Continuous Controls Monitoring

For Security Teams

Security teams live in a reactive, manual world. Teams struggle to see which risks matter most and spend their valuable time and talents on low-impact issues. Trawling spreadsheets and screenshots for data, chasing down control owners for logs and reports, maintaining homegrown and manual systems — these tasks obscure drift and gaps until they become live incidents.

With Continuous Controls Monitoring (CCM) through the JupiterOne platform, teams can automatically achieve a complete, near-real-time view of their organization's control state.

By gaining unified visibility into control health across clouds, tools, and identities, they can prioritize and fix what matters, while escaping the chore of chasing fragmented evidence.

Unified Visibility

JupiterOne's asset graph gives teams a unified view of all controls and their relationships to assets, identities, and environments, making it easier to see how gaps expose critical systems.

Continuous Validation

CCM tests controls by running queries against the asset graph on a daily or hourly basis, or when a proactive search is needed. Control health and configuration drift are detected as they happen, enabling earlier remediation and lower impact.

Automated Workflows

Each control test automatically generates stored evidence, saving teams hours of evidence-gathering. CCM logs control health over time, catching "flapping" controls and issues that appear and are remediated between checks. Control failures and status can flow into ticketing tools, closing the feedback loop with near-real-time remediation workflows. This allows issues to be addressed in the flow of normal operations, rather than creating a huge backlog.

JupiterOne

	Before	With JupiterOne CCM
Visibility	Hand-gathering data and information from numerous tools and spreadsheets.	API-driven discovery of assets, identities, dependencies, status, and more.
Continuous Control Testing	Spot checks on a small sample of assets using manually built custom scripts.	Automated queries run against your entire environment on a daily or hourly basis, and whenever a change is detected.
Ad-Hoc Questions	Time-intensive cross-referencing of tools and data to construct an answer to a seemingly simple question.	Questions can be answered in seconds, because data is always current. JupiterOne's LLM integration lets teams ask custom questions in natural language, no scripting required.
Security Posture	No way to provide historic evidence that teams are effectively improving or maintaining proper security controls.	Built-in dashboards and alerts expose actual control health, non-compliant entities, and trends over time so teams know where to focus their efforts.

Go from Reactive to Resilient

- **Detect drift as soon as it starts,** keeping risk minimal and empowering teams to be preventative.
- **Prioritize unique risks,** using the graph to map the potential blast radius of risks before they become incidents.
- **Make better-informed decisions** by drilling down to entity-level failures, understanding context, relationships, and more.
- **Remediate faster and easier** by linking failed controls to tickets and workflows.
- **Cut hours of manual toil** by automating control tests you've been manually writing scripts for.

Ready to See the Difference?

With Continuous Controls Monitoring through JupiterOne, security teams can transform manual, static validation into always-on assurance. They can detect and correct drift in near real time, save hours with automatic evidence collection, and spend more time focusing on the mission of security, rather than rote clerical work.

Contact us today to operationalize CCM and sharpen your competitive edge.

Get a Demo

JupiterOne