CROWDSTRIKE

CROWDSTRIKE **FALCON INSIGHT™** ENDPOINT DETECTION AND RESPONSE

STREAMING THE THREAT DETECTION AND RESPONSE LIFECYCLE WITH SPEED, AUTOMATION AND UNRIVALED VISIBILITY

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. Falcon Insight solves this by delivering complete endpoint visibility across your organization. Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. All endpoint activity is also streamed to the CrowdStrike Falcon® platform so that security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

FALCON INSIGHT IS THE INDUSTRY LEADER IN EDR
"Best Behavior Analytics/Enterprise Threat Detection"
Security Magazine Award 2017

"Perfect Detection Score" (5/5) and "Perfect Cost Score"
(value for the money) in 2017 Forrester Endpoint Security Wave

Scored "Strong" (highest rating possible) in all use cases evaluated in Gartner's 2017 Comparison of Endpoint Detection and Response Technologies and Solutions report

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities** — Insight uses IOAs (indicators of attack) to automatically identify attacker behavior and sends prioritized alerts to the Falcon UI, eliminating time-consuming research and manual searches.

KEY BENEFITS

» Detect advanced threats automatically

» Speed investigations with real-time forensics

» Remediate with confidence

» Conduct five-second enterprise searches

» Enable Falcon OverWatch™ threat hunting service

- **Unravel entire attacks on just one screen** — An easy-to-read process tree provides full attack details in context for faster and easier investigations.
- **Accelerate investigation workflow** — The intuitive UI allows you to pivot and run searches across your entire organization in seconds.
- **Gain context and intelligence** — Integrated threat intelligence delivers the complete context of an attack, including attribution.
- **Contain suspect systems in just one click** — It instantly puts an end to adversary activity by containing compromised systems.

GAIN FULL-SPECTRUM VISIBILITY IN REAL TIME

- **Observe every move in real time** — Immediate visibility allows you to view the activities as if you were "shoulder surfing" the adversary.
- **Capture critical details for forensic investigations** — Falcon Insight kernel-mode driver captures over 200 events and related information necessary to retrace incidents.
- **Get answers in seconds** — The CrowdStrike Threat Graph™ database stores event data and answers queries in five seconds or less, even across billions of events.
- **Recall for up to 90 days** — Falcon Insight provides a complete record of endpoint activity over time, whether your environment consists of fewer than 100 endpoints or more than 500,000.

IMMEDIATE TIME-TO-VALUE

- **Save time, effort and money** — Cloud-enabled Falcon Insight is delivered by the CrowdStrike Falcon™ platform and does not require any on-premises management infrastructure.
- **Deploy in minutes** - CrowdStrike customers can deploy the cloud-delivered Falcon agent to up to 70,000 endpoints in less than a single day.
- **Immediately operational** — With unmatched detection and visibility from Day One, Falcon Insight hits the ground running, monitoring and recording on installation without requiring reboots, fine-tuning, baselining or complex configuration.
- **Zero impact on the endpoint** — With a lightweight agent that requires only a 20MB footprint on the endpoint, searches take place in the Falcon Threat Graph™ database without any performance impact on endpoints or the network.

THE POWER TO PREVENT SILENT FAILURE AND STOP BREACHES

Prevention technologies are not perfect. If attackers manage to bypass your organization's defenses, they can go unnoticed for weeks or months because security teams lack the visibility and detection tools to identify post-breach activity. This period of "silent failure" spells success for the attacker and potential disaster for the organization. Falcon Insight quickly detects, identifies and allows you to respond to incidents that are invisible to existing defenses.

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, endpoint detection and response (EDR),and a 24/7 managed hunting service — all delivered via a single lightweight agent.

Learn more at **crowdstrike.com**