DYNAMIC RISK SCORING UNLOCKED

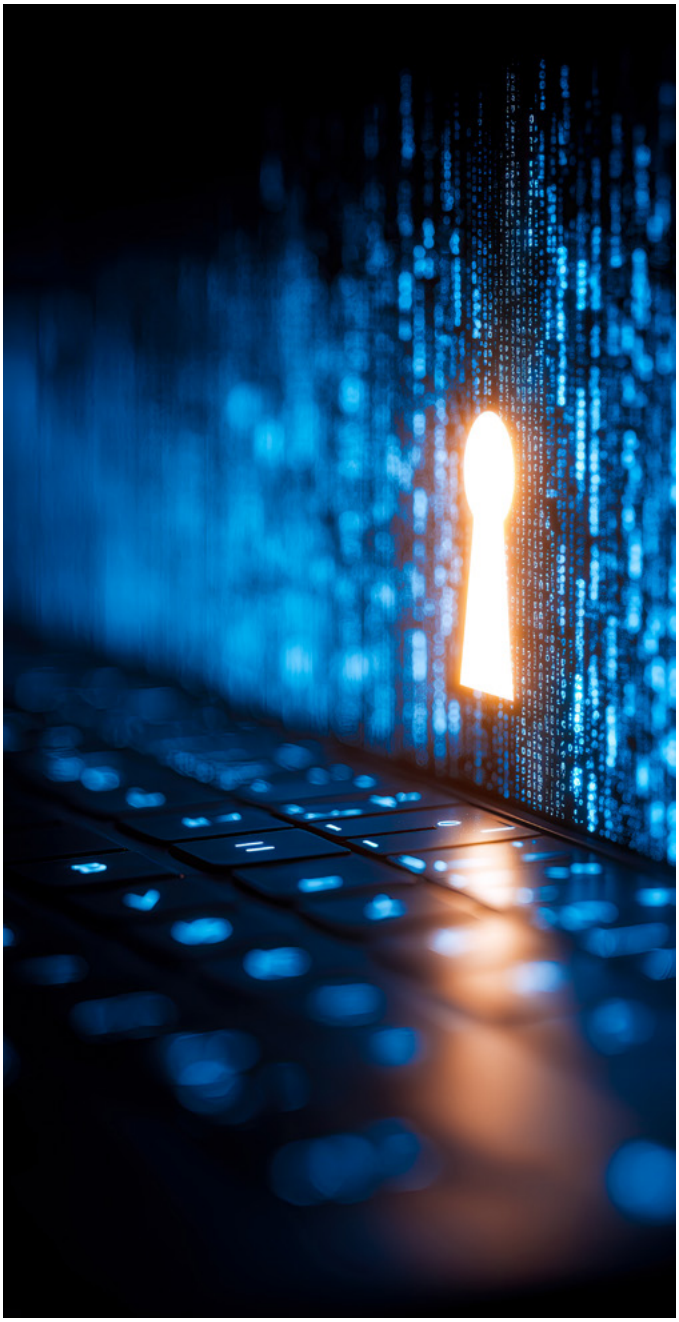
GUIDE

TRANSFORMING MDR WITH DEEPWATCH'S REAL-TIME RISK INSIGHTS

DEEPWATCH™

TABLE OF **CONTENTS**

Deepwatch Dynamic Risk Scoring (DRS) represents a modern, context-aware approach to risk-driven cybersecurity operations, delivering real-time, adaptive prioritization of threats for security teams. Below is a comprehensive guide on Deepwatch DRS.



Executive Summary

Deepwatch DRS is a real-time risk quantification engine foundational to the Deepwatch Guardian MDR Platform™ (Deepwatch MDR). Unlike static risk models that rely on outdated, one-size-fits-all detections, DRS leverages adaptive analytics, ingests multifaceted telemetry and contextual signals. This enables security teams to prioritize, escalate, and expedite their response to cyber threats.

DRS has been proven to reduce alert fatigue by more than 90%, minimize false positives, and provide customers with actionable, continuous risk insights.

Introduction: The Challenge of Modern Cyber Risk

Security teams and operational leaders today are overwhelmed by a sea of high-volume alerts, constantly shifting attack techniques, and increasing regulatory pressure to document risk-based decisions. The result is alert fatigue, prolonged adversary dwell time, and underutilized detection infrastructure.

Traditional "static" alerting has failed to adapt to:

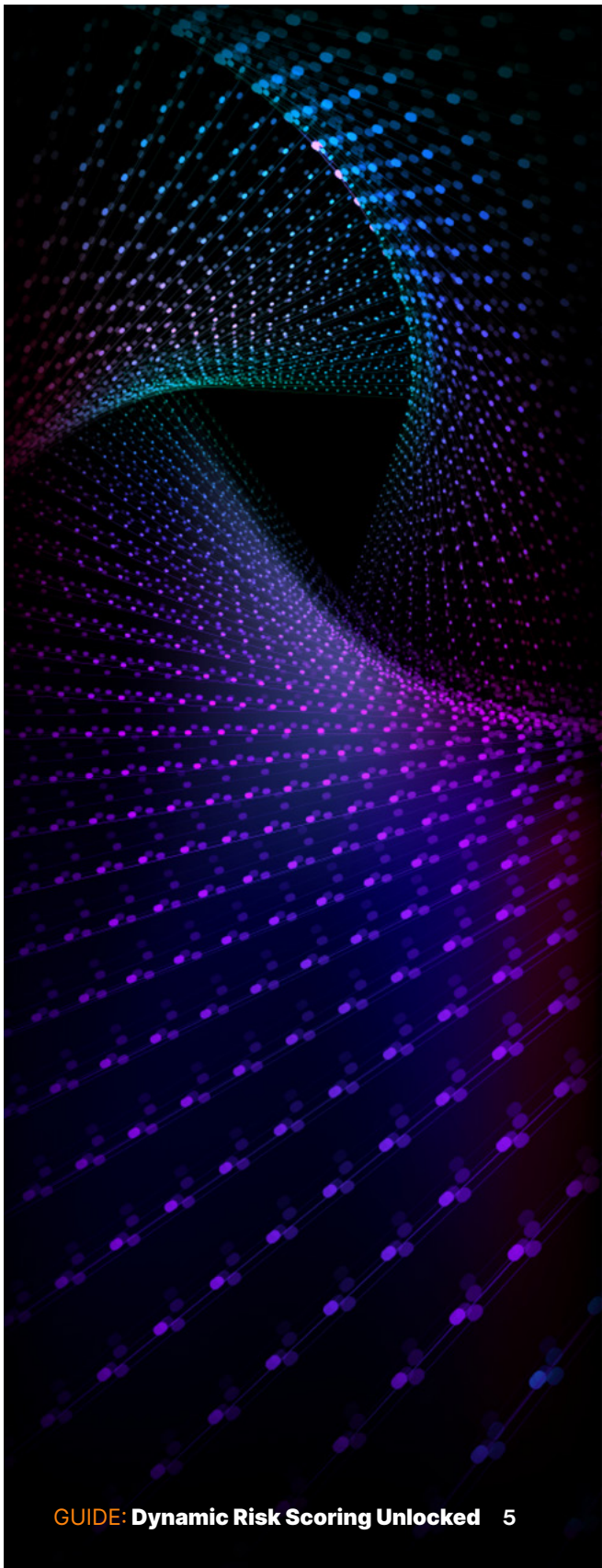
- The velocity of attack evolution and campaign tactics (e.g., ransomware, supply chain attacks).
- Heterogeneous digital environments—cloud, SaaS, remote work, and hybrid IT.
- The need for business-context relevance, including asset criticality, user roles, and operational impact.

Dynamic, real-time risk quantification and response are now essential capabilities for operational SOC and MDR platforms.

The Principles of Dynamic Risk Scoring (DRS)

WHAT MAKES DRS "DYNAMIC"?

- **Continuous Evaluation:** DRS recalculates risk in real time whenever new activity or telemetry data is detected—unlike static models that update on a fixed schedule.
- **Multiple Inputs:** Ingests and analyzes real-time data across 15 attributes, 300+ detections, and 2,500+ signatures to instantly prioritize threats. It also factors in behavioral analytics, asset sensitivity, external intelligence, detection reliability, and environmental context sensitivity, external intel, detection reliability, and environmental context.
- **Contextual Scoring:** Risk scores account for user privileges, asset sensitivity, and access context. The same action receives different risk weightings depending on factors like the user's role, the asset's criticality, device trust level, and location - ensuring that higher-stakes activities are appropriately prioritized.
- **Automated Remediation:** DRS delivers real-time risk scores that can automatically trigger SOAR actions or policy enforcement for rapid containment and response.



The Principles of Dynamic Risk Scoring (DRS) *continued*

TECHNICAL FOUNDATIONS: HOW DRS WORKS

Data Sources and Signal Ingestion

- **Integrated Telemetry:** DRS collects and normalizes signals from SIEM, EDR, firewall, identity providers (e.g., Azure AD, Okta), cloud posture management tools, and vulnerability scanners—providing a unified view across the environment.
- **Behavioral Baselines:** Applies customer-specific logic to establish normal behavior patterns for users, hosts, applications, and workloads. Deviations from these baselines are dynamically scored to surface potential threats.

Multi-Dimensional Risk Evaluation

- **Risk Factor Assigned for Action:** DRS leverages historical risk factors to determine whether a victim, threat actor, or activity has been observed previously. For example, if an action was allowed in the past, it attributes a higher risk score than if the action was blocked.
- **Asset and Environmental Sensitivity:** Consider asset value, compliance classification, exposure surface, and known vulnerabilities to assess contextual risk.
- **Detection Fidelity:** Weighs risk calculations based on MITRE ATT&CK mapping confidence, source reliability, threat intelligence, and incident severity provided by the vendor.
- **Threat Object Correlation:** Correlates related signals and activities to reveal broader campaigns, enabling detection of stealthy, multi-step attacks that traditional signature-based rules may miss.

Scoring Algorithms and Adaptive Models

- **Composite Scoring Engine:** Combines statistical, behavioral, and heuristic models, dynamically tuning thresholds to align with each customer's environment and priorities.
- **Auto-Enabling Detections:** Automatically activates and calibrates relevant detections as new log sources are added, reducing manual configuration and eliminating coverage gaps.
- **Real-Time Adjustment:** Continuously adjusts risk scores based on new threat intelligence and analyst investigations.

The Principles of Dynamic Risk Scoring (DRS) *continued*

OPERATIONALIZING DRS: USE CASES AND OUTCOMES

Alert Prioritization and Fatigue Reduction

- Deepwatch DRS reduces alert volume by more than 90%, surfacing only those events that represent business or operational risk. Analysts spend less time on low-priority investigations and more time on high-value response, reducing dwell time and improving overall efficiency and effectiveness.

Automated Response Playbooks

- **Risk-Based Orchestration:** High-risk scores automatically trigger actions—such as isolating endpoints, revoking credentials, or escalating incidents—in coordination with SOAR and identity platforms, using precisely defined risk thresholds.
- **Active Monitoring:** Lower-risk scores are continuously monitored but deprioritized, reducing noise while maintaining full visibility.

Human Investigation and Validation

- A risk score is calculated for every event. SOC analysts can pivot from an alert to conduct deeper investigations—identifying what else the victim or threat actor may be doing and uncovering related activity.

Reporting and Executive Insights

- DRS aggregates real-time risk data into a dashboard that supports alert investigations, board-level and regulatory reporting, risk quantification, and ongoing security investment decisions.

SLA-Backed Assurance

- Deepwatch supports alert triage and escalations with defined service-level agreements (SLAs), reinforcing customer trust, accountability, and compliance readiness.

Key Benefits at a Glance

- **90%+ Alert Reduction:** Significantly reduces analyst workload and false positives.
- **Real-Time, Context-Aware Detections:** Identifies emerging threats as they evolve, not after periodic reports surface them.
- **Seamless Integration:** Compatible with leading SIEM, EDR, cloud, and identity providers, ensuring minimal friction during onboarding.
- **Business-Aligned Security:** Risk scoring that considers business impact, not just technical severity.
- **Continuous Improvement:** Auto-enabling new detections and adaptive thresholding keep risk models current and effective.

Competitive Differentiation and Market Position

DEEPWATCH DRS STANDS OUT IN THE MDR LANDSCAPE BY OFFERING:

- Transparent, real-time, contextually adaptive risk scoring powered by 15 attributes, 300+ detections, and 2,500+ signatures for instant threat prioritization.
- Proven methodologies that reduce alert noise and accelerate response.
- Native integration with leading SIEM, cloud, and enterprise platforms—no rip-and-replace required.
- SLA-backed response guarantees that reinforces accountability and trust.

Other MDR and SIEM vendors may provide "risk scores," but they often lack the comprehensive automation, depth of data inputs, SLA commitments, and seamless platform integration that define Deepwatch's DRS approach.

DRS in the Modern SOC: Workforce Enablement and Outcomes

ANALYST EXPERIENCE

- Less time wasted on low-fidelity events.
- Streamlined triage workflows—with prioritized, pre-contextualized alerts.
- Direct access to playbooks and orchestration, reducing mean time to resolution.

CISO AND EXECUTIVE IMPACT

- Clear, defensible prioritization of security investments.
- Reporting aligned to business risk and compliance requirements.

BOARD AND REGULATORS

- Quantifiable risk reduction metrics.
- SLAs and continuous improvement evidence, supporting cyber insurance and compliance needs.

Frequently Asked Questions

HOW DOES DRS ADDRESS ALERT OVERLOAD?

By applying adaptive risk scores based on real-time analysis powered by 15 attributes, 300+ detections, and 2,500+ signatures, DRS filters and prioritizes alerts so analysts only receive actionable insights, reducing noise by more than 90%.

CAN DRS BE USED OUTSIDE OF SPLUNK?

While DRS is SIEM-dependent, it ingests data from a broad ecosystem of EDR, cloud, network, and SaaS platforms, adapting seamlessly to multi-cloud and hybrid environments.

DOES DRS AUTOMATE INCIDENT RESPONSE?

Yes. DRS powers automated playbooks and remediations through integrated SOAR and identity orchestration, reducing time to contain active threats.

IS DRS CUSTOMIZABLE FOR DIFFERENT RISK TOLERANCES?

Tuning and some baselines can be customized for each customer; however, the core scoring model remains consistent. Customers can modify assets/identities, base scores, and designate high-risk countries.

Conclusion

Deepwatch DRS represents a paradigm shift for MDR customers, transitioning from manual, reactive security to automated, business-aligned, and risk-prioritized defense. By leveraging advanced, multi-source heuristics and behavioral analytics, DRS enables organizations to reduce operational overhead, rapidly adapt to new threats, and deliver measurable business value through reduced risk exposure and improved analyst efficiency.

DEEPWATCH™
Always Watching. Always Protecting.™

Contact Sales at Deepwatch to
Secure your enterprise with Dynamic Risk Scoring

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.

Learn More:
www.deepwatch.com

Follow us:
Blog | LinkedIn | Facebook