DEEPWATCH™
Always Watching. Always Protecting.

SOLUTION BRIEF

Deepwatch Guardian MDR Platform™ for Microsoft Sentinel

Purpose-built Integration and Risk-aligned Detection. Operational Clarity.

OVERVIEW

Microsoft Sentinel is a powerful cloud-native SIEM and SOAR platform, delivering scalable log ingestion, AI-driven analytics, and automation across the enterprise. However, maximizing its value requires constant tuning, expert detection engineering, and operational expertise.

That's where the **Deepwatch Guardian MDR Platform™ (Deepwatch MDR) for Microsoft Sentinel** comes in.

Purpose-built for Microsoft Sentinel, Deepwatch MDR enhances customers' SIEM investment by adding **24/7/365 monitoring, curated detection engineering, and strategic insights**—all fully integrated with Sentinel workbooks, analytics rules, playbooks, and dashboards.

Deepwatch MDR enables customers to **operationalize Sentinel more effectively**, while advancing risk-based security maturity through Deepwatch's **Dynamic Risk Scoring** and the **Deepwatch Security Index™ (DSI).**

WHY DEEPWATCH MDR FOR SPLUNK?

Native Sentinel Integration

Deepwatch MDR connects directly into Microsoft Sentinel without requiring major platform changes. Telemetry is ingested, normalized, and enriched using **Azure-native tools and connectors**, allowing customers to:

- Onboard new log sources quickly with optimized Sentinel data connectors.
- Maintain customer data within Azure—Deepwatch does not duplicate or store logs externally.
- Gain transparent visibility into detections and incidents directly from the Sentinel portal.

Continuous Threat Detection & Response

Deepwatch's security experts build and tune detection rules that are mapped to **MITRE ATT&CK**, aligned to customer environments, and continuously optimized for performance, providing:

- KQL-based custom analytic rules and hunting queries.
- Suppression of false positives with contextual enrichment.
- 24/7/365 expert monitoring and incident response.

Dynamic Risk Scoring (DRS)

Deepwatch MDR provides **real-time risk scoring** for every asset and identity within Sentinel, enabling:

- Severity determination based on business criticality.
- Prioritization of response by correlating behaviors and tactics.
- Adaptive scoring that evolves as telemetry, vulnerabilities, or alerts emerge.

KEY CAPABILITIES

Embedded Threat Intelligence

- ✓ Proprietary and OSINT enrichment within Splunk.
- ✓ Contextual mapping to known threat actors and campaigns.

Deepwatch Security Index™ (DSI)

- ✓ A maturity benchmarking model tailored to a customer's detection and response capabilities.
- ✓ Highlights visibility gaps and detection opportunities.
- ✓ Helps track progress toward measurable cyber resilience.

Operational Transparency

- ✓ Every detection, investigation, and response is visible in both **Microsoft Sentinel** and the **Deepwatch MDR Security Center (portal).**
- ✓ Customers can leverage existing Sentinel workbooks or Deepwatch's advanced dashboards.

AI + Human experts

- ✓ AI accelerates correlation, alert enrichment, and triage.
- ✓ Human analysts validate and respond to high-fidelity threats.
- ✓ AI-adaptive tuning reduces false positives.
- ✓ Continuous collaboration between automated workflows and expert oversight.

www.deepwatch.com/microsoft-sentinel

DEEPWATCH™

CUSTOMER VALUE

Business Benefits

- Maximize ROI on Microsoft Sentinel with faster onboarding and optimized detection content.
- Reduce cyber risk through prioritized detection and accelerated response.
- Achieve operational alignment with existing Azure and Sentinel workflows.
- Deliver board-ready reporting and compliance support.

Technical Benefits

- Automated enrichment and correlation integrated into Sentinel.
- Adaptive hunting and detection based on real-world adversary behavior.
- Seamless integration with Sentinel's native dashboards, workbooks, and playbooks.
- End-to-end visibility and response execution from alert to containment.

WHY NOW? WHY DEEPWATCH?

Microsoft Sentinel delivers immense power but requires deep expertise to tune, maintain, and operationalize. Deepwatch MDR reduces **alert fatigue, complexity, and risk**, ensuring customers get maximum value from Sentinel.

Combined with Deepwatch **Dynamic Risk Scoring** and the **Deepwatch Security Index**™, Deepwatch MDR empowers organizations to outpace modern threats with context-driven prioritization and AI + human-powered response.

Purpose-built. Expert-driven. Sentinel-enhanced.

USE CASES

1. **Advanced Threat Detection:** Spot credential abuse, lateral movement, or exfiltration before damage occurs.
2. **Cloud Monitoring:** Detect IAM risks, misconfigurations, and anomalies across Azure, AWS, and GCP.
3. **Insider Threats:** Identify suspicious access or data movement tied to internal accounts.
4. **Risk-based Prioritization:** Focus on critical systems and high-impact risks.

WHO BENEFITS

- **Security Operations Teams:** Analysts, engineers, and SOC managers needing scalable coverage.
- **Security Leadership:** CISOs and executives requiring measurable outcomes and visibility.
- **Splunk Users:** Organizations heavily invested in Microsoft Sentinel but facing resource or expertise gaps.

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 Ave.
Palo Alto, CA 94306

www.deepwatch.com/microsoft-sentinel