonitor'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 LogicMonitor's Software as a Service System were effective throughout the period April 1, 2018 to March 31, 2019, to provide reasonable assurance that LogicMonitor's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
July 17, 2019

SECTION 2

ASSERTION OF LOGICMONITOR, INC. MANAGEMENT

LogicMonitor

Assertion of LogicMonitor, Inc. Management

We are responsible for designing, implementing, operating and maintaining effective controls within LogicMonitor, Inc.'s ("LogicMonitor") Software as a Service System (system) throughout the period April 1, 2018 to March 31, 2019, to provide reasonable assurance that LogicMonitor'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 3 of this report 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 April 1, 2018 to March 31, 2019, to provide reasonable assurance that LogicMonitor'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*). LogicMonitor'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 3 of this report.

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 April 1, 2018 to March 31, 2019, to provide reasonable assurance that LogicMonitor's service commitments and system requirements were achieved based on the applicable trust services criteria.

Very truly yours,

DocuSigned by:
Ziad Fanous
ED21170E1678416...

Ziad Fanous
Chief Financial Officer

SECTION 3

LOGICMONITOR, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS SOFTWARE AS A SERVICE SYSTEM

COMPANY BACKGROUND

Founded in 2008, LogicMonitor, Inc. (“LogicMonitor”, “the Company”) aims to simplify performance monitoring for complex technology infrastructures. LogicMonitor provides an automated, Software as a Service (“SaaS”) based Information Technology (IT) performance monitoring platform that provides the end-to-end visibility and actionable intelligence required to manage modern technology environments. The Company is headquartered in Santa Barbara CA, with offices in Austin TX, London UK, Chengdu CN, and Singapore.

OVERVIEW OF SERVICES PROVIDED

LogicMonitor’s Service (“the Service”) is a SaaS-based health and performance monitoring system designed to auto-discover, instrument, and deliver alerts for IT devices, systems, or applications. For example, the service provides comprehensive monitoring of operating systems (Windows, Linux, etc.), servers and networking equipment (Dell, HP, Cisco, Juniper, etc.), hypervisors and virtual machines (VMware, Hyper-V, etc.), storage systems, (EMC, NetApp, etc.), cloud resources (Amazon Web Services, Azure, etc.), as well as databases and applications (MSSQL, MySQL, IIS, Apache, etc.).

The Service relies on a remotely-actuated application known as the LogicMonitor Collector that is installed within a customer’s operations environment, where it performs device discovery and polling. An included feature known as LogicMonitor Websites provides for the measurement of website performance from various locations both inside and outside the customer’s infrastructure.

The scope of this report includes only the systems which provide the LogicMonitor Service. Any other LogicMonitor systems are not included within the scope of this report.

The boundaries of the system are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide the Service. Any infrastructure, software, people, procedures and data that indirectly support the Service are not included within the boundaries of the system.

The accompanying description includes only policies, procedures, and control activities at LogicMonitor and does not include policies, procedures, and control activities at any subservice organizations (see below for further discussion of subservice organizations).

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

INFRASTRUCTURE

The LogicMonitor service platform is provided out of service centers located in the US West Coast, US East Coast, and EU West Coast. Each service center is comprised of a co-located datacenter operated by Equinix along with cloud compute resources provided in an adjacent Amazon Web Services (AWS) region. Each service location employs a range of dedicated hardware used for service delivery including servers, networking hardware, application delivery controllers, and firewalls.

LogicMonitor's corporate operating environment consists of business systems and networks used for management of the enterprise. The corporate environment is separated from the Service both logically and physically, and various controls are in place to restrict traffic between the two.

SOFTWARE

The LogicMonitor Service is delivered using various software systems, with the core platform based upon an n-tier (multilayered) architecture. LogicMonitor uses multiple tools to operate the Service in a manner that ensures consistency and repeatability in all processes related to the Service's technical operations.

The software itself is comprised of a number of discrete components designed in a Service-Oriented Architecture (SOA). All components of the Service are written in the Java programming language and run in the Tomcat Java Application Server. Security-hardened Linux is used exclusively in the operation of the LogicMonitor Service.

PEOPLE

The Company's organizational structure provides a framework for planning, executing and controlling business operations. This structure ensures that LogicMonitor can maintain roles and responsibilities required to meet our commitments to provide for security, availability, and confidentiality.

LogicMonitor maintains formal procedures for the hiring and termination of employees with the goal to minimize the risk of malicious behavior. Background checks are conducted for all employees prior as part of the hiring process. Once an individual enters into an employment agreement with LogicMonitor a standardized onboarding procedure is conducted. This process includes training courses relating to general workplace standards and ethics as well as information security awareness. Ongoing compliance initiatives ensure that employees understand and follow established policies.

The Company's organizational structure includes ten functional teams including Executive Management, Product, Engineering, Technical Operations, Customer Experience, Sales, Marketing, Finance, People Operations, and Information Security. Responsibility for the Company's controls around security, availability, and confidentiality are specifically designated to the following roles: Executive Management, Engineering, Technical Operations, Customer Experience, Finance, or Information Security.

PROCEDURES

LogicMonitor has numerous operational procedures in place to help meet commitments to maintaining the security, availability, and confidentiality of customer data.

Access Management

Access to LogicMonitor's infrastructural systems is mediated by multiple levels of strong authentication and authorization controls. Requests for access follow a formal process that involves a request and subsequent approval from a data or system owner, and regular access audits ensure that each individual's rights are continually in alignment with policies of least privilege.

Secure Development

LogicMonitor's software development processes have been designed such that security is evaluated for each component at various stages in their respective lifecycles. All new initiatives and projects undergo evaluation by LogicMonitor's Architecture Review Board, which includes an analysis of security and availability categories prior to acceptance. Testing for security defects is based on a regimen that includes manual source code analysis as well as automated static code analysis (SAST) and dynamic application security testing (DAST) tools.

Change Management

The Company utilizes agile software development processes in the development of the service. Separate development, test, and production environments are maintained, and all changes are staged for formal acceptance testing prior to production release. The production change request process enforces and records request authorization, code review, acceptance testing, and release version targeting. Releases are conducted on a per-component basis and are conducted by the component team lead following management approval.

Vulnerability Assessments and Penetration Testing

Both external-facing and internal-facing vulnerability assessments are conducted against the LogicMonitor infrastructure on a continual basis to identify potential security issues with the service platform. Any discovered vulnerabilities are assessed for risk and prioritized for remediation accordingly.

The Company arranges for third-party white box penetration testing of the LogicMonitor Platform and LogicMonitor Collector at least annually. Any security defects discovered are escalated for highest-priority remediation.

Incident Management

LogicMonitor has a formal incident management process for any events that may affect the confidentiality, integrity, or availability of its systems or data. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. When an information security incident occurs, security engineering staff respond by logging and prioritizing the incident according to its severity. Events that directly impact customer data are treated with the highest priority. Following remediation, incidents undergo post-mortem investigations as necessary to determine the root cause for single events, trends spanning multiple events over time, and to develop new strategies to help prevent recurrence of similar incidents.

DATA

Various types of customer data are maintained in the operation of the LogicMonitor Service. Customer data is broadly classified into categories of account metadata and performance data. Handling of this data is governed by the Data Classification section of LogicMonitor's Information Security Policy, which requires that any data classified as sensitive is encrypted prior to storage in any target system.

All data stored within the LogicMonitor’s service platform, whether provided by the customer, collected from devices and services, or generated by the audit logging facility, are owned exclusively by the customer.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

COMMITMENTS

Commitments are declarations made by management to customers regarding the performance of the LogicMonitor Service. These commitments are documented and communicated to customers in LogicMonitor's Terms of Service. The Company's commitments include the following:

- To use commercially reasonable efforts to operate the Service such as it is available 24 hours a day, 7 days a week.
- To not use the Confidential Information disclosed for any purpose except as necessary to perform the obligations outlined under the Terms of Service.
- All aggregated information will be anonymized, de-identified, modified and rendered in such a manner to not identify the Customer.
- To notify the Customer, in writing, of any misuse or misappropriation of confidential information that may come to LogicMonitor's attention.
- Take all appropriate and commercially reasonable measures to safeguard personal data against the risks of a security incident.
- Notify customer and provide information about security incident in which LogicMonitor becomes aware of.

SYSTEM REQUIREMENTS

System requirements are specifications regarding how the Service should function to meet the Company's commitments to customers. Requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements include the following:

- User access policies and procedures.
- Operation of the LogicMonitor Service to meet commitments regarding confidentiality, high-availability and high-security.
- Formal classification of customer data, and the use of encryption technologies to protect customer data both at rest and in transit.
- Management of internal systems and services to provide for business continuity needs.
- Regular security audits of the operating environment including both the operational infrastructure and the LogicMonitor Service applications.
- Release management procedures that require formal testing of all changes prior to production deployment and communication to customers commensurate with impact.
- Incident response procedures and annual testing.
- Continual backups of customer data.

AVAILABILITY

The availability category refers to the accessibility of the LogicMonitor Service as committed by the Company in its Terms of Service. Controls addressing the availability of the LogicMonitor Service are primarily dependent on the Company's technical operations practices, including the implementation and management of production networks, systems, applications, and other service delivery components.

The risks that would prevent the Company from meeting its availability commitments and requirements are diverse. Availability includes consideration of risks during normal business operations, during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

LogicMonitor has designed controls to address the risks to service availability, including:

- Insufficient processing capacity.
- Failure of individual hardware or software systems.
- Connectivity to the public internet and/or internal private networks.
- Loss of processing capability due to failures with subservice providers.
- Loss of key processing facilities or personnel due to a natural disaster.

Availability risks are addressed through the use of heartbeat and infrastructure monitoring tools, data backup and restore processes, automated provisioning of hot-spare infrastructure, and comprehensive disaster recovery plans and procedures.

In evaluating the suitability of the design of availability controls, LogicMonitor considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of backup procedures, the reliability of the backup process, and the ability to restore data. In evaluating the design of data availability controls, the Company considers that most potential data loss events are caused by routine processing errors and failures of system elements rather than natural disasters.

INFRASTRUCTURE MONITORING

The Company monitors operational systems, networks, services, and applications as a routine part of business. A dedicated instance of the LogicMonitor Service is used for monitoring the production environment and customer support systems. LogicMonitor's SaaS System and network instrumentation includes myriad health and performance metrics including system and network performance, resource capacity, service latency, network flows, etc., with alert delivery configured to notify appropriate personnel of potentially impactful events.

All LogicMonitor devices, systems, and applications are configured to deliver operational logs to a third-party log service provider where they are stored in an immutable format. Analytical tools that automatically detect anomalous event behavior are configured to deliver alerts accordingly.

BUSINESS CONTINUITY MANAGEMENT

To minimize service interruption due to hardware failure, natural disaster, or other catastrophes the Company has built business continuity principles into the foundation of the LogicMonitor Service and business operations. LogicMonitor's disaster recovery program includes multiple components to minimize the risk of any single point of failure.

Operational Redundancy and Resiliency

The Service is operated out of three geographically distributed datacenters with ancillary services provided out of adjacent AWS regions. Network equipment is deployed in N+1 high-availability pairs to provide for immediate failover.

Customer Data Backup and Recovery

Backups of LogicMonitor customer data are conducted via customer data “snapshots” which occur every four hours. Upon generation, each snapshot is encrypted with a customer-specific key and transmitted to AWS. Once in AWS, each snapshot package is replicated across at least two availability regions. A rotation schedule is maintained for each snapshot package, with a maximum retention period of one year.

The restoration of customer data from a snapshot is an automated process that can be actuated only by LogicMonitor technical operations staff. The Company's overall backup/restore processes are employed continually in the service operation but also undergo formal testing once per quarter.

Disaster Recovery – Operational Systems

Formal disaster recovery procedures are developed and documented as part of the Company's information security policies. The recovery process involves automated provisioning and configuration of AWS resources using Terraform, Puppet, and Ansible orchestration tools followed by the restoration of backup data from affected customers. LogicMonitor's disaster recovery process is tested at least annually.

Business Operations Continuity

Continuity of non-technical business operations is built around a strategy by which all business processes are implemented using either SaaS-based tools or systems operated out within IaaS environments with high levels of resiliency. All employees are issued laptop workstations, and access to LogicMonitor’s business systems is based upon a zero-trust model by which the same authentication and authorization requirements are enforced regardless of an employee’s location. This model ensures that none of LogicMonitor’s corporate offices need to be available, as all business tools are available to LogicMonitor’s employees using any internet connection.

CONFIDENTIALITY

The confidentiality category refers to the protection of customer data stored within LogicMonitor’s service platform as committed by the Company in the provided Terms of Service. Confidentiality protections within the Service are dependent both on the design of the service platform as well as the operation of the service components. Within the software development lifecycle, protections for confidentiality are incorporated both in the requirements definition phase as well as within the software development and testing phases. Once in the operational phase, various controls have been developed to ensure protection of data within production networks, systems, applications, and other service delivery components.

Confidentiality risks are addressed by controls covering the use, retention, and disposal of confidential data including data classification policies/procedures, various encryption technologies, network segmentation, remote access and transmission restrictions, vendor risk assessments, and vendor confidentiality agreements. Changes to vendor confidentiality agreements are reviewed by the legal department and communicated to appropriate individuals.

In evaluating the design of confidentiality controls, LogicMonitor considers the likely causes of improper disclosure or handling of confidential information as well as the commitments and requirements related to confidentiality.