CATO
NETWORKS

Cato Cloud
Internal Security

Introduction

Cato serves thousands of customers, globally connecting tens of thousands of sites and hundred of thousands of remote, ZTNA users on our Cato SASE Cloud service. Our customers trust us with their business network, and we are obligated to deliver a reliable and secure service.

At Cato, we follow the CIA (Confidentiality, Integrity and Availability) principle in our cloud service internal security, where each of those 3 pillars are a key and integral part of our design, implementation, and day-to-day operations.

We work with global top-tier providers (e.g. data centers, connectivity providers, hardware, etc.) and maintain the highest standards of vendor due diligence, contracting and auditing. Cato performs annual audits by independent 3rd parties to review and affirm our service security posture.

This document details what we do with regards to Confidentiality, Integrity, Availability as well as Privacy and 3rd Party Auditing.

Confidentiality

Encryption is our primary mean for maintaining data confidentiality. As data can be transferred (i.e. in motion) and stored (i.e. at rest), different encryption techniques are applied respectively. Cato uses the strongest industry-standard cipher suites for authentication, key exchange and encryption.

Data-in-Motion Encryption

Data transmissions to and from the Cato Cloud is always through encrypted tunnels: communication between our edge SD-WAN device (the Cato Socket) and our PoPs, between cloud data centers and our PoPs and between a remote user and our PoPs. Data transmissions within the Cato Cloud, where one PoP communicates with another is also encrypted.

Our NOC (Network Operation Center) and SOC (Security Operation Center) teams have all their control and monitoring channels encrypted.

Data-at-Rest Encryption

To provide our service, we are required to store account-specific data on our servers, so we can enforce policies, authenticate users, prioritize traffic, etc. We also store statistical information to provide our customer with network analytics. Regardless of the volume of data we store, all our customer's data is kept in encrypted storage.

Keys Management System

One of the greatest challenges in the encryption domain is keys management. To deliver a keys management solution that fulfills the CIA principle on its own, we have implemented a proprietary distributed KMS (Keys Management System) that is based on industry standard secret sharing algorithm. This algorithm is designed to ensure keys are never fully stored in a single place and can become usable only after meeting certain authentication conditions.

Multi-Tenancy

Cato's service is multi-tenant by design. This means that data separation and isolation are a native part of the software delivering the service. Every piece of data (e.g. network packet) that is processed, is marked in multiple ways to denote its' single customer context. Multi-tenancy is then achieved through multiple software layers, each with its own validation point, independently preventing cross-account data leakage, and all combined delivering a comprehensive data separation architecture.

Integrity

Access to Cato's network PoPs is secured in a way that reduces attack surface to minimize exposure to malicious attacks.

Physical Access Control

Cato's PoPs are collocated in top-tier data centers (e.g. Coresite, Interaxion, Equinix, etc.) ensuring carrier-grade availability and security in compliance with international standards such as SSAE16.

All access to Cato's infrastructure is strictly controlled (biometric measures, access-controlled steel cages) and monitored (24x7 video surveillance, manned patrols).

Logical Access Control

Cato uses its own perimeter security services to control access to the core Cloud network. Each access to the network is verified, controlled and monitored. Cato employees are blocked from the internal service network. Engineers and other personnel requiring specific access, get it on a case-by-case basis. If approved, employee access to the internal service network is established for a limited time, and over a secure SSH connection after going through multi-factor authentication.

Audit logs

All access and actions both on the Cato Management Application as well as on Cato's backend systems are logged in comprehensive audit trails, providing full visibility to both automated and human activities on the service.

Monitoring software is in place to identify unauthorized access control attempts, investigate them and respond.

Hardened Cato Socket OS

Our Sockets use a dedicated, custom built Linux OS that was stripped down to the required modules and services and is periodically updated by Cato along with the Socket software update. "Root" user is disabled and cannot be used for SSH access to the Socket, and a separate, less-privileged user is used for troubleshooting Socket issues.

The Socket's web-based control interface is accessible only through HTTPS and requires changing the default password upon first access. Password complexity is enforced.

PoP OS

Cato's PoP use Linux as the underlying operating system, and in addition to hardening based on industry best-practices, our operation teams make sure to always apply the latest security updates.

Tools are in place to install new security updates as they are released on test servers, verify that they do not damage the service, and then deploy them to our production network. Such a process can be executed in hours or days, depending on the security update criticality and relevance to our cloud service.

Availability

Environmental Conditions

All data centers hosting Cato's points of presence (PoPs) follow strict regulation and industry best practices regarding humidity and temperature control, fire detection and suppression, building resiliency to local seismic, storm and flood risks, and redundant power sources.

Cato's NOC continuously monitor electrical and mechanical parameters, so any deviations are immediately identified and addressed. Preventive maintenance is routinely performed without incurring downtimes.

Self-Healing Capabilities

Cato's engineering teams have developed purpose-built software to monitor the performance and load of our PoPs, our compute nodes inside each PoP, and our global connectivity providers. This software is capable of independently taking out of service any element that is not performing within the defined parameters, and hand it over to our operation teams for investigation, remedy and re-insertion to service.

When such an event occurs, the cloud is designed with multiple layers of redundancy, so that redundant elements take over and assure the service to our customer is not degraded.

Read about our service's self-healing architecture in more details.

Business Continuity

Cato maintains documented business continuity procedures which are practiced annually. These procedures assure that in cases of catastrophe that are beyond Cato's control (e.g. an entire data center is out with no known resumption timeframe), our operations team can re-built the damaged elements from scratch at minimal time. It should be noted that if such an event will occur, our cloud's self-healing capabilities will assure service continuity through peer elements.

Privacy

GDPR Compliant

Cato's service follows the 'privacy by design' principle and complies with all GDPR requirements. According to GDPR definitions, our customers (i.e. the enterprise subscribed to the service) are the "Data Controllers", and Cato is the "Data Processor". All GDPR requirements from a data processor in regard to PII (Personal Identifiable Information) are fully implemented by either software and/or procedures. GDPR compliance has been audited and approved by a 3rd party vendor.

For more detatils, read our Data Processing and Privacy Agreement ›

3rd Party Auditing

SOC2

Our Service is SOC2 approved since 2019 and is annually audited by a 3rd party to ensure procedures and practices are followed and never neglected.

A copy of our SOC1 and SOC2 reports are attached as an appendix , and our full SOC3 report is publicly available on our website.

ISO 27000

Our service and company are ISO 27001 compliant since 2016 and ISO 27017, 27018 and 27701 compliant since 2022. We are annually audited by a 3rd party to ensure procedures and practices are followed and never neglected.

A copy of our ISO 27000 certificates is attached as an appendix.

Cyber Essentials

Our service and company complies with the UK Cyber Essentials requirements set forth by the British National Cyber Security Center (NCSC).

A copy of our Cyber Essential certificate is attached as an appendix.

Penetration Testing

Multiple internal penetration tests are performed by Cato's dedicated application security team according to an annual plan.

Annual penetration testing is performed by a 3rd party vendor to all key elements of our service.

Result are reviewed by our CISO and relevant engineers, and corrective actions are taken if and when needed.

Appendix: SOC1

Section I - Cato Networks Ltd.’s Management Assertion

January 11 , 2024

We have prepared the description of Cato Networks Ltd.s Cato Networks Platform system entitled, “Cato Networks Ltd.’s Description of Its Cato Networks Platform System for the period November 1, 2022 to October 31, 2023” (Description) for processing user entities’ transactions throughout the period November 1, 2022 to October 31, 2023 for user entities of the system during some or all of the period November 1, 2022 to October 31, 2023, and their auditors who audit and report on such user entities’ financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities’ financial statements.

Carved-out Unaffiliated Subservice Organization: Cato Networks Ltd. uses a set of hosting providers (subservice organization) to provide Infrastructure Management Services. Below is the list of infrastructure subservice organization used by Cato Networks Ltd:

- AWS - Globally.
- Equinix -Ashburn, Chicago, Dallas, Seattle, Miami, New York, Amsterdam, Perth, Sao Paulo, Paris, Zurich, Milan, Melbourne, Osaka
- Coresite - Los Angels, Denver, Santa Clara
- Interxion - Germany, England, Sweden
- Century Link / L3 - Chile, Peru
- Digital Realty - Atlanta, Charlotte, Portland
- DataHive - Calgary
- Cologix – Toronto, Minneapolis
- Switch - Las Vegas
- KIO Networks - Mexico
- MED 1 - Israel
- NXDATA - Romania
- China Telecom - Beijing, Shanghai, Shenzhen
- Cloud Times Information Technology -C Beijing, Shanghai
- Mega I - Hong Kong
- TIME - Malaysia
- ST Telemedia - India
- Datamena - UAE
- TCC Technology - Thailand
- PLDT - Philippines
- Chief Telecom - Taiwan
- 123Net - Detroit
- CyrusOne – Houston, Cincinnati
- Markley - Boston
- Teraco - South Africa
- VNTT - Vietnam
- kinx - South Korea
- INWI – Morocco
- CE Colo Czech – Prague
- DC220 – Auckland NZ

The Description includes only the control objectives and related controls of Cato Networks Ltd. and excludes the control objectives and related controls of the subservice organization. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The Description does not extend to controls of the carved-out subservice organization.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Cato Networks Ltd.'s controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

a. The Description fairly presents the *Cato Networks Platform* system (System) made available to user entities of the System during some or all of the period November 1, 2022, to October 31, 2023 for processing their transactions as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:

(1) Presents how the System made available to user entities of the system was designed and implemented to process relevant transactions, including, if applicable:

- The types of services provided, including, as appropriate, the classes of transactions processed.

- The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the System.

- The information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports prepared for user entities.

- How the System captures and addresses significant events and conditions, other than transactions.

- The process used to prepare reports and other information for user entities.

- Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

- The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.

- Other aspects of our control environment, risk assessment process, information and communication (including the related business processes), control activities, and monitoring activities that are relevant to the services provided, including processing and reporting transactions of user entities.

(2) Includes relevant details of changes to the System during the period covered by the Description.

(3) Does not omit or distort information relevant to the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors, and may not, therefore, include every aspect of the Cato Networks Platform System that each individual user entity of the System and its user auditor may consider important in the user entity's own particular environment.

b. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period November 1, 2022 to October 31, 2023 to achieve those control objectives, if subservice organizations applied the complementary subservice organization controls and user entities applied the complementary user entity controls assumed in the design of Cato Networks Ltd.'s controls throughout the period November 1, 2022 to October 31, 2023. The criteria we used in making this assertion were that.

(1) The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the service organization.

(2) The controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

(3) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

[**Signature**]
Title

Amit Spitzer
CSO
Cato Networks

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

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

Section II – Independent Service Auditor

The Board of Directors
Cato Networks Ltd.

Scope
We have examined Cato Networks Ltd.'s description entitled "Description of the Cato Networks Platform relevant for the Period November 1, 2022 to October 31, 2023." (Description) throughout the period November 1, 2022 to October 31, 2023 of its Cato Networks Platform system (System) for processing user entities' transactions and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in Cato Networks Ltd. assertion (Assertion). The Control Objectives and controls included in the Description are those that management of Cato Networks Ltd. believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of Cato Networks Ltd.'s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Cato Networks Ltd. uses a set of hosting providers (subservice organization) to provide Infrastructure Management Services. Below is the list of infrastructure subservice organization used by Cato Networks Ltd:

- AWS - Globally.
- Equinix -Ashburn, Chicago, Dallas, Seattle, Miami, New York, Amsterdam, Perth, Sao Paulo, Paris, Zurich, Milan, Melbourne, Osaka
- Coresite - Los Angels, Denver, Santa Clara
- Interxion - Germany, England, Sweden
- Century Link / L3 - Chile, Peru
- Digital Realty - Atlanta, Charlotte, Portland
- DataHive - Calgary
- Cologix – Toronto, Minneapolis
- Switch - Las Vegas
- KIO Networks - Mexico
- MED 1 - Israel
- NXDATA - Romania
- China Telecom - Beijing, Shanghai, Shenzhen
- Cloud Times Information Technology -C Beijing, Shanghai
- Mega I - Hong Kong
- TIME - Malaysia
- ST Telemedia - India
- Datamena - UAE
- TCC Technology - Thailand
- PLDT - Philippines
- Chief Telecom - Taiwan
- 123Net - Detroit
- CyrusOne – Houston, Cincinnati
- Markley - Boston
- Teraco - South Africa
- VNTT - Vietnam

- kinx - South Korea
- INWI – Morocco
- CE Colo Czech – Prague
- DC220 – Auckland NZ

The Description includes only the Control Objectives and related controls of Cato Networks Ltd. and excludes the control objectives and related controls of Amazon Web Service ("AWS"). The description also indicates that certain Control Objectives specified by Cato Networks Ltd. can be achieved only if complementary subservice organization controls assumed in the design of Cato Networks Ltd.'s controls are suitably designed and operating effectively, along with the related controls at Cato Networks Ltd. Our examination did not extend to such complementary controls of Amazon Web Service ("AWS"), and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Cato Networks Ltd.'s responsibilities

Cato Networks Ltd. has provided the accompanying assertion titled, Cato Networks Ltd. management assertion (Assertion) about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives. Cato Networks Ltd. is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the Control Objectives and stating them in the Description, identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related Control Objectives.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). Our examination was also performed in accordance with International Standard on Assurance Engagements 3402, Assurance Reports on Controls at a Service Organization, 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, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period November 1, 2022 to October 31, 2023. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related Control Objectives, based on the criteria in management's Assertion.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related Control Objectives.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved.
- Evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the Assertion.

We are required to be independent of Cato Networks Ltd. and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related Control Objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying Section IV - Cato Networks Ltd.'s Control Objectives, controls and service auditor's tests of controls and results of tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the criteria described in Cato Networks Ltd.'s Assertion:

a. The Description fairly presents the System that was designed and implemented throughout the period November 1, 2022 to October 31, 2023.
b. The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period November 1, 2022 to October 31, 2023 and if subservice organizations and user entities applied the complementary controls assumed in the design of Cato Networks Ltd.'s controls throughout the period November 1, 2022 to October 31, 2023.
c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period November 1, 2022 to October 31, 2023 if complementary subservice organization and user entity controls assumed in the design of Cato Networks Ltd.'s controls operated effectively throughout the period November 1, 2022 to October 31, 2023.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of Cato Networks Ltd., user entities of Cato Networks Ltd.'s System during some or all of the period November 1, 2022 to October 31, 2023, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Kost Forer Gabbay & Kasierer

A member of Ernst and Young Global Limited
January 11, 2024
Tel-Aviv Israel

Appendix: SOC2

Section I - Cato Networks Ltd.’s Management Assertion

January 11, 2024

We have prepared the accompanying **“**Description of the Cato Networks Platform relevant to Security, Availability and Confidentiality throughout the period November 1, 2022 to October 31, 2023**”** (Description) of Cato Networks Ltd. (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the Cato Networks Platform (System) that may be useful when assessing the risks arising from interactions with the System , particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria*.

Cato Networks Ltd. uses a set of hosting providers (subservice organization) to provide Infrastructure Management Services. Below is the list of infrastructure subservice organization used by Cato Networks Ltd:

- AWS - Globally.
- Equinix -Ashburn, Chicago, Dallas, Seattle, Miami, New York, Amsterdam, Perth, Sao Paulo, Paris, Zurich, Milan, Melbourne, Osaka
- Coresite - Los Angels, Denver, Santa Clara
- Interxion - Germany, England, Sweden
- Century Link / L3 - Chile, Peru
- Digital Realty - Atlanta, Charlotte, Portland
- DataHive - Calgary
- Cologix – Toronto, Minneapolis
- Switch - Las Vegas
- KIO Networks - Mexico
- MED 1 - Israel
- NXDATA - Romania
- China Telecom - Beijing, Shanghai, Shenzhen
- Cloud Times Information Technology -C Beijing, Shanghai
- Mega I - Hong Kong
- TIME - Malaysia
- ST Telemedia - India
- Datamena - UAE
- TCC Technology - Thailand
- PLDT - Philippines
- Chief Telecom - Taiwan
- 123Net - Detroit
- CyrusOne – Houston, Cincinnati
- Markley - Boston
- Teraco - South Africa
- VNTT - Vietnam
- kinx - South Korea
- INWI – Morocco
- CE Colo Czech – Prague
- DC220 – Auckland NZ

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Cato Networks Ltd.'s controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

We confirm, to the best of our knowledge and belief, that:

a. The Description presents the System that was designed and implemented throughout the period November 1, 2022 to October 31, 2023 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Cato Networks Ltd. service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively and if the carved-out subservice organization applied the controls assumed in the design of Cato Networks Ltd.'s controls throughout that period.

c. The Cato Networks Ltd. controls stated in the Description operated effectively throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Cato Networks Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if the carved-out subservice organization applied the controls assumed in the design of Cato Networks Ltd.'s controls throughout that period.

[**Signature**] Amit Spitzer
Title CSO
Cato Networks

Kost Forer Gabbay & Kasierer
144 Menachem Begin Road, Building A
Tel-Aviv 6492102, Israel

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

Section II – Independent Service Auditor

To the Management of Cato Networks Ltd.

Scope

We have examined Cato Networks Ltd.'s accompanying **"**Description of the Cato Networks Platform relevant to Security, Availability and Confidentiality throughout the period November 1, 2022 to October 31, 2023**"** (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022) (Description Criteria) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that the 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), in AICPA Trust Services Criteria.

Cato Networks Ltd. uses a set of hosting providers (subservice organization) to provide Infrastructure Management Services. Below is the list of infrastructure subservice organization used by Cato Networks Ltd:

- AWS - Globally.
- Equinix -Ashburn, Chicago, Dallas, Seattle, Miami, New York, Amsterdam,
Perth, Sao Paulo, Paris, Zurich, Milan, Melbourne, Osaka, Munich, Manchester, Madrid, Dublin, Brussels., Sydney
- Coresite - Los Angels, Denver, Santa Clara
- Interxion - Frankfurt, London, Sweden
- Century Link / L3 - Chile, Peru
- Digital Realty - Atlanta, Charlotte, Portland
- DataHive - Calgary
- Cologix – Toronto, Minneapolis
- Switch - Las Vegas
- KIO Networks - Mexico
- MED 1 - Israel
- NXDATA - Romania
- China Telecom - Beijing, Shanghai, Shenzhen
- Cloud Times Information Technology -C Beijing, Shanghai
- Mega I - Hong Kong
- TIME - Malaysia
- ST Telemedia - India
- Datamena - UAE
- TCC Technology - Thailand
- PLDT - Philippines
- Chief Telecom - Taiwan
- 123Net - Detroit
- CyrusOne – Houston, Cincinnati
- Markley - Boston
- Teraco - South Africa
- VNTT - Vietnam
- kinx - South Korea
- INWI – Morocco
- CE Colo Czech – Prague
- DC220 – Auckland NZ

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Cato Networks Ltd.'s controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

Cato Networks Ltd.'s responsibilities

Cato Networks Ltd. 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 its service commitments and system requirements were achieved. Cato Networks Ltd. has provided the accompanying assertion titled, Management Assertion of Cato Networks Ltd. (Assertion) about the presentation of the Description based on the Description Criteria and the suitability of design and operating effectiveness of controls stated therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Cato Networks Ltd. is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) selecting the trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the Description; (5) identifying the risks that threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of design and operating effectiveness of controls stated therein to achieve the Service Organization's service commitments and system requirements based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period November 1, 2022 to October 31, 2023. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- obtaining an understanding of the system and the service organization's service commitments and system requirements
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed or operating effectively based on the applicable trust services criteria.
- performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

- testing the operating effectiveness of those controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent of Cato Networks Ltd. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

We apply International Standard on Quality Control I and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in the accompanying Description of Criteria, Controls, Tests, and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

a. the Description presents the Cato Networks Platform system that was designed and implemented throughout the period November 1, 2022 to October 31, 2023 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Cato Networks Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Cato Networks Ltd.'s controls throughout that period.

c. the controls stated in the Description operated effectively throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Cato Networks Ltd. service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and user entity controls assumed in the design of Cato Networks Ltd.'s controls operated effectively throughout that period.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Cato Networks Ltd., user entities of Cato Networks Ltd.'s system during some or all of the period November 1, 2022 to October 31, 2023 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties.
- Internal control and its limitations
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Kost Forer Gabbay and Kasierer

Kost Forer Gabbay and Kasierer

A member firm of Ernst & Young Global

January 11, 2024
Tel-Aviv, Israel

Appendix: ISO 27000

IQC
Institute of Quality & Control

CERTIFICATE

NO. I18600

This is to certify that
the Information Security Management System of

Cato Networks Ltd

121 Menhem Begin St. Tel Aviv, Israel

Was audited by IQC and found to be
in compliance with the requirements of the standard:

ISO/ IEC 27001: 2013

This certificate is valid for
the following scope of activities:

Secure and optimized management of Cloud-based enterprise network

According to statement of applicability Date: 02.05.2022 Version: 1

This certificate is valid until:	25.06.2025
Certification cycle will end on:	25.06.2025
Date of first approval:	25.06.2016

This certificate is subject to the continuing satisfactory operation
of the Management System and periodic auditing by IQC

IQC

26.06.2022
Issue date

Nir Halpern, CEO

Institute of Quality & Control Ltd.
6 Ravnitzky St., Petah Tikva 4900617, Israel
Tel: 03-9313555, Fax: 03-9044406
E-Mail. info@iqc.co.il, www.iqc.co.il

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
MGMT. SYS.
RvA C 560

IQC
Institute of Quality & Control

CERTIFICATE

NO. I25515

This is to certify that
the Information Security Management System- Cloud Security of

Cato Networks Ltd

121 Menhem Begin St. Tel Aviv, Israel

Was audited by IQC and found to be
in compliance with the requirements of the standard:

ISO/IEC 27001: 2013 – ISO/IEC 27017:2015

This certificate is valid for
the following scope of activities:

Secure and optimized management of Cloud-based enterprise network

According to statement of applicability Date: 02.05.2022 Version: 1

This certificate is valid until:	25.06.2025
Certification cycle will end on:	25.06.2025
Date of first approval:	31.07.2022

This certificate is subject to the continuing satisfactory operation
of the Management System and periodic auditing by IQC

02.08.2022
Issue date

Nir Halpern, CEO

Institute of Quality & Control Ltd.
6 Ravnitzky St., Petah Tikva 4900617, Israel
Tel: 03-9313555, Fax: 03-9044406
E-Mail. info@iqc.co.il, www.iqc.co.il

IQC
Institute of Quality & Control

CERTIFICATE

NO. I25516

This is to certify that
the Information Security Management System-
Personally Indentifiable Information in Public Cloud of

Cato Networks Ltd

121 Menhem Begin St. Tel Aviv, Israel

Was audited by IQC and found to be
in compliance with the requirements of the standard:

ISO/IEC 27001:2013 – ISO/IEC 27018:2019

This certificate is valid for
the following scope of activities:

Secure and optimized management of Cloud-based enterprise network

According to statement of applicability Date: 02.05.2022 Version: 1

This certificate is valid until:	25.06.2025
Certification cycle will end on:	25.06.2025
Date of first approval:	31.07.2022

This certificate is subject to the continuing satisfactory operation
of the Management System and periodic auditing by IQC

02.08.2022
Issue date

Nir Halpern, CEO

Institute of Quality & Control Ltd.
6 Ravnitzky St., Petah Tikva 4900617, Israel
Tel: 03-9313555, Fax: 03-9044406
E-Mail. info@iqc.co.il, www.iqc.co.il

IQC
Institute of Quality & Control

CERTIFICATE

NO. I25517

This is to certify that
the Privacy Information Management System of

Cato Networks Ltd

121 Menhem Begin St. Tel Aviv, Israel

Was audited by IQC and found to be
in compliance with the requirements of the standard:

ISO/IEC 27001: 2013 – ISO/IEC 27701:2019

This certificate is valid for
the following scope of activities:

Secure and optimized management of Cloud-based enterprise network

According to statement of applicability Date: 02.05.2022 Version: 1

This certificate is valid until:	25.06.2025
Certification cycle will end on:	25.06.2025
Date of first approval:	31.07.2022

This certificate is subject to the continuing satisfactory operation
of the Management System and periodic auditing by IQC

02.08.2022
Issue date

Nir Halpern, CEO

Institute of Quality & Control Ltd.
6 Ravnitzky St., Petah Tikva 4900617, Israel
Tel: 03-9313555, Fax: 03-9044406
E-Mail. info@iqc.co.il, www.iqc.co.il

UK Cyber Essentials

CYBER ESSENTIALS

CERTIFICATE OF ASSURANCE

Cato Networks

Menachem Begin 121 Tel-Aviv 6701203

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS SCHEME

NAME OF ASSESSOR : Thomas West

CERTIFICATE NUMBER : d1e92e4f-e71c-4ae0-8cab-af24b3d39e5a

DATE OF CERTIFICATION : 2022-11-14

PROFILE VERSION : 3

RECERTIFICATION DUE : 2023-11-14

SCOPE : Whole Organisation

SCAN THIS QR CODE TO VERIFY THE AUTHENTICITY OF THIS CERTIFICATE

CERTIFICATION MARK

CYBER ESSENTIALS CERTIFIED

CERTIFICATION BODY

CYBER ESSENTIALS PARTNER

IASME CONSORTIUM

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials implementation profile and thus that, at the time of testing, the organisation's ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against a cyber attack.