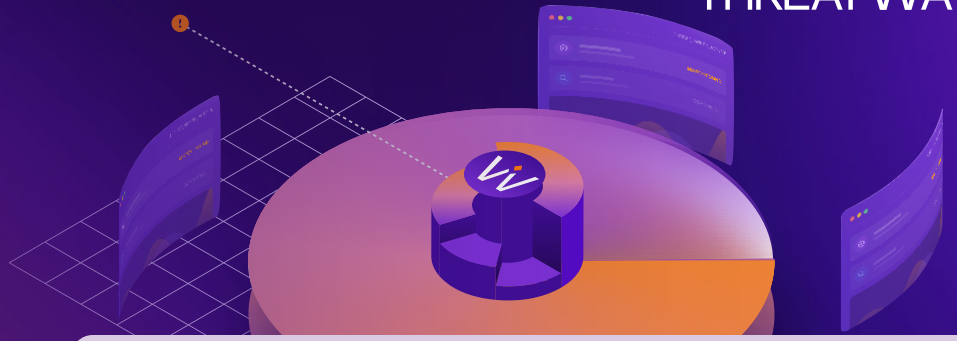
securonix DATASHEET

THREATWATCH

Securonix ThreatWatch

HUMAN-VALIDATED THREAT SWEEPS



Continuously validate exposure to emerging threats and confirm impact quickly.

The Challenge

When new campaigns break or warning signals appear, leaders need to know whether their environment shows evidence of an adversary or specific indicators of compromise. Manual hunting and ad hoc searches slow response and increase risk.

The Solution

Securonix ThreatWatch operationalizes Threat Labs intelligence into SIEM-ready queries, runs retroactive sweeps across telemetry, and applies human validation to reduce noise, delivering investigation-ready findings through the Securonix ThreatQ experience layer.

Turning Threat Intelligence into Actionable Validation

CURATE → GENERATE → SWEEP → VALIDATE → REPORT

Securonix ThreatWatch turns emerging threat intelligence into repeatable, defensible exposure validation, without adding manual work to your SOC.

Use Cases

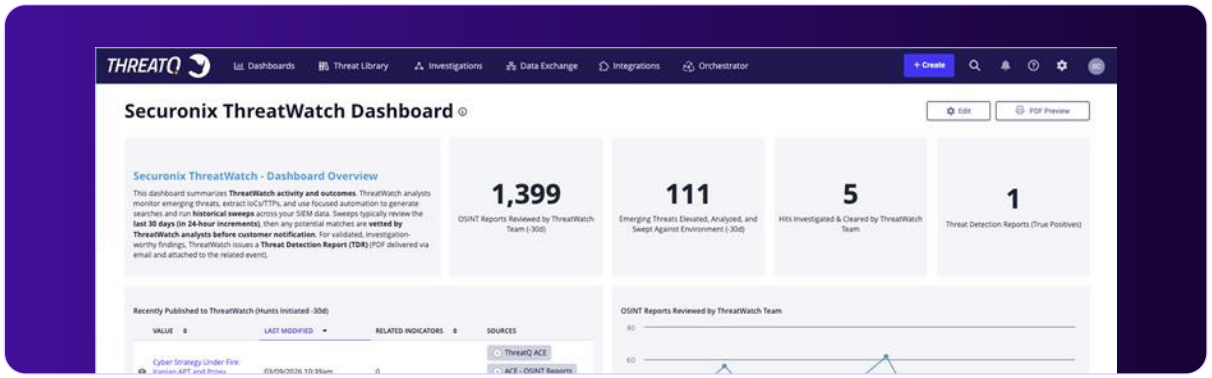
- **Emerging Threat Response:** Confirm exposure quickly when new campaigns break.
- **Retroactive Threat Hunting:** Sweep historical telemetry without analyst-built queries.
- **Executive & Board Reporting:** Provide defensible, auditable exposure documentation.
- **SOC Efficiency Optimization:** Offload manual hunt creation and validation tasks.

Securonix ThreatWatch Benefits

- **Quickly Know Your Exposure:** Auto-run SIEM queries across historical data to confirm impact.
- **Historical Proof at Scale:** Continuous validation with only investigation-worthy findings escalated.
- **Defensible Documentation:** Executive-ready reports of checks, findings, and actions taken.
- **Higher-Fidelity Escalations:** Human validation reduces noise and keeps analysts focused.

Built to Fit into Your SOC Workflow

Securonix ThreatWatch is vendor agnostic with integrations into Securonix, Splunk, and QRadar, providing direct SIEM query pivots to enable analysts to move from validation to investigation fast. Delivered through a hosted ThreatQ experience layer, any analyst can benefit from insights from ThreatQ Lite.



Compare

ThreatWatch vs. Threat Intelligence Feeds

- **Validation, not just indicators:** Confirms relevance in your environment.
- **Higher-confidence outcomes:** Human-reviewed findings reduce false positives.
- **Retroactive visibility:** Sweeps historical telemetry, not just a point in time.

ThreatWatch vs. Manual Hunting

- **Repeatable at scale:** Continuous validation without analyst-heavy cycles.
- **Consistent quality:** Human validation standardizes what gets escalated.
- **Faster execution:** Automated sweeps replace manual query creation and tuning.

Take the Next Step.

Ready to move from emerging threat awareness to defensible exposure validation? See how ThreatWatch helps your team confirm impact faster, reduce manual hunting, and deliver executive-ready reporting. Schedule a demo to see ThreatWatch in action.

Proven Results, Trusted by the Industry

Securonix has been recognized as a **6x Leader in the Gartner® Magic Quadrant™ for SIEM and achieved 193% ROI in the Forrester TEI Study.**

Visit **securonix.com** or contact sales@securonix.com.