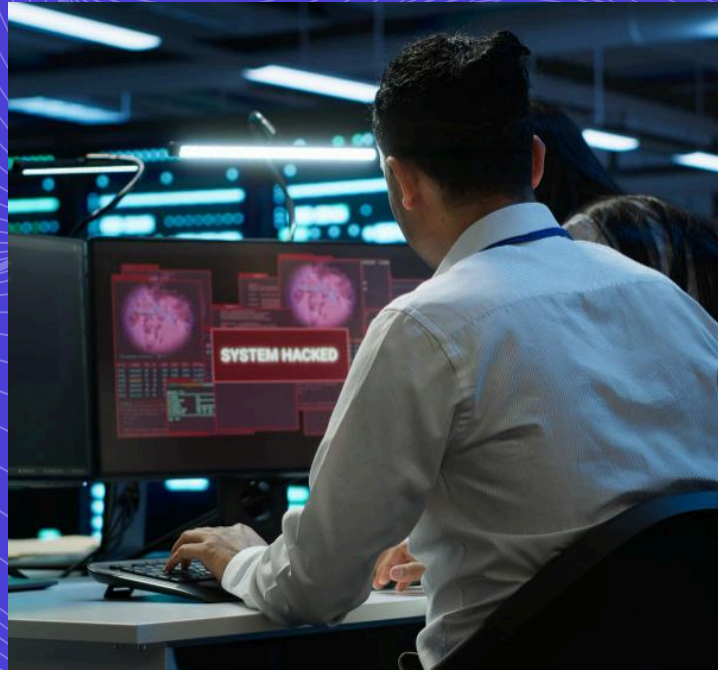
The Beginner's Guide to SOC2 Compliance with Kitecyber

Discover how Kitecyber helps service organizations achieve/maintain SOC 2 objectives by protecting customer data across endpoints, networks, cloud and SaaS, providing technical controls, monitoring, and audit-ready evidence.



What is SOC 2 Compliance

SOC 2 is an AICPA-based auditing standard that evaluates controls relevant to one or more Trust Services Criteria: Security (required), and optionally Availability, Processing Integrity, Confidentiality, and Privacy. Organizations tailor controls to their environment and auditors test operating effectiveness over time.

How Kitecyber Helps Businesses Achieve SOC 2 Compliance

Kitecyber's integrated modules and features like DLP, Data Classification, UEM, UEBA, SWG, ZTNA — produce technical and procedural controls that map directly to SOC 2 TSCs:

- Discover & classify customer data to limit scope and apply the right controls.
- Prevent and block unauthorized access or exfiltration of customer data
- Enforce device posture, encryption, and secure configurations
- Detect anomalous activity and provide prioritized alerts & timelines for investigations.
- Produce exportable logs, policy evidence, and incident timelines auditors require.

SOC 2 Trust Services Criteria → Kitecyber Mapping Table

TSC / Focus Area	Mapped Kitecyber Product(s)	How Kitecyber Helps (controls & evidence)
Security (Protect systems & data from unauthorised access / disclosure)	DLP, Data Classification, ZTNA, SWG, UEM, UEBA	- Prevent: DLP blocks unauthorized copying, uploads, email leaks and removable-media exfiltration of customer data. - Control access: ZTNA enforces identity + device trust posture (Just-in-time access). - Harden endpoints: UEM enforces encryption, patching, AV. - Detect: UEBA correlates anomalies (credential misuse, mass downloads). - Evidence: Exportable DLP incidents, ZTNA session logs, device posture reports for auditors.
Availability (Systems available for operation & use)	UEM, SWG, ZTNA, UEBA	- Resilience: UEM enforces patching, AV/EDR posture and remote remediation to reduce downtime. - Access continuity: ZTNA supports secure, policy-driven access even during network changes. - Network protection: SWG helps block DoS/malicious web vectors and control bandwidth/exfil attempts. - Evidence: uptime/incident reports, remediation ticket timelines and post-incident summaries.
Processing Integrity (System processing is complete, valid, accurate, timely)	UEBA, DLP, UEM	- Detects anomalies: UEBA surfaces abnormal processing or batch/job failures that may corrupt data. - Prevent tampering: DLP and UEM enforce controls preventing unauthorized modifications or accidental overwrites. - Evidence: transaction/session logs, alerts with timestamps and remediation actions._
Confidentiality (Restrict access & disclosure of sensitive/ confidential data)	Data Classification, DLP, SWG, ZTNA	- Scope & classify: Data Classification identifies confidential data (customer, IP, secrets) to limit scope. - Prevent leaks: DLP blocks transfer to unapproved SaaS, cloud, email, or removable media. - Secure channels: SWG inspects and enforces TLS/ secure uploads; ZTNA limits external exposure. - Evidence: classification inventories, policy enforcement reports, blocked transfer logs.
Privacy (Personal data handling: collection, use, disclosure & retention)	DLP, Data Classification, Compliance Workflows, UEBA	- Discover & fulfill rights: DLP + classification locate personal data for access/erasure requests. - Limit retention: Workflows + UEM/DLP enforce retention and deletion policies. - Detect misuse: UEBA flags unauthorized use of personal data. - Evidence: subject access reports, deletion/retention logs, incident reports for privacy breaches._

Practical SOC 2 outcomes Kitecyber delivers

- Scope reduction — Classify and isolate systems that process sensitive customer data to shrink audit scope.
- Preventive controls — Stop the common paths of data loss (email, SaaS/ Gen AI uploads, USB, copy/paste).
- Detect & prioritize — UEBA prioritizes high-risk events (insider exfiltration, compromised creds) for faster response.
- Auditability — Exportable, tamper-evident logs (DLP incidents, ZTNA sessions, device posture) and policy enforcement records.
- Faster readiness — Combine technical controls with playbooks and evidence exports to accelerate SOC 2 readiness and Type II testing.

Quick SOC 2 Checklist — How to start with Kitecyber (30–90 days)

1. **Scope & classify:** Run Data Classification to locate customer and regulated data on devices; build a minimal SOC-in-scope footprint.
2. **Deploy preventive DLP:** Create DLP policies to block or quarantine unapproved CHD/PDI transfers (email, SaaS, Airplay, USB).
3. **Enforce device posture:** Roll out UEM baseline (hard disk encryption, AV, patching) on all in-scope endpoints.
4. **Implement ZTNA:** Require identity + device checks for access to sensitive systems (no shared accounts, enforce MFA).
5. **Enable UEBA & central logging:** Stream logs and alerts to SIEM/SOC; tune UEBA to reduce noise and identify high-risk events.
6. **Create evidence packs:** Configure regular exports: DLP incidents, device posture reports, ZTNA session logs, incident timelines.
7. **Run tabletop & readiness tests:** Validate controls, simulate incidents, and update playbooks and evidence collection processes.

KITE CYBER

Kitecyber, 691 S Milpitas Blvd, Ste 217, Milpitas, CA 95035
Email: info@kitecyber.com
Website: www.kitecyber.com

LinkedIn Twitter YouTube