



Reveal(x) Advisor

# FAQ



## What is Reveal(x) Advisor?

ExtraHop Reveal(x) Advisor is a managed service responsible for detecting network vulnerabilities, incidents, and adversaries that may otherwise go undetected by limited or overwhelmed security teams.

Advisor augments security teams by providing threat analysts and security advisors who prepare your network, clear the queues, and hunt for threats to provide assurance your network is free of compromise and security risks. We call these the three pillars of network assurance.

Advisor also helps customers drive maturity through on-demand expertise. An assigned security advisor delivers proactive security checks, executive threat reports, platform tuning, quarterly briefings, targeted recommendations, and coaching to help improve analyst threat investigation skills and reduce incident response times.

## I already have an MSSP, why would I need Advisor?

Advisor has a different mission than MSSPs, which are typically used to operate and manage a customer's security technology stack. Advisor does not manage Reveal(x) or any of the other technologies or integrations within the customer environment. We augment the existing security team that is responsible for monitoring all alerts—NDR, EDR, SIEM, IDS/IPS, Firewall, email, etc.—but is typically overwhelmed by ever-increasing threat intelligence, CVEs, and detection volumes. Overwhelmed staff results in missed threats and unnoticed vulnerabilities that put the business at risk.

Advisor teams proactively monitor, investigate, and notify your security team about priority (P1) alerts generated by Reveal(x) that are determined, by human analysis, to be true indicators of compromise. The team does not monitor the general alert volume, which is the responsibility of the customer's security team.

Advisor proactively hunts for threats using industry threat intelligence, CVE reports, and specific threat actor TTPs that should be of most concern or importance to a particular customer. This personalized approach to proactive threat notifications and hunting services frees up security teams to focus more on incident response and less on chasing false positives and investigating volumes of detections—or the thousands of CVEs generated each year.

Advisor also leverages the AI capabilities of Reveal(x) to correlate network anomalies and events with security threats to identify vulnerabilities and to make specific recommendations for remediation that assure the network is threat free. This offloads a tremendous amount of responsibility from burdened ITOps and SecOps teams and identifies hidden threats that would otherwise go undetected.

## Does Advisor work with any of the other ExtraHop teams?

Advisor teams routinely engage with the ExtraHop Services, Threat Research, and Incident Response teams assisting with attribution and identification of the activities and malware found during their investigations. In incident response cases where Advisor is engaged, the team works closely with security response services to exchange information derived from investigations.

When a hidden adversary or priority CVE is identified, Advisor teams work with ExtraHop Solution Architects to develop custom detection triggers and artifacts that can be uploaded to Reveal(x) to detect and prevent future breaches.

## Advisor Pricing

Advisor is licensed on an annual subscription. There are five tiers of service which start from basic detection services (TIER 1) to the highest tier (TIER 5) which includes proactive threat hunting services—[read the data sheet for details](#).

| REVEAL(X) ADVISOR PLANS            | TIER 1      | TIER 2    | TIER 3    | TIER 4    | TIER 5    |
|------------------------------------|-------------|-----------|-----------|-----------|-----------|
| Threat Detection Analysis & Review | On-Demand   | On-Demand | On-Demand | On-Demand | On-Demand |
| Threat Analyst Sessions            | Monthly     | Bi-weekly | Bi-weekly | Weekly    | Weekly    |
| Threat-Free Network Hygiene        | Semi-annual | Quarterly | Quarterly | Quarterly | Quarterly |
| Executive Threat Summary Report    | Monthly     | Bi-weekly | Bi-weekly | Weekly    | Weekly    |
| Executive Account Reviews          | Semi-annual | Quarterly | Quarterly | Quarterly | Quarterly |
| Dedicated Security Advisor         | --          | --        | ✓         | ✓         | ✓         |
| Formal Investigation Reports       | --          | --        | ✓         | ✓         | ✓         |
| Proactive Threat Notification      | --          | --        | --        | ✓         | ✓         |
| Proactive Threat Hunting           | --          | --        | --        | --        | ✓         |

## Learn More

Reach out to your ExtraHop representative for more information or to subscribe to Reveal(x) Advisor.

### ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.



info@extrahop.com  
www.extrahop.com