Delinea

Delinea and SOC 2 Compliance

A control-by-control map of where Delinea supports the SOC 2 Trust Services Criteria

System and Organization Controls 2 (SOC 2) is a framework developed by the American Institute of Certified Public Accountants (AICPA) that specifies how software vendors and other organizations should manage customer data. Service providers are asked for a SOC 2 report during procurement and again at renewal, covering the systems in scope, which include environments they run on a client's behalf. Delinea holds a SOC 2 Type 2 report covering the Security, Availability and Confidentiality Trust Services Criteria. The tables that follow map the criteria where Delinea can support your own SOC 2 examination and the evidence available for each.

Capability summary

Centralized audit trail
Audit logs for all access to configured resources, plus recordings of SSH and RDP sessions, held in one place and streamable to the security information and event management (SIEM) of your choice.

Time-bound access
Just-in-time and time-bound grants with least privilege by default, revocable instantly or on expiry.

Point-in-time access history
The command line interface shows users, roles and access as they are now or as they were at any point in the past.

Immediate revocation
Revoke access to a system or data source instantly when an account may be compromised.

Where Delinea maps to the Trust Services Criteria

This table maps AICPA criteria to Delinea capabilities. It is not an attestation, your auditor determines whether each control is satisfied.

Logical and physical access controls

Point of focus	Requirement detail	How Delinea helps
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Identifies and manages the inventory of information assets	The entity identifies, inventories, classifies and manages information assets.	Delinea discovers databases, servers and Kubernetes clusters in AWS, Azure and GCP, plus privileged accounts and shadow admins across endpoints, directories and clouds.
Restricts logical access	Logical access to information assets, including hardware, data (at-rest, during processing or in transmission), software, administrative authorities, mobile devices, output and offline system components is restricted through the use of access control software and rule sets.	Enforce role-based (RBAC) and attribute-based (ABAC) access control with just-in-time, least privilege access. Delinea removes local admin rights on endpoints and enforces least privilege on servers and cloud entitlements.

Point of focus	Requirement detail	How Delinea helps
CC6.1 The entity implements logical access security software, infrastructure and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
Identifies and authenticates users	Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely.	Authenticate through your identity provider or the Delinea Platform with multi-factor authentication (MFA) at server login and privilege elevation.
Considers network segmentation	Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.	Users reach resources only through Delinea gateways, and only the resources you grant, which limits lateral movement from user sessions. Keep your existing network segmentation to isolate resources from each other.
Manages points of access	Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented and managed.	Manage and audit all activity against backend infrastructure, whether by employees, contractors or other third parties.
Restricts access to information assets	Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification and digital certificates are used to establish access-control rules for information assets.	Delinea uses a combination of user identities, network segmentation (making only gateways public) and roles or groups to generate and enforce access control rules.
Manages identification and authentication	Identification and authentication requirements are established, documented and managed for individuals and systems accessing entity information, infrastructure and software.	Federate with your identity provider or use Delinea's native authentication with minimum password requirements.
Manages credentials for infrastructure and software	New internal and external infrastructure and software are registered, authorized and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.	Delinea vaults and automatically rotates credentials, governs service accounts through decommissioning and can pull credentials from your existing secret store.
Uses encryption to protect data	The entity uses encryption to supplement other measures used to protect data at rest, when such protections are deemed appropriate based on assessed risk.	Delinea encrypts stored secrets with AES-256 using a unique key per secret.
Protects encryption keys	Processes are in place to protect encryption keys during generation, storage, use and destruction.	Delinea supports hardware security modules (HSMs) including customer-held master keys in Azure Managed HSM.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
Controls access credentials to protected assets	Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.	The gateway or relay closest to the resource authenticates on the last hop using credentials from Delinea or your existing secrets manager.
Removes access to protected assets when appropriate	Processes are in place to remove credential access when an individual no longer requires such access.	Instantly grant and revoke permanent or just-in-time access to resources through the Delinea admin UI or through an identity provider.
Reviews appropriateness of access credentials	The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.	Delinea Fastpath runs scheduled access reviews and validates that access marked for removal was actually removed. The Delinea admin UI lists every user and what they can reach.

Point of focus	Requirement detail	How Delinea helps
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions and other protected information assets based on roles, responsibilities or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
Creates or modifies access to protected information assets	Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.	Users inherit access from their roles, except for temporary access. Delinea can grant temporary access from Slack and Microsoft Teams.
Removes access to protected information assets	Processes are in place to remove access to protected information assets when an individual no longer requires access.	Revoke access instantly or on a time-bound basis. Delinea can automatically disable compromised Microsoft Entra ID and Okta accounts when those integrations are granted write access.
Uses role-based access controls	Role-based access control is utilized to support segregation of incompatible functions.	Grant access through role-based access control. Delinea Fastpath flags segregation of duties (SoD) conflicts across SAP, Oracle, Salesforce, Workday and other business applications.
Reviews access roles and rules	The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals with access and access rules are modified as appropriate.	Use the Delinea command line interface (CLI) to view users, roles and access at any point in the past. Delinea Fastpath reviews access by security role.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
Restricts access	The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.	Configuring a data source with a particular driver restricts communication over that connection to that specific driver protocol. SSH cannot be tunneled through a port set up for MySQL.
Protects identification and authentication credentials	Identification and authentication credentials are protected during transmission outside its system boundaries.	Delinea uses mutually verified TLS 1.2 between clients and gateways, TLS 1.2 or 1.3 for the admin UI, and signs every API call with device and session keys.
Requires additional authentication or credentials	Additional authentication information or credentials are required when accessing the system from outside its boundaries.	Delinea enforces MFA through your identity provider or Delinea Platform methods, including Duo, a mobile authenticator and FIDO2 security keys. Available methods vary by product and tenant.
Implements boundary protection systems	Boundary protection systems (e.g., firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.	By deploying Delinea gateways and relays, customers can make all of their resources internal-only and not visible through their system boundary.
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
Uses encryption technologies or secure communication channels to protect data	Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.	Delinea carries client traffic to its gateways over mutually verified TLS 1.2, uses each resource's native encryption on the last hop, logs every session and records SSH and RDP sessions.
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.		
Restricts application and software installation	The ability to install applications and software is restricted to authorized individuals.	Delinea removes local admin rights on endpoints and applies allow, deny and restrict policies to applications, with sandboxing and reputation checks for unknown apps.

System operations

Point of focus	Requirement detail	How Delinea helps
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify changes to configurations that result in the introduction of new vulnerabilities, and susceptibilities to newly discovered vulnerabilities.		
Monitors infrastructure and software	The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	Delinea logs every command, streams logs to your security information and event management (SIEM) system and flags new admin accounts and privilege changes.
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.		
Implements detection policies, procedures, and tools	Detection policies and procedures are defined and implemented and detection tools are implemented on infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include a defined governance process for security event detection and management that includes provision of resources; use of intelligence sources to identify newly discovered threats and vulnerabilities; and logging of unusual system activities.	Delinea captures every authentication, query and SSH or RDP command, plus admin permission changes, and detects brute force and MFA bombing.
Designs detection measures	Detection measures are designed to identify anomalies that could result from actual or attempted compromise of physical barriers; unauthorized actions of authorized personnel; use of compromised identification and authentication credentials; unauthorized access from outside the system boundaries; compromise of authorized external parties; and implementation or connection of unauthorized hardware and software.	Delinea streams audit logs to your SIEM for anomaly detection and lets admins watch and end live privileged sessions.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
Communicates and reviews detected security events	Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.	Centralized logs and session recordings show who accessed what and what they did.
Develops and implements procedures to analyze security incidents	Procedures are in place to analyze security incidents and determine system impact.	Delinea provides detailed audit logs for all access to configured data sources, which can assist in evaluations and investigations of security incidents.
CC7.4 The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
Contains security incidents	Procedures are in place to contain security incidents that actively threaten entity objectives.	Delinea lets admins immediately revoke access to systems and data sources for accounts that may be compromised.
Mitigates ongoing security incidents	Procedures are in place to mitigate the effects of ongoing security incidents.	Delinea rotates exposed credentials on demand, on a schedule, or automatically when it detects an out-of-band password change, and admins can end live privileged sessions.
Ends threats posed by security incidents	Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.	Delinea can automatically disable compromised Microsoft Entra ID and Okta accounts when those integrations are granted write access.

Point of focus	Requirement detail	How Delinea helps
CC7.4 The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
Obtains understanding of nature of incident and determines containment strategy	An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including a determination of the appropriate response time frame, and the determination and execution of the containment approach.	Delinea provides comprehensive audit logs for all access to configured data sources, which are central to security incident investigations.
Evaluates the effectiveness of incident response	The design of incident-response activities is evaluated for effectiveness on a periodic basis.	Periodically review audit logs and session recordings to identify potential gaps in your incident response plan and adjust accordingly.
Periodically evaluates incidents	Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.	Review audit logs and session recordings to identify opportunities to improve your security posture.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.		
Determines root cause of the event	The root cause of the event is determined.	Delinea provides audit logs for all access to configured resources and recordings of SSH and RDP sessions, which are central to identifying root cause in security incidents.
Improves response and recovery procedures	Lessons learned are analyzed and the incident-response plan and recovery procedures are improved.	Use audit logs to analyze incidents and to develop appropriate responses.

Change management

Point of focus	Requirement detail	How Delinea helps
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.		
Provides for changes necessary in emergency situations	A process is in place for authorizing, designing, testing, approving and implementing changes necessary in emergency situations. These include changes that need to be implemented in an urgent time frame).	Grant just-in-time access with least privilege by default, including automatic access during PagerDuty on-call shifts or from Slack and Microsoft Teams. Delinea records every privileged session for review.

Evidence available to an auditor

The controls above produce evidence your auditor can review, including user access lists, captured commands and permission changes, session recordings, point-in-time access history and completed access reviews. Bring one client environment and walk through it against your own criteria.

Contact an expert to learn more

Delinea

Delinea is an identity security platform governing what AI agents, humans and machines can do, and for how long. Just-in-time authorization extends privileged access management from access to action, cutting standing privilege across on-premise, multi-cloud and ephemeral infrastructure. Its platform scores identity risk and keeps access decisions auditable. Over 9,000 organizations, including two-thirds of the Fortune 100, rely on Delinea. Learn more at **delinea.com**.

© Delinea SOC2-DS-1026-EN