deepwatch™

DATA SHEET

Active Response

Automated Precision Response for Cyber Resilience

OVERVIEW

As the threat landscape continues to evolve and increase in complexity, enterprises must do more to protect themselves. Traditionally, defending against relentless attackers requires specialized expertise, multiple costly technology investments, and constant vigilance.

Speed of detection and coordination of response are most critical to minimize the impact of a cyber attack. Effective detection requires cutting through alert noise to rapidly detect real threats, combined with the ability to quickly mitigate identified threats across the environment, ensuring precise response.

Deepwatch Active Response is added to Deepwatch MDR to help minimize the impact of threats by establishing automated response actions across multiple security tools.

ADVANTAGE

The Deepwatch 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, alerts are created and analyzed using a combination of anomaly detection and advanced correlation of security events over a period of time.

Alerts are then further scored, enriched, contextualized, and processed through Deepwatch threat analytics technology, combining related alerts pertaining to a single risk object to prescribe a precise response. Response actions address the asset or identity identified in the initial alert, executing a rapid response across endpoint, network, and identity.

ACTIVE RESPONSE BENEFITS

- ✓ 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™

DEEPWATCH ACTIVE RESPONSE SERVICE

Automated Precision Response

Deepwatch Active Response services leverage high-fidelity, contextualized alerts from the Deepwatch Security Center to deliver automated precision response across the enterprise. Deepwatch Active Response is used in combination with Deepwatch's MDR service as part of an advanced enterprise security effort. We deliver Active Response through integration with industry-standard security technologies such as AWS, Splunk, Crowdstrike and others via API.

ENDPOINT

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

CROWDSTRIKE | Microsoft Defender | SentinelOne

IDENTITY

Deepwatch Active Response for Identity with our co-managed Identity Management effort, Deepwatch Active Response for Identity extends the native security capabilities of identity provider tools by monitoring and correlating detections across the entire attack surface. We deliver contextualized alerts on potentially compromised identities and rapidly execute 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. Our solution integrates with Okta and Azure AD.

okta | Azure

FIREWALL

Deepwatch Active Response for Firewall our co-managed firewall service enables automated addition and removal of Indicators of compromise and malicious URLs in response to both global and custom Deepwatch detections or alerts. This features dedicated Firewall engineers and the use of our dynamic block lists. Our solution integrates with Palo Alto Networks, Fortinet, Checkpoint, and Cisco firewalls.

paloalto NETWORKS | CHECK POINT | FORTINET | CISCO

deepwatch™

ABOUT DEEPWATCH

Deepwatch is the leading managed security platform for the cyber resilient enterprise. Our platform combines comprehensive threat management capabilities, expert practitioners, and precise automated actions. Embrace preventative actions to improve your security posture and enhance your speed of response. Join leading global brands relying on Deepwatch for cyber resiliency and security peace of mind.

CONTACT US

GET STARTED

4030 W Boy Scout Blvd. Suite 550
Tampa, FL 33607

www.deepwatch.com