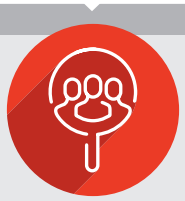
CROWDSTRIKE

CROWDSTRIKE FALCON OVERWATCH MANAGED THREAT HUNTING

STOP INCIDENTS BEFORE THEY TURN INTO BREACHES



FALCON OVERWATCH — STOPPING THE MEGA BREACH

Falcon OverWatch is a managed threat hunting service built on the CrowdStrike Falcon platform to ensure that threats don't get missed and ultimately, to prevent a mega breach. This service is comprised of an elite team of security experts who proactively hunt, investigate and advise on threat activity in your environment. When they find a threat, they work alongside your team to triage, investigate and remediate the incident, before it has the chance to become a full-blown breach.

KEY PRODUCT FEATURES

MANAGED THREAT HUNTING SERVICES LIKE NO OTHER

- **Built on the Falcon Platform** — The Falcon platform enables OverWatch to process more than 40 billion events per day. The seamless integration with the powerful Falcon platform allows customers to receive OverWatch protection instantly, without requiring additional deployments or infrastructure.
- **24/7 Operational Readiness —** The Falcon OverWatch™ team identifies and stops more than 15,000 breach attempts a year thanks to the expertise gained from daily "hand-to-hand combat" with sophisticated adversaries. In addition, the OverWatch team is poised to take action on your behalf, within seconds, if required.
- **The Power of the Crowd —** Leveraging the power of the crowd, OverWatch can identify new and emerging threats and instantly protect you and all customers against an attack detected in only one environment. We call that "community immunity."

KEY BENEFITS

» Threat Hunting — Proactively hunts for threats in your environment on a 24x7x365 basis, eliminating false negatives

Alert Prioritization — Uniquely pinpoints the most urgent threats in your environment and resolves false positives

Guided Response — Threat hunters partner with your security operations team to provide clarity on an attack and guidance on what to do next

"OverWatch contacted me a week ago to tell me that they had detected some activity that was associated with a known server-hijacking organization. Their call allowed us to go in and address that very issue specifically. OverWatch very quickly responded and said, 'Here's the information that we know about this.' Their actions prevented us from having one of our servers sold on the black market for spammers or other bad actors to use."

— MARK SAUER, DIRECTOR OF INFORMATION TECHNOLOGY, TRANSPAK

- **Eliminate alert fatigue —** OverWatch finds, investigates and prioritizes suspicious activities that might indicate an active attack. This allows OverWatch to identify and notify you of real threats only, eliminating alert fatigue and the drain of chasing false positives.

WORLD-CLASS SECURITY EXPERTS BY YOUR SIDE AROUND THE CLOCK

- **Instantly multiply your security capabilities —** Falcon OverWatch is a team of dedicated, proactive threat hunters working for you 24/7, augmenting the detection and protection offered by your current security team and security solutions.
- **Expert advice when you need it most —** OverWatch provides actionable alerts with remediation recommendations. The alerts are individually crafted to provide the detailed analysis you need to understand how to respond, allowing you to implement mitigation steps immediately, considerably reducing time to resolution.
- **Get an edge on attackers —** Benefit from having elite security experts by your side, not just technology, to outmatch sophisticated human attackers and insider threats.

INSTANTANEOUSLY ENJOY THE VALUE OF NEXT-GENERATION PROTECTION

- **Save time, effort and money —** OverWatch leverages cloud-native Falcon Insight™ and the CrowdStrike Falcon® platform, which do not require any on-premises management infrastructure, to provide a turnkey endpoint security solution at a fraction of the cost of a fully staffed on-premises SOC.
- **Immediately operational —** It provides managed threat hunting from the get-go. Falcon OverWatch hits the ground running, monitoring and recording immediately upon installation without requiring reboots, fine-tuning, baselining or complex configuration.
- **Zero impact on the endpoint —** CrowdStrike Falcon requires only a 20MB footprint on the endpoint from initial installation to ongoing day-to-day use. In addition, searches take place in the Falcon Threat Graph™ database and do not impact endpoints or the network.

PREVENT INCIDENTS FROM BECOMING BREACHES

Human investigation is often required to identify cutting-edge targeted attacks using stealthy techniques. That's why Falcon OverWatch has been designed to hunt, investigate and quickly 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**