OUR PLATFORM

Expel Workbench™ Powered by Ruxie™

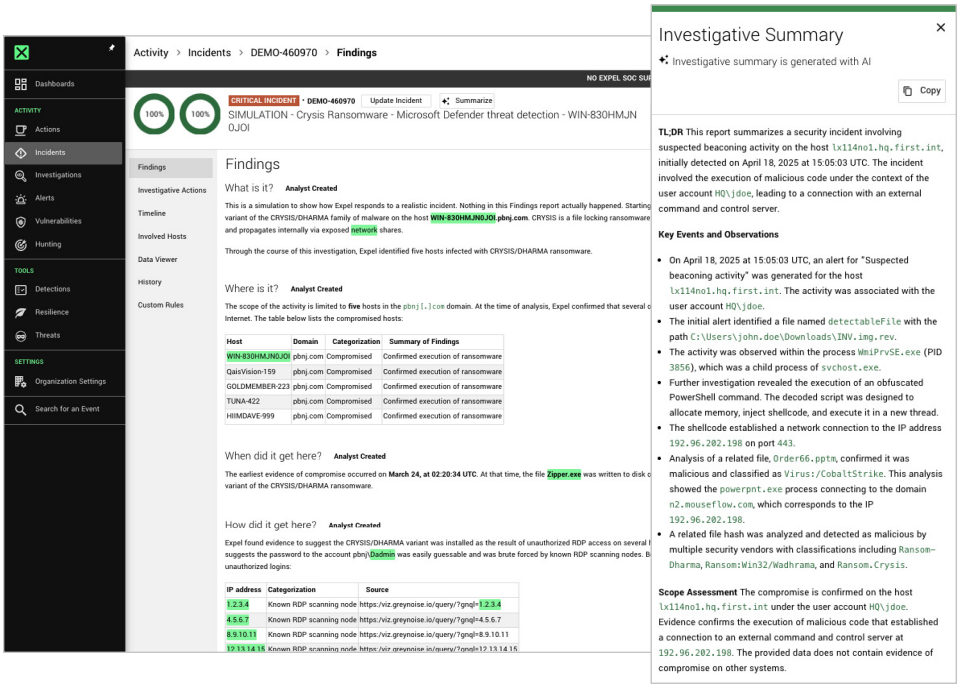
Accurate defense at AI speed—without sacrificing human judgment.

Your challenge

AI-powered attackers compress the timeline from initial access to full impact. Human-paced security operations simply cannot move fast enough to contain the blast radius at scale. Breaches often occur not from a lack of visibility, but due to the friction and operational delay between receiving an alert and executing the fix. Getting ahead requires AI working across every stage of the threat lifecycle, and a platform that keeps everyone—including you—in the loop.

How we help

Expel Workbench™ utilizes Ruxie™, our AI SOC manager, to apply specialized AI capabilities across every stage of the threat lifecycle. Ruxie eliminates the lag between a signal firing and an analyst acting by processing signals, enriching alerts, and making high-confidence triage calls. Ruxie handles the immense data volume, allowing Expel's MDR analysts to focus entirely on complex decisions where accuracy determines the final result. You see every decision, every action, and every outcome in real time in Workbench.



ELITE OUTCOMES, ZERO BLACK BOXES

Coverage for every surface
Detection strategies and signal correlation across your environment—endpoint, identity, network, cloud, IaaS, Kubernetes, SaaS, AI, email, SIEM, and more.

Accurate defense at AI speed
Ruxie's specialized AI capabilities resolve high-confidence noise and queues deeply enriched context so our SOC analysts make better decisions on your behalf.

Built on 10 years of data
Ruxie's models are built on a decade of real security data and MDR outcomes, ensuring your SOC is not a proving ground for untested AI.

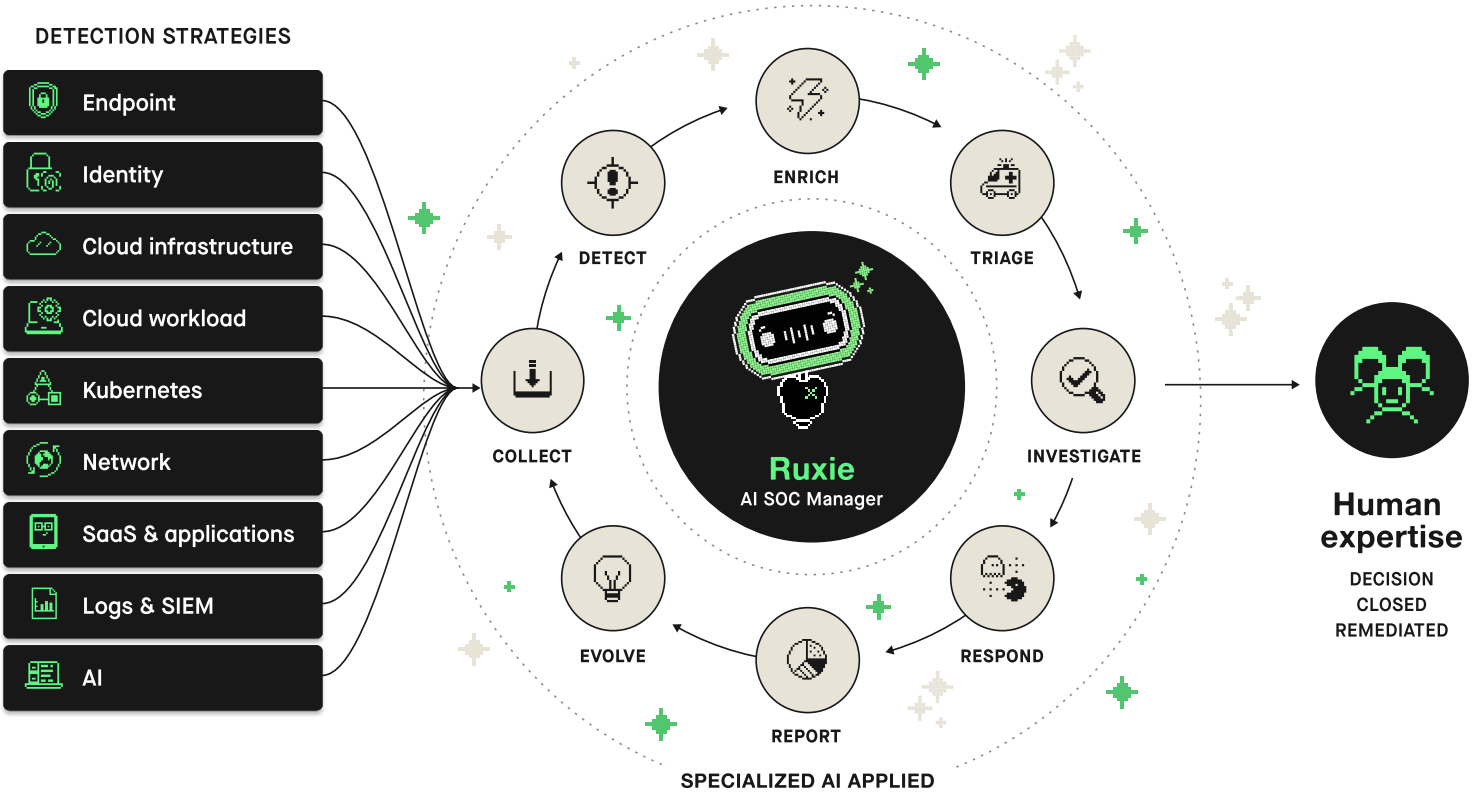
A front-row seat to everything
Workbench gives you real-time visibility into every alert, every Ruxie action, and every analyst decision.

AI applied across the threat lifecycle

Expel Workbench unlocks your security tools. Powered by Ruxie, the platform seamlessly connects your tech and our experts, delivering speed and accuracy neither accomplishes alone.

Faster decisions. Better outcomes.

Ruxie receives signals from across your environment and directs her specialized AI and agentic capabilities inside Expel Workbench, covering every stage of the threat lifecycle.



Ruxie's AI capabilities

Each capability targets a specific friction point between detecting a threat and acting on it, built from a decade of real customer signal and incident data.

ENRICHMENT
Pre-enriches alerts by pulling telemetry and context from 160+ tools and external intelligence sources automatically so your environment is fully protected.

CONTEXT
Automatically aggregates live telemetry and asset, user, and historical context to build your team an investigation-ready picture of what's happening.

DETECTION
Correlates cross-surface signals to identify threats across cloud, identity, endpoint, network, and other surfaces in your environment.

TRIAGE
Analyzes evidence to confidently auto-close benign alerts and route real, verified threats directly to analysts, resulting in less signal noise for you.

INVESTIGATION
Assembles cross-tool evidence and applies structured reasoning to deliver clear recommendations before an analyst opens the alert.

RESPONSE
Executes targeted, automated response actions to instantly contain and neutralize threats the moment they are confirmed and blocking your environment from further damage.

REPORTING
Automatically documents every closed alert and incident in plain English, ensuring all outcomes are fully traceable for your team.

COLLABORATION
Syncs Workbench investigations with Slack and Teams for real-time multi-channel visibility, escalation, and easy communication with your team.

PHISHING
Automates phishing triage by scoring, clustering, and detonating emails to identify when large malicious campaigns are targeting your organization.

DETECTION ENGINEERING
Agentic workflows generate new rules whenever a coverage gap is identified against existing detections and new vendor alerts.

Accurate defense at AI speed

Ruxie is faster than traditional SOCs, and more accurate than just AI. She accelerates the lifecycle from first signal to the stopped attack, leaving nuanced judgment calls to Expel analysts. Together, they deliver a superior defense neither could achieve alone.

	EXPEL MDR powered by Ruxie AI	OTHER SOCS using AI-driven platforms
Mean time to detect (MTTD)	**5 minutes**	**Minutes to months**
Mean time to touch for all alert severities (MTTT)	**9 minutes**	**Minutes to hours**
Mean time to remediate (MTTR)	**14 minutes**	**Hours to days**
Alerts investigated	**100%**	**~30%**
Investigation time spent per alert	**~3 minutes**	**~30 minutes**
Your time spent triaging	**~0%**	**~80% on Tier-1 triage**

Why Expel

Technology agnostic

We don't force you into restrictive vendor lock-ins or prescribe tech you must use. Ruxie runs across data from over 160+ third-party security tools to maximize the ROI of your existing tech stack.

Continuously evolving

Ruxie's proprietary models are continuously trained on data from multiple tools, attack surfaces, and incident outcomes. Ruxie adapts over time to deliver faster, better outcomes for customers.

Complete transparency

Collaborate directly with the Expel SOC using tools you already have. See every signal, AI reasoning path, and automated action in real time. No black boxes.

CentroMotion™

"Out of a million events, I would say 99.5% of them are filtered out in triage by AI and machine learning before we actually need to have eyes on the actual issue."

BEN UHLIG
Global Cybersecurity & Compliance Manager