DEEPWATCH™
Always Watching. Always Protecting.™

SOLUTION BRIEF

# Deepwatch Active Response for Identity and Endpoint

Accelerate Threat Containment. Reduce Risk. Operate with Confidence.

## OVERVIEW

Deepwatch Active Response for Identity and Endpoint extends the power of the Deepwatch Guardian MDR Platform™ by enabling rapid, decisive action against threats—when and how you choose.

Rather than stopping at detection, Deepwatch empowers your organization to **contain threats in real time**, minimizing impact and reducing attacker dwell time. With flexible execution options and expert oversight, you stay in control while benefiting from automated and analyst-driven response.

Active Response is **opt-in and fully customizable**, ensuring alignment with your organization's risk tolerance, operational workflows, and security priorities. *This capability is currently available for customers leveraging Splunk and Google SecOps within their MDR deployment.*

## WHY IT MATTERS

Modern attacks move fast—your response should too.

With Deepwatch Active Response for Identity and Endpoint, you can:

- **Stop threats earlier** by taking action at the first sign of compromise
- **Reduce operational burden** with automation and expert-led response
- **Minimize business disruption** through precise, policy-driven containment
- **Maintain control** with approval workflows and customizable response policies
- **Extend your team** with Deepwatch experts executing on your behalf

## HOW IT WORKS

Deepwatch collaborates with your team to build a custom **Active Response Matrix**, defining:

- ✓ **When response actions are triggered**
- ✓ **What actions are allowed**
- ✓ **Who approves or authorizes actions**
- ✓ **How actions are executed across endpoint and identity systems**

Every action is performed in alignment with your defined policies, supported integrations, and granted permissions—ensuring transparency and control at every step.

## FLEXIBLE RESPONSE MODES

Adapt response to your environment and risk appetite:

**Monitor Mode (What-If)**

- Validate decisions before enabling actions
- Full visibility with zero risk

**Approval-Based Response**

- Human-in-the-loop control (customer or Deepwatch analyst)
- Ideal for business hours or sensitive actions

**Fully Autonomous Response**

- Immediate, automated containment
- Best for high-confidence threats or off-hours protection

DEEPWATCH™

## COMPREHENSIVE THREAT COVERAGE

Active Response spans both **endpoint and identity attack surfaces**, enabling coordinated defense across your environment.

**Identity Threats**

- Account compromise and risky sign-ins
- Phishing and adversary-in-the-middle attacks
- Suspicious authentication and session activity
- Mailbox manipulation and threat intelligence matches

**Endpoint Threats**

- EDR-detected incidents (CrowdStrike, Defender, SentinelOne)
- Malware, exploit tools, and ransomware behavior
- Credential abuse (Pass-the-Hash / Pass-the-Ticket)
- Lateral movement and attacker tooling

## RESPONSE ACTIONS THAT MAKE AN IMPACT

Take decisive action to contain threats instantly:

**Identity Threats**

- Reset passwords
- Disable compromised accounts
- Revoke sessions and force reauthentication

**Endpoint Threats**

- Terminate malicious processes
- Isolate compromised hosts

## SEAMLESS ONBOARDING & CONTINUOUS OPTIMIZATION

- Start safely in **monitor mode** to evaluate impact
- Transition to active response with guided onboarding
- Continuously refine policies with Deepwatch experts

Your response strategy evolves alongside your environment—ensuring ongoing effectiveness without added complexity.

## REQUIREMENTS

- **Endpoint:** Read/Write access to supported EDR platforms
- **Identity:** Write access to identity providers (Okta, Microsoft Entra ID)
- **Approval workflows:** Slack (or equivalent) for customer-approved actions

## THE DEEPWATCH ADVANTAGE

With Deepwatch Active Response for Identity and Endpoint, Deepwatch goes beyond detection—delivering **actionable security outcomes:**

- Faster containment and reduced attacker dwell time
- Lower risk of breach escalation
- Increased security team efficiency
- Confidence in every response decision

**Contain threats faster.**
**Respond smarter.**
**Stay in control.**

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