Cayosoft

Built for the Moment

Cayosoft Guardian SaaS Security, Trust, & Compliance Overview

This document provides a high-level overview of how Cayosoft secures and operates its Software-as-a-Service (SaaS) platform. It is intended for customers and prospects evaluating Cayosoft SaaS from a security, privacy, and compliance perspective.

Purpose and Scope

Cayosoft SaaS is designed to help organizations monitor, protect, and recover identity systems across Microsoft Active Directory, Microsoft Entra ID, Intune and Microsoft 365. Because identity represents a critical control plane in modern environments, Cayosoft applies security-by-design principles throughout the SaaS platform lifecycle. This document describes the security controls implemented and operated by Cayosoft for the SaaS platform itself. It does not replace customer security responsibilities and does not describe controls implemented within customer-managed environments.

SaaS Architecture and Tenant Isolation

Cayosoft operates a centralized SaaS control plane that is logically isolated from customer environments. Each customer tenant is logically separated to prevent unauthorized access to data or services across tenants.

Key architectural principles include:

- Dedicated Cayosoft-operated SaaS tenant and infrastructure
- Logical tenant isolation for customer data and configuration
- No cross-tenant data access or visibility
- Separation between Cayosoft corporate IT, SaaS operations, and customer tenants

The Cayosoft SaaS platform incorporates backup and recovery mechanisms designed to support data protection and service continuity. Backup and recovery controls are maintained and exercised as part of Cayosoft's operational resilience practices.

Customer Data Handling and Privacy

Cayosoft is committed to protecting the confidentiality and integrity of customer data processed within the SaaS platform.

Cayosoft affirms the following data-handling principles:

- Customer data is used solely to deliver the contracted SaaS service
- Customer data is not sold or monetized
- Customer data is not used to train artificial intelligence or machine learning models
- Customer data is not shared with third-party providers except where required for core cloud hosting services
- Access to customer data by Cayosoft personnel is restricted, logged, and provided only when necessary for support or operations

Cayosoft SaaS is hosted in cloud provider data centers within defined geographic regions. Customer data is stored and processed within the selected service region. Detailed regional availability and residency details are available under NDA.

Encryption and Data Protection

Cayosoft applies industry-standard encryption mechanisms to protect data both in transit and at rest.

- Data in transit is protected using secure, encrypted communication protocols
- Data at rest is encrypted using cloud-provider managed encryption services
- Secrets and credentials are stored using managed secret storage services

- Hard-coded credentials are prohibited in production systems

Identity, Access, and Operations Security

Access to the Cayosoft SaaS platform is governed by strong identity and access management controls designed to minimize risk.

- Cloud-only administrative identities are used for SaaS operations
- Phishing-resistant multifactor authentication is enforced for all administrative access
- Conditional Access policies restrict how and where access is permitted
- Privileged access is time-bound and approved using just-in-time access principles
- Support and DevOps access are segregated and scoped to defined operational needs

Secure Development Lifecycle (SDLC)

Security is integrated into the Cayosoft software development lifecycle. Controls are applied from design through deployment and ongoing maintenance.

- Security considerations are incorporated during product design and architecture reviews
- Code changes undergo peer review prior to release
- Automated testing is used to validate functionality and reduce regression risk
- Regular patching and update processes are applied to the SaaS platform
- Reported security vulnerabilities are assessed, prioritized, and remediated

Cayosoft maintains a process for receiving, assessing, and remediating reported security vulnerabilities.

Compliance and Assurance

The Cayosoft SaaS platform is audited under SOC 2 Type II against the Security, Availability, and Confidentiality Trust Services Criteria. Due to the sensitive nature of audit reports, the SOC 2 Type II report is made available to customers and prospects under a non-disclosure agreement upon request.

Cayosoft

Built for the Moment

Cayosoft has completed a Cybersecurity Maturity Model Certification (CMMC) Level 1 self-assessment in accordance with U.S. Department of Defense requirements for safeguarding Federal Contract Information (FCI) under FAR clause 52.204-21. CMMC Level 1 is a foundational, self-attested assessment and does not represent a third-party certification. Additional information regarding Cayosoft's CMMC posture is available upon request.

Incident response and customer notification

Cayosoft maintains a formal incident response process designed to identify, contain, investigate, and remediate security incidents affecting the SaaS platform. Security incidents are managed in accordance with established internal procedures and applicable regulatory requirements. Customers are notified of security incidents impacting their data in alignment with contractual obligations and legal requirements.

Shared Responsibility Model

Cayosoft SaaS operates under a shared responsibility model.

Cayosoft is responsible for securing and operating the SaaS platform, including infrastructure, application security, and service availability. Customers are responsible for securing their own identity environments, user access, configurations, and on-premises components that integrate with the SaaS service.

Contact and Additional Information

Cayosoft provides additional security, compliance, and availability information through controlled disclosure mechanisms, including NDA protected documentation and direct engagement with our security and compliance teams.

For additional information regarding security, privacy, or compliance, customers and prospects may contact Cayosoft directly. SOC 2 and compliance-related inquiries can be addressed through Cayosoft's compliance team.