Service Organization Control 3 (SOC 3)

For the Period November 1, 2020 to October 31, 2021

Report of Cato Networks Platform System

Relevant to Security, Availability and Confidentiality

Kost Forer Gabbay & Kasierer
144 Menachem Begin St.
Tel-Aviv 6492102, Israel

Tel: +972-3-6232525
Fax: +972-3-5622555
ey.com

Report of Independent Accountants

To the Management of Cato Networks:

We have examined management's assertion that Cato Networks, during the period November 1, 2020 to October 31, 2021, maintained effective controls to provide reasonable assurance that:

- The System was protected against unauthorized access, use, or modification
- The System was available for operation and use, as committed or agreed
- Information within the System designated as confidential is protected as committed or agreed

Based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100 (2017), Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of Cato Networks's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included:

- (1) Obtaining an understanding of Cato Networks's relevant to security, availability and confidentiality controls.
- (2) Testing and evaluating the operating effectiveness of the controls.
- (3) Performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, Cato Networks's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

Very truly yours,

Kost Forrer Gabbay & Kasierer
A member firm of Ernst & Young Global
December 1, 2021
Tel Aviv, Israel

Management Assertion on the controls over Cato Networks Platform System, based on the AICPA Trust Services Principles and Criteria for security, availability and confidentiality

We, as management of, Cato Networks Ltd. ("Cato Networks" or " the Company") are responsible for:

- Identifying the Cato Networks Platform System (system) and describing the boundaries of the system, as presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of our system, as presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the Cato Networks Platform System (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

We assert that the controls over the system were effective throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that the principal service commitments and system requirements were achieved, based on the criteria relevant to security, availability and confidentiality set forth in the AICPA's TSP Section 100 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016).

Yours sincerely,

Signature 

Title Amit Spitzer I Chief Security Officer

Description of the Cato Networks Platform System

Company Overview and Background

Cato provides the world's first SASE platform, converging SD-WAN, Zero Trust Network Access (ZTNA), network security, and Cloud Access Security Broker (CASB) into a global, cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and remote users into the network with a zero-trust architecture.

Organizational structure

Cato Networks's organizational structure provides the overall framework for planning, directing and controlling operations for Cato Networks Platform System. It utilizes an approach whereby personnel and business functions are segregated according to job responsibilities. This approach allows the Company to clearly define responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their clients.

COO: The Chief Operating Officer manages all technical and operational aspects of the company. The COO is in charge of driving the company's technology path, maintaining its' leading technological edge, and researching the Networking and Security fields for innovations.

Security department: The Security team is responsible for operating the security features offered by the product and for security research.

CISO: The Chief Information Security Officer is responsible for the security of the Cato Cloud service and for general Information Security within the company.

CRO: The Chief Revenue Officer is in charge of all sales activities worldwide, support, technical sales aspects, and demand generation.

Components of the system providing the defined services

Cato Networks's Policies and Communication

Formal written policies for the principles and processes within the organization are developed and communicated so that personnel understand Cato Networks' objectives. The assigned policy owner updates the policy annually and the policy is reviewed and approved by designated members of management. In addition, responsibility, and accountability for developing and maintaining the policies are assigned to relevant teams and are reviewed and approved on an annual basis by the management team. Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to Cato Networks employees within the internal network

Significant components of these policies include, among others:

- Organizational structure
- Responsibility for information assets
- Information classification and sensitivity
- Access Control
- Security incident response
- Communication security
- Change management
- Physical security

A description of the Cato Networks Platform System and its boundaries is documented and communicated to Cato Networks employees and customers within the internal portal and the Cato Networks application. Cato Networks has implemented multiple communication channels to monitor that processes function as they were designed, and potential issues are identified and resolved in a timely manner. Various operations and synchronization meetings are generally conducted on a monthly basis or other timely basis in accordance with the operational needs. Cato Networks managers are responsible for communicating relevant corporate information and job-related data to their direct employees.

Availability, confidentiality and security-related obligations are communicated to Cato Networks's employees through the confidentiality and non-disclosure agreements while client obligations are communicated within their contracts. In addition, an incident management application is available to Cato Networks employees in order to report breaches of the system security, availability, and confidentiality. Customer issues are reported within a dedicated CRM application.

Security and Logical Access

Logical Access Overview

Cato Networks has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission.

Production environment

Access to the AWS management interface is restricted to authorized personnel. In addition, access to the production environment and databases is granted by the appropriate personnel, based on the employee role and documented. Access to the backup and offline storage is restricted to authorized individuals Employees are provided with the minimal access rights required to carry out their duties. A detailed ticket is opened in the ticketing system for new hire provisioning. This template includes all user detailed permissions. Additionally, strong password configuration settings, where applicable, are enabled on the domain, application and database.

User Permissions management

Cato Networks builds its production environment system architecture using the AWS services and other hosting providers. Firewall detailed configuration is defined and performed by the Cato Networks Operations team. In addition, the global management of the Cato Networks infrastructure is performed by Cato Networks using a dedicated AWS workspace. This interface allows Cato Networks to, among others, (1) add, modify, and manage servers, (2) create security policies as they relate to these servers, (3) configure network and firewall parameters, (4) manage the databases and (5) manage AWS users. Firewalls separate the internal network from the internet.

Recertification of Access Permissions

Cato Networks has implemented an access recertification process to help monitor that only authorized personnel have access to the systems, environments and databases. Permissions with the different production services in use by Cato Networks are reviewed and approved by Cato Networks's security team on a quarterly basis.

Access Revocation

User accounts are disabled or deleted on the production, application and database and the Company's assets are returned in a timely manner upon notification of job termination. Termination notifications indicating the employee's expected last day are sent to the relevant function: Management, HR, Finance, and IT. Terminated employees complete a termination clearance process on their last day at Cato Networks. This process includes revocation of access permissions to the systems and premises, as well as the return of the Company property, data and equipment.

Physical Access

Cato Networks recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets, and restricted areas. Physical access to the Cato Networks office is restricted to authorized personnel using personal electronic identification cards. These access cards are issued to Cato Networks' employees by the administrative manager. Permissions to issue cards and grant access are restricted to the administrative manager and the authorized designees. Visitors to the CATO's office are accompanied while on premises.

Remote Access

Cato Networks' internal networks are protected using commercial firewalls configured and administered by the IT department. In addition, Cato Networks' production environment servers are protected by the AWS tools and controls configured by Cato Networks. Cato Networks employees are granted remote access to the internal production network environment based on the need-to-work principle. Traffic entering Cato Networks' production network is monitored and screened by a firewall and monitoring tools implemented by AWS and configured by Cato Networks. Remote users are automatically disconnected from the production servers after a pre-defined period of inactivity and need to login again in order to re-establish connection to the network.

Vulnerability and penetration testing

A penetration test is performed on an annual basis and high issues are resolved in a timely manner through the SDLC process. The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. In addition, security scans are performed on a semi-annual basis. Furthermore, vulnerability scans are performed to the production environment on a quarterly basis, using an external tool, in order to detect potential security breaches. Web application architecture and implementation follow OWASP guidelines. The application is regularly tested for common vulnerabilities (such as CSRF, XSS, SQL Injection).

Security Awareness and Training

To help ensure that Cato Networks employees are aligned with the security practices and are aware of their duties,

Cato Networks has implemented an internal security awareness program, for all the Cato Networks employees, including conducting a quiz in order to measure the effectiveness of this program.

Software Development Lifecycle ("SDLC") and Change Management

Software development at Cato Networks is performed in a controlled manner, to help ensure applications are properly designed, tested, approved and aligned to the Cato Networks business objectives. Personnel responsible for the design, development, implementation and operation of systems affecting Security, Availability and Confidentiality related issues have the qualifications and resources to fulfill their responsibilities. The R&D team conducts regular sessions and training in order to keep the teams up to date with the latest technologies and techniques, while creating awareness of the latest threats and methods to mitigate them. Changes are documented and prioritized using tasks within the change management application. Changes are tagged within the change management application in order to identify changes that impact security, availability and confidentiality. The permission to merge tested versions into Master branch is restricted to authorized personnel. Administrative access to the source control application is restricted to authorized personnel.

Cato Networks Quality Assurance (QA) is constantly involved from early development stages. Based on the PRD, QA creates internal test plans. Test plans are reviewed by Product Managers and by R&D Team Leader responsible for the feature design. Cato Networks uses a set of automated testing in order to check the versions deployed to production. The tests include Unit, regression, and QA testing. Alerts are sent in case of test failure **(38).** A full QA cycle (Stabilization) includes regression and progression tests according to test plan documents. During this stage bugs are reported in the ticketing system. Manual tests are performed by the QA team. Each bug is assigned to an R&D Engineer for resolving with severity and a target version. Bugs that were targeted to the current version are fixed and verified as closed or are reopened.

Software Release: It is mandatory that all automation tests pass and that scans are free of Critical and High findings. Automation tests are performed using dedicated mechanisms on a regular basis in order to identify issues within the application. Cato Networks secured development process also includes an annual pen testing, whose findings are promptly fixed in following releases. Bugs or functional requests that are made by customers are reported in the ticketing system and marked with customer tag. Requests for functional enhancements are going to Product Managers backlog for future Releases.

Emergency Procedures

Emergency changes are performed and updated as part of hot fixes, which follow the same process as described above though the timeframe may be shortened, and approvals may be provided after the change was already performed.

The R&D Managers review the PRD and provide a high-level effort estimation for every feature. The product managers work with the R&D managers to create a prioritized features list based on the effort estimation and required timeline of the release.

R&D Engineers are engaged with ongoing enhancements of the product functionality. R&D engineers check-in their respective code to a common source control system that provides extensive version tracking functionality and other software building abilities. All changes which are added to the Source Control contain information linking them to the relevant features and bugs.

Monitoring

The management team is updated on an annual basis on security, confidentiality and availability non-compliance issues that may come up and address them as needed. Such issues are documented as part of a support process and if necessary, notifications are sent to relevant teams within Cato Networks. Change reports, vulnerability reports from

production and monitoring tools as well as support metrics are reviewed and discussed in relation to organization's system security, availability, and confidentiality policies. In addition, environmental, regulatory, and technological changes are monitored. Their effects are assessed, and their policies are updated accordingly. A summarized protocol is made available to relevant managers and team members.

Infrastructure Change Management Overview

Cato Networks regularly makes changes within its production environment in response to the evolving client and market needs. These changes include adding/removing/changing the configuration policies of existing servers or performing routine maintenance activities, software updates, and other infrastructure-related changes accordingly to available possibilities provides by the third-party vendors.

Support and Operations

Cato Networks' customer support procedures are designed to handle and resolve issues and requests in a timely manner. These includes issues that are internally identified, or issues submitted by clients. Support is available via support hotline and customer support portal. A support portal is available in order to guide the customer as to the correct use of the service. Support meetings with the management are performed regularly, in order to report major open issues to the management.

Escalation Process

Cato Networks' goal is to resolve issues in an efficient manner. The issue is tracked and updated in the ticketing system. Tickets are escalated as deemed necessary to the R&D or Security teams. Response time to customer's issues is defined within the Service Level Agreement. The agreement is communicated to the customers as part of the contract. Client issues are taken care according to the SLA. Moreover, service interruptions, maintenance and updates are communicated to customers through the account manager in the customer service software or Email. In addition, to maintain visibility on current support issues and potential problem trends, support metrics (including Key Performance Indicators) are generated from the support application and sent to Company's stakeholders on a regular basis.

Availability procedures

Cato Networks' production environment is fully managed as part of the AWS and other hosting providers and monitored by Cato Networks Operations team using various tools. The application level is fully managed by the Cato Networks. Admin access to the Cato Networks' application is restricted to authorized personnel. Cato Networks has implemented the operations management controls described below to manage and execute production operations.

Database backup and restoration

Cato Networks application database is fully backed up according to the backup policy. The logs are replicated every day. In case of failure, a notification is sent to the Operations team. The access to the backup and offline storage is restricted to authorized individuals. The backup data captured as part of backup procedure is restored automatically into a separate environment in order to determine the integrity of data and potential data recovery issues. A log of the restoring process is sent to management for review.

Disaster Recovery Plan (DRP)

Cato Networks has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of disaster. The DRP is tested on an annual basis. Cato Networks maintains a backup infrastructure at various locations within the hosting environments. The backup infrastructure has been designed to provide clients with business-critical services until the disaster has been resolved and the primary system is fully restored. The alternative processing environment is wholly managed by appropriate Cato Networks personnel, as is the case with the primary production environment.

Confidentiality Procedures

Customer confidentiality is key factor in Cato Networks. As such, Cato Networks has implemented security measures to ensure the confidentiality of its customer's sensitive personal information. The security measures aim to prevent unauthorized access, disclosure, alteration, or destruction of sensitive personal information. Customers' passwords and PII are encrypted within the application database according to the Cato Networks security policy and according to SSS algorithm (Shamir`s secret Sharing). Customers are restricted to their own web interface environment and do not have access to view data from other environments. The infrastructure third party providers sign confidentiality agreements with Cato Networks in order to maintain the system confidentiality conform to Cato Networks confidentiality policy. In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, impacted customers are notified as defined within their Service Level Agreements. Connections to the Cato Networks system are obtained through a secured tunnel, only accessible from within the production network. Traffic between Cato Networks' customers and the service, and connection to the production environments are encrypted using respectively HTTPS and SSH protocols.

****