The Power of SentinelOne & Cynomi

Turn SentinelOne Endpoint and Vulnerability Data into Revenue Driving Managed Security and Compliance Programs

Delivering security services starts with good data. MSPs need continuous visibility into vulnerabilities and endpoint posture across every client - and a way to turn those technical findings into prioritized action, measurable progress, and services clients pay for every month.

Together, SentinelOne and Cynomi close that gap. SentinelOne continuously monitors vulnerability and endpoint posture across every managed device. Cynomi turns those findings into structured assessments, prioritized remediation plans, compliance progress, and client-ready reporting, providing a repeatable workflow that helps you standardize and scale your cyber advisory, compliance, and security program management services.

Who Is Cynomi?

Cynomi is the agentic Security Growth Platform for service providers, powered by CISO Intelligence, the decision-making logic of an experienced security leader, embedded into every workflow. Built for MSPs, MSSPs, and advisory firms, Cynomi runs the full security and compliance program for every client: assessment, risk management, remediation, and reporting - from one multi-tenant platform so any team member can deliver consistent, defensible work, not just your senior experts.

Rather than requiring manual collection to run your security & compliance services, Cynomi centralizes data from across your existing stack including cloud platforms, vulnerability scanners, PSA systems, and endpoint sources like SentinelOne. Findings are ingested automatically, mapped to the relevant framework controls, and converted into prioritized tasks, so every client's task plan reflects live reality without anyone re-entering data by hand.

How The Integration Works

The Cynomi x SentinelOne integration covers both vulnerability and endpoint data.
Cynomi reads the Singularity Management API directly and evaluates 14 posture checks across every managed endpoint, spanning:

- Deployment & protection — EDR coverage, anti-malware currency, protect vs. detect-only mode
- Configuration controls — firewall, disk encryption, device control, application control
- Inventory & hygiene — asset and software inventory, policy exclusions, admin activity cadence
- Negative evidence — prohibited or high-risk software, end-of-life operating systems, unmanaged devices

Each check resolves to one of three states: Pass, Gap, or At Risk - and links directly to the relevant Cynomi task, so a single task can be evidenced by multiple checks and the task plan stays in sync with actual endpoint reality automatically. That means an MSP no longer has to manually confirm that EDR is deployed and active on every device, for every client, every reporting cycle. SentinelOne's own telemetry closes the loop and updates each client's compliance posture in real time, alongside vulnerability management findings feeding the same task-and-remediation engine.

The integration is also license-aware: coverage adapts to each tenant's SentinelOne tier, so a partner only sees the checks their license can actually evidence, with no noise from capabilities they haven't licensed. For MSPs managing SentinelOne across a mixed client base that means one integration, consistent behavior, and no manual reconciliation of what each client's license does or doesn't support.

What This Means for your Security and Compliance Managed Service Delivery

- **Less manual evidence work:** Cynomi reads SentinelOne continuously, so no one has to log in each cycle to confirm a control is in place.
- **A sellable service, not just a technical report:** Every finding becomes a scoped, evidenced task, from closing a control gap to upgrading a SentinelOne tier.
- **One consistent model, any client:** The same posture-to-task pipeline works across your whole book of business, regardless of SentinelOne tier.
- **One platform, every use case:** The same agentic engine that runs your SentinelOne findings also standardizes assessment, risk management, compliance, and reporting across your entire practice, so delivery looks the same whether it's an analyst or your most senior expert running it.
- **One picture for the client:** Vulnerability and endpoint data feed the same task plan, posture score, and compliance tracker powering a single, coherent story instead of disconnected tool outputs.

Why Cynomi

- **Easy to Use**
  Intuitive, wizard-driven experience.
- **Fast Time to Value**
  Rapid onboarding for partners and your customers.
- **Revenue Growth**
  Built-in opportunity identification, business translation and proof of value.
- **Operational Efficiency**
  No more spreadsheets, scalable delivery.
- **Expert Outcomes at Scale**
  We carry the complexity, you take the credit..
- **GTM Enablement & Community**
  Education, sales and co-marketing supporting your success
- **Cybersecurity Mission-Driven**
  Empowering you to protect every client
- **100% Partner-Only**
  No conflict, ever.

See your SentinelOne data go to work.

Book a demo and we'll show you what your client endpoint and vulnerability data looks like running through Cynomi. Real tasks, real posture score, real client reports.

About Cynomi

Cynomi is the agentic Security Growth Platform for service providers, powered by CISO Intelligence that delivers the decision-making logic of an experienced security leader embedded into every workflow. Purpose built for MSPs, MSSPs and consultancies, Cynomi helps service providers deliver, scale, and grow cybersecurity services across every client and every maturity level. By combining complete security program management with portfolio-level revenue insights, Cynomi turns cybersecurity into a repeatable, profitable growth engine that improves margins, standardizes delivery, strengthens client trust, and uncovers new recurring revenue opportunities. Partner with us at www.cynomi.com.