



CLAROTY LTD.

SOC 3 REPORT

FOR THE

XDOME PLATFORM AND XDOME SECURE ACCESS (XSA) PLATFORM

FOR THE PERIOD OF SEPTEMBER 1, 2025, TO JUNE 30, 2026

Attestation and Compliance Services



INDEPENDENT SERVICE AUDITOR'S REPORT

To Claroty Ltd.:

Scope

We have examined Claroty Ltd.'s ("Claroty") accompanying assertion titled "Assertion of Claroty Ltd. Service Organization Management" ("assertion") that the controls within Claroty's xDome Platform and XSA Platform system ("system") were effective throughout the period September 1, 2025, to June 30, 2026, to provide reasonable assurance that Claroty'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Claroty uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Claroty, to achieve Claroty's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Claroty 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 Claroty's service commitments and system requirements were achieved. Claroty has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Claroty is responsible for selecting, and identifying in its assertion, the applicable trust services 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 (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 (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 the following:

- 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 Claroty'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 Claroty'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.

Service Auditor's Independence and Quality Management

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement, including the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statement on Quality Management Standards established by the AICPA and the International Standard on Quality Management established by the IAASB and, accordingly, maintain a comprehensive system of quality management including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

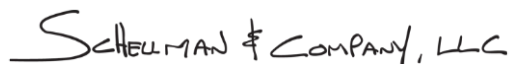
Inherent Limitations

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 Claroty's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, 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 Claroty's xDome Platform and XSA Platform system were effective throughout the period September 1, 2025, to June 30, 2026, to provide reasonable assurance that Claroty's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Handwritten signature of Schellman & Company, LLC in black ink.

Columbus, Ohio
September 1, 2026

ASSERTION OF CLAROTY SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Claroty Ltd.'s ("Claroty") xDome Platform and XSA Platform system ("system") throughout the period September 1, 2025, to June 30, 2026, to provide reasonable assurance that Claroty's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2025, to June 30, 2026, to provide reasonable assurance that Claroty'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Claroty'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 below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period September 1, 2025, to June 30, 2026, to provide reasonable assurance that Claroty's service commitments and system requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE xDOME PLATFORM AND XSA PLATFORM SYSTEM

Company Background

Claroty is a global cybersecurity company specializing in the protection of cyber-physical systems (CPS) and the Extended Internet of Things (XIoT) across industrial, healthcare, commercial, and critical infrastructure sectors. The company provides a platform and services designed to address the unique security challenges inherent in these environments. Claroty was founded in 2015 and is headquartered in New York, USA supported by an additional corporate office facility in Tel Aviv, Israel and serves customers worldwide.

Description of Services Provided

xDome Platform

xDome is a modular, SaaS-based industrial cybersecurity platform that provides a unified solution for CPS security without disrupting critical operations. The platform's architecture relies on data collected from the customer's environment via Claroty-provided collectors, which are on-premise physical or virtual servers, which transmit metadata to the Claroty cloud for analysis, correlation, and management.

The platform's core capabilities include:

- **Asset Discovery and Visibility:** Provides a foundational layer of security by creating a detailed and continuously updated inventory of connected assets. This inventory includes critical attributes such as device type, vendor, model, firmware version, and communication patterns.
- **Exposure Management:** Building on the asset inventory, the platform delivers continuous risk assessment. It identifies known vulnerabilities (CVEs), insecure configurations, and missing patches, then prioritizes them based on asset criticality and exploitability to provide clear and actionable remediation guidance. This also evaluates the environment to find risky or exposed devices and provides recommendations on how to remediate these devices.
- **Network Security Management:** Facilitates effective network segmentation by providing a visual map of network communications. This allows organizations to understand, model, and verify segmentation policies, thereby helping to limit the potential for lateral movement of threats across the network. This also integrates with existing networking tools such as NACs and firewalls to both recommend and implement segmentation policies.
- **Anomaly and Threat Detection:** Employs a detection engine for active defense. It uses a combination of signature-based detection for known threats, proprietary-threat intelligence from Claroty's research team, and behavioral analysis to alert on anomalous activities that may indicate a sophisticated or previously unknown attack.

xDome Secure Access (XSA) Platform

XSA is a secure remote access solution for internal staff and authorized third parties connecting to OT assets. The service provides controlled, time-bound, and policy-driven access over supported protocols without requiring agents on target systems. Access requests are authenticated and authorized via integrated identity providers, and sessions can be monitored in real-time, recorded in full, and logged for audit purposes. XSA also enforces file transfer restrictions and integrates with security monitoring tools.

The platform's core capabilities include:

- **Granular Access Control:** Enables organizations to enforce highly specific, policy-based controls for connection. Policies dictate precisely which users or groups can access which assets, for how long, from which locations, and using specific protocols.

- **Just-in-Time (JIT) Access:** Access is granted on a temporary, "just-in-time" basis. Permissions are provisioned for a limited session and automatically expire, significantly reducing the attack surface associated with standing privileges.
- **Full Session Auditability:** Remote user sessions are fully monitored and recorded. This provides a searchable, video-based audit trail of user actions, which is critical for compliance, forensic investigations, and incident response.
- **Credential Management:** The solution includes a secure vault to manage and rotate credentials for target systems. This abstracts passwords from the end-user, preventing credential exposure and simplifying management.
- **Secure File Transfer:** The solution allows customers to manage files that need to be uploaded to or downloaded from remote systems, including role-based access controls on who can manage what files, and automated virus scanning of files before they are introduced to remote systems.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Claroty designs its processes and procedures to meet its objectives for the xDome Platform and XSA Platform. Those objectives are based on the service commitments that Claroty makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that Claroty has established for the services. The xDome Platform and XSA Platform services of Claroty are subject to the relevant regulatory and industry information and data security requirements in which Claroty operates.

Claroty is committed to providing user entities with a secure platform that protects customer data that is stored and processed within the service. Those commitments and the associated system requirements are documented and communicated in customer agreements and the service level agreements (SLA), as well as on the company website and Claroty Support Center.

The principal service commitments are standardized and include:

Security

- System access is granted to authorized personnel based on logical access and employee provisioning and deprovisioning standards.
- Formal encryption standards are utilized for protection of data at rest and in transit.
- The use of secure cloud environments in accordance with configuration management and change management standards.
- Regular security assessments and system updates based on risk and vulnerability standards, such as perimeter access controls and intrusion detection and prevention standards.
- An incident response plan, including the identification and remediation of security incidents/events.

Availability

- Continuous monitoring of the platform for system availability, performance indicators, and operational health.
- Hosting production platform services in several availability zones to maintain high availability standards.
- Maintaining a disaster recovery program that is tested on an annual basis.

Confidentiality

- Restriction of access to customer data through role-based access controls and logical isolation to help ensure information is accessible only to authorized personnel.
- Disposal of confidential customer data upon termination of the services.

Such requirements are communicated in Claroty's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around 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, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the xDome Platform and XSA Platform.

In accordance with Claroty's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

The production infrastructure supporting the xDome Platform and XSA Platform systems is hosted within Amazon Web Services, Inc. (AWS). Additionally, Claroty utilizes an identity and access management (IAM) system and VPN.

People

Personnel involved in the operation and use of the system are:

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- Administration - responsible for overseeing HR and Office administration.
- R&D - responsible for software development and quality assurance activities. R&D creates the software packages required to implement Claroty's products and services. The R&D department includes backend and frontend software development, DevOps and Integration, Research, QA and Visibility.
- Product - responsible for defining Claroty's product requirements and priorities. It includes, among others, analyzing market needs and incorporating client feedback into the product roadmaps. The Product department is in charge of product management, product analysis and user interface / user experience.
- Data - responsible for network research and analysis activities required for the development and operation of Claroty's products.
- Sales - responsible for direct sales activities, sales channel operations, inside sales, and lead generation.
- Marketing - responsible for building the company's brand, generating sales opportunities and other marketing activities.
- System Engineering - responsible for technical client-facing activities required for pre-sales and deployment projects.
- Finance - responsible for the company's financial, and control activities including financial planning and reporting.

- Legal - responsible for helping to ensure Claroty's global compliance with applicable laws and regulations. This team provides legal counsel on corporate matters, from commercial contracts to intellectual property.
- IT & Security - responsible for safeguarding Claroty's information assets and infrastructure. This team focuses on implementing and maintaining security controls to protect company data, help ensure confidentiality, and support regulatory compliance for internal systems. They also manage disaster recovery planning to help ensure the continuity of Claroty's operations.

Procedures

Management has implemented an information security program to govern information security standards consisting of a set of policies and SOPs supporting operation of the system that define how information is managed and protected. Claroty has implemented automated and manual processes, including those relating to product management, engineering, technical operations, security, IT, and HR. These procedures are designed to align with Claroty's information security policy and are reviewed at least annually, or as necessary based on business-related changes.

HR and Training

Job descriptions are documented and utilized to outline the required skills needed and the employee responsibilities for the job. As part of the hiring process, employment candidates are interviewed for the required skillset of the job position the employment candidate is applying for, and employment candidates must go through a screening process prior to being hired.

Upon hire, employees are required to sign an acknowledgment of the receipt and understanding of the employee handbook and information security policies as well as agreeing to follow Claroty's policies and procedures. Additionally, an employee remedial procedure is documented within the employee handbook and information security policies that outlines that employees may be disciplined up to termination for non-compliance with Claroty's policies and procedures. Access to company systems is granted only with appropriate authorization, based on job responsibilities and in accordance with the principles of least privilege and need-to-know.

Employees are required to complete security awareness training upon hire and on an annual basis thereafter to understand their responsibilities for security and complying with Claroty's security policies and procedures. Employees also go through a feedback process to evaluate performance against expected levels of performance and conduct.

Access, Authentication, and Authorization

Claroty builds its production environment system architecture using the AWS cloud environment. The global management of Claroty infrastructure is performed by Claroty. Users first access the systems using their IAM credentials and multifactor authentication (MFA). Access to the production environment is through SSO using IAM credentials. Administrative and privileged access to the in-scope systems is restricted to system and user accounts accessible by authorized personnel.

Support administrative access to the AWS services is performed via an encrypted tunnel, requires MFA and is restricted only to relevant users. Employees are provided with the minimal access rights required to carry out their duties. Access to the production environment is limited and segregated.

Claroty's internal networks are protected using commercial firewalls configured and administered by IT. Claroty's production environment is protected by layered security tools and mechanisms configured by Claroty and complimentary to the AWS environment. Remote users are connected to a secure VPN tunnel and automatically disconnected from the production instances after a pre-defined period of inactivity and need to login again to re-establish connection to the network. Access to clients' databases is managed through IAM permissions and it is restricted to authorized groups or personnel.

Access Requests and Access Revocation

New employees are granted access to the different environments by a ticketing system process and subject to manager approval. New users gain initial access to Claroty's internal systems upon a notification of recruitment from the HR department to the IT department and their direct manager. A set of (requested by HR and approved

by direct manager) access privileges will be granted by the IT team. Access to a customer's production environment is strictly limited to authorized personnel, logged, documented, monitored and is conducted in accordance with pre-defined roles and the principle of least privilege.

Leaving employees who had access to the production environment have their permissions removed in a timely manner. Terminated employees' access privileges are revoked during the termination process. Additionally, the termination process includes user disablement, as well as the return of company property, data, and equipment.

System Security, Encryption, and Antivirus

Security groups are configured with access control rules to restrict inbound and outbound traffic. The connection to the production environments is performed through an encrypted tunnel based on an authenticated transport layer security (TLS) connection. Antivirus software is installed on workstations and laptops and laptops are also encrypted.

System Monitoring

Claroty uses a suite of monitoring tools to monitor its production environment for system availability, performance indicators, and operational health. Alerts are sent to relevant stakeholders based on pre-defined rules. The notifications are reviewed and processed through remediation. Actions performed on the production environment, are monitored and logged using a centralized security information and event management (SIEM) platform. Alerts are sent to relevant stakeholders based on pre-defined rules. The notifications are reviewed and processed through remediation.

Vulnerability scans are performed on an ongoing basis to detect potential product issues. Tickets are created to track the issues found. Claroty performs these scans across code, network, and infrastructure layers, and any potential issues are addressed in accordance with defined processes. An external penetration test is performed on an annual basis. High severity issues are investigated and resolved. The penetration test is conducted in order to identify vulnerabilities and attack vectors that can be used to exploit Claroty's system. The penetration tests include, among others, checks verifying that customers, groups of individuals, or other entities are prevented from accessing confidential information other than their own.

Incident Response

Claroty has a documented security incident response management policy that details procedures related to internal or customer reported incidents or issues. Incident forms are utilized to document security violations, responses, and resolution. Root cause analysis is performed following security incidents. Incidents are sent to relevant personnel and classified according to the level of urgency and importance. Resources are allocated in order to investigate the incident and resolve the issue.

Claroty's customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified, or issues submitted by clients. Claroty offers many support channels for its clients, allowing them to submit issues or request assistance directly via the Claroty Support Center, email, or a channel-based messaging platform. Upon submission or when an issue is proactively identified, Claroty creates a support ticket using a dedicated tracking system. This system is used to effectively manage, classify, and track client support-related issues. Tickets are prioritized based on their urgency and importance and are documented, resolved, and closed within Claroty's customer relationship management (CRM) application.

Change Management

The secure software development lifecycle (SDLC) follows the Open Worldwide Application Security Project (OWASP) best practice strategy. Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team as part of the sprint meeting that occurs weekly. Infrastructure Changes follow the same process as the code changes. Product requirements are collected from customers and from market research by Claroty product managers. These requirements combined with additional engineering improvement requirements are discussed by R&D managers and product managers and are converted to product requirements that contain more specific description of required features and changes. Changes are documented and prioritized using tasks within the ticketing system. Actions performed on the production environment are monitored and logged. The product managers work with the R&D managers to create a prioritized feature list based on effort estimation and required timeline of the release.

Claroty maintains documented change management and secure software development lifecycle processes for software and infrastructure changes. Changes are documented and tracked, tested, reviewed, and approved prior to production deployment. Access to develop, approve, and deploy changes is restricted to authorized personnel, and identified defects are tracked through resolution. Emergency changes follow defined procedures for expedited authorization, testing, documentation, and post-implementation review.

Data Backup and Disaster Recovery

Claroty has developed disaster recovery policies and procedures in order to continue to provide critical services in the event of disaster. The disaster recovery plan (DRP) is tested on annual basis. The Claroty production environment is also located in several availability zones to maintain high availability standards.

Claroty's databases are backed up in accordance with the defined backup policy. The automated backup system alerts engineering personnel upon the detection of a backup failure.

A restore process is performed and documented on an annual basis. The restore test includes a full restore to a separate database server and bringing up the database to verify data integrity and accessibility.

Vendor Management

To address risks associated with vendors, management maintains vendor security risk assessment procedures which provide guidelines for managing risk during vendor onboarding assessments and reassessments. Per the procedure, vendors are generally asked to complete vendor questionnaires during the vendor screening process to assess the vendor's security posture, unless Claroty obtained enough information about the vendor to conduct an assessment without the questionnaire.

Vendor contracts are in place to communicate security commitments between the vendor and Claroty. Monitoring procedures over existing vendors are performed as a part of ongoing day-to-day operations, as well as formally, to help ensure compliance by vendors and business partners with Claroty's expectations. The formal evaluation includes completing vendor risk assessments and reviews on at least an annual basis for critical vendors.

Claroty assesses on an annual basis, the risks that vendors and business partners represent to the achievement of their objectives. Claroty performs an information security review of critical vendors and subservice organizations on an annual basis. Results of the review and information security approval are documented within the vendor management system.

Data

Claroty has implemented controls around the identification and maintenance of confidential information to meet its objectives related to confidentiality. Confidential information is stored within encrypted databases. Access to confidential information is restricted to user accounts accessible by authorized personnel.

Claroty stores personal data including cookies, analytic tools and log files, IP addresses, and browser and device information to analyze, support and improve the website, contact and communicate with customers, enable access and use of the website, associated applications, and platforms, create aggregate/anonymous use pattern reports, provide fraud prevention and security of Claroty websites, and to conduct audits and maintain security for access control/authentication.

Claroty has also implemented controls around the destruction of confidential information to meet its objectives related to confidentiality. Customer data is encrypted at rest and in transit. Customers are responsible for taking measures to protect user identifications and passwords. Data is retained for as long as necessary to provide the services and as required by applicable laws, unless requested for deletion by the data subject. When data is no longer deemed necessary, it's securely deleted or destroyed.

Subservice Organizations

The cloud hosting services provided by AWS were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at Claroty, and the types of controls expected to be implemented at AWS to meet those criteria.

Control Activities Expected to be Implemented at Subservice Organization	Applicable Trust Services Criteria
AWS is expected to implement control activities for managing and monitoring logical access to the underlying network and virtualization management software for its cloud hosting services where in-scope systems reside.	CC6.1, CC6.2, CC6.3, CC6.5
AWS is expected to implement control activities for restricting physical access to facilities, offline storage and backup media, and other system components such as firewalls, routers, and servers for its cloud hosting services where in-scope systems reside.	CC6.4, CC6.5
AWS is expected to implement control activities for ensuring the data center facility is equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Complementary User Entity Controls

Claroty's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

User Entity Responsibilities

In order for user entities to benefit from the xDome Platform and XSA Platform system and its controls, the following responsibilities should be considered by user entities:

Ref.	Control Activities Expected to be Implemented at User Entities
UER-01	Customers are responsible for reviewing alerts, logs, and audit records provided by the platform, investigating anomalies, and responding in accordance with their security policies and procedures.
UER-02	Customers are responsible for integrating the platform with their organizational Identity Provider (IdP) for SSO, or using the application's native authentication method, while ensuring strong authentication is enforced through password policies and MFA in accordance with security best practices. Additionally, customers are strongly recommended to enable Just-In-Time (JIT) provisioning via the IdP, allowing user roles and permissions to be inherited directly without manual configuration in the system.
UER-03	Customers are responsible for provisioning and deprovisioning user accounts in a timely manner, including removal of access for terminated users.
UER-04	Customers are responsible for assigning roles and permissions according to business needs, implementing Role-Based Access Control (RBAC) in line with the principles of least privilege and need-to-know basis. Customers may leverage the system's default roles or define additional roles with the appropriate level of access.
UER-05	Customers are responsible for creating and managing API user accounts with the minimum privileges required, enforcing token expiration, and removing inactive or expired API credentials.

Ref.	Control Activities Expected to be Implemented at User Entities
UER-06	Customers are responsible for reviewing and authorizing any contractor or vendor access, ensuring it is limited in scope and duration, and monitoring such sessions where applicable.
UER-07	Customers are responsible for performing periodic reviews of user access rights to ensure they remain appropriate to each user's role and responsibilities.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the xDome Platform and XSA Platform system.