SOC 3® Report

On Devo Technology, Inc.'s Assertion for the Security Data Platform System Relevant to Security, Availability, Confidentiality, and Processing Integrity

For the Period April 1, 2023 to March 31, 2024

Devo Technology, Inc.
Three Center Plaza (3CP), Suite 302
Boston, Massachusetts 02108

Frazier & Deeter
CPAs & ADVISORS

Table of Contents

Frazier & Deeter
CPAs & ADVISORS

Section One

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of Devo Technology, Inc.:

Scope

We have examined Devo Technology, Inc.'s ("Devo" or "the Company") accompanying assertion titled "Management of Devo Technology, Inc.'s Assertion" (the Assertion) that the controls within Devo's Security Data Platform System (the System) were effective throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that Devo's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA Trust Services Criteria.

Devo uses the subservice organization identified in Attachment A to perform some of the services provided to the user entities. Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Devo, to achieve Devo's service commitments and system requirements based on the applicable trust services criteria. Attachment A 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

Devo 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 Devo's service commitments and system requirements were achieved. Devo has also provided the accompanying Assertion about the effectiveness of controls within the System. When preparing its Assertion, Devo 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 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA. We have applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Independent Service Auditor's Report

Our examination included:

- Obtaining an understanding of the System and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Devo's 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 Devo'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.

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 nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Opinion

In our opinion, management's Assertion that the controls within Devo's Security Data Platform System were effective throughout the period April 1, 2023, to March 31, 2024, to provide reasonable assurance that Devo's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Frazier & Deeter, LLC

June 18, 2024
Atlanta, Georgia

Section Two

Management of Devo Technology, Inc.'s Assertion

Management of Devo Technology, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Devo Technology, Inc.'s ("Devo" or "the Company") Security Data Platform System (the System) throughout the period April 1, 2023, to March 31, 2024, to provide reasonable assurance that Devo's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Our description of the boundaries of the System is presented in Attachment A 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 April 1, 2023, to March 31, 2024, to provide reasonable assurance that Devo's service commitments and system requirements were achieved based on the applicable trust services criteria. Devo's objectives for the System in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment A.

Devo uses the subservice organization identified in Attachment A to perform some of the services provided to the user entities. Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Devo, to achieve Devo's service commitments and system requirements based on the applicable trust services criteria. Attachment A does not disclose the actual controls implemented at the complementary subservice organization.

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 April 1, 2023, to March 31, 2024, to provide reasonable assurance that Devo's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A

Devo Technology, Inc.'s Principal Service Commitments and System Requirements and Description of Its Security Data Platform System

Principal Service Commitments and System Requirements

Service Commitments

Devo designs its processes and procedures to meet the objectives of its Security Data Platform services. Those processes and procedures are based on the service commitments that Devo makes to user entities, and the operational requirements that Devo has established for its services. Devo's principal security, availability, processing integrity and confidentiality service commitments are:

- Logical access controls are in place to provision users based on job functionality.
- Centrally managed antivirus solutions are in place to protect employee workstations.
- Business continuity and disaster recovery procedures are in place to guide personnel in resuming and/or recovering from system outages.
- Restoration of backup data is tested annually.
- Network compartmentalization is in place to separate the internal network based on security classifications.
- Data processing specifications are defined and made available to internal and external users via Devo Docs.
- Encryption technologies are in place to protect customer data at rest and in transit.
- Data classification and handling procedures are maintained and define handing data based on its classification.

System Requirements

Devo establishes operational requirements that support the achievement of service commitments. System requirements are documented in Devo's policies and procedures, system design documentation, and contracts with customers. Devo's principal system requirements are:

- New personnel requests are documented and require approval from management prior to being provisioned.
- Centralized management of antivirus software configured to automatically scan and update definitions.
- Documented Business Continuity (BC) and Disaster Recovery Plans (DRP), to guide personnel in restoring operations in the event of a business interruption or disaster.
- Testing of backup restoration performed annually.
- Configuration of load balancers to distribute network traffic across cloud resources to support availability and processing integrity.
- Encryption of sensitive and confidential customer data at rest with hard drive encryption and encrypted transport layer security (TLS) session for data in transit.
- Protection of data and information, including data classification and requirements for the storage, transmission, use, destruction, disposal, sharing, and security of confidential information as required by Devo's Information Security Framework.

- Defined and communicated Devo data processing specifications include aggregation tasks, injections, application programming interface (API) feeds, and open data protocol (OData) feeds to support processing integrity.
- Defined and communicated Devo data types.

Description of the Boundaries of Devo Technology Inc.'s Security Data Platform System

Company Overview and Services Provided

Devo Technology, Inc. ("Devo" or the "Company") was founded as Logtrust in Madrid, Spain in 2011 and rebranded to Devo in 2018. Devo is headquartered in Boston, Massachusetts with offices in Madrid, Spain and Noida, India.

Security Data Platform

The Security Data Platform, powered by proprietary HyperStream technology, is built to provide speed and scale, real-time analytics, and actionable intelligence to support an organization's Security Operation Center (SOC) performance by accelerating threat detection and response across demanding environments.

HyperStream ingests data from any source, at any volume, and contributes to the end-to-end security capabilities of the overall Security Data Platform, which also includes security information and event management (SIEM) and security orchestration, automation and response (SOAR) capabilities. HyperStream also includes artificial intelligence (AI) powered DeepTrace, Devo's autonomous threat hunting and investigation capability to augment security teams. The Security Data Platform supports SOC teams by:

- Obtaining visibility as infrastructure scales and evolves to have a complete picture to support faster action.
- Finding threats with zero lag using streaming alerts.
- Pinpointing threat actor actions with full context and precision while also assessing threat trends across an environment at scale.
- Visualizing threat posture and efficacy of security operations.
- Obtaining actionable intelligence with attack-tracing AI and community-based threat intelligence.

HyperStream

HyperStream is Devo's proprietary data analytics engine which powers the Security Data Platform. HyperStream enables data ingestion and querying, adapts to infrastructure for integration, and scales on demand. Capabilities of HyperStream are:

- No-indexing or normalization at ingestion allowing SOCs to act against their data.
- Streaming architecture for real-time insights to allow SOCs to detect and track threat actors.
- Enriching data on-query for unlimited context to support threat investigation speed by arming SOCs with actionable context.
- Querying without limits to provide security analysts automation playbooks and AI workloads, such as Devo DeepTrace, to use data to detect, investigate, and remediate cyber threats.
- Enabling AI and machine learning (ML).

Devo SOAR

Devo SOAR, a key element of the Security Data Platform, is Devo's SaaS cloud-native security orchestration, automation, and response (SOAR) solution, which uses AI-powered playbooks and decision automation to handle volumes of alerts consistently and accurately while reducing response times. SOAR is powered by Devo's HyperStream data analytics engine and security content created by Devo's research and data science teams, and integrates with Devo's Security Data Platform's SIEM capabilities, including Devo DeepTrace, to remediate threats and respond to attacks. Devo SOAR supports SOC teams in incident response and detection to resolve threats on large-scale, cloud, and legacy infrastructures. Capabilities of SOAR are:

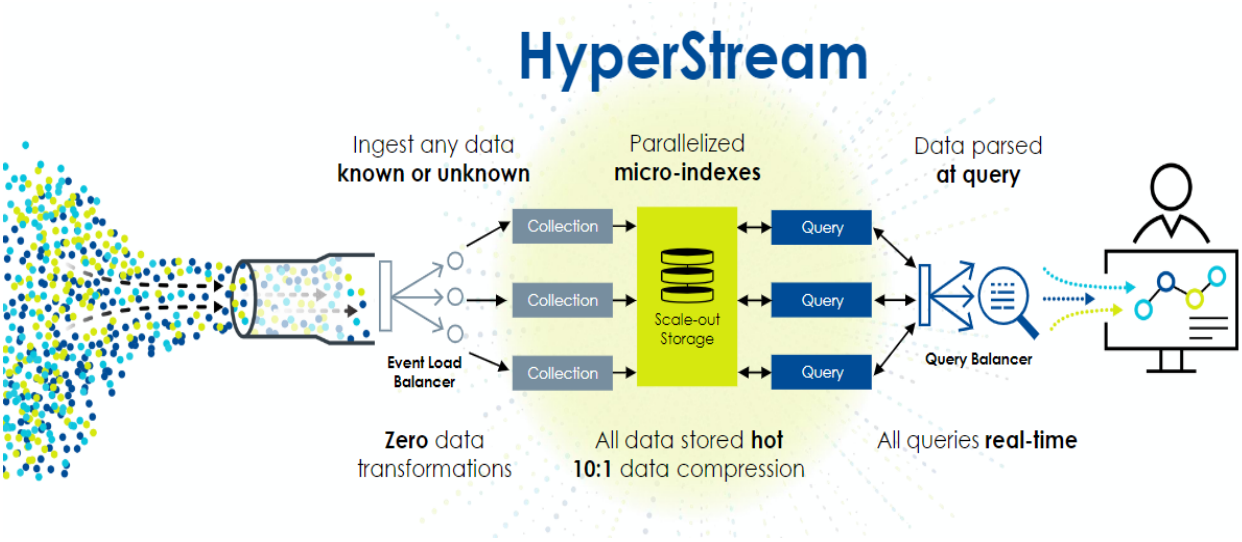
- **Intuitive Case Management:** Provides tracking and collaborating on security investigations, to support consistency in applying standard operating procedures.
- **Focus Efforts on the Cases that Matter:** Devo's ThreatLink playbook automatically correlates and enriches alerts into high-fidelity cases, reducing the number of alerts per day.
- **Continuous Measurement and Reporting:** Devo SOAR continuously captures metrics that matter most to security teams and stakeholders to support visibility into an organization's security outcomes.
- **Seamless Integration:** Devo SOAR is prepacked with more than 300 integrations for use with security teams' environments.

Devo DeepTrace

Devo DeepTrace performs autonomous investigation and threat hunting using attack-tracing AI, advancing how security teams identify attacks and investigate threats to support the security of the organization. DeepTrace augments security analysts' work by building complete traces of suspicious activity detected across an organization's infrastructure. Devo DeepTrace's autonomous, AI-powered investigations provide intelligence that supports security use cases, including malware, ransomware, and insider threats. Once an alert or event occurs, DeepTrace automatically produces a trace, providing analysts with evidence and insights that can be tracked and remediated. Devo DeepTrace supports security teams' investigation of alerts and suspicious events through threat hunting which includes:

- **Documented Attack Chains:** Utilizing attack-tracing AI and relationship graph technology, DeepTrace builds artifacts known as traces, which chronologically document each attack chain.
- **AI Engine:** Starting with an event or an alert, the AI engine asks questions to autonomously construct traces detailing an attacker's actions. DeepTrace automatically overlays its results against the MITRE ATT&CK® framework (MITRE Adversarial Tactics, Techniques, and Common Knowledge), providing analysts with additional context and reference points to analyze attacks, identify patterns, and assess existing defenses within the organization.
- **Autonomous Investigations:** DeepTrace autonomously traverses historical data to document an adversary's behavior from start to finish of an attack, providing facts to support analysts' actions.
- **Autonomous Threat Hunting:** DeepTrace helps threat hunters construct and configure new hunts that map to MITRE ATT&CK framework tactics and techniques. Once refined and validated, hunts can be converted to new cadence-based threat detections.
- **Single-Click Investigations:** Analysts can launch DeepTrace investigations from the Security Data Platform to support analysts' review and insights to supports decisions and actions.

The following schematic represents Devo's HyperStream data analytics engine, depicting data intake and query processing.



Infrastructure

Devo utilizes Amazon Web Services (AWS) cloud infrastructure to support its computing resources for processing and storage including the facilities, network, hardware, and operational software that supports the provisioning and hosting of the Security Data Platform. Devo does not maintain any of its own servers and relies on redundant cloud-based services for storage of documents and records.

Software/Tools

The Platform offers data isolation and consists of the following software components:

- **Devo Relay -** Software that receives, encrypts, and transmits customer log data to the Security Data Platform.
- **Devo Cloud Collector -** Software that receives, encrypts, and transmits customer log data from cloud-based services to the Security Data Platform.
- **Graphical User Interface (GUI) -** A web based application used by the customer to interact with data.
- **Event Load Balancer (ELB)** - Devo proprietary software that accepts incoming data from relays or other sources and forwards on to the next component (data nodes).
- **Data Nodes** - Two key software processes referred to as "collectors" and "query engines" occur inside of data nodes. "Collectors" receive the log data and write it, completely unmodified, to disk. "Query engines" are responsible for retrieving data from disk as the response to queries. Devo scales "up" and "out" because the architecture allows an unrestricted number of data nodes.
- **Meta Nodes –** When a customer makes a query using the GUI, the GUI translates it to the appropriate syntax and sends it to "meta nodes". These nodes distribute the query across the data nodes it connects to.
- **Correlation Engine –** Devo can provide batch query results from data stored on disk and real-time query results using the correlation engine.

- **Alert Engine** – When the correlation engine finds matching data from a continuous query, it creates a new correlation event. The alert engine receives these events and uses them to alert customers using a set of predefined contact methods and rules.
- **Aggregation Engine –** Allows for data to be queried (e.g., data visualization) in "buckets". Customers can aggregate data to get summary information. The role of the aggregation engine is to keep track of data and store the statistical measures associated with aggregations.
- **Back–End** – The back-end is a set of services that connect to the Red Hat Enterprise Linux operating system (RHEL) and provides traditional services like the web server for the GUI, access to the file system, time synchronization, and other services.

The following commercial software is used to support the delivery of the Security Data Platform:

- Email and secure document repository
- Wiki
- Customer help desk ticketing
- Human resources information system
- Source code repository for version, configuration and deployment management
- Project and task management
- Automation server for the Software Development Lifecycle (SDLC)
- Platform performance analytics
- Privileged credential management
- Antivirus software installed on Devo employee workstations and servers
- Vulnerability management scanning tool
- Mobile Device management (MDM) platform
- Endpoint Detection and Response (EDR) platform
- Internal and external customer communication system
- Security Data Platform - Devo's internal SOC and SOAR

People

Governance and management of Devo is vested in the Executive Leadership Team, which is supported by the Board of Directors. The Devo Board of Directors (BoD) is comprised of a majority of members that are independent from management. The Board meets quarterly to evaluate the Company's organizational structure, reporting lines, authorities and responsibilities as a part of its business planning process and to support the Company's risk assessment process to achieve its objectives.

Devo's Executive Leadership Team consists of key personnel from functional departments, including: the Chief Executive Officer (CEO); Chief Technology Officer (CTO); Chief Financial Officer (CFO); General Counsel (GC); Senior Vice President, Marketing; Chief Revenue Officer; Senior Vice President, Product; and Senior Vice President

Engineering Security. The Chief Information Security Officer (CISO) is responsible for developing, implementing and monitoring Devo's information security programs. The CISO is also tasked with enforcing the alignment with requirements and industry standards, identifying gaps, and working with the functional departments to remediate issues. The Governance, Risk and Compliance (GRC) department, under the direction of the CISO, is responsible for establishing and maintaining organization-wide information security policies and standards, and completing compliance audits to monitor the effectiveness of information security policies and procedures.

Data

Devo, a security data platform, ingests data from threat intelligence feeds, third-party security orchestration, automation and response (SOAR) platforms, and IT service management (ITSM) tools to support user entities' security automation, response efficiency, and cross-functional collaboration.

Data Classification

Data is protected in a manner commensurate with its sensitivity and criticality from its origination to destruction. The Acceptable Use Policy defines how the organization categorizes and handles the data it stores.

Data Storage

Confidential information and data at rest on file systems and servers are encrypted. Additionally, employee workstations are secured with hard drive encryption.

Data Destruction

Management disposes of customer data upon authorized customer request in accordance with the Data Disposal Policy and Information Security Standard.

Data Processing

Devo data processing specifications are classified as aggregation tasks, injections, API feeds, and OData feeds in support of information quality. Data processing specifications are defined and made available to internal and external users via Devo Docs. Additionally, data types are defined including the data name, description, and an example, and are made available to internal and external users via Devo Docs.

During customer onboarding, customer data environments are configured within the system to enforce segregation. Customers are provisioned access only to data associated with their own organization, preventing access to data from other organizations or underlying system infrastructure.

Configured load balancers are used to distribute network traffic across cloud resources in an effort to support availability and processing integrity. Performance monitoring tools are configured to monitor the System's availability and performance, and alerts are generated when specific predefined thresholds are met for resolution.

Guidelines for sending data to the Security Data Platform from open-source and/or third-party log collection tools are defined.

Data Backup and Recovery

Devo's infrastructure is supported by AWS and relies on AWS to implement preventive measures to minimize operational disruptions and recover as rapidly as possible when an operational incident occurs. Procedures to support business continuity and disaster recovery are in place to guide personnel in resuming and/or recovering from system outages.

An automated backup system is utilized to perform scheduled system backups. Alerts are configured to notify IT personnel if backups fail.

The Company maintains a Business Continuity Management Policy and Disaster Recovery (DR) Plan, both reviewed annually, which outline impact areas, continuity measures, recovery steps, roles, responsibilities, test scenarios, and conducts annual tests of system restoration capabilities.

Processes and Procedures

The Devo Information Security Framework consists of a set of information security policies, procedures, guidelines. The scope of the Information Security Framework includes the Company's information systems and resources, company data stored on these systems as well as backups or hardcopies of this data. The Information Security Standard falls beneath the Devo Information Security Policy and establishes the requirements for protecting information and information systems. Policies are reviewed and approved by management annually and are available to employees.

The documented policies and standards presented below are in place to address the roles and responsibilities of users for information security; assignment of responsibility and accountability for system security, availability, processing integrity, and confidentiality; information and data classification; user account management; prevention of unauthorized access user access provisioning / deprovisioning, addressing and resolving security, availability, processing integrity, and confidentiality concerns, incidents or breaches; third party information sharing; non-compliance with security policies; and handling of exceptions not specifically addressed within corporate or IT policies.

- Information Security Policy
- Information Security Standard
- Acceptable Use Policy
- Code of Business Conduct and Ethics Standard
- Incident Response Standard
- Business Continuity Management Policy
- Software Development Lifecycle Policy
- Procurement Policy
- Vendor Security Risk Assurance Policy
- Vulnerability Management Plan
- Data Protection Policy
- Whistleblower Policy
- Anti-Corruption and Bribery Policy
- Disaster Recovery Plan
- Business Continuity Plan
- Risk Management Policy
- Devo Employee Handbook
- Combating Trafficking in Persons Policy

Subservice Organizations and Complementary Subservice Organization Controls

Devo's Security Data Platform System uses the subservice organization identified below to perform some of the services provided to user entities. Although the subservice organization has been carved out for the purposes of this report, Devo management has assumed, in the design of the system, that certain complementary subservice organization controls (CSOCs) would be implemented by the subservice organization. CSOCs that are suitably designed and operating effectively are necessary, along with controls at Devo, to achieve Devo's service commitments and system requirements based on the applicable trust services criteria. The CSOCs presented below should not be regarded as a comprehensive list of all controls that should be designed, implemented, or operated by carved out subservice organization.

The carved out subservice organization and CSOCs relevant to Devo's Security Data Platform System are described in the following table:

Subservice Organizations	Service(s) Provided	Types of Expected Controls
Amazon Web Services (AWS)	Cloud data center hosting services	Firewalls are in place to prevent unauthorized external access to the AWS network. User provisioning is performed for authorization of access to AWS resources, including revocation when access is no longer required. Physical access control mechanisms are in place at the AWS data center, and access to data centers is restricted to authorized AWS employees and third-party users. Secure sanitization and destruction of hardware and media upon decommission. Security events and incidents are logged, monitored, analyzed, and responded to in a timely manner. Infrastructure capacity is monitored and managed to meet capacity demands. Environmental controls are in place and monitored.