DEEPWATCH™
Always Watching. Always Protecting.™

SOLUTION BRIEF

Deepwatch CTEM: Preemptive and Proactive Threat Defense

Unified Context for Intelligent Security Operations

OVERVIEW

Modern security teams face a flood of evolving threats, complex investigation workflows, and evolving attacker techniques. Deepwatch Continuous Threat Exposure Management (Deepwatch CTEM) transforms detection and response with dynamic automation, seamless enrichment, and unified incident context. By connecting people, processes, and tools, Deepwatch CTEM empowers SOCs to correlate, prioritize, and respond to threats—faster and more accurately.

Deepwatch CTEM enables preemptive and proactive defense at scale—breaking down data silos, orchestrating enrichment, and automating remediation of threats before they can be exploited.

WHY DEEPWATCH CTEM?

Automated, High Context Enrichment

Deepwatch CTEM automatically aggregates signals from your existing technology stack, enriching each with threat intelligence, asset, vulnerability, and user context. This transforms raw signals into actionable incidents for SOC teams, reducing response time and ensuring no threat is missed.

Smart Orchestration + Human Expertise

Deepwatch CTEM's no-code playbooks let security teams automate investigation and response across the Deepwatch Guardian MDR Platform™ (Deepwatch MDR) and broader security stack—while retaining analyst oversight. From triage to remediation, processes are fast, consistent, and auditable. Every incident is also expert-reviewed for continuous improvement.

Continouse Threat Exposure Management Enhances Deepwatch MDR

Built to work with Deepwatch MDR, Deepwatch CTEM amplifies the value of managed detection and response by providing real-time correlation, context, and automation—right where teams need it.

KEY BENEFITS

- **Business Insights:** Deepwatch CTEM translates technical cyber data into clear, business-focused insights and reports that executives and boards can act on.
- **Agentic AI:** The agentic AI interface lets security leaders generate tailored business impact reports on demand without relying on manual analyst effort.
- **Real-time Signal Aggregation:** Collects and normalizes signals and telemetry from EDR/XDR, cloud, identity, and network sources.
- **Context-driven Triage:** Automatically enriches incidents with internal and external threat intel, asset data, and vulnerability status.
- **Dynamic Automation:** No-code workflows automate investigations, approvals, and responses (e.g., user disablement, network quarantine).
- **Expert-Validated Outcomes:** Every critical workflow can include approval and oversight steps by Deepwatch or in-house analysts, maximizing security and auditability.

DEEPWATCH™

CUSTOMER VALUE

Business Benefits

- Transitions security operations from reactive (responding to incidents) to proactive and preventive strategies—detecting risks and closing gaps before a breach occurs.
- Helps find the needles in the haystack—top 3 prioritization.
- Board-level reports on metrics that show the business impact of critical risks.
- Reduces mean time to resolution (MTTR) and business risk.
- Extends Deepwatch MDR's reach via seamless automation and orchestration.
- Ensures compliance with evidence and audit trails for actions taken.

Technical Benefits

- Unified incident context slashes signal fatigue.
- Drag-and-drop playbooks accelerate the onboarding of new processes.
- Scalable, tested integrations covering leading security controls.
- Optional human-in-the-loop for high-risk actions.
- Frees analysts for higher-value work by automating signal triage.

WHY NOW?

Attackers move fast—and manual response isn't enough. Deepwatch CTEM closes the loop with automation, context, business risk impact and trusted human oversight—so you can see threats sooner and stop them before they impact your organization.

ABOUT CONTINOUS THREAT EXPOSURE MANAGEMENT (CTEM)

Deepwatch CTEM delivers intelligent automation for modern security teams, combining dynamic workflows, deep integrations, and continuous learning. Deepwatch CTEM enables Deepwatch MDR customers to operationalize detection, investigation, and response with greater confidence and lower risk.

USE CASES

1. **Proactive Risk and Threat Exposure Management**
   Deepwatch CTEM's AI continually scans critical assets, identifies vulnerabilities, and prioritizes exposures based on business impact. This allows security teams to fix issues before attackers can exploit them, shifting operations from reactive to proactive risk mitigation.
2. **Unified, Real-time Visibility into Security Posture**
   Deepwatch CTEM aggregates and normalizes data from diverse security tools (SIEM, EDR, CNAPP, AppSec, etc.), providing a holistic, real-time picture of the organization's risk surface. This unified view expedites up investigations and supports more transparent executive reporting.
3. **Automated Risk Analytics and Compliance Reporting**
   Deepwatch CTEM automates the process of risk analysis and compliance validation. With customizable dashboards and real-time data, security teams can demonstrate to executives exposure reduction, compliance status, and progress toward regulatory goals.
4. **Accelerated Detection and Response**
   By correlating telemetry data with threat intelligence, Deepwatch CTEM enables faster detection of active threats, targeted attacks, and suspicious behaviors. This allows for rapid response, containment, and detailed forensics with minimal operational overhead.
5. **Seamless Integration and Ecosystem Connectivity**
   Deepwatch CTEM supports extensive integration across enterprise security and business tools, ensuring organizations can maximize current investments while expanding security coverage. This flexibility allows for broad adoption and reduces vendor lock-in, all while driving greater automation across the security ecosystem.

WHO BENEFITS

- **Security Operations:** SOC Managers, Analysts, Threat Intel teams.
- **Security Leadership:** CISOs, VPs, Risk and Compliance Managers.
- **Regulated Industries:** Financial Services, Healthcare, Retail, Manufacturing, and any MDR customer seeking improved visibility, automation, and compliance.

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/continuous-threat-exposure-management