CCPA compliance with Coro

The California Consumer Privacy Act (CCPA) gives consumers more control over the personal information that businesses collect about them. It secures privacy rights, including:

- The right to delete personal information collected about you (with some exceptions).
- The right to opt out of the sale of your personal information.
- The right to non-discrimination for exercising your CCPA rights.

In order to comply with the CCPA regulation, businesses are required to give consumers notices explaining their privacy practices.

How CCPA relates to cybersecurity

The CCPA requires that a business behave responsibly with personal information collected or processed for specific purposes. This includes consumer requests and information provided in response to access requests.

How Coro handles CCPA compliance for you

At Coro, we regularly track updates to the CCPA to make sure you're covered when we are protecting your systems.

Requirements described by CCPA that Coro handles for you:

CATEGORY	REQUIREMENT	HOW CORO HELPS
Cloud security & privacy	Malware and ransomware injection	Detects and remediates malware and ransomware files in cloud drives
	Cloud app account takeover	Monitors access to cloud apps and user/admin activities on them
	MFA	Enforces multi-factor authentication on cloud app access
	DLP over cloud drive files exposure	Provides data loss prevention (DLP) for regulatorily and business-sensitive data
	Audit and activity logs	Archives all system activities for a period of seven years, supporting referencing and auditing

info@coro.net | coro.net | 844-926-7663

CATEGORY	REQUIREMENT	HOW CORO HELPS
Email Security & Privacy	Generic and spear phishing	Detects and remediates social engineering attacks based on email content analysis
	Identity spoofing	Detects and remediates social engineering attacks based on adaptive identity monitoring
	Malware and ransomware injection	Detects and remediates malware and ransomware in email attachments
	Embedded links to malicious URLs	Detects and remediates embedded links to malicious servers
	DLP over outgoing/incoming email	Encrypts emails before they are sent, which are then decrypted by their recipients at the other end.
	Business email compromise (BEC)	Scans business email, detects and protects against social engineering attacks
	Email account takeover	Monitors email attacks from within the organization
	Audit and activity logs	Archives all system activities for a period of seven years, supporting referencing and auditing
Endpoint Security & Privacy	Antivirus (AV)	Detects and remediates files with high-risk content based on their signatures
	ATP (NGAV)	Detects and remediates processes exhibiting high-risk behaviors with behavioral analysis
	Device security posture	Detects security vulnerabilities on endpoint devices and enforces device security posture
	Data recovery	Stores local snapshots of data
	EDR	Enables post-breach analysis of endpoint activities across the organization
	DLP on endpoint devices	Provides data loss prevention (DLP) for business-sensitive data and data defined as sensitive by regulations
	Audit and activity logs	Archives all system activities for a period of seven years, supporting referencing and auditing
Data Governance	Data distribution governance and role management	Provides data loss prevention (DLP) for data defined as sensitive by regulations
	Security and business-specific data monitoring	Monitors sensitive data according to business and security best practices, including passwords, certificates, source code, proprietary data, etc.
	PHI monitoring	Monitors PHI (also: personal health information) that healthcare professionals collect to identify an individual and determine appropriate care
	Audit and activity logs	Archives all system activities for a period of seven years, supporting referencing and auditing