System and Organization Controls (SOC) 3 Report

SecurityGate.io™

Report on the SecurityGate Platform relevant to Security, Availability, and Confidentiality

Throughout the period April 1, 2022 to September 30, 2022

Table of Contents

Independent Service Auditor's Report Provided by Laika Compliance LLC

To: SecurityGate, Inc. (“SecurityGate” or “the Company”)

Scope

We have examined SecurityGate’s accompanying assertion titled “Assertion of SecurityGate, Inc.’s Management” (assertion) that the controls within the Company’s SecurityGate Platform (system) were effective throughout the period April 1, 2022 to September 30, 2022, to provide reasonable assurance that SecurityGate’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 CriteService Organization’s Responsibilities

SecurityGate 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 SecurityGate’s service commitments and system requirements were achieved. SecurityGate has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, SecurityGate 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 Company’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 the Company’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 the Company'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 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 SecurityGate's controls over the SecurityGate Platform were effective throughout the period April 1, 2022 to September 30, 2022, to provide reasonable assurance that SecurityGate's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Laika Compliance LLC

Arlington, Virginia
November 8, 2022

Assertion of SecurityGate, Inc.'s Management

We, as management of SecurityGate, Inc., are responsible for:

- Identifying the SecurityGate Platform (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion.

SecurityGate uses a subservice organization for data center colocation services. The boundaries of the System presented in Attachment A includes only the controls of SecurityGate and excludes controls of the subservice organization. However, the description of the boundaries of the system does present the types of controls SecurityGate assumes have been implemented, suitably designed, and operating effectively at the subservice organization. Certain trust services criteria can be met only if the subservice organization's controls are suitably designed and operating effectively along with the related controls at SecurityGate. However, we perform monitoring procedures for the subservice organization and based on procedures performed, nothing has been identified that prevents us from achieving our specified service commitments and system requirements.

We assert that the controls over the system were effective throughout the period April 1, 2022 to September 30, 2022, to provide reasonable assurance that SecurityGate's service commitments and system requirements would be achieved based on the criteria relevant to Security, Availability, and Confidentiality set forth in the AICPA's TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Very truly yours,

SecurityGate, Inc.

Attachment A – SecurityGate Platform Overview

SERVICES PROVIDED

SecurityGate, Inc. ("SecurityGate" or "the Company") is a Software-as-a-Service ("SaaS") company. SecurityGate offers a SaaS application, known as the SecurityGate Platform, which acts as a risk management acceleration platform that helps industrial companies understand cyber risks and make improvements.

INFRASTRUCTURE

The Company utilizes Amazon Web Service (AWS) to provide the resources to host the SecurityGate Platform. The Company leverages the experience and resources of AWS to quickly and securely scale as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the architecture within AWS to ensure security and resiliency requirements are met. Controls operated by AWS are not included in the scope of this report.

The affected criteria are included below along with the minimum controls expected to be in place at the aforementioned hosting provider:

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.4	• AWS is responsible for restricting data center access to authorized personnel • AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel
CC6.5	• AWS is responsible for securely decommissioning and physically destroying production assets in its control
CC7.2	• AWS is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers • AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS) • AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

SOFTWARE

Software consists of the programs and software that support the SecurityGate Platform. Software and ancillary software is used to build, support, secure, maintain, and monitor the SecurityGate Platform.

PEOPLE

The Company develops, manages, and secures the SecurityGate Platform via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the SecurityGate Platform.
Product	Responsible for overseeing the day-to-day operations of the SecurityGate Platform and implementing new features.
Customer Experience	Responsible for engaging and maintaining customer relationships, and addressing customer issues.

PROCEDURES

Procedures include the automated and manual procedures involved in the operation of the SecurityGate Platform. Procedures are developed and documented by the respective teams for a variety of processes. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of SecurityGate Platform:

Procedure	Description
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.

System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change and Configuration Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk and Compliance	How the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Data Backup and Storage	How the Company manages data backups to allow for data restorations to occur if needed.
Business Continuity and Disaster Recovery (BC/DR)	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
Data Classification and Handling	How the company classifies data included in the service and the procedures for handling the data.

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 SecurityGate Platform production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

SecurityGate's controls were designed with the assumption that certain controls would be implemented by user entities (or "customers"). Certain requirements can be met only if complementary user entity controls assumed in the design of SecurityGate's controls are suitably designed and operating effectively, along with related controls at SecurityGate. Identified complementary user entity controls were included in the service auditor's examination of SOC 2 controls.

Attachment B – Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of SecurityGate Platform. The Subscription Services Agreement includes the communication of the Company's commitments to its customers.

System requirements are specifications regarding how SecurityGate 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 SecurityGate Platform include the following:

Trust Services Category	Service Commitments	System Requirements
Security	SecurityGate implements and maintains reasonable security measures to protect customer information. Such measures include procedures for detecting, preventing, and responding to attacks, intrusions, or other system failures.	• Identity and access control • Security monitoring and reporting • Threat management • Security incident response • Security awareness training • Third party provider controls (vendor risk management) • Change control procedures
Confidentiality	SecurityGate implements reasonable measures to protect the confidentiality of customer information that could result in the unauthorized disclosure of such information.	• Data Retention and Disposal • Data Classification
Availability	SecurityGate will maintain the availability of services to customers and issue an availability warranty if availability drops below predefined levels.	• BC/DR plan and procedures • Data backups