DEEPWATCH™
Always Watching. Always Protecting.

SOLUTION BRIEF

Deepwatch Guardian MDR Platform™ for Splunk

Purpose-Built Integration. Risk-Aligned Detection. Operational Clarity.

OVERVIEW

Splunk is one of the most powerful SIEM platforms available today, but it requires expert care and continuous optimization to maximize its value for threat detection and response. That's where the **Deepwatch Guardian MDR Platform for Splunk** (Deepwatch MDR) comes in.

Purpose-built for Splunk Enterprise and Splunk Cloud Platform, the Deepwatch Guardian MDR Platform enhances customers' existing SIEM investment by adding 24/7/365 monitoring, curated detection engineering, and strategic insights—all fully integrated with Splunk dashboards, data models, and Enterprise Security (ES) workflows.

Deepwatch enables customers to operationalize Splunk more effectively while advancing risk-based security maturity through **Dynamic Risk Scoring** and the **Deepwatch Security Index™.**

WHY DEEPWATCH MDR FOR SPLUNK?

Native Splunk Integration

Deepwatch connects directly into a customer's Splunk instance—on-premises or cloud—without requiring platform changes. Deepwatch ingests, normalizes, and enriches telemetry using Splunk-native tools and dashboards, allowing customers to:

- Onboard new log sources with ease using optimized TAs and CIM alignment
- Maintain customer data where it lives—Deepwatch doesn't duplicate or store logs externally
- Gain transparent visibility into all detections and incidents from within customer's Splunk UI

Continuous Threat Detection & Response

Deewatch team of experts builds and tunes detection rules mapped to MITRE ATT&CK, aligned to a customer's environment, and continuously optimized for performance. This offers:

- Custom SPL-based correlation searches
- False-positive suppression and rule enrichment
- 24/7/365 monitoring by security experts

Detection Risk Scoring

Deepwatch introduces real-time risk scoring for every asset and identity, directly in a customer's Splunk environment which:

- Determines severity based on business criticality
- Prioritizes response by correlating behaviors and threat actor tactics
- Evolves in real time as new 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 Splunk and the Deepwatch MDR Portal (Service Center)
- ✓ Customers can use existing Splunk dashboards or Deepwatch's

Human Experts + AI

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

www.deepwatch.com/mdr-for-splunk

DEEPWATCH™

CUSTOMER VALUE

Business Benefits

- Maximize ROI on Splunk with faster onboarding, tuned content, and full transparency
- Proactive risk reduction through prioritized detection and accelerated response
- Operational alignment with customers' existing Splunk deployment and processes
- Actionable reporting for board-level visibility and compliance support

Technical Benefits

- Automated enrichment, correlation, and analyst-driven decisions
- Adaptive threat hunting and detection based on real-world actor behavior
- Seamless integration with Splunk dashboards, apps, and APIs
- End-to-end visibility and playbook execution from alert to containment

WHY NOW? WHY DEEPWATCH?

Splunk is powerful—but only if operationalized. **The Deepwatch Guardian MDR Platform for Splunk** helps security teams overcome noise, alert fatigue, and tuning complexity with AI-powered enrichment and expert-led response.

Combined with Dynamic Risk Scoring and the Security Index™, Deepwatch MDR provides the guidance, context, and automation necessary to outpace modern threats.

Purpose-built. Expert-driven. Splunk-enhanced.

Learn how Deepwatch can transform your Splunk investment into a fully operational, risk-aware, and mature security operations center.

USE CASES

1. **Advanced Threat Detection:** Catch credential misuse, lateral movement, or data exfiltration before damage is done
2. **Cloud Monitoring:** Identify IAM risks, misconfigurations, and anomalous activity across AWS, Azure, GCP
3. **Insider Threats:** Detect suspicious access or data movement tied to internal actors
4. **Risk-Based Prioritization:** Focus efforts on critical systems and high-impact risks

WHO BENEFITS

- **Security Operations Teams:** Analysts, engineers, and SOC managers needing scalable detection coverage
- **Security Leadership:** CISOs and security leaders seeking operational insight and measurable outcomes
- **Splunk Users:** Teams heavily invested in Splunk 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. Suite 202
Palo Alto, CA 94306

www.deepwatch.com/mdr-for-splunk