

**SOLUTION BRIEF**

# Deepwatch & CrowdStrike Joint Solution Brief

## Endpoint Detection and Response

### OVERVIEW

After rigorous testing and customer feedback, Deepwatch selected Falcon Insight as its platform to deliver Managed Endpoint Detection & Response (MEDR) services to our customers.

Falcon Platform enables Deepwatch to protect and defend customer networks by fully managing their endpoint threat detection and response program. Falcon Insight is fully integrated with our Cloud SecOps Platform, enabling Deepwatch to manage endpoint detection, behavior analytics, and response to threats and anomalous behaviors on the network.

### DEEPWATCH & FALCON INSIGHT USE CASE

Deepwatch leverages Falcon Insight as a single endpoint threat detection and response technology. Customers are able to take advantage of the full Falcon Insight feature set quickly and effectively when partnering with Deepwatch to manage the implementation, followed by continuous monitoring, tuning, and response. Deepwatch covers a variety of important use cases that bring compelling value to our customers.

- **Next Generation Antivirus Protection**  
Falcon Prevent replaces legacy Antivirus solutions and allows Deepwatch to modernize customer endpoint threat detection practices
- **Host Level Firewall Management**  
Deepwatch is able to manage customer firewalls at the host level and is able to enhance firewall threat detection and mitigation
- **Endpoint Forensics and Historical Data**  
Falcon Insight delivers continuous, comprehensive endpoint visibility that spans detection, response and forensics to ensure nothing is missed and potential breaches are stopped (company sponsored and BYOD). Deepwatch provides rich threat context and endpoint data so that security teams know exactly what happened on the endpoint, how it happened, and how to stop the threat from moving laterally within the environment
- **Automated Threat Remediation**  
With Falcon Insight, Deepwatch provides specific information on which endpoints have been compromised and how to resolve security incidents. Deepwatch configures real-time automated response policies to isolate hosts, delete files, kill processes and/or initiate scans

### JOINT SOLUTION BENEFITS

- **Next Generation Antivirus Protection**
- **Host Level Firewall Management**
- **Endpoint Threat Detection and Response**
- **Rich Threat Intelligence for Immediate Response**

### ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered next generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next generation antivirus (AV), endpoint detection and response (EDR), and a 24/7 managed hunting service — all delivered via a single lightweight agent.

### 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

4030 W Boy Scout Blvd. Suite  
550 Tampa, FL 33

[GET STARTED](#)