We own the R in MXDR.

A 24×7×365 agentic Security Operations Center on Microsoft Defender XDR, Sentinel, and Security Copilot — AI agents triage and investigate every incident, and our experts move from detection to containment in minutes, not days.

- Rapid detect
- Rapid respond
- Agentic SOC
- Microsoft-native

24x7x365
Always-on SOC

Every incident
Auto-triaged by AI

Minutes
To contain & isolate

3-layer
XDR
Sentinel
Copilot

The Mid-Market is Outgunned

Growing companies face the same threats as the global enterprise — identity compromise, automated lateral movement, cloud-based exploitation — but rarely have the same security bench, and the alerts never stop.

Traditional managed services stop at detection: they hand you a ticket and the attacker keeps moving. **The gap isn't seeing the threat — it's acting on it fast enough.**

Always-on coverage
24×7×365 monitoring across endpoints, identities, cloud apps, and networks — without building a SOC.

Fewer, better alerts
AI agents suppress known false positives so your team sees only what matters.

Action in minutes
We isolate the device or kill the compromised session — not just file an alert.

Posture that matures
Ongoing guidance steadily hardens controls and reduces risk over time.

The Agentic SOC, Powered by Security Copilot

AI agents run the first and second shift of analyst work. For Microsoft E5 clients with provisioned Security Compute Units, Security Copilot is the orchestration brain — driving our investigation workflows natively, with the compute staying inside your own tenant.

L1 Agent	AUTONOMOUS TRIAGE

Runs on every Sentinel incident, the moment it fires:

- Scores and correlates related signals
- Suppresses known false positives automatically
- Escalates real threats to L2 with a pre-built brief

L2 Agent	DEEP INVESTIGATION

Triggered by L1 escalation — runs the full investigation toolkit:

- User investigation & scope-drift analysis
- IoC enrichment and authentication tracing
- Produces a structured, decision-ready report

TWO WAYS TO DEPLOY

1 FOR E5 + SCU CLIENTS

Microsoft Security Copilot
Copilot drives the investigation skills natively; SCU cost stays in your tenant. We run the managed service on top.

2 FOR MID-MARKET & SMB

Refoundry Agent Layer
Our own orchestrator routes each task to the right model for the job — AI cost absorbed into the contract.

UNDER THE HOOD

Both agents sit on **Refoundry's Security Investigator layer** — investigation skills, a curated KQL library, IoC/IP enrichment, and live tool integrations. Whether the brain is Security Copilot or our own orchestrator, the same proven playbooks run every time.

REFOUNDRY

We Don't Just Detect. We Respond.

Detection is table stakes. Owning the response is where the threat actually ends — investigation agents hand off directly to orchestrated containment playbooks, governed by our SOC team.

STEP 1 — DETECT
Signal to incident
Defender XDR and Sentinel surface the threat; the L1 agent triages it instantly

STEP 2 — INVESTIGATE
Scope & confirm
The L2 agent enriches, traces auth, and confirms blast radius in a structured report

STEP 3 — RESPOND
Contain & recover
Orchestrated playbooks — revoke, reset, isolate — shut the attacker down

RESPONSE PLAYBOOKS, BUILT IN

REVOKE

Invalidates active sessions and tokens for a compromised identity

- Session hijack
- Token theft
- Rogue OAuth grant

RESET

Forces credential reset and re-authentication

- Credential compromise or suspected exposure

ISOLATE

Cuts the affected endpoint off from the network

- Malware
- Lateral movement
- Ransomware precursors

Why Refoundry

AI-First
Triage & investigation at machine speed, so analysts focus on judgment.

Code-Driven
Engineered skills, KQL, and integrations — repeatable, never ad- hoc.

Expert-Led
Seasoned SOC operators govern every automated action.

Response-Owned
We close the loop — alert to contained, end to end.

What's Included

ONE MANAGED SERVICE — DETECTION THROUGH RESPONSE

01. 24×7×365 monitoring
Continuous coverage across endpoints, identities, cloud apps, and network telemetry

02. Agentic L1/L2 triage
Autonomous scoring, correlation, false-positive suppression, and AI-led investigation

03. Security Copilot orchestration
For E5 + SCU clients, Copilot drives investigations natively — compute stays in your tenant

04. Owned response
Orchestrated revoke / reset / isolate playbooks executed by our SOC, not a ticket back to you

05. Proactive threat hunting
Hunting subtle signals — early lateral movement, anomalous logins — before they escalate

06. Posture guidance
Ongoing recommendations that harden controls and steadily reduce risk

Built on the Microsoft Security Stack

No rip-and-replace — Refoundry MXDR fits naturally into the Microsoft investment you already own and amplifies it with an agentic operating layer.

READY TO OWN YOUR RESPONSE?

Turn your Microsoft investment into an agentic SOC

Let's walk through how Refoundry MXDR plugs into your environment — and how fast we get from alert to contained.

sales@refoundry.com
200 S. Wacker Dr., Ste. 3100
Chicago, IL 60606

CONTACT US