

Falcon OverWatch Elite Dedicated

Dive deeper into CrowdStrike's global 24/7 threat hunting operations with tailored insights and personalized support from a dedicated threat hunting expert who works exclusively for you and your team

Drive Security Maturity

CrowdStrike® Falcon OverWatch™ is a proactive threat hunting service built on top of the CrowdStrike Falcon® platform to augment the Falcon platform's powerful autonomous protection with deep and continuous 24/7 human analysis that relentlessly hunts for — and alerts customers to — the advanced, anomalous and novel adversarial tradecraft in use today.

CrowdStrike® Falcon OverWatch™ Elite extends the standard Falcon OverWatch offering by introducing assigned threat response analysts who expertly contextualize targeted and emerging adversarial tradecraft impacting customer organizations. Falcon OverWatch Elite analysts work with customers strategically to drive continuous threat hunting improvements, build deeper attack insights, and more effectively defend against the stealthiest and most advanced adversaries.

CrowdStrike® Falcon OverWatch™ Elite Dedicated commits a Falcon OverWatch Elite analyst to work exclusively for the customer organization, ensuring a deep, symbiotic relationship between analyst and customer, and a keen understanding of the team's threat hunting requirements, priorities and missions. The Falcon OverWatch Elite Dedicated analyst works in lockstep with the customer to conduct tailored threat hunts and strategic advisory while leveraging the advanced resources, tooling and proprietary tradecraft built and maintained by Falcon OverWatch.

What Customers Say

"CrowdStrike found the issue, mobilized immediately and got us back to a point where we had no data loss, no major issues and were able to continue normal operations in 24 hours."

Michael Sherwood,
Chief Innovation Officer, City of Las Vegas

Key benefits

Focus on what matters: Assess your organization's threats from new angles through contextualized insights and guidance from a dedicated threat hunting expert with years of diverse training and experience.

Respond with speed and confidence: Quickly triage and understand threats, including identity-based attacks, in your environment with proactive outreach and highly tailored threat hunting analysis from your Falcon OverWatch Elite Dedicated analyst.

Supercharge your threat hunting operations: Use your Falcon OverWatch Elite Dedicated analyst to hunt threats using the advanced, battle-tested tooling and proprietary tradecraft designed by Falcon OverWatch.

Key Capabilities

Personalized Threat Hunting Expertise

- **Dedicated analyst:** Embed a Falcon OverWatch Elite analyst into your team to accelerate your threat hunting operations and tailor your insights and results.
- **New perspectives:** Use tailored threat hunting insights to assess existing controls and design purposeful countermeasures with a trusted analyst who knows your organization's requirements.
- **Laser focus:** Develop a shared understanding of your organization's unique structure and requirements.

Tactical Threat Hunting Insights

- **Tailored threat hunting:** Develop, operationalize and tune your threat hunting program with unique visibility and telemetry at unprecedented scale.
- **Proactively hunt identity-based attacks:** Outpace adversaries by bringing the most experienced Falcon OverWatch threat hunters to the identity attack surface. These threat hunters' capabilities are powered by world-class threat intelligence, augmented by AI and aided by patented hunting techniques.
- **Custom investigation support:** Request custom hunts to gain an even deeper understanding of the threats and adversary tradecraft affecting your environment.
- **Fast, closed-loop communications:** Get on-demand access to expertise via multiple channels, including email and Slack.
- **Proactive escalation:** If you miss a critical alert and don't acknowledge it within 60 minutes, Falcon OverWatch Elite begins contacting you directly and repeatedly to ensure you're informed of the new severe threat impacting your organization.

Strategic Threat Hunting Advisory

- **Expert coaching:** Work side-by-side with experienced threat hunting experts to develop your personalized plan to tailored threat hunting in your organization.
- **Falcon OverWatch Elite threat hunting reports:** Use your tailored threat hunting reports to identify and close gaps in your environment, and to reduce your attack surface against advanced adversaries and targeted attacks.

24/7 Proactive Threat Hunting

- **Attacker mentality:** Effective threat hunting requires the ability and expertise to think like an attacker.
- **Cross-disciplinary expertise:** Falcon OverWatch Elite employs highly skilled experts from a wide range of backgrounds, including government, law enforcement, commercial enterprise and the intelligence community.
- **Continuous vigilance:** When sophisticated intrusions occur, time is critical. Your adversaries don't sleep and aren't restricted by time zones or geography — and neither should your threat hunting team. Your dedicated threat hunter is supported by a global team of threat hunters for around-the-clock threat hunting support.

Cloud-scale Security Telemetry

- **Massive data:** The CrowdStrike® Security Cloud ingests trillions of events every day, giving your Falcon OverWatch Elite analyst a global, real-time view into live threat activity.
- **Real-time visibility:** Falcon OverWatch Elite Dedicated takes advantage of the cloud-scale telemetry of the proprietary CrowdStrike Threat Graph® to get broad and deep visibility delivered in real time.
- **Tools for the hunt:** Threat hunting requires more than just experienced analysts — hunters also need the right tools. Falcon OverWatch Elite uses patented tools to hunt at scale across vast amounts of data and identify even faint traces of stealthy intrusions.

Up-to-the-minute Threat Intelligence

- **Threat context:** Understanding the threat and its motives is key to proactive, hypothesis-driven hunting.
- **CrowdStrike threat intelligence:** CrowdStrike threat intelligence powers Falcon OverWatch Elite with detailed, always-current knowledge of tradecraft and indicators of compromise (IOCs) for more than 180 adversary groups, ensuring holistic and accurate hypothesis-led threat hunting.

Dedicated Benefits and Engagements

- **In-person meetings and collaboration:** Work with your Falcon OverWatch Elite Dedicated analyst onsite to ensure tight alignment with your team and strategic objectives.
- **Vertical-aligned threat hunting SMEs:** Falcon OverWatch Elite Dedicated customers gain exclusive access to the Falcon OverWatch Elite team's internal pool of industry-aligned threat hunting subject matter experts (SMEs).
- **More frequent interactions and insights:** Falcon OverWatch Elite Dedicated customers receive more frequent threat hunting deliverables, interactions and reports — maintaining a close pulse on attack trends and tradecraft developments impacting your organization.
- **Your choice of communication platform:** With Falcon OverWatch Elite Dedicated, CrowdStrike makes a best effort to support and integrate with the third-party or in-house communication platform of your choosing.

Do more with Falcon OverWatch Elite Dedicated

Falcon OverWatch offerings provide a variety of delivery and support options to meet the needs and specifications of every organization. Use the comparison table below to see the tangible benefits of Falcon OverWatch Elite Dedicated and determine the delivery model best suited to achieve your team's proactive threat hunting missions.

Capabilities	Falcon OverWatch	Falcon OverWatch Elite	Falcon OverWatch Elite Dedicated
24/7 Threat Hunting Vigilance			
Global, 24/7 human-led operations	■	■	■
Relentless vigilance	■	■	■
Telemetry at unprecedented scale	■	■	■
Cutting-edge processes and tooling	■	■	■
Cross-disciplinary expertise	■	■	■
Integrated IOCs and threat intelligence	■	■	■
Tactical Hunting Collaboration			
Actionable alerts with detailed context	■	■	■
Personalized guidance, insights and support		■	■
Identity threat hunting capability*		■	■
Frictionless two-way communications		■	■
Hunting exchanges		Monthly	Weekly
Expert advisory and coaching		■	■
Strategic Hunting Insights			
Hunting reviews		Quarterly	Monthly
Tailored hunting assessments and reports		Monthly	Weekly
Falcon OverWatch Elite threat hunting library		■	■
Dedicated Analyst Support			
Falcon OverWatch Elite analyst exclusive to you			■
In-person meetings and collaboration			■
Access to vertically aligned hunting SMEs			■
Quarterly hunting training sessions			■
Choice of support communication platform			■

*Customers must have CrowdStrike Falcon OverWatch Elite and CrowdStrike Identity Protection or Identity Detection to take advantage of the new capability.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

© 2023 CrowdStrike, Inc.
All rights reserved.



[Start a Free Trial](#)

Learn more at www.crowdstrike.com