DEEPWATCH™
Always Watching. Always Protecting.™

DATA SHEET

# Active Response for Identity

## Automated Identity Containment—With Control You Can Trust

## OVERVIEW

Identity-based attacks are now the fastest path to compromise. Techniques such as password spraying, risky authentications, malicious infrastructure use, and mailbox rule abuse allow attackers to bypass traditional controls and move laterally with speed.

Detection alone is no longer enough. Organizations increasingly expect their MDR provider to help **contain identity threats quickly**, without introducing unnecessary operational or business risk.

**Active Response for Identity** extends Deepwatch's managed detection capabilities with **precision identity response actions**, executed only when—and how—you choose.

## THE DEEPWATCH DIFFERENCE

Active Response for Identity is designed to balance **speed, safety, and trust.**

**It does this through four core principles:**

- **Opt-in by design—**no changes to your environment by default
- **Risk-aware automation—**responses align to your tolerance and intent
- **Service-led execution—**guided by Deepwatch analysts, not generic playbooks
- **Focused scope—**built around high-confidence identity detections

This ensures response actions are intentional, predictable, and auditable.

## SUPPORTED IDENTITY RESPONSE ACTIONS

When enabled, Deepwatch can execute the following identity containment actions:

- **Password Reset**
- **Session Revocation**
- **Account Disablement**

Actions are performed only under customer-approved conditions and execution modes.

## SUPPORTED IDENTITY DETECTIONS (INITIAL SCOPE)

Active Response for Identity is available for a curated set of high-confidence detections, including:

- High-Risk Authentication
- Successful Login After Password Spray Activity
- Unusual Foreign Authentication
- Authentication from Malicious ASN
- Suspicious Authentication Patterns
- Threat Intelligence–Matched Authentication Sources
- O365 Suspicious Mailbox Rule Activity

This focused approach ensures automation is applied where it is most effective.

DEEPWATCH™

## YOU CONTROL HOW RESPONSE IS EXECUTED

Active Response for Identity is configured collaboratively using a Response Intent Matrix, allowing you to define:

- Which detections trigger response
- Which identity actions are taken
- Under what conditions (identity, network, risk, and time-based context)
- How actions are executed:
  - ▶ Monitor-only (observe what would happen)
  - ▶ Analyst-approved
  - ▶ Customer-approved
  - ▶ Fully automated

Execution modes can vary by business hours, off-hours, and weekends.

## WHAT'S NEXT?

Active Response for Identity launches first on Splunk, with expansion planned across additional SIEM platforms, endpoints, networks, and cloud environments.

## IDENTITY PLATFORM INTEGRATION

As part of the Deepwatch Guardian MDR Platform™, Deepwatch maintains read access to identity providers.

Active Response for Identity requires **customer-approved write permissions** for supported platforms (e.g., Okta and Microsoft Entra ID) to execute response actions. Permissions are scoped strictly to approved actions and policies.

okta Microsoft Entra

## WHY CUSTOMERS CHOOSE ACTIVE RESPONSE FOR IDENTITY

- Reduce time to contain identity-based attacks
- Minimize attacker dwell time and lateral movement
- Eliminate response delays during off-hours
- Maintain full control over automation and risk

## BUILT FOR TRUST

- Active Response for Identity is never enabled by default
- Customers can start in monitor mode to validate behavior safely
- Different identities (e.g., employees vs. executives) can be treated differently
- Automation increases only as confidence increases

This enables organizations to adopt automation at their own pace.

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