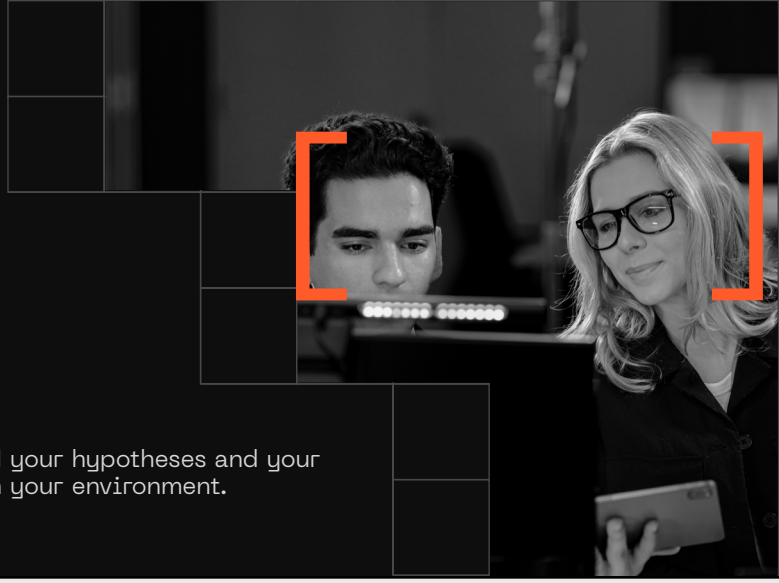
DATASHEET

Premium Threat Hunting.

A white-glove, analyst-led threat hunting service built around your hypotheses and your security tools, designed to catch the quiet attackers lurking in your environment.



The same threat hunters work alongside your team, month after month.

- 100% US-based Threat hunters
- Direct access to your threat hunters
- Monthly hypothesis-driven hunts

Human-driven hunting, tuned to your environment.

Premium Threat Hunting is a consultative, hypothesis-based service for organizations that want a personalized, analyst-led approach to uncovering sophisticated, environment-specific threats. The same hunters work alongside your team month after month, learning your environment, building custom hunts around your priorities, and turning what they find into stronger detections. When you need follow-up investigation, analysis, or even malware reverse engineering, they're already your partners in defense.

Delivery model	Approach	Cadence	Access
Dedicated, high-touch, & consultative	Hypothesis-driven hunts	Regular monthly hunts & working sessions	Direct line to your threat hunters

Why advanced threats stay hidden.

Tools miss what they weren't trained on

AI and signature-based tooling are useful, but they fall short against stealthy attacks, emerging exploits, and novel tradecraft that don't match a known pattern.

Anomalies surface only over time

Detecting quiet attackers takes intelligence, intuition, and the experience to recognize patterns of activity that build slowly across an environment.

Expert threat hunters are hard to find

The specialized skills behind effective threat hunting, such as adversarial research, malware analysis, and detection engineering, are scarce and hard to retain on staff.

In-house threat hunting is expensive

Standing up a hunting capability demands time, dedicated talent, and tooling that quickly becomes costly to build and sustain internally.

1 Proactive Detection	2 Strengthen Detections	3 Hunt Emerging Tradecraft	4 Build Resilience	5 Reduce Dwell Time
Find threats that have bypassed traditional security controls.	Turn every hunt into new, environment-specific detections that close coverage gaps.	Surface novel attacker techniques and exploitation of newly-disclosed vulnerabilities.	Stay ahead of emerging threats and adapt defensive strategies.	Catch attackers early, before lateral movement and privilege escalation.

How a hunt unfolds.

Every engagement follows a deliberate, repeatable cycle, driven by threat intelligence, validated in the lab, and tuned to your environment.

1 Threat Hunting Hypothesis	2 Threat Research & Modeling	3 The Hunt	4 Tuned Queries	5 Detailed Overview	6 Query Tuning & Updates
Drawn from internal threat intelligence, intel feeds, security blogs, trust groups, sandboxes, malware samples, and lab research.	Hunters research the identified threat in depth, modeling it in a lab environment to uncover the tactics, techniques, and procedures behind it.	Hunters develop tailored hunting queries that match the hypothesis and the behaviors observed during research.	With a deep understanding of your environment, hunters baseline and tune queries to cut false positives while building strong behavior-based detections.	On completion, you receive a write-up covering the hypothesis and threat, escalated findings, and the new detection queries created.	Detections are tuned on an ongoing basis and updated as the threat landscape evolves.

Uncover hidden threats	Strengthen detection
Hunt advanced persistent threats, stealthy tactics, and exploitation of newly-disclosed techniques Focus on attacker behaviors and anomalies that automated tools miss Reduce blind spots for comprehensive threat visibility	Develop hunting queries and detection rules specific to your environment Reduce false positives by refining and tuning alert systems Increase the accuracy and precision of your monitoring tools
Improve response & resilience	**Expert threat hunters**
Get actionable insights that enable faster, more effective responses Identify and close gaps in your security posture to reduce future risk Build lasting resilience through continuously improving defenses	Analysts with advanced malware analysis and investigation skills Guidance that integrates seamlessly with incident response 100% US-based, with law enforcement and IT security backgrounds

The premium difference.

Direct access to your threat hunters

An open line to the threat hunting team, not a ticket queue.

Regular hunts on your priorities

Typically monthly, aligned to your evolving risk profile.

Deep environment knowledge

The same hunters build sustained familiarity with your stack.

Collaborative, custom hypotheses

Hunts designed together around the threats that matter to you.

Detailed, context-rich findings

Analysis and strategic recommendations, not just alerts.

Malware reverse engineering

Decode attacker tradecraft when an investigation calls for it.

Where hunters go to work.

- Find misconfigurations, network anomalies & coverage gaps
- Develop new detections & harden configurations
- Test new attacker techniques & detection methods
- Evaluate current security platforms & event logs
- Research emerging attacker techniques & tools

Supported platforms.

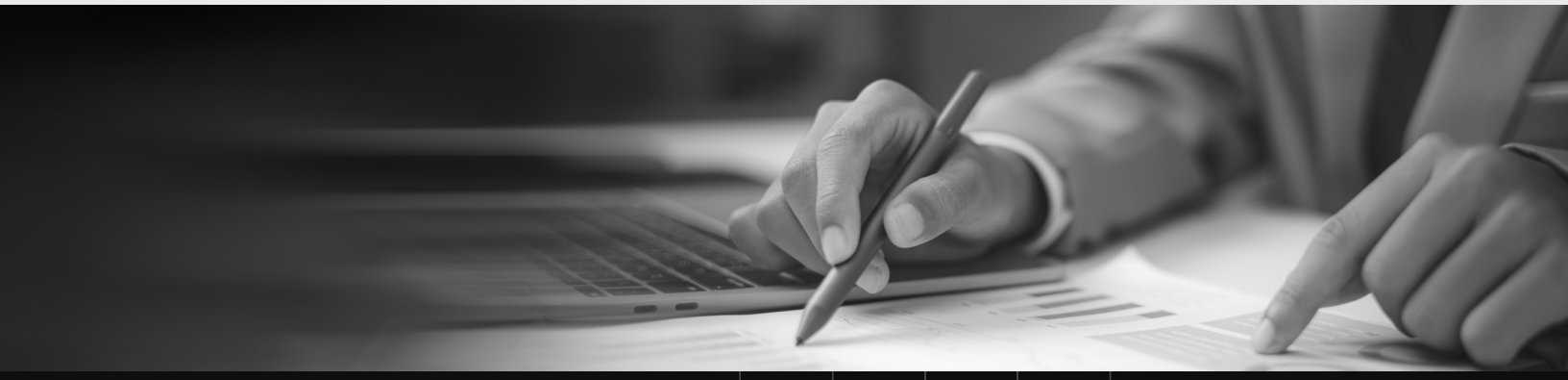
Primary (EDR preferred)

- Palo Alto Networks Cortex XDR
- CrowdStrike Falcon EDR
- SentinelOne
- Microsoft Defender for Endpoint

Secondary

- Palo Alto Networks Cortex XSIAM
- CrowdStrike NG SIEM
- Sumo Logic
- ExtraHop
- Splunk
- Microsoft Sentinel
- Google SecOps

A supported EDR is preferred for threat hunting; results are strongest when paired with one. Hunters can hunt in SIEMs provided the applicable data is available. Have only one of these technologies? Reach out to scope it.



"With Binary Defense Threat Hunting, we have skilled, experienced threat hunters watching and creating new detections for our environment at all times. We wouldn't be able to afford that level of talent at an Energy Company of our size. They feel like an extension of our team."

— Senior Security Engineer, Energy Company

Put expert threat hunters on your environment.

Surface the stealthy attacks your tools were never tuned to catch, close the gaps before they're exploited, and shorten the time between intrusion and response.

Binary Defense is a trusted leader in Managed Detection and Response (MDR), helping organizations across industries stay ahead of modern cyber threats. Our team of SOC analysts, threat hunters, detection engineers, and researchers works around the clock to deliver outcomes that matter: earlier threat detection, faster response, and stronger long-term security.

We take an attacker's mindset to defense, combining deep expertise with proactive tradecraft to protect what matters most.

Learn more at binarydefense.com, explore our blog for the latest insights, or follow us on LinkedIn.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com

FORRESTER®
WAVE STRONG PERFORMER 2025
Managed Detection And Response Services

BINARY DEFENSE