DEEPWATCH™
Always Watching. Always Protecting.™

SOLUTION BRIEF

Deepwatch Guardian MDR Platform™ for CrowdStrike Next-Gen SIEM

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

OVERVIEW

The Deepwatch Guardian MDR Platform™ (Deepwatch MDR) enables organizations to fully operationalize CrowdStrike Next-Gen SIEM. By combining CrowdStrike's real-time detection with Deepwatch's 24/7 SOC, precision detection engineering, and NEXA™ Agentic AI, organizations achieve faster response, reduced alert fatigue, and improved security outcomes, without adding operational burden.

WHY DEEPWATCH MDR FOR CROWDSTRIKE NEXT-GEN SIEM?

Turn CrowdStrike Analytics into Operational Outcomes
CrowdStrike delivers high-fidelity detections and rich telemetry. Deepwatch ensures those detections translate into consistent, real-world responses:

- Continuous 24/7 triage across all alert severities within the Deepwatch Platform
- Streamlined investigation workflows that improve consistency and speed decision-making
- Structured 5W case summaries to quickly communicate context and next steps

Reduce Noise, Improve Detection Fidelity
Alert volume at scale can obscure real risk. Deepwatch enhances CrowdStrike detections with context, correlation, and expert validation to focus attention on what matters most:

- Enriched threat intelligence for faster context and prioritization
- Normalization and correlation to streamline investigation workflows
- Expert-led validation to reduce noise and improve detection fidelity

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 Guardian MDR Platform™
- Transparent visibility into detection coverage and performance metrics
- Seamless ServiceNow integration for structured, end-to-end case management

KEY CAPABILITIES

Native CrowdStrike Detection & Triage

- ✓ Direct ingestion of CrowdStrike alerts into the Deepwatch Platform to enable structured case management
- ✓ Standardized 5W investigation summaries that drive fast clarity and informed action
- ✓ Consistent, analyst-led triage workflows integrated within the Deepwatch Platform

Enrichment & Contextual Insight

- ✓ Real-time threat intelligence adds meaningful context to every investigation
- ✓ Correlation and case-linking reduce noise and improve investigative clarity
- ✓ Enrichment pipelines power reporting and actionable operational insights

Operational Integration & Case Management

- ✓ Tight integration with CrowdStrike enables scalable ingestion and processing of alerts
- ✓ ServiceNow-driven workflows ensure consistent case handling and escalation
- ✓ Full case transparency available through the Deepwatch Platform

DEEPWATCH™

CUSTOMER VALUE

Business Benefits:

- Advance security operations maturity faster with continuous, expert-led triage and response aligned to your CrowdStrike environment
- Reduce risk and operational noise through validated investigations, prioritized signals, and consistent containment execution
- Unlock greater value from CrowdStrike by turning real-time detections into measurable security outcomes
- Equip stakeholders with clear visibility through transparent reporting, case narratives, and performance-driven insights

Technical Benefits:

- Seamless ingestion and normalization of CrowdStrike alerts within the Deepwatch Platform for consistent triage workflows
- Context-rich investigations powered by integrated threat intelligence, enabling faster understanding and root-cause analysis
- Structured case workflows via ServiceNow integration, supporting end-to-end lifecycle management
- Real-time operational visibility through the Deepwatch Platform, including detection insights and analyst-driven context

WHO BENEFITS

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

WHY NOW? WHY DEEPWATCH?

CrowdStrike delivers real-time detection and rich telemetry - 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 CrowdStrike 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.

ABOUT DEEPWATCH MDR AND CROWDSTRIKE

Together, Deepwatch MDR and CrowdStrike Next-Gen SIEM transform powerful detection and telemetry 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.

Precision detection.
Expert execution.
CrowdStrike fully operationalized.

DEEPWATCH™
Always Watching. Always Protecting.

ABOUT DEEPWATCH

Deepwatch® is the leader in Precision MDR powered by AI and humans. We amplify human expertise with AI insights to reduce the risks that matter most to your business. Our protection is proactive, preemptive and responsive, tuned to your business, with no black boxes, and watched by experts 24/7/365.

CONTACT US

GET STARTED

250 Cambridge Avenue
Palo Alto, CA 94306
www.deepwatch.com