COALFIRE CONTROLS

Report on LogicMonitor, Inc.'s Software-as-a-Service (SaaS) System Relevant to Security, Availability, and Confidentiality Throughout the Period April 1, 2022 to March 31, 2023

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

LogicMonitor

Table of Contents

Section 1

Section 2

Attachment A

Attachment B

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 (SaaS) System (system) were effective throughout the period April 1, 2022 to March 31, 2023, 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 (With Revised Points of Focus—2022)* (2017 TSC).

LogicMonitor uses subservice organizations to provide data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LogicMonitor, to achieve LogicMonitor's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of LogicMonitor's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 SaaS System were effective throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that LogicMonitor’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of LogicMonitor’s controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
August 17, 2023

Section 2

Assertion of LogicMonitor, Inc. Management

LogicMonitor

Assertion of LogicMonitor, Inc. (“LogicMonitor”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within LogicMonitor’s Software-as-a-Service (SaaS) System (system) throughout the period April 1, 2022 to March 31, 2023, 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 (With Revised Points of Focus—2022)* (2017 TSC). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

LogicMonitor uses subservice organizations for data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LogicMonitor, to achieve LogicMonitor’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of LogicMonitor’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that LogicMonitor’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of LogicMonitor’s controls operated effectively throughout that period. 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 attachment 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 April 1, 2022 to March 31, 2023, to provide reasonable assurance that LogicMonitor’s service commitments and system requirements were achieved based on the applicable trust services criteria.

LogicMonitor, Inc.

DocuSigned by:
Adam Healy
5DBA3FA5D0A849E...
Adam Healy

CISO

Attachment A

LogicMonitor, Inc.’s Description of the Boundaries of Its Software-as-a-Service (SaaS) System

Type of Services Provided

LogicMonitor, Inc. (“LogicMonitor” or “the Company”) provides LM Envision, a Software-as-a-Service (SaaS)-based unified observability platform (“the LogicMonitor SaaS System” or “the Service”), designed to help information technology operations (ITOps), cloud operations (CloudOps), development operations (DevOps), managed service providers (MSPs), and business leaders gain visibility and predictability across the technologies that deliver employee and customer experiences. LM Envision enables observability across technology infrastructure, networks, clouds, containers, and applications, empowering companies to focus less on troubleshooting and more on innovation. The LogicMonitor SaaS System automatically discovers technology infrastructure and applications; monitors instrument health and performance via metrics, logs, and traces; detects issues and correlates anomalies; and delivers notifications as appropriate to technical teams, application owners, and service management platforms.

The Service relies on the LogicMonitor Collector, a remotely actuated application installed within each customer’s environments that performs infrastructure discovery and polling.

The boundaries of the system in this section details the LogicMonitor SaaS System. Any other LogicMonitor services are not included in the scope of this report.

The Components of the System Used to Provide the Services

The boundaries of the Service are the specific aspects of LogicMonitor’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Service.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The LogicMonitor SaaS System is hosted out of service centers located in the US West; US East; European Union (EU) West; Europe, the Middle East, and Africa (EMEA) West; and Southeast Asia-Pacific (SE AsiaPac) regions. Each service center is composed of a co-located data center operated by Equinix along with cloud compute resources provided in an adjacent Amazon Web Services (AWS) region, with the exception of AsiaPac and EMEA West, which operate solely in AWS. Each service location uses a range of dedicated hardware for service delivery, including servers, networking hardware, application delivery controllers, and firewalls. All network equipment is deployed with n+1 redundancy to provide for automatic failover. LogicMonitor's Website Check facility runs on systems within some data center locations, as well as in global AWS regions.

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

Software

The LogicMonitor SaaS System is delivered using various software systems, with the core platform based upon an n-tier (multilayered) architecture. Many tools are used to operate the LogicMonitor SaaS System to ensure consistency and repeatability in all processes related to its technical operations. These tools are listed below:

Business Function

- LogicMonitor's infrastructure performance monitoring system
- LogicMonitor's customer-installed data collection application
- Operating system and application configuration management
- Automated deployment of software applications
- Automated provisioning of cloud infrastructure
- Credential management service
- Source code management
- Secure remote access to the production environment
- Identity and single sign-on (SSO) service provider
- Log analytics service provider
- Endpoint detection and response
- Privileged access management (PAM)
- Workload protection and detection
- Network intrusion detection and prevention

The LogicMonitor SaaS System software comprises many discrete components that operate as a service-oriented architecture.

People

The Company’s organizational structure includes eight core teams that roll up through Executive Management, including Product, Technology, Financial, Customer, Human Resources, Legal, Revenue, and Marketing. Responsibility for the Company’s controls around security, availability, and confidentiality are specifically designated to the roles defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for the security of both the Service and business operations, including overall enforcement of security policies across the organization.
Technical Operations	Responsible for implementation and management of security controls targeted at the operation and management of the LogicMonitor SaaS System.
Business Technology	Responsible for operating LogicMonitor’s business systems and networks, managing corporate offices, employee identity management, and digital supplier management.
Software Development	Responsible for the development, management, and support of the application components on which the LogicMonitor SaaS System is based. Secure software development practices are employed in the development of all software components.

People	
Group/Role Name	**Function**
Customer Support	Responsible for fielding customer calls around the LogicMonitor SaaS System, managing trouble tickets based on customer requests, and communicating with customers regarding service outages and other issues.
Information Security	Responsible for security program strategy and oversight of tactical security initiatives across the organization, including in-product security designs, operational security analytics, secure software engineering processes, development of security policies, and security compliance initiatives.

The following organization chart reflects the Company's internal structure related to the groups discussed above:

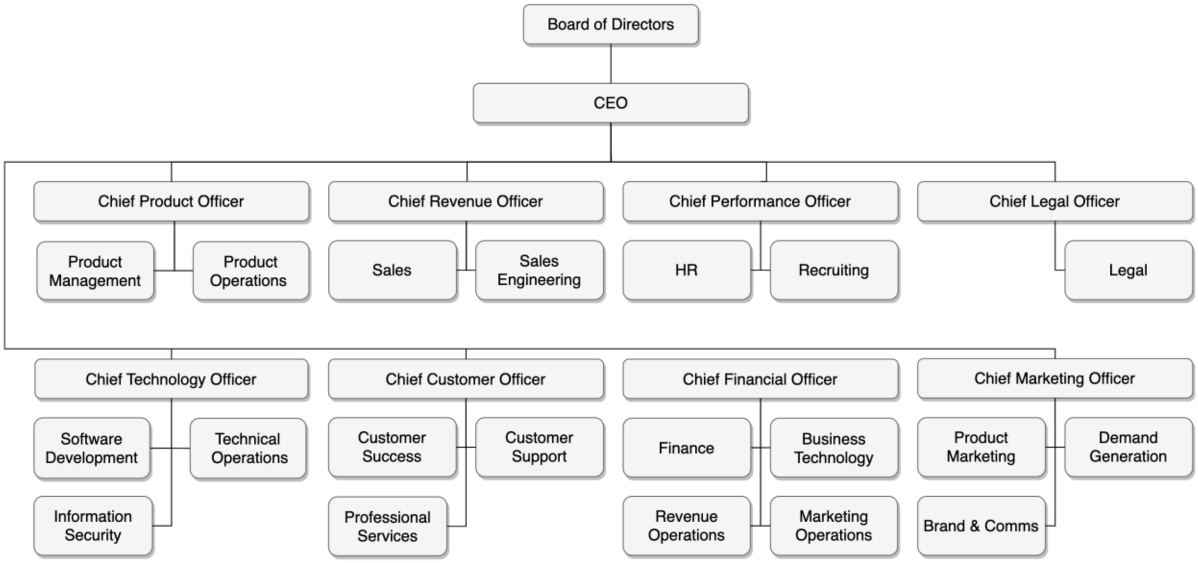

Figure 1: LogicMonitor's Organization Chart

Procedures

LogicMonitor has operational procedures in place to help maintain the security, availability, and confidentiality of customer data. The procedures to help meet these commitments include the following:

- Formal business continuity and disaster recovery procedures to ensure minimal interruption to critical business processes.
- Incident management procedures to appropriately react to events that may impact service availability or security.
- Formal processes around people operations, including background checks, security awareness training, and required acknowledgement of security policies and confidentiality agreements.
- Access management policies for all business systems based on two-factor authentication and authorization based on the principle of least privilege.

In addition to the procedures stated above, standard operating procedures document how to carry out specific manual and automated processes required to operate and develop the Service.

All policies and procedures are made available to employees on the LogicMonitor internal wiki for personnel to review and understand their responsibilities in adhering to the requirements documented therein. These policies are reviewed and updated continually to meet best practices and undergo annual review by senior management to ensure alignment with business objectives.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the LogicMonitor SaaS System production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data at Equinix are encrypted at rest. Encryption is enabled for databases housing sensitive customer data in the AWS environment.

Several types of customer data are maintained in the operation of the 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 is summarized below:

Data	
Data Description	**Classification**
End User Personal Information • Name, email address, user ID, password, and mobile device number	Customer Confidential
Device and Website Metadata • Hostnames, Internet Protocol (IP) addresses, website addresses, firmware versions, etc.	Customer Sensitive
Device and Website Access Credentials • Monitoring access credentials (Simple Network Management Protocol [SNMP] community, application programming interface [API] tokens, Windows Management Instrumentation [WMI] authentication, Hypertext Transfer Protocol [HTTP] basic authentication, etc.)	Customer Confidential
Audit Log Metadata • Account telemetry, including authentication actions and operational changes	Customer Sensitive
Device Performance Data • Memory utilization, network throughput, storage capacity, etc.	Customer Sensitive
Website Performance Data • Website response time, health status, synthetic transactions, etc.	Customer Sensitive
Device Logs and Event Data • Textual messages generated by a device, as either log data or event data	Customer Sensitive
Device Configuration Data • Text-based directives used to establish a devices' operating configuration	Customer Confidential

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS and Equinix as subservice organizations for data center colocation services. The Company's controls related to the LogicMonitor SaaS System cover only a portion of the overall internal control for each user entity of the LogicMonitor SaaS System.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at AWS and Equinix related to physical security and environmental protection, as well as backup, recovery and redundancy controls related to availability. AWS and Equinix's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS and Equinix's environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS and Equinix SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS and Equinix to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS and Equinix management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the LogicMonitor SaaS System to be achieved solely by the Company. AWS and Equinix are expected to have implemented the following CSOCs.

Criteria	Complementary Subservice Organization Controls
CC6.1	• AWS encrypts databases in its control.
CC6.4	• AWS and Equinix restrict data center access to authorized personnel. • AWS and Equinix monitor data centers 24/7 by closed circuit cameras and security personnel.
CC6.5 CC6.7	• AWS and Equinix securely decommission and physically destroy production assets in their control.
CC7.2 A1.2	• AWS and Equinix install fire suppression and detection and environmental monitoring systems at their data centers. • AWS and Equinix protect data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS and Equinix oversee the regular maintenance of environmental protections at their data centers.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the LogicMonitor SaaS System. Commitments are communicated in LogicMonitor's Master Subscription Agreement.

System requirements are specifications regarding how the LogicMonitor SaaS System should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the LogicMonitor SaaS System include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Take all appropriate and commercially reasonable measures to safeguard customer data against the risks of unauthorized access or use. • Notify and provide information to customers about security incidents that LogicMonitor becomes aware of.	• User access policies and procedures based on the principle of least privilege. • Multi-factor authentication to secure employee access to operational systems. • Secure software development life cycle with multiple types of security testing. • Platform operating system vulnerability scanning and management processes. • System hardening. • Management procedures that require formal testing of all changes prior to production deployment and communication to customers commensurate with impact. • Security incident handling procedures. • Onboarding procedures for new personnel.
Availability	• Use commercially reasonable efforts to operate the LogicMonitor SaaS System 24 hours a day, 7 days a week.	• Disaster recovery considerations fundamental to operational architecture design. • Continual backups of customer data to meet recovery point objective (RPO) and recovery time objective (RTO) targets.

Trust Services Category	Service Commitments	System Requirements
Confidentiality	• Do not use or disclose confidential information for any purpose except as necessary to perform the obligations outlined under the Master Subscription Agreement. • Anonymize and render all aggregated information in such a manner as to not identify the customer. • Notify the customer, in writing, of any misuse or misappropriation of confidential information that may come to LogicMonitor's attention. • Return or destroy all copies of the customer's confidential information if the services expire or terminate, or upon request. • Protect customer confidential information by using the same standard of care that it uses in protecting its own confidential information.	• Formal classification of customer data. • Encryption technologies to protect customer data both at rest and in transit.