Deepwatch Guardian MDR Platform™ for Securonix

Precision Detection. Elite 24/7 Coverage. Measurable Security Outcomes

OVERVIEW

The Deepwatch Guardian MDR Platform™ (Deepwatch MDR) transforms your Securonix investment into real-world security outcomes. Securonix delivers powerful cloud-native detection and behavioral analytics—but technology alone doesn't stop threats. Deepwatch adds 24/7 elite SOC coverage, precision detection engineering, and NEXA™ Agentic AI to close the SIEM capability gap: reducing alert fatigue, accelerating response, and cutting dwell time without replacing your existing platform.

WHY DEEPWATCH MDR FOR SECURONIX?

Turn Securonix Analytics into Operational Outcomes. Securonix delivers powerful analytics and behavioral detection. Deepwatch ensures those detections translate into consistent, real-world responses:

- 24/7 alert triage across all severities within the Deepwatch Platform.
- Standardized investigation workflows that reduce variability and accelerate decisions.
- Structured 5W case summaries for rapid understanding and action.

Reduce Noise, Improve Detection Fidelity. Modern environments generate overwhelming alert volumes. Deepwatch enhances Securonix detections with enrichment, validation, and analyst oversight to surface what truly matters:

- Threat intelligence enrichment for immediate contextual clarity.
- Alert normalization and linked-case automation to eliminate duplication.
- Expert analyst validation to suppress false positives and elevate real threats..

Deliver Transparency and Measurable Performance. Security operations demand visibility — not black-box processing. Deepwatch provides clear insight into every detection, investigation, and outcome:

- Real-time case visibility through the Deepwatch Security Center.
- Detection inventory transparency and performance reporting.
- Seamless ServiceNow integration for structured case management.

KEY CAPABILITIES

Native Securonix Detection & Triage

- ✓ Direct ingestion of Securonix alerts into the Deepwatch Platform for structured case management.
- ✓ Standardized 5W investigation summaries for rapid clarity and action.
- ✓ Consistent analyst-led triage workflows embedded within the Deepwatch Platform.

Enrichment & Contextualization

- ✓ Threat intelligence enrichment integrated into every investigation.
- ✓ Alert normalization and linked-case automation to reduce duplication and provide enhanced clarity.
- ✓ Backend enrichment pipelines supporting reporting and operational insight.

Operational Integration & Case Management

- ✓ Deepwatch – Securonix connector for alert ingestion and normalization.
- ✓ Seamless ServiceNow integration for case routing and lifecycle management.
- ✓ Transparent case visibility in the Deepwatch Security Center.

www.deepwatch.com

CUSTOMER VALUE

Business Benefits

- Accelerate operational maturity with 24/7 expert-led triage and response built on your Securonix environment.
- Reduce cyber risk and alert fatigue through structured investigations, prioritized detections, and consistent containment workflows.
- Maximize Securonix ROI by converting advanced analytics into measurable security outcomes.
- Deliver executive-ready visibility with transparent reporting, case documentation, and performance metrics.

Technical Benefits

- Native alert ingestion and normalization from Securonix into the Deepwatch Platform for standardized triage.
- Threat intelligence enrichment embedded into every investigation for faster context and root-cause clarity.
- ServiceNow integration for seamless case routing and lifecycle management.
- Real-time visibility in the Deepwatch Security Center with detection inventory transparency and analyst commentary.

ABOUT DEEPWATCH MDR AND SECURONIX

Together, Deepwatch MDR and Securonix transform powerful SIEM analytics into measurable security outcomes. With continuous monitoring, AI-enhanced investigations, and expert-led response, organizations gain end-to-end visibility, faster threat containment, and improved operational clarity across complex environments.

WHY NOW? WHY DEEPWATCH?

Securonix delivers advanced analytics and behavioral detection—but cloud growth, identity sprawl, and escalating threat sophistication have widened the gap between what a SIEM detects and what internal teams can operationalize at scale.

Deepwatch MDR closes that gap. With 24/7 expert-led triage, structured investigation workflows, and AI-enhanced enrichment built directly into your Securonix environment, detections become consistent, measurable outcomes—not just alerts. The result: less alert fatigue, faster response, and full operational transparency without disrupting your existing investment.

Precision detection. Expert execution. Securonix fully operationalized.

WHO BENEFITS

SOC teams, CISOs, and risk/compliance leaders across Financial Services, Healthcare, Retail, and Manufacturing.

Always Watching. Always Protecting.