Today, securing enterprises is harder than ever. With the growth of remote workforces, the migration of data from on-premise to the cloud, and an increased reliance on third parties, the attack surface continues to expand in size and complexity.

Speed of detection and coordination of response is critical to minimizing the impact of a cyber attack. To realize real security benefits requires cutting through alert noise to rapidly detect real threats, along with the ability to quickly mitigate identified threats across the environment, while ensuring completeness of response.

Deepwatch Active Response is added to or combined with Deepwatch MDR to help minimize the impact of threats by taking automated response actions to stop attacks in their tracks throughout your complex environment.

Benefits of Deepwatch Active Response
- Reduced security risk with continuous monitoring and threat hunting, identifying and mitigating threats before they can cause harm
- Reduce MTTR to seconds with automated rapid response across endpoint, network, and identity
- Ensure consistency and completeness with automated response, using tailored playbooks and existing security tools
- Realize XDR-delivered outcomes at lower TCO compared to product-based approaches
- Leverage existing security investments and best-in-class security tools with no single-vendor lock-in required

Deepwatch SecOps Platform
- Active Response
- Endpoint Detection & Response
- Vulnerability Management
- Firewall Management
- Cyber Threat Intel
- Threat Analytics
- Malware Analysis
- Precision Response
- Machine Learning

SECURITY TOOLS | SIEM & SOAR | CURATED THREAT INTEL

www.deepwatch.com
Deepwatch **Active Response**

Deepwatch Active Response services leverage high-fidelity, contextualized alerts from the Deepwatch SecOps Platform to deliver automated precision responses across the enterprise. Deepwatch Active Response services are used in combination with Deepwatch's Managed Detection and Response (MDR) service. Deepwatch Active Response integrates with best-of-breed security technologies via API.

- **Deepwatch Active Response for Endpoint** provides automated response capabilities for threat containment on endpoints to support ransomware mitigation strategies. The solution integrates with Crowdstrike, Microsoft Windows Defender, and SentinelOne.

- **Deepwatch Active Response for Identity** extends the native security capabilities of identity provider tools by monitoring and correlating detections across the entire attack surface. Active Response for Identity delivers contextualized alerts on potentially compromised identities and rapidly executes critical response actions such as isolating, reducing privileged access or enforcing step-up authorization against a session to contain the threat. Response actions can be configured based on risk tolerance. The solution integrates with Okta, Ping Identity, and Azure AD.

Deepwatch **Active Response in Action**

The Deepwatch SecOps Platform collects, processes, and analyzes security telemetry from numerous controls and data sources in order to detect and mitigate complex threats. To ensure high-fidelity alerting, alerts are created and analyzed using a combination of anomaly detection and advanced correlation of security events over a period of time. They are then further enriched, contextualized, and processed through Deepwatch Threat Analytics technology that combines all related alerts pertaining to the risk or threat objects to deliver a complete picture of the threat. The Deepwatch SecOps Platform initiates a response action on the asset or identity identified in the initial alert, executing a rapid response across endpoint, network, and identity.