MT4 Tecnologia Ltda.

System and Organization Control (SOC) 3 for Service Organizations Report for the period from January 1, 2025, to October 31, 2025

Ref.: Report No. 261T3-023-EN

Contents

I. Report of Independent Auditors

Grant Thornton Auditoria e Consultoria Ltda.
Av. Eng. Luiz Carlos Berrini, 105 -
12º andar, Itaim Bibi - São Paulo (SP)
Brasil
T +55 11 3886-5100
www.grantthornton.com.br

To the Management and the Board of Directors of MT4 Tecnologia Ltda.

Scope

We have examined MT4 Tecnologia Ltda. ("the Company or "Segura® ") accompanying assertion titled "Assertion of MT4 Tecnologia Ltda." (assertion) to determine that the controls within its Segura® SaaS 360o Identity Platform ("description" or "system") were effective throughout the period January 1, 2025 to October 31, 2025, to provide reasonable assurance that Segura®'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity 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

Segura® 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 Segura®'s service commitments and system requirements were achieved. Segura® has also provided an accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Segura® 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 and the International Standard on Assurance Engagements (ISAE) 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board ("IAASB"). 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 Segura®'s service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Segura®'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 these 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 Segura®'s system were effective throughout the period January 1, 2025, through October 31, 2025, to provide reasonable assurance that Segura®'s service commitments and system requirements were achieved based on the applicable trust services criteria, and is fairly stated, in all material respects.

São Paulo, January 30, 2026

Grant Thornton Auditoria e Consultoria Ltda.
CRC 2SP-034.766/O-0

Maikon Melo da Silva
Contador CRC 1SP-352.178/O-8

II. MT4 Tecnologia Ltda. Assertion

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2025, to October 31, 2025, to provide reasonable assurance that Segura®'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, 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).* Segura®'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.

Attachment A – Segura® SaaS 360o Identity Platform

About Segura®

Segura® is a global cybersecurity technology provider with a comprehensive SaaS portfolio and operations worldwide. senhasegura USA LLC ("Segura®") is the subsidiary company of MT4 Tecnologia Ltda.

With more than 300 partners, Segura® enhanced its global presence on all continents, and the company is expanding rapidly in North America and EMEA with new distributors and several resellers. Segura® has customers in more than 70 countries.

Segura® has a wide list of Mid-size and Large Corporate companies in its portfolio. Our customers span a wide range of industries, with the most prominent being financial services, manufacturing, services, government, and retail.

Key Achievements

Segura® has been recognized as a leader in 11 out of 23 market reports in 2025. See below for Segura®'s key achievements:

- **Gartner®:** Segura® was recognized as a Challenger in the 2025 Gartner® Magic Quadrant™ for Privileged Access Management (PAM). The company was acknowledged for its capabilities in account discovery, credential management, and lifecycle governance, highlighted for simplifying secure integration across cloud, Operational Technology (OT), Internet of Things (IoT), and on-premises environments, and cited as one of the fastest-growing PAM vendors.

- **Gartner Peer Insights™:** Segura® was named Customers' Choice 2025 for Privileged Access Management (PAM) for the second consecutive year and the fourth time overall. This recognition reflects strong customer trust, with a 4.9 overall rating, 98% willingness to recommend, and high scores in Product Capabilities and Sales Experience (4.8).

- **G2®:** Segura® was named a Leader in the Grid® Report for Privileged Access Management (PAM) – Winter 2025, earning multiple distinctions, including Best Relationship (Enterprise), High Performer (Enterprise and Mid-Market), Momentum Leader, and Users Most Likely to Recommend, reinforcing its reputation for strong security, ease of use, and high customer satisfaction.

Segura® SaaS 360° Identity Platform architecture was designed and developed to deliver the smallest total cost of ownership with the best time to value in the market.

Software

Segura® SaaS 360° Identity Platform is composed of nine products that allow total protection for privileges everywhere in the infrastructure including:

- Segura® PAM (Privileged Access Manager) for credential vaulting and session management for both datacenter infrastructure and cloud providers.
- Segura® RPAM (Remote PAM) for Privileged Remote Access from employees and 3rd party VPN-less.
- Segura® WPM (Workforce Password Manager) for Workforce Password Management.
- Segura® EPM (Endpoint Privilege Manager) for Privileged Elevation and Delegation Management (PEDM).
- Segura® CLM (Certificate Lifecycle Manager) for centralized management of digital certificate lifecycle.
- Segura® CIEM (Cloud Infrastructure Entitlements Manager) for managing and optimizing access control and permissions in cloud environments.
- Segura® Cloud IAM for user management in cloud IAM resources and services.
- Segura® SM (Secret Manager) for machine identities management in DevOps environments.

In terms of licensing, Segura®'s products are sold as SaaS offerings, with subscription (self-managed) or perpetual licensing for on-premises installations.

Solutions overview

Segura® SaaS 360° Identity Platform addresses the full privileges lifecycle with a 360-degree approach before, during and after an access event from the initial request to the provisioning of access, and finally to verifying and auditing anything that was done. Segura® SaaS 360° Identity Platform is a cloud-native solution that protects privileged credentials in managing, password rotation, auditing and monitoring privileged actions in the environment.

Segura® SaaS 360° Identity Platform requires only the deployment of the network connector in the customer environment. No servers or controllers are required, reducing the cost and operational burden of managing on-premises software and hardware.

Infrastructure

Google Cloud Platform

Segura® is powered by Google Cloud Platform ("GCP").

The service delivers a high level of security, software as a service, guaranteed performance, and maintenance aligned with business needs, while maintaining compliance with applicable data protection regulations (e.g., LGPD, GDPR, CCPA) and data protection requirements.

Control environment

Segura® has established policies, processes, and procedures to formulate control activities and support the achievement of security, availability and confidentiality commitments, relevant laws and regulations, and other system requirements. These processes and procedures cover the following areas:

Compliance Program

An effective compliance program is essential to ensure that the company complies with relevant laws and regulations, helping us to protect the company's reputation and stakeholder confidence, and demonstrate the company's commitment to ethics and social responsibility.

Business Resilience

Business resilience allows the company to recover from disruptions and continue operating in adverse scenarios, such as natural disasters, cyber-attacks, or economic crises, minimizing reputational damage, and increase users’ confidence in the company's ability to deal with challenges.

Change Management

An established and effective change management program is crucial for the successful implementation of any alterations to our application, minimizing risks and disruptions associated with the change, ensures efficient execution, and provides more trust to our service.

Human Resources

Effective human resource management is essential to the success of our organization. Recruiting and selecting qualified and reliable people, continuous training and development of employees, performance evaluation and reward, and promoting an ethical and safe organizational culture are all important aspects that contribute to achieving the company's goals.

Information Security

Information security is essential to protect the confidentiality, integrity, and availability of the company's information, minimizing the risk of data loss, cyber-attacks, and fraud, and ensuring compliance with data protection laws and regulations.

Risk Management

Risk management is an ongoing process that aims to identify, assess, and mitigate the risks that may affect the company, allowing for more informed and strategic decision-making, protecting the company's assets and stakeholders' interests.

Logical Access

Logical access controls are essential to restrict access to information and systems to authorized employees only, minimizing the risk of misuse of information and systems, and protecting the confidentiality and integrity of data.

Operation Processing

Efficient and effective processing of operations is essential to the success of our organization, minimizing the risk of errors and financial losses, and enabling the optimization of the company's processes and resources.

Attachment B – Principle Service Commitments and System Requirements

Segura® designs its processes and procedures related to an extensive cyber security portfolio, called Segura® SaaS 360o Identity Platform, which meets the company's goals for their services. Objectives are based on the service commitments Segura® makes to user entities, regulations governing service delivery and compliance requirements established by Segura® for the services.

Security commitments are standardized and include but are not limited to:

1. Protecting access of information based on user roles in the system, on a need-to-know basis, whilst restricting them from accessing information not required for their role.

2. Protection of user entities' information against unauthorized access, modification, or disclosure.

3. Providing for the availability of services supporting user accounts.

4. Use of encryption technologies to protect customer data both at rest and in transit; and

5. Conduct standards dictating security, availability, and processing integrity standards.

Segura® establishes operational requirements that support the achievement of security commitments, relevant laws, regulations, and system requirements. Such requirements are communicated in Segura®'s system policies and procedures, system design documentation, and customer contracts. Information security policies define an organization-wide approach to protecting systems and data. These include online documentation that describes how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented for conducting the specific manual and automated processes required in the operation and development of the Segura® SaaS 360o Identity Platform.

Grant Thornton Auditoria e Consultoria Ltda. refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton Auditoria e Consultoria Ltda. is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

Grant Thornton

grantthornton.com.br