CONTRAFORCE AI AGENT – RETURN ON INVESTMENT (ROI)

Introducing the ContraForce AI Agent for Microsoft Security

Today, the ContraForce Platform leverages AI and automation to upskill SOC teams and boost their efficiency. Analysts can view all Microsoft Sentinel and Microsoft Defender XDR alerts in a single console, with core engineering tasks—such as analytic rule creation, incident enrichment, and response actions—automated for speed and consistency.

ContraForce is now taking analyst productivity even further with the launch of the ContraForce AI Agent for Microsoft Security. The ContraForce AI Agent fully automates triage, investigation, and response.

Immediate ROI – Reduce Incident Investigation Costs by 2.5-10X

We conservatively estimate that the cost for a security analyst to investigate a security incident is $10 using the following assumptions:

SECURITY ANALYST SALARY	$100,000
DIVIDED BY HOURS WORKED PER YEAR	÷ 2000
DIVIDED BY INCIDENTS INVESTIGATED PER HOUR	÷ 5
COST PER INVESTIGATED INCIDENT	**$10**

We recognize that each organization is unique and encourage SOC teams to do their own calculations.

By comparison, the Azure compute cost for the ContraForce AI Agent has been approximately $4 per case during the beta program, and is expected to drop to approximately $1 per case when it is generally available (GA).

Using the ContraForce AI Agent reduces incident investigation costs by 2.5-10X.

The ContraForce AI Agent – How It Works

The ContraForce AI Agent begins by rapidly determining whether an incident warrants deeper investigation, human interaction, or automated response. To make decisions, the agent leverages historical and environmental context, including past incidents, executed response actions, entity behavior, and workspace configurations.

When the agent escalates an alert for investigation, it autonomously adds detailed information about impacted entities and other context, and—when appropriate—executes ContraForce Gamebooks: automated response actions determined by mapping MITRE D3FEND counter-measures to MITRE ATT&CK TTPs.

After an incident is closed, the agent generates a summary report with a confidence score indicating the likelihood of a true threat. MSSP teams can configure minimum confidence thresholds that determine when the agent should provide an incident response plan, contain the threat, or run full remediation actions.

Full transparency is built in. Security teams can monitor the agent's activity in real time, track which alerts are under investigation, see when Gamebooks are triggered, and review detailed logs behind every decision.

The ContraForce AI Agent was jointly developed with Microsoft using the Azure AI Foundry as part of ContraForce's broader relationship with Microsoft.