CONTRAFORCE

Microsoft Security

Selling Microsoft Sentinel with ContraForce

Sales Guide

Prepare

- Learn about the target markets and prioritized industries for ContraForce's hyperautomated SOC platform that helps organizations extend the value of their Microsoft Sentinel investment.
- Understand the target customer audience and how to engage specific security roles.

Sell

- Ask the right questions to uncover your customer's needs and demonstrate how ContraForce can help address common pain points.
- Learn how to address customer objections.
- Understand the competitive landscape and how to position ContraForce as the ideal solution.

Close

- Determine if customers are a good fit for ContraForce using the qualifying criteria.
- Discuss next steps and share additional public-facing resources.

Prepare

Familiarize yourself with the target market and business opportunity

ContraForce

Industry

Financial services, healthcare, manufacturing, construction, public sector, local government, education, and legal services.

Market trends

- $4.35M global average cost of a data breach[1]
- 3.5 million cybersecurity jobs predicted to be unfilled by 2025[2]

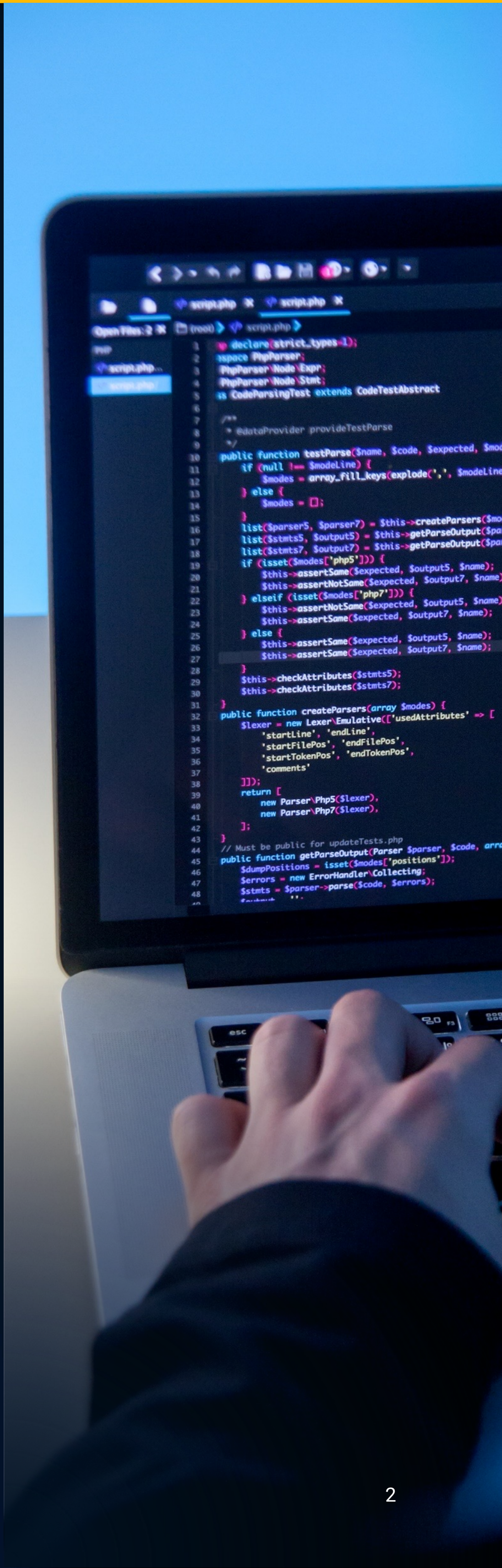
Customer positioning statement

ContraForce condenses your Microsoft Security product portfolio into one easy-to-use platform that leverages AI and hyperautomation to streamline security operations (SecOps) without requiring you to maintain a SecOps team in-house.

Customer value proposition

As today's digital environments become more complex, cybercrime is growing in sophistication and volume. This makes continuous threat detection and remediation a critical capability to protect against future data breaches. However, not all companies have the budget to build and maintain a highly skilled SecOps team to mitigate threats 24x7.

ContraForce is a user-friendly solution to this problem. Use the AI-based hyperautomation platform to reduce security operations processes and stop real threats faster using the Microsoft Security products you likely already own. Take full advantage of your Business Premium, E3, or E5 license as well as other highly advanced technologies like Microsoft Sentinel without needing to manually deploy, use, or maintain Microsoft's robust security tools. Instead, condense everything into one simple platform that requires no expert management and effectively automates threat detection with one-click incident response and actionable insights all in one place.



[1] Cost of a data breach 2022 | IBM
[2] 2023 Official Cybersecurity Jobs Report | Cybersecurity Ventures

Prepare

Dig deeper into the target customer personas

Understand your audience

CIO, CTO

Responsible for overall business strategy, risk management, and ROI for information and technology. Tasked with maintaining business continuity and introducing greater operational efficiencies.

CISO, SOC MANAGER

Responsible for the strategy, implementation, and management of an organization's cybersecurity infrastructure. Tasked with ensuring the company complies with all relevant industry regulations, protecting the company's data and reputation, and recommending the best cybersecurity solutions within budget.

Pains and needs

LACK OF EXPERTISE

The cybersecurity skills gap has left many companies struggling to recruit and retain their own in-house cybersecurity professionals. Many IT teams are made up of generalists who lack the specific experience to configure and maintain a robust cybersecurity system.

LACK OF RESOURCES

Even teams who do have cybersecurity professionals on staff may struggle with the volume of alerts they receive each day. Investigating countless alerts diverts focus away from real incidents and other value-added activities.

Purchasing drivers

INCREASINGLY TARGETED BY THREAT ACTORS

Cyberattacks are increasingly becoming a part of day-to-day business operations. A recent breach attempt may shift businesses into the "not when, but how" mindset when it comes to future attacks.

MOVING MORE WORKLOADS TO THE CLOUD

Movement to the cloud creates a new digital landscape to protect and, fortunately, new and innovative opportunities for protection. Businesses may be ready to capitalize on the new security capabilities of a cloud-based system.

RECENT ENGAGEMENT OF AN MSSP OR MXDR PROVIDER

The engagement of a third party to provide managed security services may open opportunities to implement solutions that increase the provider's efficiency and effectiveness in monitoring and managing the organization's cybersecurity.

Existing investments

- Already invested in M365, Microsoft 365 Defender, Microsoft Teams, and possibly Microsoft Sentinel.
- May be using Microsoft Business Premium, E3, or E5 licenses.
- Migrated or in the process of migrating to the cloud.
- Migrated or in the process of migrating to Azure Active Directory, part of Microsoft Entra.
- Typically using Endpoint Detection and Response (EDR), Firewalls, Identity Provider, Email Gateway, and Multifactor Authentication (MFA).
- Managed Extended Detection & Response (MXDR) Services – ContraForce is a Partner-enabled solution that allows Managed Security Service Providers (MSSPs) and MXDR providers to use ContraForce on behalf of the customer to deliver advanced security monitoring and incident response capabilities.

Sell

Use the questions below to uncover your customer's needs

Open, probe, pitch, and prove

	Automated deployment	Simplified operations	Maximized investments
OPEN Start your conversation with an open-ended question to capture your customer's interest.	• How many data sources must your team monitor for threats? • How familiar are you with Microsoft Sentinel and Microsoft 365 Defender?	• Can you walk me through the roles and range of skillsets you currently have in-house to support your security operations? • How many security professionals do you have at your company that are solely devoted to threat detection and remediation?	• What cybersecurity tools are you currently investing in? • Do you currently own any other Microsoft licenses such as Business Premium, E3, or E5?
PROBE Ask qualifying questions to understand your customer's specific pains.	• Can you share your experience managing and operating these robust Microsoft technologies? Are they a core part of your security operations strategy? • What are the barriers that are preventing you from deploying more advanced security technologies like Microsoft Sentinel?	• How much of your team's time is spent investigating alerts or on other repetitive tasks?	• Do you feel your team has the capacity to fully maximize your investment at your current size and strategy?
PITCH Demonstrate how ContraForce can help customers address their pain points.	Deploying Microsoft Sentinel has never been simpler. ContraForce uses AI and automated engineering to automatically configure Microsoft Sentinel across your organization in weeks, not months. It also makes Microsoft's robust cloud-based SIEM easier to manage by connecting it to ContraForce's all-in-one defense platform.	ContraForce takes the time-consuming manual tasks out of the equation. The platform's AI will automatically detect and verify threats, only alerting your team to what matters most while automatically resolving the false positives. It also allows you to deploy your incident response playbooks with a single click to save even more time.	Centralize your data and connect the powerful Microsoft Security tools you already own through one central, easy-to-use platform. Even non-cybersecurity experts can leverage the ContraForce dashboard to configure security solutions such as Microsoft Sentinel and extend the value of their investment.
PROVE Explain why ContraForce is the best option on the market.	90% reduction of onboarding time for Microsoft Sentinel.[3]	62% reduction of Mean Time to Respond (MTTR).[3]	60% reduction of operational costs for your Security Operations.[3]

[3] ContraForce Internal Study

Sell

Learn how to address customer objections

Customer objections

"I DON'T THINK IT'S IN MY BUDGET TO INVEST IN ANY NEW SECURITY TOOLS RIGHT NOW."

ContraForce is designed to enhance your team's efficiency and extend your existing Microsoft technology investments. By centralizing and simplifying management through AI and automation, you can increase visibility and response capacity without the need to hire additional senior-level cybersecurity professionals.

"WE HAVE OUR OWN SYSTEM; SWITCHING TO MICROSOFT SENTINEL SEEMS LIKE A LOT OF WORK."

Microsoft Sentinel and the Microsoft 365 Defender product portfolio are designed to holistically and seamlessly integrate with your broader Microsoft ecosystem, giving you full interconnected coverage. For those not currently using Microsoft Sentinel, ContraForce was designed to make the deployment as quick and easy as possible to help you start enjoying the benefits of this powerful Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution faster.

"I ALREADY HAVE MICROSOFT SENTINEL DEPLOYED AND DON'T WANT TO DEPLOY A NEW INSTANCE. WHY DO I NEED CONTRAFORCE?"

ContraForce is designed to integrate even into existing Microsoft Sentinel deployments. You can use the detection rules and response playbooks you have already developed and feed them through a Continuous Integration (CI)/Continuous Delivery (CD) pipeline directly into ContraForce. ContraForce uses its AI and security content library to add additional coverage to your existing detection and response capabilities and improve their tuning without the need to recreate them manually every time. Maximize the value of your cybersecurity experts' time by allowing them to focus on more complex and strategic tasks for your business.

"I HAVE SEVERAL DEPLOYMENTS OF MICROSOFT SENTINEL. DOES THIS SOLUTION HELP ME MANAGE MY MULTIPLE MICROSOFT SENTINEL INSTANCES?"

ContraForce was designed with its own multi-tenant Microsoft Sentinel management capabilities. This enables you to onboard as many Microsoft Sentinel instances as you would like and manage them all in one place.

Sell

Understand the competitive landscape and how to differentiate

Competitive landscape

Competitor positioning	How ContraForce wins
Outsource security operations to a dedicated SOC team that can manage your Microsoft Sentinel instance and broader cybersecurity for you.	ContraForce streamlines the tasks of a SOC through full integration, automation, and simplification. In other words, it empowers any security team to do more and doesn't require a huge learning curve to manage.
Implement a custom dashboard to manage Microsoft Sentinel.	The ContraForce platform leverages no-code integrations that make managing Microsoft Sentinel and your other Microsoft Security products simpler than ever.
Benefit from integrations with Microsoft Sentinel that provide automatic threat monitoring.	The ContraForce dashboard does more than monitor. You can develop infinite threat response playbooks and deploy them with a single click to instantly remediate threats without draining your resources.
Integrate with other third-party security tools outside of Microsoft.	ContraForce is an Application Programming Interface (API) first platform that supports simple integrations to over 130+ data connectors from various vendors. This enables you to easily pull in telemetry from any vendor, even if it's not Microsoft native.

Sell

Articulate how ContraForce can support your customer's security journey

What's included in the ContraForce platform?

AUTOMATED SECURITY MONITORING

Leverage the power of AI to automatically detect and verify threats, eliminating false positives and flagging only what matters to your team.

ONE-CLICK INCIDENT RESPONSE

Deploy your playbooks to respond to incidents with the click of a button. Stack multiple playbooks together into a gamebook and deploy simultaneously.

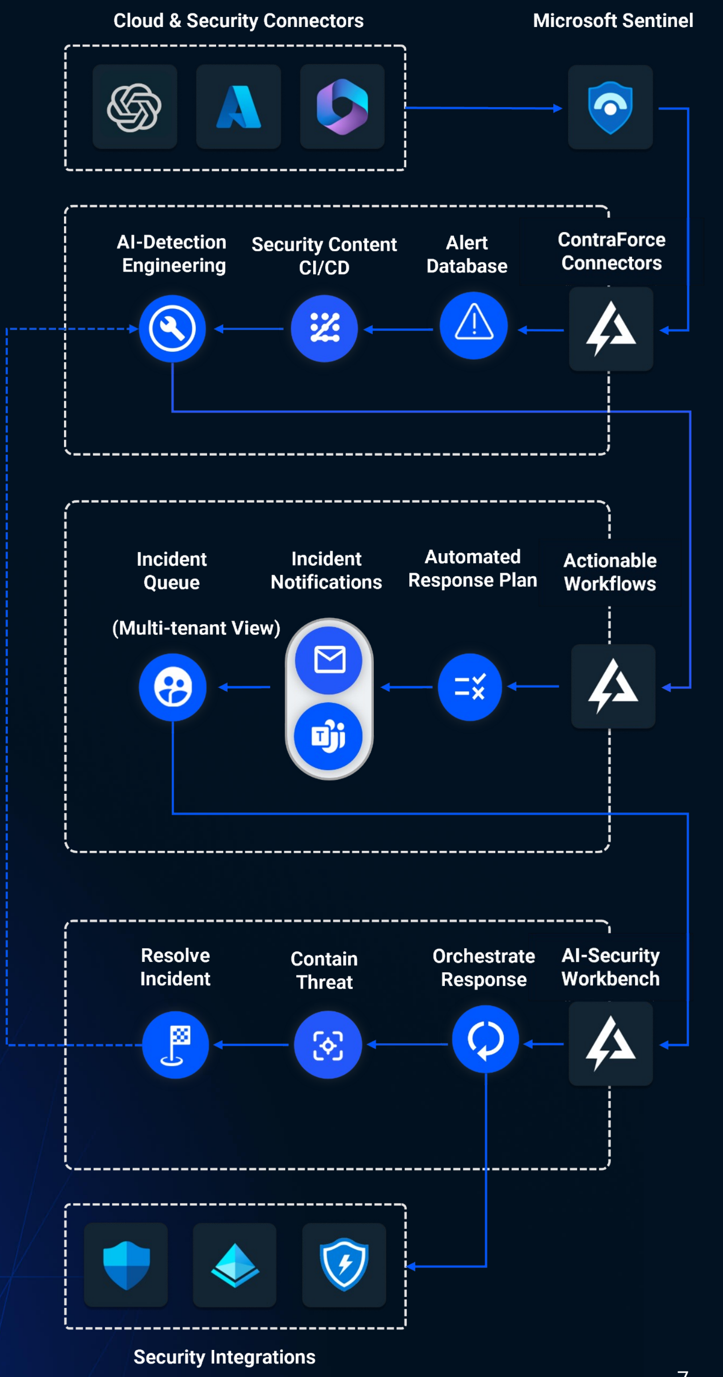
CENTRALIZED VISIBILITY

Bring all your solutions, integrations, and data together through a single centralized hub to streamline the visibility and management of your entire cybersecurity posture.

SIMPLIFY DATA INGESTION AND CONNECTOR MANAGEMENT

Connect your native Microsoft sources in one click and simplify third party connector configuration using native Infrastructure-as-Code (IaC) templates to deploy your connectors in minutes.

THE PLATFORM



Close

Close the call by qualifying the lead and agreeing on next steps

Close the call

Qualifying criteria

❑ **BUDGET**

- Do you currently own and operate any Microsoft products?
- How much of your budget is allocated toward security?

❑ **AUTHORITY**

- Are you the decision maker with authority to implement ContraForce?
- If no, can you put me in contact with the person who has decision-making authority?

❑ **NEED**

- Would you like to reduce your current security spend and gain greater peace of mind by consolidating your security tools and increasing visibility into your security posture?
- Would you like to conserve your own resources and outsource the bulk of threat detection and monitoring?

❑ **TIMELINE**

Do you plan to implement a solution in the next three, six, or twelve months?

Next steps

If the customer meets three of the four qualification criteria: Thank them for their time and offer to schedule a follow-up meeting, demo, or workshop.

If the customer is interested, but not qualified: Thank them for their time and check back in 30 days. Send information to help them consider ContraForce.

If the customer is not interested: Thank them for their time and update your CRM system appropriately.

Resources

Customer-facing assets to drive sales opportunities:

- Microsoft Commercial Marketplace
- Learn more about the ContraForce platform
- Contact ContraForce
- Schedule a Demo and Discovery Call

CONTRAFORCE

Microsoft Security