SOC Type 2

Complementary Subservice Organization Controls

Microsoft Azure & Auth0's Identity Services

Dated 2022-01-05

Introduction

This document describes complementary controls applied in conjunction with Azure and Auth0's SOC Type 2 Certifications.

Government Regulation and Requirements

Notwithstanding the foregoing limits on updates, Sales Cookie may modify or terminate the Services in any country or jurisdiction where there is any current or future government requirement or obligation that (1) subjects Sales Cookie to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for Sales Cookie to continue operating the Services without modification, and/or (3) causes Sales Cookie to believe described controls may conflict with any such requirement or obligation.

Electronic Notices

Sales Cookie may provide Customer with information and notices about the Services electronically, including via email, through the Sales Cookie website, or through a website that Sales Cookie identifies. Notice is given as of the date it is made available by Sales Cookie.

Azure SOC Type 2 Complementary Controls

Type of Services Provided	**Subservice Organization Name**	**Complementary Subservice Organization Controls**	**Relevant Applicable Trust Services Criteria**	**Sales Cookie's Controls**
Secrets Management	Microsoft Azure	Azure is responsible for encryption and back up of secrets stored on Azure Key Vault service.	CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	1. Sales Cookie stores secrets in Azure Key Vault 2. Sales Cookie references secrets by name (not value) in configuration files 3. Sales Cookie does not use production secrets during development or testing 4. Sales Cookie grants access to secrets as per our data access policy (principle of least privilege) 5. Sales Cookie protects access to secrets using MFA and SSO 6. Sales Cookie protects access to secrets using Azure RBAC and PIM (privileged identity management) 7. Sales Cookie protects access to secrets by IP

			CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	1. Sales Cookie uses Azure Monitoring, Azure Active Directory, Azure Activity Logs, SumoLog to detect anomalies related to secrets
			A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	1. Sales Cookie uses multi-zone redundancy to store secrets 2. Sales Cookie references secrets by name (not value) in configuration files 3. Sales Cookie leverages SSO, MFA, Azure RBAC, Azure PIM, and IP to control access to secrets 4. Sales Cookie rotates secrets every 3 months 5. Sales Cookie deletes secrets which are no longer needed 6. Sales Cookie does not use production secrets during development or testing

			PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity’s objectives.	1. Sales Cookie regularly verifies secret access and secret backup health 2. Sales Cookie uses high-priority alerts to report security-related issues 3. Sales Cookie uses on-call rotations to respond to high-priority alerts 4. Sales Cookie uses well-defined escalation and incident response policies 5. Sales Cookie documents issues using RCAs (root cause analysis documents) 6. Sales Cookie rotates secrets every 3 months 7. Sales Cookie deletes secrets which are no longer needed 8. Sales Cookie does not use production secrets during development or testing 9. Sales Cookie grants access to production secrets as per our data access policy (principle of least privilege) 10. Sales Cookie protects access to secrets using MFA

				and SSO 11. Sales Cookie protects access to secrets using Azure RBAC and PIM (privileged identity management) 12. Sales Cookie protects access to secrets by IP
			PI1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity’s objectives.	1. Sales Cookie wipes secrets from memory after usage 2. Sales Cookie encrypts secrets in memory 3. Sales Cookie rotates secrets every 3 months 4. Sales Cookie deletes secrets which are no longer needed

Backup of SQL Database	Microsoft Azure	Azure is responsible for maintaining Point in time Restore (PITR) capabilities for the Azure DevOps data stored on Azure SQL Database.	CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	1. Sales Cookie uses Azure SQL databases 2. Sales Cookie uses Azure SQL automated backups to eliminate manual intervention and associated risks 3. Sales Cookie regularly verifies the schedule and health of SQL backups 4. Sales Cookie uses Azure Monitoring, Azure Active Directory, Azure Activity Logs, SQL Advanced Threat Analytics, SumoLog events to detect anomalies related to backups
			A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	1. Sales Cookie uses Azure SQL automated backups to eliminate manual user intervention 2. Sales Cookie regularly verifies the schedule and health of SQL backups 3. Sales Cookie uses SQL encryption for all backups 4. Sales Cookie never copies SQL data outside of Azure 5. Sales Cookie uses multi-zone

				redundancy to store SQL backups 6. Sales Cookie uses Azure Monitoring, Azure Active Directory, Azure Activity Logs, SQL Advanced Threat Analytics, SumoLog events to detect anomalies related to SQL backups 7. Sales Cookie leverages SSO, MFA, Azure RBAC, Azure PIM, and IP to control access to SQL backups
			C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	1. Sales Cookie identifies customer ownership of each data set within databases 2. Sales Cookie allows customers to control data retention 3. Sales Cookie uses encrypted SQL backups 4. Sales Cookie never copies SQL data outside of Azure 5. Sales Cookie uses SQL Data Loss Protection

			PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity’s objectives.	1. Sales Cookie uses high-priority alerts to report data-related issues 2. Sales Cookie uses on-call rotations to respond to high-priority alerts 3. Sales Cookie uses well-defined escalation and incident response policies 4. Sales Cookie documents issues using RCAs (root cause analysis documents) 5. Sales Cookie implements clear backup and data retention policies 3. Sales Cookie does not use backup SQL data during development or testing 4. Sales Cookie grants access to SQL backups as per our data access policy (principle of least privilege) 5. Sales Cookie protects access to SQL backups using MFA and SSO 6. Sales Cookie protects access to SQL backups using Azure RBAC and PIM (privileged identity management)

				7. Sales Cookie protects access to SQL backups by IP
			PI1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity’s objectives.	1. Sales Cookie uses Azure SQL automated backups to eliminate manual user intervention 2. Sales Cookie does not store backups outside of Azure SQL 3. Sales Cookie regularly verifies the schedule and health of SQL backups 4. Sales Cookie does not use backup SQL data during development or testing

Security and anti-malware logging and vulnerability and baseline scanning	Microsoft Azure	Azure DevOps leverages Azure's logging and reporting capabilities for appropriate monitoring of security and antimalware events and vulnerability and baseline alerts.	CC4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	1. Sales Cookie documents its policy to notify internal and external parties of application security issues / breaches (with SLA) 2. Sales Cookie uses high-priority alerts to report security-related issues 3. Sales Cookie uses on-call rotations to respond to alerts 4. Sales Cookie uses well-defined escalation and incident response policies 5. Sales Cookie documents issues using RCAs (root cause analysis)
			CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	1. Sales Cookie uses anti-virus scanning 2. Sales Cookie uses static code analysis to detect potential vulnerabilities 3. Sales Cookie uses penetration testing & port scanning to detect vulnerabilities 4. Sales Cookie uses hundreds of security tests which must pass on deployment 5. Sales Cookie uses Auth0 to manage all end-

				user authentication 6. Sales Cookie uses Azure Monitoring, Azure Active Directory, Azure Activity Logs, SQL Advanced Threat Analytics, SumoLog, Auth0 events to monitor application security 7. Sales Cookie uses SQL Advanced Threat Analytics and SQL Data Loss Protection 8. Sales Cookie uses a library to encode all strings within HTML output 9. Sales Cookie protects access to source code using MFA and SSO 10. Sales Cookie uses anti-virus scanning
			CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	1. Sales Cookie uses automated Azure Pipelines to eliminate human intervention during deployment 2. Sales Cookie uses code reviews (approvals required) to manage changes to source code 3. Sales Cookie uses hundreds of security tests

				which must pass on deployment 4. Sales Cookie uses static code analysis to detect potential vulnerabilities 5. Sales Cookie protects access to source code using MFA and SSO
			CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	1. Sales Cookie uses Azure Monitoring, Azure Active Directory, Azure Activity Logs, SQL Advanced Threat Analytics, SumoLog, Auth0 events to monitor application security 2. Sales Cookie application code logs events when anomalies related to application behavior are detected 3. Sales Cookie uses on-call rotations to respond to high-priority alerts 4. Sales Cookie uses well-defined escalation and incident response policies 5. Sales Cookie documents issues using RCAs (root cause analysis documents)

			CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	1. Sales Cookie uses automated Azure Pipelines to eliminate human intervention during deployment 2. Sales Cookie uses code reviews (with approvals required) to manage changes to source code 3. Sales Cookie uses hundreds of security tests which must pass on deployment 4. Sales Cookie protects access to source code using MFA and SSO
Physical and Environmental Security of Azure DevOps information	Microsoft Azure	Azure is responsible for providing physical and environmental security to Azure DevOps application and data hosted at Microsoft datacenters.	CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	1. Sales Cookie requires disk encryption to access DevOps data (for source code repository copies) 2. Sales Cookie requires badge access for physical entry to facilities 3. Sales Cookie uses clear policies for data disposal (ex: shredding, disk erasing)
			CC6.5 The entity 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	1. Sales Cookie grants access to DevOps resources as per our data access policy (principle of least privilege) 2. Sales Cookie protects access to DevOps resources

			is no longer required to meet the entity’s objectives.	using MFA and SSO 3. Sales Cookie uses clear policies for data disposal (ex: shredding, disk erasing) 4. Sales Cookie does not grant access to DevOps production resources for development / testing
			CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	1. Sales Cookie regularly reviews changes to DevOps resources (code changes) 2. Sales Cookie uses hundreds of security tests which must pass on deployment

Auth0 SOC Type 2 Complementary Controls

#	Complementary User Entity Control	Sales Cookie's Controls

1	User entities are responsible for maintaining formal policies and procedures that provide guidance for information security within the organization and the supporting IT environment	1. Sales Cookie does not use Auth0 production credentials during development or testing 2. Sales Cookie uses Azure secrets to manage access to the Auth0 platform 3. Sales Cookie grants access to Auth0 resources as per our data access policy (principle of least privilege) 4. Sales Cookie protects access to Auth0 resources using MFA and SSO 5. Sales Cookie actively monitors and reviews access to Auth0 resources
2	User entities are responsible for establishing logical access controls, such as user access provisioning, role-based access, user access deprovisioning, and user access reviews to the Auth0 Identity Platform, as well as all the systems that interact with the Auth0 Identity Platform.	1. Sales Cookie does not use Auth0 production credentials during development or testing 2. Sales Cookie uses Azure secrets to manage access to the Auth0 platform 3. Sales Cookie grants access to Auth0 resources as per our data access policy (principle of least privilege) 4. Sales Cookie protects access to Auth0 resources using MFA and SSO 5. Sales Cookie actively monitors and reviews access to Auth0 resources
3	User entities are responsible for implementing strong password parameters (i.e. multi-factor authentication, password history, complexity, etc.) utilizing the features offered by the Auth0 Identity Platform	1. Sales Cookie requires MFA and SSO to access Auth0 resources
4	User Entities are responsible for implementing IT Security controls, such as antivirus, network penetration scanning, vulnerability assessments, etc.	1. Sales Cookie uses Azure secrets to manage access to the Auth0 platform 2. Refer to complementary controls related to Azure secrets and Azure DevOps data
5	User Entities are responsible for notifying Auth0 of unusual activity, violations, and/or security breaches identified.	1. Sales Cookie has a documented procedure to notify Auth0 of issues 2. Sales Cookie has chosen Auth0 because it provides the ability to notify users of breaches, suspicious logins, etc.

6	User Entities are responsible for performing backups and storing Auth0 logs and data.	1. Sales Cookie only stores end-user authentication in Auth0 2. Sales Cookie has the ability to ask users to reset their credentials should Auth0 lose access to data