ThreatBook

INTEGRATION BRIEF

Bridge Network Detection with Endpoint Response

ThreatBook & SentinelOne Joint Solution Brief

Market Challenges

NDR provides broad visibility into suspicious network activity, while endpoint security delivers the process-level context and containment capabilities needed to act. When these tools operate in silos, analysts often lack visibility into the endpoint process behind suspicious connections, spend valuable time correlating hosts and events across separate consoles, and face additional handoffs when containment is required.

For lean SOC teams, these disconnected workflows increase investigation effort and slow the transition from threat validation to response.

Joint Solution

ThreatBook TDP integrates with SentinelOne to create a connected workflow across network detection, endpoint investigation, and response. TDP maps network alerts to the relevant SentinelOne endpoints and retrieves available process and DNS context on demand, helping analysts quickly understand the activity behind suspicious connections.

When malicious activity is confirmed, authorized analysts can isolate the affected endpoint through SentinelOne directly from the TDP workflow and reconnect it after remediation. The integration gives security teams the endpoint context and response capabilities they need at the point of investigation, reducing tool switching and enabling more efficient threat containment.

How It Works

Administrators configure the SentinelOne API address and API token in TDP. The integration provides the following capabilities:

01 Synchronize Endpoint Assets

- Sync SentinelOne endpoint assets into TDP.

INTEGRATION BENEFITS

Accelerate Threat Investigation

Give security teams the endpoint context they need to validate network-detected threats faster and reduce time spent switching between tools.

Improve Containment Decisions

Combine network and endpoint evidence to help analysts make faster, better-informed isolate-or-monitor decisions.

Strengthen Response Accountability

Maintain clear endpoint status, integration records, and audit trails to support traceable and consistent response processes.

- Collects available asset information, including IP address, hostname, MAC address, operating system, and online status.
- Associate each endpoint with its SentinelOne Agent UUID.

02 Investigate Network Alerts

- Associate TDP network alerts with the relevant SentinelOne endpoint.
- Query context by alert time, destination IP, port, domain, or URL.
- Display process, command-line, file-path, signature, parent-process, and DNS details.

03 Respond and Recover

- Authorized analysts can isolate or release associated endpoints directly from TDP.
- Integration and audit logs remain visible for traceability and post-incident review.

Use Cases

Network Alert Enrichment

Enrich TDP network alerts with SentinelOne process and DNS context to quickly distinguish legitimate activity from potential threats.

Lateral Movement Containment

Validate suspected lateral movement with combined network and endpoint evidence, then isolate affected endpoints directly from the TDP workflow.

Traceable Recovery

Isolate and release endpoints from TDP while retaining the associated integration and audit logs for traceability and post-incident review.

Conclusion

The integration helps security teams move from network signal to endpoint action faster, with richer context, fewer manual pivots, and clearer response accountability.

Gartner

TDP was recognized in the Gartner Magic Quadrant for Network Detection and Response (2025)

Gartner Peer Insights™

TDP was recognized as a Strong Performer in Voice of the Customer for Network Detection and Response (2023, 2024, 2025)

FORRESTER

TDP was included in The Network Analysis and Visibility Solutions Landscape (2025)

About ThreatBook

ThreatBook is The Agentic Security Company. Its TDP NDR platform unifies full-traffic visibility, firsthand threat intelligence and AI models to help SecOps teams expose attack surfaces, detect sophisticated threats with greater accuracy, and accelerate containment across network, cloud, and AI environments.

About SentinelOne

SentinelOne delivers an AI-powered cybersecurity platform for prevention, detection, response, and threat hunting across endpoint, cloud, identity, and other environments. The Singularity Platform is built to help defenders detect, contain, and remediate attacks at machine speed.