CROWDSTRIKE

FALCON OVERWATCH MANAGED THREAT HUNTING

See and stop hidden advanced attacks

FALCON OVERWATCH — STOPPING THE MEGA BREACH

Falcon OverWatch™ is CrowdStrike's managed threat hunting service, built on the CrowdStrike Falcon® platform. OverWatch provides deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft that is designed to evade standard security technologies.

OverWatch is comprised of an elite team of cross-disciplinary specialists who harness the massive power of the CrowdStrike Threat Graph®, enriched with CrowdStrike threat intelligence, to continuously hunt, investigate and advise on sophisticated threat activity in customer environments. Armed with cloud-scale telemetry and detailed tradecraft on more than 130 adversary groups, OverWatch provides unparalleled ability to see and stop the most advanced threats.

"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 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

KEY BENEFITS

See and stop hidden advanced attacks: The OverWatch team hunts relentlessly to see and stop the stealthiest sophisticated threats: the 1% of 1% of threats that blend in silently and lead to a breach if they remain undetected.

Achieve maximum effectiveness and efficiency: OverWatch delivers the best results by augmenting skilled analysts with the most advanced technology. CrowdStrike's elite human experts use cloud-scale data, custom tools and up-to-the-minute threat intelligence to hunt with unprecedented speed and scale.

Gain a seamless extension of your team: As a core component of the Falcon platform, OverWatch delivers results for organizations of all sizes, operating as a seamless extension of your team — minimizing overhead, complexity and cost.

KEY PRODUCT CAPABILITIES

24/7 HUMAN EXPERTISE

- **Attacker mentality:** Effective threat hunting requires the ability and expertise to think like an attacker.
- **Cross-disciplinary expertise:** OverWatch employs elite experts from a wide range of backgrounds, including government, law enforcement, commercial enterprise, the intelligence community and defense.
- **24/7/365 availability:** When a sophisticated intrusion occurs, time is critical. Your adversaries do not sleep and are not restricted by time zones or geography — and neither should your threat hunting team.
- **Continuous vigilance:** OverWatch's continuous, proactive operations deliver results every minute of every day.
- **Finely tuned response:** OverWatch identifies and responds to hundreds of potential breaches per week. Each threat handled helps team members fine-tune their skills and processes, ensuring they are always sharp and effective.

CLOUD-SCALE SECURITY TELEMETRY

- **Tools for the hunt:** Threat hunting requires more than just expert hunters — those hunters need the right tools. Scalable and effective threat hunting requires access to vast amounts of data and also the ability to mine that data in real time for signs of intrusions.
- **Real-time visibility:** OverWatch takes advantage of the cloud-scale telemetry of the proprietary CrowdStrike Threat Graph to get broad, deep visibility, delivered in real time.
- **Massive data:** Threat Graph ingests trillions of events each week, giving Falcon OverWatch an extensive, global real-time view of threat activity, as it happens.

UP-TO-THE-MINUTE THREAT INTELLIGENCE

- **Threat context:** You can't detect a threat you don't understand.
- **CrowdStrike threat intelligence:** This intel empowers OverWatch with detailed, always-current knowledge of tradecraft from more than 130 adversaries.
- **Current TTPs:** This intimate knowledge of the latest TTPs (tactics, techniques and procedures) in use today ensures that OverWatch is able to hunt effectively and efficiently.

SEAMLESS PART OF THE FALCON PLATFORM

- **One team, one fight:** OverWatch operates as an extension of the Falcon platform and your team, delivering timely threat information via the single cloud-native console.
- **Alerts augmented with context:** OverWatch analysts deliver alerts that are augmented with contextual details and global insights to help organizations understand threats and act faster.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

CROWDSTRIKE MANAGED THREAT HUNTING OFFERINGS

Falcon OverWatch sees and stops sophisticated threats by relying on elite human expertise and cloud-scale data to hunt relentlessly for advanced attacks that can otherwise go undetected. There are two offerings to meet the unique needs of your organization.

Feature	Falcon OverWatch	Falcon OverWatch Elite
Cross-disciplinary human experts	X	X
Continuous vigilance	X	X
Cloud-scale telemetry	X	X
Intelligence-driven	X	X
Seamless integration with the Falcon platform	X	X
Alerts augmented with context	X	X
Email notifications	X	X
Assigned threat analyst		X
Personalized onboarding		X
Hunting and investigation coaching		X
Recurring environmental checkups		X
Proactive tuning		X
Tailored threat reports and briefings		X
Response advice, advanced investigation and context support		X
Proactive, closed-loop communications		X