CONTRAFORCE

Hyperautomation for Security Operations

Over the past few years, we've experienced a volume and sophistication of cyberattacks unlike anything we've seen before. With the increase in threats, risk, and industry nuance came a market saturated with security tools and recommended "best practice."

Now, with the adoption of Zero-Trust policies, security teams are forced to verify every user, endpoint, and application, adding an unprecedented amount of work to their plate. Security teams are sifting through thousands of unverified alerts, laborious remediation practices and complex detection and response engineering.

Many organizations have invested in Sentinel, Microsoft's native SIEM and SOAR platform, to help stay ahead of risk— but despite the robust capabilities of Sentinel, the tool is incredibly challenging for end-users. While Sentinel is robust, ContraForce makes it simple.

CONNECTING THE DOTS

ContraForce works with Sentinel to provide comprehensive visibility and control of your data. With a combination of SIEM, SOAR, and MDR capabilities, ContraForce enables users to investigate, detect and respond to threats like never before.

The majority of businesses operate in a Microsoft ecosystem. Because of this, ContraForce was designed with a heavy Microsoft-focus, architected on top of Azure and deeply integrated with native Microsoft technologies. Though Microsoft technologies are the most common, ContraForce also supports over one hundred other integrations across network, endpoint, cloud, identity and SaaS vectors.

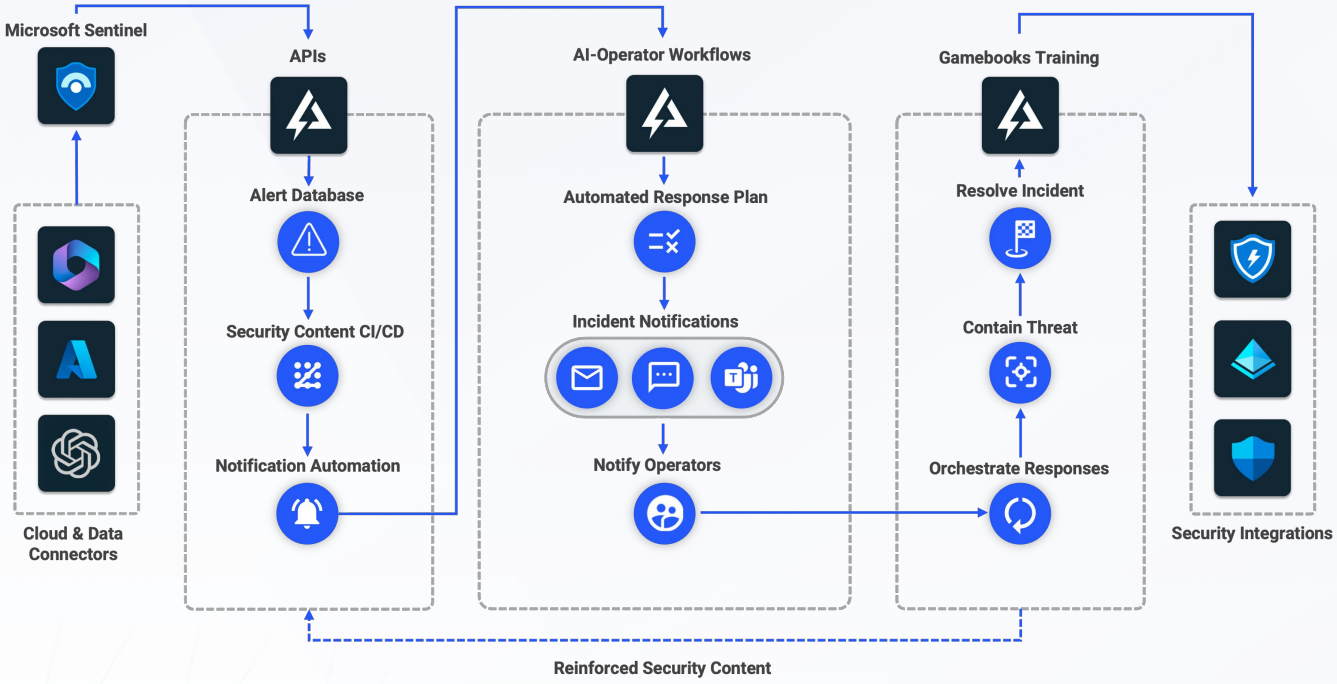
CONTRAFORCE ELIMINATES CHALLENGES LIKE:

- → **Tool sprawl and decentralized portal management**
- → **Security alert overload and inefficient response workflows**
- → **Broken detection and response engineering**
- → **Big data and security engineering complexity**

HOW IT WORKS

ContraForce is a **hyperautomation** platform that integrates **deeply** with Sentinel (customers can host their own Sentinel or ContraForce can host it as a SaaS offering). The ContraForce platform leverages Sentinel to process security data, then uses automated security monitoring to verify threats— distilling millions of events into thousands of alerts, then into a handful of incidents. When an alert is verified, ContraForce immediately notifies users via email, Teams, or SMS. **Incident recommendations can be executed in email or Teams with a click of a button.**

Within the ContraForce portal, users can quickly respond to an incident with the click of a button (using the One-Click Response feature to deploy a playbook). Playbooks can be daisy-chained together to create a gamebook, a series of playbooks that can be deployed and run simultaneously. These playbooks are faster and easier to use than Sentinel's OOTB incident response content, and there's no configuration necessary. ContraForce also leverages automated security engineering and detection rules to build a stronger, more resilient security architecture.



BY THE NUMBERS

Same-day deployment, with Sentinel fully optimized in 2 weeks (compared to a 6-month industry average)

90%

Reduction of time to onboard Sentinel

62%

Reduction of Mean Time to Respond (MTTR)

60%

Reduction of OpEx for your SecOps

Optimize security operations with cloud-native SIEM, powered by ContraForce's AI and automated security engineering

HARNESS THE SCALE OF THE CLOUD

DETECT EVOLVING THREATS

EXPEDITE INCIDENT RESPONSE

GET AHEAD OF ATTACKERS

When it comes to security, timing is everything. Our goal, first and foremost, is to minimize the amount of time it takes to complete a task.

Chasing data takes time. When you know how and where your data is used, you can build playbooks and deploy them with the click of a button. With gamebooks, you can daisy-chain multiple playbooks together and deploy them simultaneously.

Disjointed, sloppy data takes more time to use. ContraForce Connectors provide data normalization and streamlined API wrappers to ensure hassle free ingestion of native and 3rd party data sources. Native Microsoft Connectors can be connected with one-click, and non-native Connectors can be deployed in a few steps with infrastructure as code (IaC) templates for fast and simple data ingestion.

Uncoordinated incident activities create confusion and take time to resolve. Coordinate entity and incident activity into one consolidated view to reduce confusion of the root of the attack and how to resolve the incident. ContraForce enables evidence driven security incidents to be distilled down to the most critical issues that need to be resolved with urgency.

WANT TO LEARN MORE?

To learn more about ContraForce, please visit our website at **www.ContraForce.com**. You can also send us an email at **info@contraforce.com** if you have questions or comments. We'd love to hear from you!