System and Organization Controls (SOC) 3 Report

Report on Etlworks LLC's Data Integration Platform Relevant to Security

For the period August 1, 2023 to October 31, 2023

Modern Assurance

The report accompanying this description was issued by Modern Assurance, LLC.

Table of Contents

Section I: Independent Service Auditor's Report

Independent Service Auditor's Report

To Management of Etlworks LLC,

Scope

We have examined Etlworks LLC's (Etlworks) accompanying assertion, titled "Etlworks LLC's Management Assertion" (assertion) that the controls within Etlworks' Data Integration Platform (system) were effective throughout the period August 1, 2023 to October 31, 2023 to provide reasonable assurance that Etlworks' service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity,* Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Etlworks uses the subservice organizations described in the "Subservice Organizations" subsection of Attachment A of the report. The information included within the Boundaries of Etlworks LLC's System (Attachment A) indicates that Etlworks' controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if the subservice organizations controls, assumed in the design of Etlworks' controls, are suitably designed and operating effectively along with related controls at the service organization. The information included within the boundaries of the system presents Etlworks' system and the types of controls that the services organization assumes have been implemented, suitably designed, and operating effectively at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations and we have not evaluated whether the controls management assumes have been implemented at the subservice organizations or whether such controls were suitably designed and operating effectively throughout the period August 1, 2023 to October 31, 2023.

The information included within the Boundaries of Etlworks LLC's System (Attachment A) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Etlworks, to achieve the service commitments and system requirements of Etlworks based on the applicable trust service criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Etlworks 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 Etlworks' service commitments and system requirements were achieved. Etlworks has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Etlworks 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 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 AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the controls were not effective to achieve Etlworks' service commitments and system requirements based on the applicable trust services criteria.
- performing procedures to obtain evidence about whether controls within the system were effective to achieve Etlworks' 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 Etlworks' data integration platform were effective throughout the period August 1, 2023 to October 31, 2023 to provide reasonable assurance that Etlworks' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Modern Assurance, LLC

November 3, 2023
Bend, Oregon

Section II: Etlworks LLC's Management Assertion

Etlworks LLC's Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Etlworks LLC's (Etlworks') data integration platform (system) throughout the period August 1, 2023 to October 31, 2023 to provide reasonable assurance that Etlworks' service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

The information included within the Boundaries of Etlworks LLC's System (Attachment A) indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Etlworks, to achieve Etlworks' service commitments and system requirements based on the applicable trust services criteria. The Boundaries Etlworks LLC's System (Attachment A) presents the types of complementary subservice organization controls assumed in the design of Etlworks' controls, and does not disclose the actual controls at the subservice organizations.

The information included within the Boundaries of Etlworks LLC's System (Attachment A) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Etlworks, to achieve the service commitments and system requirements of Etlworks based on the applicable trust service criteria. Attachment A presents those complementary user entity controls assumed in the design of Etlworks' controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 1, 2023 to October 31, 2023 to provide reasonable assurance that Etlworks' service commitments and system requirements would be achieved based on the applicable trust services criteria, if user entities and the subservice organizations applied the complementary controls assumed in the design of Etlworks' controls throughout that period. Etlworks' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

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

We assert that the controls within the system were effective throughout the period August 1, 2023 to October 31, 2023 to provide reasonable assurance that Etlworks' service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A

Boundaries of Etlworks LLC's system

Attachment B

Etlworks LLC's Service Commitments and System Requirements

Attachment A: Boundaries of Etlworks LLC's System

Etlworks LLC's Data Integration Platform

Overview of the Company and Types of Services Provided

Etlworks LLC ("Etlworks" or "the Company") was founded in 2016 and provides data integration services through a Software as a Service platform to companies of all sizes. Etlworks' mission is to build the best self-service data integration platform on the planet available in the cloud and on-premise. The Company serves hundreds of customers in healthcare, finance, manufacturing, media business, government, education, marketing, logistics, and many other industries.

Etlworks is a modern, scalable, cloud-first, any-to-any data integration platform. It works equally well in the cloud, on-premises and in hybrid cloud environments. Etlworks platform solves fundamental data integration problems: change data capture (CDC), extract transfer load (ETL), extract load transfer (ELT), automated programming interface (API) integration, and event-driven data integration.

Components of the System

Infrastructure

The Data Integration Platform is comprised of the following components:

Component	Description	Cloud Provider
Data Integration Platform	The software extracts data, transforms, and loads to other systems/databases based on customer preferences and needs. Includes a user interface for customers to manage the dataflows.	AWS

Software

Etlworks utilizes the following software to support the platform:

Function	Software used
Authentication manager	Office 365
Human resources	Quickbooks Online
Ticketing	Trello

Function	Software used
Change management and deployment	Bitbucket & Jenkins
Monitoring and logging	AWS CloudTrail, AWS CloudWatch & AWS GuardDuty
Vulnerability scanning	Docker service subscription and Intruder.io

Data

Data is classified in accordance with the written Data Classification Policy. The platform extracts, transforms, and loads data from various sources to various destinations in micro-batches and in real-time. The data integration flows can be triggered via APIs, customer-installed ETL agents, or the platform user interface. The Etlworks platform only stores customer credentials in the Etlworks' PostgreSQL database. Other customer data is not stored in Etlworks' PostgreSQL, Redis, AWS S3 Buckets, and AWS EBS Volumes unless the customer explicitly opts-in to temporary stage elements of the data within the Etlworks platform in AWS EBS Volumes. The databases housing sensitive customer credentials are encrypted at rest **(AC-10)**. Sensitive data is not transmitted outside of Etlworks' environment. SSL & TLS are used to encrypt data when transmitted over public and private networks **(AC-11)**. All in-scope cloud resources containing either customer data or production infrastructure are restricted to not allow public access without first authenticating **(AC-13)**.

People

Etlworks' organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored.

Etlworks has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting.

Policies

Etlworks has implemented the following policies, which serve as the basis for Company procedures, are made accessible to all relevant employees and contractors, and are reviewed annually:

- Acceptable Use Policy - defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and

internet access. This policy is acknowledged by new hire employees and contractors upon hire **(ORG-10).**

- Access Control and Termination Policy - governs authentication and access to applications, resources, and tools **(AC-04).**
- Business Continuity and Disaster Recovery Policy - governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption **(AVA-04).**
- Change Management Policy - governs the documentation, tracking, testing, and approving of system, network, security, and infrastructure changes for applications, resources, and tools **(CM-07).**
- Code of Conduct - outlines ethical expectations, behavior standards, and ramifications of non compliance. This policy is acknowledged by new hire employees and contractors upon hire **(ORG-01).**
- Configuration and Asset Management Policy - governs configurations for new applications, resources, and tools **(CM-06).**
- Data Classification Policy - details the security and handling protocols for sensitive data **(C-04).**
- Data Retention and Disposal Policy - specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations **(C-05).**
- Encryption and Key Management Policy - supports the requirements for secure encryption and decryption of app secrets, and governs the use of cryptographic controls **(AC-12).**
- Information Security Policy - establishes the security requirements for maintaining the security of applications, resources, and tools **(ORG-12).**
- Internal Control Policy - identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies **(ORG-14).**
- Network Security Policy - identifies the requirements for protecting information and systems within and across networks **(NET-06).**
- Performance Review Policy - provides personnel context and transparency into their performance and career development processes **(ORG-15).**
- Risk Assessment and Treatment Policy - governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners **(RA-01).**

- Secure Development Policy - defines the requirements for secure software and system development and maintenance **(CM-08).**
- Security Incident Response Plan - outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution **(IR-01).**
- Vendor Risk Management Policy - defines a framework for the onboarding and management of the vendor relationship cycle **(RA-04).**
- Vulnerability Management and Patch Management Policy - outlines the processes to identify and respond to vulnerabilities **(VM-01).**

Control Environment

The objectives of internal control as it relates to the data integration platform are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant control objectives, that assets are protected from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and client instructions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of Etlworks employees, the policies and procedures, the risk management process and monitoring, and the roles of significant control groups. The internal control structure is established and refreshed based on Etlworks' assessment of risk facing the organization.

Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of Etlworks' ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and Code of Conduct, and by the examples the executives set. Etlworks' executive management recognizes their responsibility to foster a strong ethical environment within Etlworks to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Code of Conduct, which is distributed to all applicable personnel of the organization.

Risk Assessment Process

Etlworks has defined a risk management framework for evaluating information security risk and other relevant forms of business risk. A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud **(RA-02).** A risk register is maintained to record the risk mitigation

strategies for identified risks, and to track the development or modification of controls consistent with the risk mitigation strategy **(RA-03).**

Due to the company's heavy reliance on outside vendors for critical infrastructure, processing capabilities, and business functions, the company has developed a Vendor Risk Management policy which establishes the compliance and performance expectations required of vendors, and the due diligence and monitoring expectations required of the Company's personnel. Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy **(RA-06).** Etlworks collects and reviews the security compliance reports (i.e. SOC 2, SOC 3, or ISO 27001) for its high-risk vendors on at least an annual basis **(RA-05).**

Monitoring Activities

Etlworks performs several types of monitoring to assess the security of health of the in-scope environment and the related controls. The company leverages a continuous monitoring solution that monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve **(ORG-05).**

Logging is enabled and monitoring software is configured to collect metrics from ingested logs to detect potential security threats, unusual system activity, and monitor system performance, as applicable **(NET-04).** Alerting software is used to notify impacted teams of potential security events, and identified events are tracked to resolution **(NET-05).** The Security Steering Committee meets quarterly to coordinate security initiatives and review network security, management of infrastructure and discuss security risks **(NET-07)**.

Incident Response

The Company employs multiple mechanisms to identify potential security incidents as discussed in the *Communication* and *Monitoring* sections above. Confirmed incidents are documented, tracked, and responded to according to the Security Incident Response Plan **(IR-02).** Following an incident, a 'lessons learned' document is created and shared with relevant internal personnel to make any required changes **(IR-03).** The Security Incident Response Plan is tested at least annually to assess effectiveness, and management makes changes to the Security Incident Response Plan based on the test results **(IR-04).**

Business Continuity

The company helps to ensure its ability to continue operations in the event of a disaster or third party attack by maintaining back ups of production data. Backed-up data is restored to a non-production environment at least annually to validate the integrity of backups **(AVA-05).** Cybersecurity insurance has been procured to help minimize the financial impact of cybersecurity loss events **(ORG-13).**

Complementary User Entity Controls

The following user entity controls are assumed to be implemented by user entities and are necessary for the service organization's service commitments and system requirements to be achieved.

User Entity Control
User entities are responsible for setting up, monitoring, and removing user entity access to the system and ensuring that it is appropriate. User entities are responsible for ensuring that any access granted to Etlworks is appropriate.
User entities are responsible for understanding and complying with their contractual obligations to Etlworks.
User entities are responsible for immediately notifying Etlworks of any actual or suspected information security breaches, including compromised user accounts.
User entities are responsible for ensuring the supervision, management, and control of the use of Etlworks's services by their personnel.
User entities are responsible for ensuring that only authorized and properly trained personnel are allowed access to the Etlworks services.
User entities are responsible for secure transmission of any data sent to ETLWorks.

Subservice Organizations

The Company utilizes the subservice organizations in the below tables to achieve its objectives.

Subservice Organization	Services Provided
Amazon Web Services, Inc. (AWS)	The subservice organization provides the Company with cloud computing services. This organization was carved out of the SOC 3 report.

Complementary Subservice Organization Controls

- The subservice organization performs periodic vulnerability assessments (CC 3.2).
- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved (CC 5.2, CC 8.1).

Subservice Organization	Services Provided
Amazon Web Services, Inc. (AWS)	The subservice organization provides the Company with cloud computing services. This organization was carved out of the SOC 3 report.

Complementary Subservice Organization Controls

- The subservice organization performs integrity checks of the data at rest (CC 5.2).
- The subservice organization implements redundancy and replication to ensure that the system is able to sustain the loss of a data center facility without interruption to the service (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains contingency planning and incident response procedures to reflect emerging continuity risks and lessons learned from past incidents (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains a capacity planning model to periodically assess infrastructure usage and demands (CC 5.2).
- The subservice organization ensures that logical IT access is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents (CC 7.1, CC 7.5).
- The subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.3, CC 7.4, CC 7.5).
- The subservice organization ensures that customer information, including personal information, and customer content are not used in test and development environments (CC 8.1).
- The subservice organization maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives, regulatory requirements, and customers (CC 9.2).
- The subservice organization discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required (CC6.5).

Subservice Organization	Services Provided
Atlassian US, Inc. (Bitbucket)	The subservice organization provides the Company with software development and version control software. This organization was carved out of the SOC 3 report.

Complementary Subservice Organization Controls

- The subservice organization performs periodic vulnerability assessments (CC 3.2).
- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved (CC 5.2, CC 8.1).
- The subservice organization performs integrity checks of the data at rest (CC 5.2).
- The subservice organization implements redundancy and replication to ensure that the system is able to sustain the loss of a data center facility without interruption to the service (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains contingency planning and incident response procedures to reflect emerging continuity risks and lessons learned from past incidents (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains a capacity planning model to periodically assess infrastructure usage and demands (CC 5.2).
- The subservice organization ensures that logical IT access is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents (CC 7.1, CC 7.5).
- The subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.3, CC 7.4, CC 7.5).
- The subservice organization ensures that customer information, including personal information, and customer content are not used in test and development environments (CC 8.1).
- The subservice organization maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives, regulatory requirements, and customers (CC 9.2).
- The subservice organization discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required (CC6.5).

Attachment B: Etlworks LLC's Service Commitments and System Requirements

Etlworks LLC's Service Commitments and System Requirements

Etlworks and its customers have a shared responsibility in maintaining the security of the data integration platform. Etlworks has established principal service commitments, which are communicated via service agreements and consist of the following:

- Uses only SSL Connections.
- Uses two-factor authentication to add an extra layer of security on top of the username and password when logging into the Etlworks Integrator.
- Enforces strong passwords.
- Etlworks strictly controls access to data and credentials and requires them to be encrypted using industry-standard methods both at rest and in transit within the environment.
- The Etlworks Integrator web application uses encrypted communication.
- Etlworks monitors application, system, and data access logs within its production environment for anomalous behavior.
- Etlworks maintains documented policies and procedures for handling security incidents, including timely notifications to affected customers in case of a verified data breach.

Etlworks has established system requirements, which are communicated via service agreements and consist of the following:

- Employee provisioning and deprovisioning standards
- User access reviews
- Logical access controls, such as the user of user IDs and passwords to access systems
- Risk assessment standards
- Change management controls
- Incident response plan